IBM Security AppScan Standard
Version 9.0.3.12

Guide d'utilisation

Table des matières

Chapitre 1. Introduction

Présentation du produit, récapitulatif des nouveautés de cette version et coordonnées des contacts.

Présentation du produit

IBM Security AppScan Standard est un outil de test de la vulnérabilité de la sécurité des applications et des services Web. Il offre les méthodes de test les plus avancées pour vous aider à protéger votre site contre les menaces de cyber-attaque, ainsi qu'un vaste choix d'options de génération de données d'application.

IBM SecurityAppScan Standard utilise trois techniques de test différentes qui se complètent et s'enrichissent mutuellement :

Analyse dynamique ("examen de type boîte noire")
Il s'agit de la méthode principale, qui teste et évalue les réponses des applications en phase d'exécution.

Analyse statique ("examen de type boîte blanche")
Technologie unique qui analyse le code JavaScript dans le contexte d'une page Web intégrale.

Analyse interactive ("examen glass box")
Le moteur de test dynamique peut entrer en interaction avec un agent Glass Box qui réside sur le serveur Web lui-même, permettant ainsi à AppScan d'identifier plus de problèmes, et avec une plus grande précision, qu'en exécutant un test dynamique conventionnel seul.

Exemples de fonctions avancées d'AppScan :

- Rapport sur la conformité légale et générale, avec plus de 40 schémas différents prêts à l'emploi à votre disposition.
- Personnalisation et extensibilité via AppScan eXtension Framework, ou par intégration directe dans des systèmes existants à l'aide du kit SDK AppScan.
- Fonctions de catégorisation des liens dépassant la sécurité des applications pour identifier les risques encourus par les utilisateurs à partir de liens dirigés vers des sites malveillants ou indésirables.

AppScan Standard vous permet de réduire les risques d'attaque des applications Web et d'atteinte à la protection des données, à la fois avant le déploiement de sites et dans le cadre de l'évaluation des risques dans la production.

Technologies prises en charge

Cette section vous aide à comprendre comment les technologies utilisées par votre site peuvent affecter la capacité d'examen d'AppScan.

Certaines technologies utilisées par votre site peuvent avoir une incidence sur la capacité d'examen d'AppScan, tandis que d'autres n'en ont aucune.

- AppScan est un outil de "boîte noire" (DAST) qui examine votre site en utilisant les mêmes mécanismes qu'un navigateur. Ainsi, les technologies côté serveur qui sont transparentes pour un navigateur sont généralement transparentes pour AppScan, et n'affectent pas l'examen.
- Les technologies côté client comme JavaScript et le protocole HTTP n'affectent pas AppScan. Contrairement à un navigateur, AppScan a besoin de comprendre ces technologies à un niveau qui permette l'exploration automatique, la maintenance des sessions et, bien évidemment, le test. Dans ces cas, vous devez configurer AppScan afin qu'il effectue les examens correctement.

Un examen AppScan consiste en deux étapes : l'exploration et le test. Pour chaque étape, le tableau ci-dessous contient des instructions pour comprendre quelles technologies côté client et côté serveur peuvent avoir une incidence sur l'examen, et dans quels cas une configuration s'avère nécessaire.

	Technologies côté serveur	**Technologies côté client**
Etape d'exploration	Les technologies côté serveur qui n'ont pas d'incidence sur le client, telles que la base de données spécifique utilisée, n'ont aucun effet sur l'examen. De nombreux mécanismes qui ont une *réelle* incidence sur le client (comme la gestion de session) ne limitent pas l'examen tant qu'AppScan est configuré correctement. Par exemple, les serveurs Web et les serveurs d'applications ont une incidence sur la gestion des ID, auquel cas AppScan doit être configuré pour pouvoir en effectuer le suivi. De nombreux ID de session courants sont prédéfinis ou peuvent être automatiquement détectés par AppScan et ne nécessitent pas de configuration supplémentaire. Une configuration supplémentaire peut toutefois s'avérer nécessaire pour certains mécanismes personnalisés. AppScan prend particulièrement en charge les URL personnalisées de WebSphere Portal. WSP code les URL d'une manière qui les rend difficiles à suivre lorsqu'elles apparaissent. AppScan décode les URL de sorte qu'elles peuvent être reconnues et optimisées. L'examen glass box n'est pris en charge que pour Java et .NET.	Les deux principales technologies côté client utilisées aujourd'hui sont HTML5 et JavaScript. Elles ont toutes deux une incidence sur l'étape d'exploration de l'examen : AppScan prend en charge HTML lors de l'étape d'exploration. Cela signifie que les liens peuvent être extraits, les formats détectés et remplis, etc. AppScan prend en charge (exécute) le code JavaScript standard. Les principales infrastructures sont prises en charge, dont JQuery, AngularJS et PrototypeJS. De nombreuses autres infrastructures JS ne sont pas prises en charge mais ne limitent l'examen en aucune façon. Si des pages sont omises lors de l'étape d'exploration automatique suite à une technologie spécifique, elles peuvent être ajoutées à l'examen par l'exploration manuelle du site après l'étape d'exploration automatique, et avant l'étape de test.
Etape de test	AppScan est conçu pour tester l'application mais pas les technologies de prise en charge associées : celles-ci n'ont donc pas d'incidence sur le test. Au niveau des bases de données, la suite d'AppScan fournit des tests d'injection SQL qui sont indépendants de la base de données utilisée. Elle fournit également des tests spécifiques pour le contrôle tierce partie (celui des vulnérabilités courantes, par exemple).	Le test côté client s'effectue seulement sur le code JavaScript. Actuellement, seules les vulnérabilités JS en clair sont détectées. Comme les infrastructures JS ne sont prises en charge, le code JS qui les utilise n'est pas toujours correctement analysé. HTML5 est entièrement pris en charge.

Nouveautés

Cette section décrit les nouvelles fonctionnalités et améliorations de ce groupe de correctifs.

La liste complète des correctifs est disponible à l'adresse suivante : http://www.ibm.com/support/docview.wss?uid=swg27021374

Nouveautés de la version IBM Security AppScan Standard 9.0.3.12

Configuration requise
Microsoft .NET Framework 4.7.2 est à présent requis.

Exécution JavaScript basée sur les demandes
En raison de l'efficacité de l'exécution JavaScript basée sur les actions, l'exécution JavaScript basée sur les demandes (Configuration > Options d'exploration > Basée sur les demandes > Exécuter le code JavaScript pour reconnaître les adresses URL et le contenu dynamique) est redondante et la case est désormais décochée par défaut. Si vous chargez un examen dans lequel l'option a été sélectionnée, elle restera sélectionnée, bien que nous recommandions de la désélectionner. Reportez-vous à la section ci-dessous pour prendre connaissance du raisonnement à l'origine de cette modification.

Rapports de sécurité
Les rapports sont désormais nettoyés par défaut (le mot de passe défini dans Remplissage automatique de formulaires ne s'affiche pas dans les rapports). Vous pouvez modifier ce paramètre dans Configuration > Configuration avancée > Général : Nettoyez les rapports.

Assistant de configuration des examens
Dans la dernière étape de l'assistant, la case Démarrer Start Scan est à présent *désactivée* par défaut.

Comprendre la modification de l'exécution JavaScript

Au cours de ces dernières années, nous avons mis au point un mécanisme de remplacement de l'exploration basée sur les demandes, qui imitait et s'approchait du fonctionnement d'un navigateur. Le nouveau mécanisme, intitulé "Exploration basée sur les actions", utilise un véritable navigateur intégré (basé sur Chromium). Les deux mécanismes comprennent l'exécution JavaScript (JSX), mais ils sont en train de retirer le mécanisme de JSX basée sur les demandes, étant donné que la technologie plus récente est capable de la dupliquer et de la surpasser.

L'exécution JavaScript basée sur les actions ressemble davantage à la manière dont un utilisateur interagit avec le navigateur. En effet, elle propose une couverture et une précision accrues, ainsi qu'une meilleure prise en charge des nouveaux cadres JavaScript dès leur apparition. L'exécution JavaScript basée sur les demandes se fait désormais de façon progressive et par étapes :

- Dans ce groupe de correctifs, la case JSX est décochée par défaut, mais vous pouvez toujours la cocher si vous estimez que l'exploration basée sur les actions échoue pour une application spécifique.
- Ce mécanisme sera entièrement supprimé dans les éditions à venir.

Notez que lorsque vous chargez un examen ou un modèle enregistré dans lequel la case JSX a été cochée (Configuration > Options d'exploration > Basée sur les demandes > Exécuter le code JavaScript pour reconnaître les adresses URL et le contenu dynamique), elle reste sélectionnée. Cependant, nous suggérons de décocher la case.

Si vous constatez une différence de résultats en raison de la modification, nous vous prions de créer un ticket de demande de service afin que nous puissions vous expliquer la différence ou corriger le mécanisme basé sur les actions.

Informations de contact et support

AppScan Informations de contact du support technique d' pour signaler des résultats de test faussement positifs et pour informations générales, techniques et commerciales.

Elément	Détails
Documentation	La Bibliothèque des publications d'AppScan Standard contient des liens vers toute la documentation, utilisateur en ligne, notamment : • Version PDF de ce guide d'utilisation • Fichier Readme contenant toutes les informations de dernière minute n'ayant pas pu être intégrées à cette aide • Liste de correctifs, décrivant en détail les APAR corrigés par version • Configurations requises • Les problèmes connus d'intérêt général dans la version actuelle (mis à jour au fur et à mesure que les problèmes sont découverts et résolus dans les groupes de correctifs) • Instructions de téléchargement d'AppScan Standard http://www.ibm.com/support/docview.wss?uid=swg27024868
AppScan Standard - Portail de support	http://www.ibm.com/support/entry/portal/product/software/security_systems/ibm_security_appscan_standard
AppScan Standard - Forum	https://developer.ibm.com/answers/topics/appscan-standard/
Pour ouvrir une demande de service	https://www.ibm.com/support/servicerequest/Home.action
Pour rapporter des résultats de test "faussement positifs"	http://www.ibm.com/support/docview.wss?uid=swg21295428 Pour plus de détails, voir : «Rapport Faux positif des résultats de test», à la page 222
Structure AppScan eXtensions Framework	http://www.ibm.com/developerworks/rational/downloads/08/appscan_ext_framework/ Pour plus de détails, voir «Extensions», à la page 294
Ressources de support	http://www.ibm.com/support/docview.wss?uid=swg21672099
Informations générales et commerciales	http://www.ibm.com/software/rational/offerings/testing/webapplicationsecurity/

Lorsque vous appelez ou soumettez un incident au service AppScan pour une demande de service particulière, pensez à préparer les informations suivantes :

- Une description de l'opération que vous avez effectuée et le message d'erreur que vous avez reçu
- Des informations contextuelles pour nous aider à comprendre le problème
- La version d'AppScan Standard que vous utilisez
- L'impact du problème sur votre organisation, votre planning et vos délais
- Téléchargez les journaux, les données et des captures d'écran dans la demande de service

Chapitre 2. Installation

Procédures d'installation et de licence

Configurations requises

Récapitulatif des configurations matérielle et logicielle minimales requises *pour la machine qui exécute AppScan Standard*.

Important : Une liste plus complète pouvant contenir des mises à jour ajoutées après la publication du produit est disponible en ligne à l'adresse suivante : http://www.ibm.com/support/docview.wss?uid=swg27024155

Pour une discussion sur les technologies *utilisées par votre site* susceptibles d'affecter la capacité d'examen d'AppScan, voir «Technologies prises en charge», à la page 1

Configuration matérielle

Matériel	Configuration minimale
Processeur	Core 2 Duo 2 GHz (ou équivalent)
Mémoire	4 Go de mémoire vive
Espace disque	30 Go
Réseau	Une carte d'interface réseau 100 Mbit/s pour les communications réseau avec TCP/IP configuré

Syst. d'expl. et configuration logicielle

Logiciel	Détails
Système d'exploitation	Systèmes d'exploitation pris en charge : • Microsoft Windows Server 2016 : Standard et Datacenter • Microsoft Windows Server 2012 : Essentials, Standard et Datacenter • Microsoft Windows Server 2012 R2 : Essentials, Standard et Datacenter • Microsoft Windows Server 2008 R2 : Standard et Enterprise, avec ou sans SP1 • Microsoft Windows 10 : Pro et Enterprise • Microsoft Windows 8.1 : Pro et Enterprise • Microsoft Windows 8 : Standard, Pro et Enterprise • Microsoft Windows 7 : Enterprise, Professional et Ultimate, avec ou sans SP1 **Remarque :** Les éditions 32–bits et 64–bits sont toutes deux prises en charge, mais l'édition 64–bits est préférable. Tous les groupes de correctifs sont pris en charge.
Navigateur	Microsoft Internet Explorer version 11 Recommandation : Internet Explorer version 11.0.9600.18537, versions de mise à jour 11.0.38 KB3203621

Logiciel	Détails
Autre	Microsoft .NET Framework 4.7.2 Si vous utilisez des licences flottantes ou de jeton : Rational License Key Server 8.1.1, 8.1.2, 8.1.3, 8.1.4, 8.1.5 (Facultatif) Adobe Flash Player for Internet Explorer est nécessaire pour l'exécution de Flash (et pour l'affichage des vidéos d'explication de certains conseils). Les versions 9.0.124.0 à 14.0.0.125 sont prises en charge. Les versions précédentes ne sont pas prises en charge et une configuration peut s'avérer nécessaire pour certaines versions. Pour plus de détails, voir «Contenus Flash», à la page 326. (Facultatif) Microsoft Word 2007, 2010, 2013 pour les modèles de rapport personnalisé.

Important : Les clients ne disposant pas d'une licence locale sur leur machine requièrent une connexion réseau à leur serveur de clés de licence lorsqu'ils utilisent AppScan.

Important : Un pare-feu personnel s'exécutant sur le même ordinateur que AppScan peut bloquer la communication et produire des résultats inexacts et une performance réduite. Pour de meilleurs résultats, n'exécutez pas de pare-feu personnel sur l'ordinateur exécutant AppScan.

Configuration requise pour le serveur glass box

La fonction d'examen de glass box nécessite d'installer un agent glass box sur le serveur d'applications. Pour plus de détails, voir «Installation de l'agent glass box», à la page 166.

Pour plateformes Java : Sur les plateformes Java, les plateformes de serveur et les technologies suivantes sont prises en charge.

Logiciel	Détails
JRE	Les versions 6 et 7 de JRE sont prises en charge. La version 8 *ne l'est pas*.
Système d'exploitation	Systèmes Microsoft Windows pris en charge (version 32–bits et 64–bits) : • Microsoft Windows Server 2012 • Microsoft Windows Server 2012 R2 • Microsoft Windows Server 2008 R2 Systèmes Linux pris en charge : • Linux RHEL 5, 6, 6.1, 6.2, 6.3, 6.4 Systèmes UNIX pris en charge : • UNIX AIX 6.1, 7.1 • UNIX Solaris (SPARC) 10, 11
Conteneur Java™ EE	JBoss AS 6, 7; JBoss EAP 6.1; Tomcat 6.0, 7.0; WebLogic 10, 11, 12; WebSphere 7.0, 8.0, 8.5, 8.5.5

Plateformes .NET : Sur les plateformes .NET, les technologies et systèmes suivants sont pris en charge :

Elément	Détails
Système d'exploitation	Systèmes d'exploitation pris en charge (versions 32–bits et 64–bits) : • Microsoft Windows Server 2012 • Microsoft Windows Server 2012 R2 • Microsoft Windows Server 2008 R2

Elément	Détails
Autre	Microsoft IIS 7.0 ou ultérieure Microsoft .NET Framework 4.0 ou 4.5 doit être installé, et IIS doit être configuré au niveau racine pour pouvoir fonctionner avec cette version d'ASP.net.

Remarque : L'utilisateur doit disposer des privilèges d'administrateur lors de l'exécution de l'application sur le serveur.

Remarque : L'agent doit être installé *après* l'installation réussie de l'application que vous souhaitez tester sur le serveur.

Utilisation des cookies

Bien qu'AppScan effectue le suivi des cookies définis par l'application qu'il examine, il ne définit pas ses propres cookies pour authentification ou pour tout autre objectif.

Langues prises en charge

L'interface utilisateur d'AppScan peut s'exécuter dans les langues suivantes : chinois (simplifié), chinois (traditionnel), anglais (Etats-Unis), français, allemand, italien*, japonais, coréen*, portugais (Brésil), russe*, espagnol (Espagne). Pour modifier la langue de l'interface utilisateur, accédez à **Outils > Options > onglet Général**

Remarque : Pour les interfaces utilisateur en italien et en coréen, la documentation est en anglais. Pour l'interface en russe, l'aide est traduite, mais toutes les autres sections de la documentation sont en anglais.

Concepts associés:

«Technologies prises en charge», à la page 1
Cette section vous aide à comprendre comment les technologies utilisées par votre site peuvent affecter la capacité d'examen d'AppScan.

Mise à niveau de Flash Player

Pourquoi et quand exécuter cette tâche

Pour permettre à AppScan d'exécuter des contenus Adobe Flash lors des analyses, vous devez disposer d'une version Adobe Flash Player pour Internet Explorer prise en charge installée sur l'ordinateur. Les versions 9.0.124.0 à 14.0.0.125 sont prises en charge. Les versions antérieures ne sont pas prises en charge et des opérations de configuration peuvent s'avérer nécessaires pour certaines versions prises en charge. Vous devez disposez d'une version prise en charge pour exécuter les fichiers Flash au cours de l'examen.

Remarque : Sans mise à niveau, Flash ne s'exécutera pas même si la case correspondante (Configuration des examens > Options d'exploration) est cochée.

Procédure

1. Fermez AppScan et les fenêtres Microsoft Internet Explorer.
2. Pour télécharger et installer la version la plus récente de Flash Player, consultez le site http://get.adobe.com/flashplayer/

Configuration de Flash Player

Pourquoi et quand exécuter cette tâche

Afin que AppScan puisse exécuter des contenus Flash Adobe lors des analyses, vous devez disposer d'une version Adobe Flash Player pour Internet Explorer. Dans certains cas, il peut s'avérer nécessaire de

configurer Flash Player Version 10.1 ou suivante pour qu'il fonctionne avec AppScan. Si vous obtenez un message indiquant que votre version de Flash Player requiert une configuration, suivez la procédure ci-dessous.

Remarque : Sans configuration, Flash ne s'exécutera pas même si la case correspondante (Configuration des examens > Options d'exploration) est cochée.

Remarque : Des droits d'accès Administrateur sont requis pour l'exécution de cette procédure.

Procédure

1. Fermez AppScan.
2. *Avec des droits d'accès Administrateur,* ouvrez le dossier contenant les fichiers d'installation Flash.
   - Pour les systèmes 32 bits, le chemin est généralement le suivant :
     `C:\WINDOWS\System32\Macromed\Flash`
   - Pour les systèmes 64 bits, le chemin est généralement le suivant :
     `C:\WINDOWS\SysWow64\Macromed\Flash`
3. Recherchez un fichier nommé `mms.cfg` dans le dossier Flash. S'il n'existe pas, créez un fichier TXT vide de ce nom.
4. Ouvrez `mms.cfg` avec un éditeur de texte tel que Microsoft Notepad, et recherchez l'entrée `FullFramerateWhenInvisible`
   - Si elle existe, attribuez-lui la valeur 1
   - Si elle n'existe pas, ajoutez la ligne suivante, *sur une ligne distincte*, à la fin du fichier (si celui-ci a déjà un contenu) :
     `FullFramerateWhenInvisible = 1`
5. Sauvegardez.
   Flash Player est maintenant configuré pour l'exécution de Flash dans AppScan.

Installer

L'assistant d'installation vous guide tout au long de la procédure, simple et rapide.

Procédure

1. Si une version d'AppScan Standard ultérieure à 8.5 est installée sur votre machine, vous devez la désinstaller avant d'installer cette version.
2. Fermez toutes les applications Microsoft Office ouvertes.
3. Lancez l'installation d'AppScan.
   L'assistant InstallShield démarre et vérifie que votre poste de travail présente la configuration minimale requise pour l'installation. L'écran d'accueil de l'assistant d'installation d'AppScan s'affiche.
4. Suivez les instructions de l'assistant pour procéder à l'installation d'AppScan.

   Remarque : Vous serez invité à installer ou télécharger GSC (Generic Service Client). Cette étape vous est nécessaire pour l'exploration des services Web afin de configurer un examen de ces derniers. Vous n'en aurez pas l'utilité si vous ne procéderez pas à l'examen des services Web.

Installation en mode silencieux

Instructions d'installation en mode silencieux à l'aide de la ligne de commande.

Vous pouvez installer AppScan "silencieusement", à l'aide de la ligne de commande et des paramètres suivants :

```
AppScan_Setup.exe /l"LanguageCode" /s /v"/qn INSTALLDIR=\"InstallPath\""
```

Paramètre	Fonction
/l	Code de langue. Les options sont les suivantes : • Anglais : **1033** • Chinois (traditionnel) : **1028** • Chinois (simplifié) : **2052** • Français : **1036** • Allemand : **1031** • Italien : **1040** • Japonais : **1041** • Coréen : **1042** • Portugais : **1033** • Espagnol : **1034**
/s	Active le "mode silencieux" (sinon, l'installation standard est lancée). **Remarque :** A utiliser conjointement avec /v"/qn" (voir la ligne suivante)
/v	Définit les autres propriétés MSI, telles que le mode d'interface utilisateur et le chemin d'installation d'AppScan. **Mode d'interface utilisateur :** Pour le "mode silencieux", ajoutez `/qn` en tant que paramètre (placé entre guillemets). **Chemin d'accès :** Si vous ne définissez pas de chemin d'installation, le chemin par défaut est utilisé par l'installation : Program Files\IBM\AppScan Standard\ Pour définir un autre chemin d'installation, ajoutez `INSTALLDIR=\"InstallPath\"` en tant que paramètre (entre guillemets). Le chemin peut inclure des espaces. Exemple : `/v"/qn INSTALLDIR=\"D:\Program Files\AppScan\""`

Exemples :

- Pour procéder à l'installation en mode silencieux de la version anglaise d'AppScan dans le répertoire par défaut, entrez :

  ```
  AppScan_Setup.exe /s /v"/qn"
  ```

- Pour procéder à l'installation en mode silencieux de la version japonaise d'AppScan dans le répertoire par défaut, entrez :

  ```
  AppScan_Setup.exe /l"1041" /s /v"/qn"
  ```

- Pour procéder à l'installation en mode silencieux de la version coréenne d'AppScan dans D:\Program Files\AppScan\, entrez :

  ```
  AppScan_Setup.exe /l"1042" /s /v"/qn INSTALLDIR=\"D:\Program Files\AppScan\""
  ```

Désinstaller

Instructions de désinstallation d'AppScan sur votre ordinateur.

Pourquoi et quand exécuter cette tâche

Vous pouvez exécuter l'assistant de désinstallation à partir du menu Démarrer de Windows (décrit ci-dessous) ou à l'aide de la fonction Ajouter/Supprimer des programmes du Panneau de configuration Windows. Les procédures à suivre peuvent varier selon la version de Windows installée.

Procédure

1. Accédez à Démarrer > Tous les programmes > IBM Security AppScan Standard
2. Sélectionnez Désinstallation IBM Security AppScan Standard et suivez les instructions.

   Remarque : L'assistant de désinstallation ne supprime pas les fichiers ou les rapports d'examen créés par AppScan. Si vous souhaitez supprimer ces fichiers, faites-le manuellement.

Licence

La présente section décrit la procédure d'installation et de gestion des licences.

L'installation d'AppScan comprend une licence par défaut qui vous permet d'examiner le site Web de test AppScan spécialement conçu par IBM (demo.testfire.net), mais pas d'autres sites. Pour effectuer un examen de votre propre site, vous devez installer une licence valide fournie par IBM®. Tant que cela n'est pas fait, AppScan charge et enregistre des examens et des modèles d'examen mais n'exécute pas de nouveaux examens sur votre site.

IBM Security AppScan Standard Licences

Il existe trois types de licence :

Licences "affectées à un poste"
Ces licences sont installées sur la machine exécutant AppScan. Chaque licence est affectée à une seule machine.

Licences "flottantes"
Ces licences sont installées sur le serveur de clés de licence IBM Rational (qui peut être le même que celui sur lequel AppScan s'exécute). Tout serveur sur lequel AppScan est utilisé doit disposer d'une connexion réseau avec le serveur de clés de licence. Chaque fois qu'un utilisateur ouvre AppScan, une licence est extraite (et restituée à la fermeture d'AppScan).

Licences de "jeton"
Ces licences sont installées sur le serveur de clés de licence IBM Rational (qui peut être le même que celui sur lequel AppScan s'exécute). Tout serveur sur lequel AppScan est utilisé doit disposer d'une connexion réseau avec le serveur de clés de licence. Chaque fois qu'un utilisateur ouvre AppScan, le nombre requis de jetons est extrait (et restitué à la fermeture d'AppScan).

Etat de la licence

Pour afficher et modifier les licences AppScan, cliquez sur **Aide > Licence**. Vous avez le choix entre trois options :

Ouvrir AppScan Standard - Gestionnaire de licences	Ouvre la liste des licences actuellement chargées et vous permet de : • Ajouter ou supprimer des licences affectées à un poste • Définir des serveurs de clés de licence pour des licences flottantes ou de jeton
Ajouter une licence AppScan Enterprise	Si votre organisation dispose d'une licence AppScan Enterprise permettant l'examen de sites autres que ceux autorisés par votre licence locale AppScan Standard, vous pouvez importer ces autorisations pour les utiliser sur votre poste local en plus de votre licence existante. **Remarque :** Cette option est disponible uniquement lorsqu'une licence AppScan Standard complète (et non une licence de démonstration) est chargée. Voir «Importation des autorisations de licence pour AppScan Enterprise», à la page 305.
Afficher le contrat de licence	Cliquez ici pour voir le contrat de licence.

Remarque : Vous pouvez régénérer les informations de licence affichées dans la boîte de dialogue en cliquant sur  .

Remarque : Si une licence flottante ou une licence de jeton a été vérifiée mais que le serveur de clés de licence devient par la suite indisponible, AppScan peut fonctionner en "mode déconnecté" pendant trois jours. Durant cette période, vous pouvez examiner votre application comme vous le faites d'habitude.

Voir aussi :

«Traitement des incidents liés aux licences», à la page 331

«Importation des autorisations de licence pour AppScan Enterprise», à la page 305

Chargement d'une licence affectée à un poste

Chargement d'une licence affectée à un poste.

Pourquoi et quand exécuter cette tâche

Les licences "affectées à un poste" sont installées sur la machine sur laquelle AppScan Standard s'exécute, et non sur un serveur distinct.

Procédure

1. Téléchargez votre fichier de licence à partir du site Rational License Key Center et sauvegardez-le sur votre machine.
2. Dans AppScan Standard, cliquez sur **Aide > Licence > Ouvrir AppScan Standard - Gestionnaire de licences**.
3. Cliquez sur **Configuration de la licence**.
4. Au-dessus de la sous-fenêtre *supérieure* (Fichiers de licences affectées à un poste), cliquez sur  .
5. Naviguez jusqu'au fichier de licence.
6. (Facultatif) Si vous ajoutez plusieurs fichiers, utilisez les flèches **vers le haut et vers le bas** pour faire monter ou descendre les licences dans la liste.
7. Dans la boîte de dialogue des licences AppScan, cliquez sur  pour charger votre licence.

   Remarque : Le nom de licence doit contenir des caractères ASCII uniquement. Si nécessaire, renommez le fichier afin de pouvoir le charger.

Chargement d'une licence flottante ou d'une licence de jeton

Cette rubrique explique comment charger une licence flottante ou une licence de jeton pour l'utiliser avec AppScan Standard Edition.

Pourquoi et quand exécuter cette tâche

Pour installer une licence flottante ou une licence de jeton, vous devez d'abord disposer d'un serveur de clés de licence sur lequel IBM Rational License Key Server (version 8.1.2 ou ultérieure) est installé. Le serveur de clés de licence peut être une autre machine ou la même machine sur laquelle AppScan est installé. La procédure ci-dessous décrit la configuration du serveur et le chargement de la licence flottante.

Procédure

1. Téléchargez IBM Rational License Key Server (version 8.1.2 ou ultérieure) à partir de Passport Advantage.

2. Installez License Key Server. Vous pouvez l'installer sur le même ordinateur qu'AppScan ou sur le serveur de licences central de votre réseau.
3. Téléchargez vos fichiers de licence à partir du site Rational License Key Center, puis sauvegardez-les sur la machine sur laquelle vous avez installé Rational License Key Server.
4. Cliquez sur **Démarrer > Programmes > IBM Rational > License Key Administrator (version)**, puis utilisez l'assistant d'importation d'un fichier de licence Rational pour importer le fichier de licence sur le serveur de clés de licence.
5. Dans AppScan Standard, cliquez sur **Aide > Licence > Ouvrir AppScan Standard - Gestionnaire de licences**.
6. Cliquez sur **Configuration de la licence**.
7. Au-dessus de la sous-fenêtre *inférieure* (Serveurs de licences), cliquez sur  .
8. Dans la boîte de dialogue qui s'affiche, entrez l'hôte et le port de la licence.
9. (Facultatif) Si vous ajoutez plusieurs serveurs de licences, utilisez les flèches **vers le haut et vers le bas** pour faire monter ou descendre les serveurs dans la liste.
10. Dans la boîte de dialogue des licences AppScan, cliquez sur  pour charger votre licence.

Mises à jour

Maintien de votre installation à jour.

Pourquoi et quand exécuter cette tâche

Les mises à jour d'abonnement comprennent de nouveaux types de techniques d'exploitation d'application Web ainsi que de nouveaux types de correctifs d'erreur. Nous vous recommandons d'installer ces fichiers dès que vous recevez notification de leur disponibilité.

AppScan recherche régulièrement les mises à jour sur le site Web IBM et vous informe lorsque de nouvelles sont disponibles. Vous pouvez également lancer une recherche de mise à jour.

Lorsque AppScan a détecté de nouvelles mises à jour disponibles, vous avez la possibilité de télécharger et d'installer les nouveaux fichiers de mise à jour sur votre machine.

Procédure

1. Dans la barre d'outils, cliquez sur  .
   AppScan vérifie l'existence de mises à jour. Si une mise à jour est disponible, le bouton **Installer** devient actif. (Si votre version d'AppScan est à jour, le bouton reste grisé.)
2. Pour installer la mise à jour, cliquez sur **Installer**.

Que faire ensuite

Vous pouvez vérifier le statut de mise à jour dans le «Journal des mises à jour», à la page 302.

Emplacement des fichiers temporaires

Indique l'emplacement où AppScan enregistre ses fichiers temporaires lors d'une opération normale et comment modifier cet emplacement.

Par défaut, AppScan stocke ses fichiers temporaires dans :

```
C:\Documents and Settings\All Users\Application Data\IBM\AppScan Standard\temp
```

Si vous devez modifier cet emplacement par défaut, éditez le chemin de la variable d'environnement APPSCAN_TEMP comme nécessaire. (Les variables d'environnement sont accessibles en cliquant avec le bouton droit de la souris sur **Poste de travail**, puis en sélectionnant **Propriétés > Avancé > Variables d'environnement**.)

Restriction : Le chemin du nouvel emplacement ne doit contenir aucun caractère Unicode.

Chapitre 3. Mise en route

La présente section fournit un court descriptif des fonctions et des procédures de base du produit.

Fonctionnement d'un examen automatique

Cette rubrique explique la différence entre les "étapes" et les "phases" d'un examen.

Un examen intégral AppScan est constitué de deux étapes : l'exploration et le test. Il est utile de comprendre l'idée principale d'un examen, même si le processus de l'examen est en fait continu pour l'utilisateur et que celui-ci n'a pas beaucoup d'opérations à effectuer jusqu'à ce que l'examen soit terminé.

Etape d'exploration

Lors de la première étape, AppScan explore le site (application Web ou service Web) en simulant un utilisateur Web qui clique sur des liens et renseigne des zones de formulaire. Il s'agit de l'étape d'exploration.

AppScan analyse les réponses à chaque demande qu'il envoie, recherchant toute indication de vulnérabilité potentielle. Lorsqu'AppScan reçoit une réponse pouvant indiquer une vulnérabilité de sécurité, il crée automatiquement un test (ou des tests) basé sur la réponse et note les règles de validation nécessaires pour déterminer quels résultats constituent la vulnérabilité ainsi que le niveau de risque pour la sécurité impliqué.

Avant d'envoyer les tests créés spécifiques au site, AppScan envoie plusieurs demandes syntaxiquement incorrectes à l'application pour déterminer de quelle manière elle génère des messages d'erreur. Ces informations sont ensuite utilisées pour améliorer la précision du processus de validation de test automatique d'AppScan.

Etape de test

Lors de la seconde étape, AppScan envoie des milliers de demandes de test personnalisées créées pendant l'étape d'exploration. Il enregistre et analyse la réponse de l'application pour chacun des tests à l'aide des règles de validation personnalisées. Ces règles identifient les problèmes de sécurité au sein de l'application et les classent selon leur niveau de risque pour la sécurité.

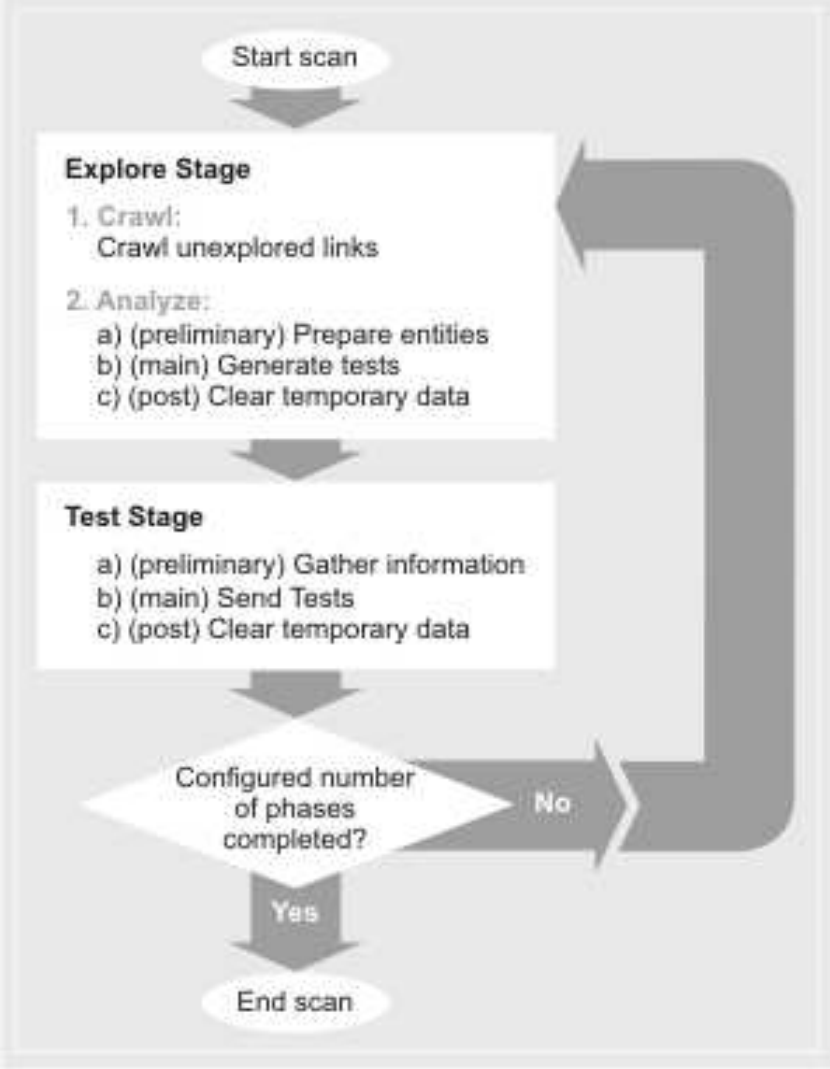
Phases de l'examen

En pratique, l'étape de test révèle souvent de nouveaux liens au sein d'un site, et des risques pour la sécurité plus potentiels. Cependant, une fois la première "phase" des étapes d'exploration et de test terminée, AppScan commence automatiquement une seconde "phase" pour traiter les nouvelles informations. Si de nouveaux liens sont découverts pendant la deuxième phase, une troisième phase est exécutée, etc.

Une fois que le nombre de phases d'examen configuré par l'utilisateur (ou valeur par défaut de quatre phases) est atteint, l'examen s'arrête et les résultats obtenus sont disponibles.

Illustration d'un flux d'examens automatique

Le diagramme suivant illustre les étapes et les phases d'un flux d'examens automatique. Notez que ce processus ne requiert pas d'actions de la part de l'utilisateur, mais vous pourrez trouver des références à ces dernières dans le journal d'AppScan.



Différences entre applications Web et services Web

Cette rubrique présente les différentes méthodes d'exploration de sites avant que ceux-ci soient testés par AppScan.

L'examen d'un site commence par une exploration qui, en fonction des données rassemblées, est suivie d'un test. Les "données d'exploration" peuvent être rassemblées en utilisant une ou plusieurs méthodes d'exploration. Dans tous les cas, ces données, une fois rassemblées sont utilisées par AppScan pour créer et envoyer des tests au site pendant l'étape de test.

Exploration d'applications web (sites avec interface utilisateur)

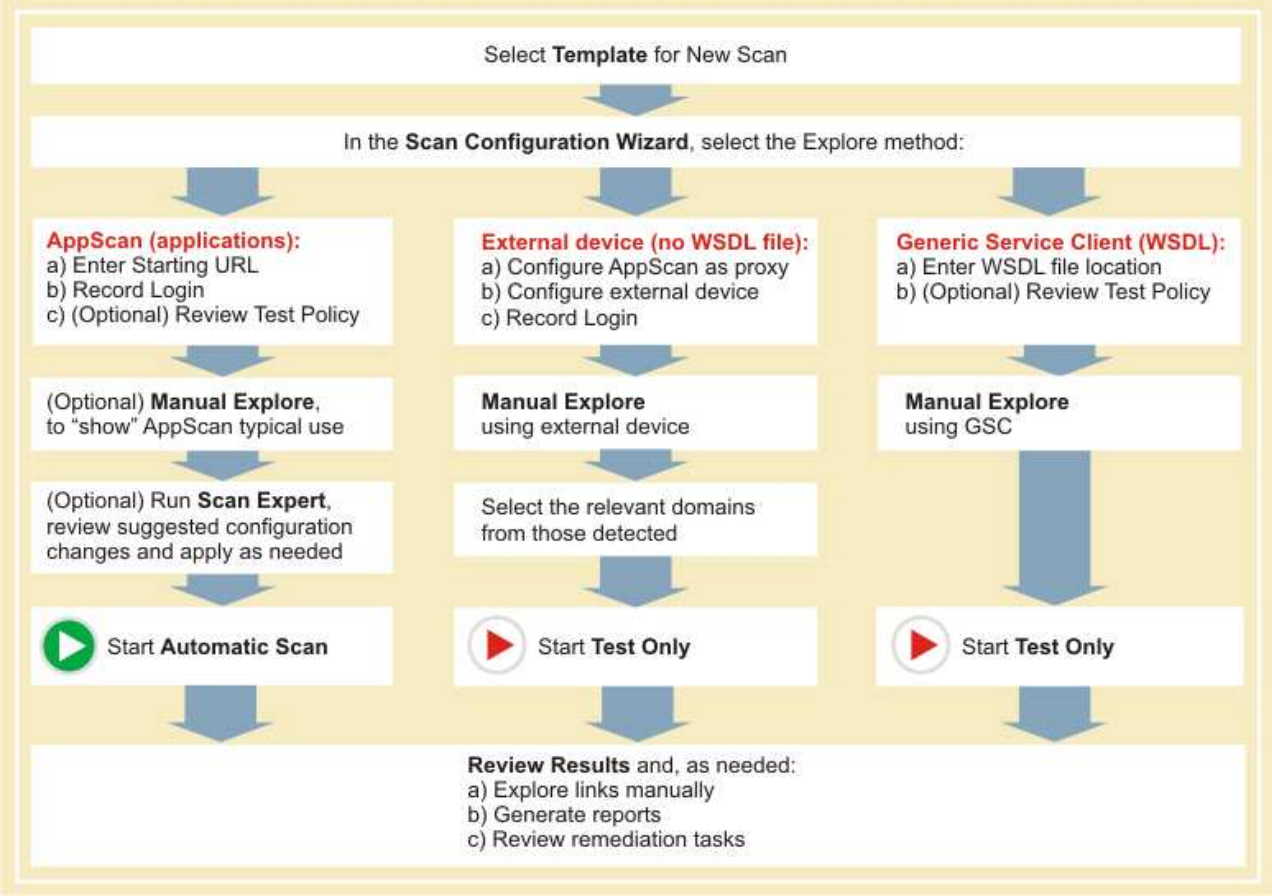
- Dans le cas d'applications (sites) sans services web, il suffit souvent de fournir à AppScan l'adresse URL de départ et les données d'authentification pour lancer le test sur le site.
- Si nécessaire, vous pouvez parcourir manuellement le site *via AppScan* afin d'accéder à des zones accessibles uniquement à l'aide d'entrées utilisateur spécifiques.
- Pour les pages accessibles uniquement via des pages sélectionnées dans un ordre spécifique, vous pouvez enregistrer une opération incluant plusieurs étapes à utiliser par AppScan.
- Alors que l'Assistant de configuration vous permet de configurer et de démarrer votre numérisation en quelques étapes, pour les sites complexes, la boîte de dialogue Configuration vous permet d'affiner et de personnaliser de nombreux autres paramètres.

Exploration de services Web

- Vous pouvez configurer AppScan comme proxy d'enregistrement pour l'appareil (tel qu'un téléphone mobile ou un simulateur) que vous utilisez pour explorer le service. AppScan peut alors analyser les données d'exploration et créer des tests. Vous pouvez également utiliser AppScan pour enregistrer le trafic à l'aide d'un outil externe, tel qu'un testeur fonctionnel de services Web. Voir «Utilisation d'AppScan comme proxy d'enregistrement», à la page 150.
- Si vous avez des fichiers de description Open API (JSON ou YAML) pour votre service Web, vous pouvez utiliser l'extension Web Services Wizard pour configurer une analyse et les séquences en plusieurs étapes nécessaires pour utiliser le service. AppScan analysera alors automatiquement le service.
- Si vous ne pouvez pas utiliser les deux premières méthodes et que vous disposez d'un fichier WSDL pour votre service Web (tel qu'un service Web SOAP), l'installation AppScan comprend en option un outil séparé qui permet aux utilisateurs de visualiser les différentes méthodes intégrées au service Web, de manipuler les données d'entrée et d'examiner les commentaires du service. Vous devez tout d'abord indiquer à AppScan l'adresse URL du service. Le "Generic Service Client" (GSC) intégré utilise le fichier WSDL pour afficher les différentes méthodes disponibles dans un format arborescent et créer une interface graphique conviviale pour envoyer des requêtes au service. Vous pouvez utiliser cette interface pour entrer des paramètres et en visualiser les résultats. Le processus est "enregistré" par AppScan et utilisé afin de créer des tests pour le service lorsqu'AppScan effectue l'examen du site. GSC peut aussi être utilisé comme client pour les requêtes REST, sans analyser un fichier WSDL, comme un simple client HTTP. Voir «Utilisation de GSC», à la page 153.

Flux de travaux de base

Diagramme affichant un flux de travaux AppScan simple utilisant l'assistant de configuration d'examen.



Pour plus de détails sur le flux de travaux standard, voir «Description du flux de travaux»

Les utilisateurs expérimentés dans le domaine de la sécurité Web peuvent se reporter à la rubrique . «Flux de travaux pour les utilisateurs avancés», à la page 313

Description du flux de travaux

AppScan offre une évaluation détaillée de votre application Web. Il exécute des milliers de tests basés sur tous les niveaux de techniques utilisateur classiques ainsi que sur les accès non autorisés et les injections de code.

Lorsque vous exécutez un examen sur votre application, AppScan envoie les tests à votre application Web. Les résultats des tests sont fournis par le moteur intelligent de site d'AppScan. Ils sont présentés dans des rapports volumineux et proposent des recommandations de correctifs, disponibles pour la révision et la manipulation améliorées.

AppScan est un outil interactif : vous décidez de la configuration de l'examen et déterminez les mesures à prendre d'après les résultats.

Le flux de travaux AppScan comprend les étapes suivantes :

1. **Sélection d'un modèle :** Une configuration d'examen prédéfinie est un *modèle d'examen*. Vous pouvez charger le modèle d'examen standard, un autre modèle prédéfini ou un modèle que vous avez précédemment enregistré. (Vous pouvez ensuite ajuster la configuration selon les besoins de l'examen courant.)
2. **Examen d'une application ou d'un service Web :** L'examen des services Web requiert un certain nombre d'entrées manuelles de l'utilisateur à l'aide de GSC (Generic Service Client) pour indiquer à AppScan comment *utiliser* le service.
   - **AppScan :** Si l'examen ne porte *pas* sur un service Web, ou si vous voulez analyser les parties d'une application *autres* que ses services Web, gardez cette option par défaut sélectionnée.
   - **Client/périphérique externe :** Sélectionnez cette option si vous voulez examiner un service pour lequel vous ne disposez pas d'un fichier WSDL. Vous configurez alors AppScan comme proxy d'enregistrement, et envoyez des demandes à partir de votre client externe via AppScan.
   - **Client de service générique :** Sélectionnez cette option si vous voulez examiner un service. GSC (Generic Service Client) s'ouvrira ensuite pour vous permettre d'envoyer des demandes au service et collecter des résultats, que AppScan analysera et utilisera pour créer des tests.
3. **Configuration des examens :** Configurez l'examen en tenant compte des caractéristiques de votre site, de votre environnement et des autres exigences.
4. (Facultatif) **Exploration manuelle :** Connectez-vous au site, cliquez sur les liens et remplissez les formulaires comme le ferait un utilisateur. C'est un bon moyen d'"indiquer" à AppScan comment un utilisateur standard peut naviguer sur le site, de garantir que les parties importantes du site soient examinées et de fournir des données pour remplir les formulaires.
5. (Services Web uniquement) **Envoi de demandes à l'aide de GSC :** Ouvrez GSC et envoyez des demandes valides au service.
6. (Facultatif) **Exécutez Scan Expert :** Permet d'effectuer un pré-examen rapide de votre site afin d'évaluer la configuration. Scan Expert peut suggérer des modifications afin d'augmenter l'efficacité de l'examen principal.
7. **Examen de l'application ou du service :** Il s'agit de l'examen principal, constitué des étapes d'exploration et de test.

   Étape d'exploration : AppScan balaye votre site, visite les liens comme le ferait un utilisateur standard et enregistre les réponses. Il crée une hiérarchie des adresses URL, des répertoires, des fichiers, etc., trouvés dans votre application. Cette liste s'affiche dans l'Arborescence de l'application (voir «Arborescence de l'application», à la page 21).

   L'étape d'exploration peut être automatique, manuelle ou combiner les deux modes. Vous pouvez également importer un fichier des données d'exploration (voir «Exporter des données d'exploration manuelle», à la page 147), qui consiste en une séquence d'exploration manuelle précédemment enregistrée. AppScan analyse ensuite les données qu'il a collectées sur le site et, en fonction de ces dernières, crée des tests pour le site. Ces tests sont conçus pour détecter les faiblesses de l'infrastructure (par exemple, les faiblesses de la sécurité pour les opérations commerciales, les produits tiers ou les systèmes Internet) et de l'application elle-même.

   Etape de test : Pendant l'étape de test, AppScan teste votre application, en fonction des réponses reçues lors de l'étape d'exploration, afin de détecter les faiblesses et évaluer leur degré de gravité.

   Une liste actualisée de tous les tests inclus à votre version courante d'AppScan peut être visualisée dans la boîte de dialogue Configuration d'examens (voir «Vue Stratégie de test», à la page 109).

   Vous pouvez également créer des tests définis par l'utilisateur en plus des tests créés et exécutés automatiquement par AppScan (voir «Tests définis par l'utilisateur», à la page 273). Vos tests peuvent compléter ceux générés par AppScan et vérifier les résultats trouvés par ce dernier.

   Les résultats des tests sont affichés dans la Liste des résultats où vous pouvez les visualiser et les modifier. Les détails complets des résultats sont affichés dans le Panneau des détails.
8. (Facultatif) **Exécution d'un test de recherche de logiciels malveillants :** Lancez ce test pour analyser les pages et les liens trouvés sur votre site lors de la recherche de logiciels malveillants et d'autres contenus indésirables.

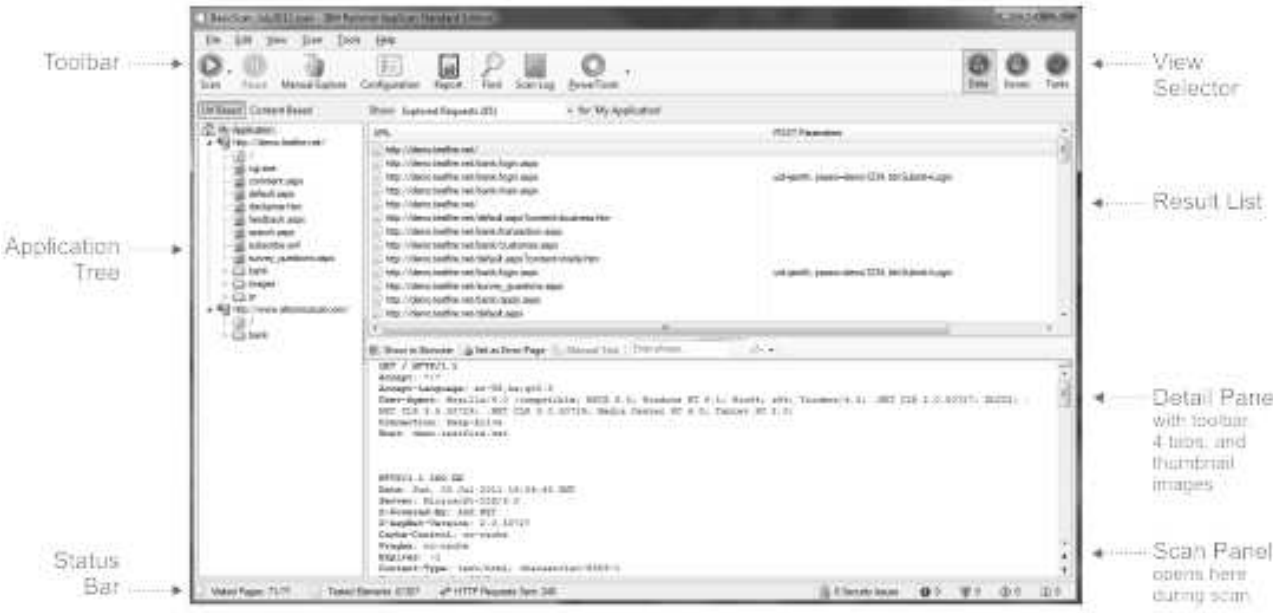
Remarque : Bien qu'un Test de recherche de logiciels malveillants puisse, en principe, être effectué à ce stade (dans ce cas, les résultats de l'étape d'exploration de l'examen principal seront utilisés), il est généralement exécuté sur un site *opérationnel* alors qu'un examen standard s'exécute plutôt sur un site *test* (l'examen d'un site *opérationnel* risquant d'interrompre les opérations).

9. **Réviser les résultats** : permet d'évaluer le statut de sécurité du site. Vous pouvez également :
   - explorer manuellement des liens supplémentaires ;
   - réviser des tâches de résolution ;
   - imprimer des rapports ;
   - ajuster la configuration des examens, si nécessaire, en fonction de l'étude des résultats et relancer les examens.

Remarque : Vous trouverez une illustration simplifiée de ce flux de travaux dans la section «Flux de travaux de base», à la page 18.

Présentation de la fenêtre principale

Décrit les différents composants de la fenêtre principale AppScan, ainsi que l'ensemble des menus et barres d'outils.



Vous pouvez redimensionner les sous-fenêtres en cliquant sur la section en pointillés de n'importe quelle barre de séparation (barre entre deux sous-fenêtres).

Vous pouvez réorganiser les deux sous-fenêtres de droite verticalement ou horizontalement en cliquant sur **Afficher > Présentation > Verticale/Horizontale**.

Voir aussi : Chapitre 16, «Menus, barres d'outils et raccourcis clavier», à la page 373.

Sélecteur de vue

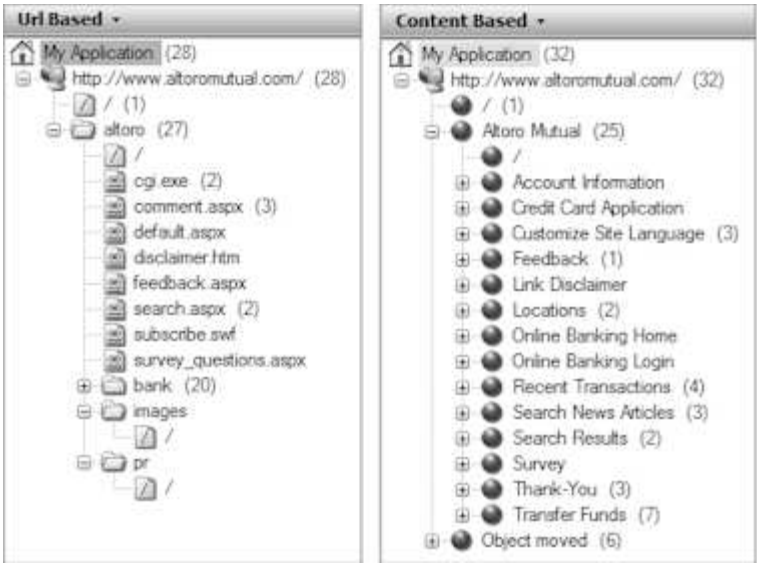
Les icônes de sélection de vue à droite de la barre d'outils permettent de passer d'une vue de résultats à une autre.

Lorsque vous sélectionnez une vue différente dans le sélecteur de vue, les informations affichées dans l'arborescence de l'application, dans la Liste des résultats et dans le Panneau des détails changent. Les trois parties de l'écran sont récapitulées dans le tableau suivant.

	**Vue Données**	Affiche les paramètres de script, les URL interactives, les URL visitées, les liens rompus, les URL filtrées, les commentaires, les JavaScripts et cookies de l'étape d'exploration. **Arborescence de l'application :** arborescence de l'application complète. **Liste des résultats :** Sélectionnez un filtre dans la liste en incrustation située en haut de la Liste des résultats pour déterminer quelles informations afficher. **Sous-fenêtre Détail :** Liste filtrée des paramètres de script, URL interactives, URL visitées, liens rompus, URL filtrées, commentaires, scripts JavaScripts et cookies. Contrairement aux deux autres vues, la vue Données d'application est disponible même si AppScan a uniquement terminé l'étape d'exploration. Utilisez la liste en incrustation dans la partie supérieure de la liste des résultats pour filtrer les données. Raccourci clavier : **F2** Chapitre 7, «Résultats : Données d'application», à la page 199
	**Vue Problèmes**	Indique les problèmes actuels détectés, au niveau de la présentation jusqu'aux demandes/réponses individuelles. Il s'agit de la vue par défaut. **Arborescence de l'application :** arborescence de l'application complète. Des compteurs situés à côté de chaque élément indiquent le nombre de problèmes trouvés pour l'élément. **Liste des résultats :** Répertorie les problèmes pour le nœud sélectionné dans l'arborescence de l'application, et la gravité de chaque problème. **Sous-fenêtre Détail :** Affiche les conseils, les recommandations de correction, et les demandes/réponses (y compris toutes les variantes utilisées) pour le problème sélectionné dans la Liste des résultats. Raccourci clavier : **F3** Chapitre 8, «Résultats : Problèmes de sécurité», à la page 207
	**Vue Tâches**	Fournit une liste de tâches des tâches de résolution spécifiques pour corriger les problèmes trouvés lors de l'examen. **Arborescence de l'application :** arborescence de l'application complète. Les compteurs situés à côté de chaque élément affichent le nombre de recommandations de correction pour chacun des éléments. **Liste des résultats :** Répertorie les tâches de résolution pour le nœud sélectionné dans l'arborescence de l'application, et la priorité de chaque tâche. **Sous-fenêtre Détail :** Affiche les détails de la tâche de résolution sélectionnée dans la liste des résultats, ainsi que tous les problèmes que cette résolution va permettre de résoudre. Raccourci clavier : **F4** Chapitre 9, «Résultats : Tâches de résolution», à la page 229

Arborescence de l'application

L'arborescence de l'application est un affichage sous forme d'arbre des dossiers, des URL et des fichiers trouvés par AppScan sur votre application.



Remarque : Dans le cas d'applications sans structure URL hiérarchique, telles que des applications à point d'entrée unique (par exemple MVC), ou d'applications dans lesquelles la structure hiérarchique n'est pas logique, vous pouvez créer une arborescence d'application "basée sur le contenu" en définissant un ensemble d'expressions régulières qui extrait le chemin logique à partir des pages. (Voir «Vue Résultats basés sur le contenu», à la page 103.)

Icônes Arborescence d'application

Chacun des divers types de nœud de l'Arborescence d'application est indiqué par sa propre icône.

Icône	Indique
	Mon application, nœud racine.
	Hôte examiné. Si vous avez défini des Serveurs et domaines supplémentaires («Vue URL et serveurs», à la page 47), ou si vous avez un serveur sur différents ports, vous pouvez avoir plusieurs nœuds de ce type.
	Dossier (chemin) trouvé dans votre application.
	Barre oblique ; résultats des tests pour le dossier parent.
	Fichier trouvé dans votre application.
	Un X rouge sur n'importe quelle icône de l'arborescence de l'application (icône Fichier illustrée ici) indique que le nœud et tous ses nœuds enfants ont été exclus des examens par l'utilisateur. (Pour inclure à nouveau un tel nœud dans de futurs examens, cliquez avec le bouton droit de la souris et sélectionnez **Inclure dans l'examen**.) Remarque : Un nœud enfant peut être inclus, même si son nœud parent est exclu.

Remarque : Si une adresse URL figurant dans l'arborescence d'application contient *uniquement* des réponses d'erreur, elle est barrée.

Compteurs d'arborescence d'application

Les compteurs d'arborescence d'application (nombres entre parenthèses situés à côté de chaque nœud de l'arborescence) changent selon la vue que vous sélectionnez dans le sélecteur de vue :

- **Problèmes de sécurité :** Les compteurs indiquent le nombre de problèmes appropriés au nœud, ainsi que tous ses nœuds enfants. (Le nombre total de problèmes est affiché en haut de la liste «Liste de résultats».)
- **Tâches de résolution :** Les compteurs indiquent le nombre de tâches de résolution appropriées au nœud et à tous ses nœuds enfants.
- **Données d'application :** Aucun compteur.

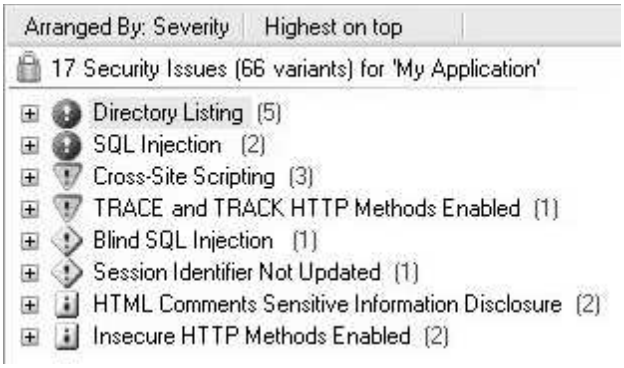
Menu "clic droit" de l'arborescence de l'application

Si vous cliquez avec le bouton droit de la souris sur un élément (autre que Mon application) de l'arborescence de l'application, le menu contextuel propose certaines ou toutes les options suivantes :

Elément du menu	Fonction
Afficher dans le navigateur	Ouvre le navigateur intégré sur l'URL sélectionnée.
Exploration manuelle	Démarre une exploration manuelle de l'élément sélectionné. Pour plus de détails, voir «Utilisation d'AppScan», à la page 143.
Test manuel	Ouvre la boîte de dialogue Test manuel. Pour plus de détails, voir «Tests manuels», à la page 223.
Enregistrement d'opérations en plusieurs étapes	Enregistre une séquence d'opérations en plusieurs étapes en vue de tester les parties du site accessibles uniquement en cliquant sur les liens dans un ordre spécifique. Pour plus de détails, voir «Vue Opérations en plusieurs étapes», à la page 95.
Copier l'URL	Copie l'URL sélectionnée dans le presse-papiers. (Lorsqu'il y a plusieurs sous-nœuds, l'URL du premier est copiée.)
Rapport pour ce nœud	Créez un rapport pour le nœud couramment sélectionné dans l'arborescence de l'application (y compris tous ses nœuds enfants). Pour plus de détails, voir «Création de rapports partiels», à la page 234.
Exclure de l'examen	Exclut l'URL sélectionnée (ou toutes les URL sous le nœud sélectionné) des examens. (Bascule sur "Inclure dans l'examen"). Pour plus de détails, voir «Exclure une URL de l'examen», à la page 208.

Liste de résultats

Les résultats de l'examen exécuté sur votre application Web sont affichés dans la Liste des résultats. Le nombre total de problèmes et de variantes apparaît en haut de la liste.



Compteurs de la liste des résultats

Les compteurs de la liste des résultats (nombres entre parenthèses situés à côté de chaque nœud) changent selon la vue que vous sélectionnez dans le sélecteur de vue :

- **Problèmes de sécurité :** Les compteurs indiquent le nombre de problèmes appropriés au nœud et à tous ses nœuds enfants.

  Remarque : Le nombre total de problèmes de sécurité (en haut de la liste des résultats) est une mesure des emplacements vulnérables du site et dépend en partie de sa structure. Si vous définissez une structure basée sur le contenu, le nombre total de problèmes dans l'arborescence de l'application peut ne pas être identique à celui de l'arborescence de l'application basée sur l'URL (pour les mêmes résultats). Lorsque la structure du site est basée sur le contenu (plutôt que sur l'URL), et que la vue basée sur le contenu est correctement configurée, le nombre de problèmes de la vue basée sur le contenu représente plus précisément le nombre "d'emplacements vulnérables" existant dans le site. Le nombre total de *variantes* (en haut de la Liste des résultats entre parenthèses) est indépendant de la structure du site et ne change pas entre la vue basée sur le contenu et la vue basée sur l'URL.
- **Tâches de résolution :** Les compteurs indiquent le nombre de tâches de résolution appropriées au nœud et à tous ses nœuds enfants.
- **Données d'application :** Aucun compteur.

Voir aussi : «Vue Résultats basés sur le contenu», à la page 103

Panneau des détails

Ce panneau affiche des détails sur l'élément sélectionné dans la Liste des résultats.

Les informations disponibles dans le Panneau des détails dépendent de l'élément sélectionné et de la vue sélectionnée.

- «Données d'application : Panneau des détails», à la page 205
- «Problèmes de sécurité : Panneau des détails», à la page 212
- «Tâches de résolution : Panneau des détails», à la page 232

Panneaux d'examen

Panneaux de progression et de notification

Panneau de progression

Le panneau de progression apparaît au-dessous de la liste des résultats lors d'un examen. Il s'affiche lorsque vous démarrez un examen et présente des informations de progression pendant que l'examen se poursuit.

Panneau de notification

Le panneau de notification s'affiche à la place du panneau de progression si AppScan ne parvient pas à se connecter à votre serveur Web ou si l'examen a été arrêté avant son terme. Il affiche de brèves informations (telles que `"Serveur arrêté"`, ou `"L'examen est incomplet"`), avec un lien permettant

d'ouvrir une boîte de dialogue contenant plus de détails.

Barre d'état

La barre d'état située en bas de la fenêtre principale affiche des informations relatives à l'examen actuellement en cours ou chargé.

Icône	Indique
	**Pages visitées :** Nombre de pages visitées/nombre total de pages à visiter Le deuxième nombre peut augmenter puis diminuer au cours de l'examen, selon que des pages sont détectées, puis rejetées si elles ne requièrent pas d'examen.
	**Eléments testés :** Nombre d'éléments testés/nombre total d'éléments à tester Le *deuxième* nombre augmente au cours de l'étape d'exploration, car des éléments à tester sont découverts. Au cours de l'étape de test, c'est le *premier* nombre qui augmente. A la fin de l'examen, les deux nombres doivent être égaux.
	**Demandes HTTP envoyées** Ce nombre représente toutes les demandes envoyées, y compris les demandes de détection en session, les demandes de détection des serveurs arrêtés, les demandes de connexion, les opérations en plusieurs étapes et les demandes de test. Par conséquent, au cours de l'examen, il indique qu'AppScan fonctionne. Toutefois, le nombre lui-même ne signifie rien de spécial pendant ou après l'examen.
	**Problèmes de sécurité** Nombre total de problèmes de sécurité trouvés, suivi du nombre dans chaque catégorie : Elevée, Moyenne, Faible et Information.

Tutoriel

Ce tutoriel présente les étapes de configuration de l'examen simple d'une application à l'aide de l'assistant de configuration des examens, d'exécution de l'examen et de révision des résultats.

Ce tutoriel simple utilise l'assistant de configuration des examens pour examiner le site Web "AltoroMutual Bank", qui a été créé à des fins de démonstrations.

Les utilisateurs expérimentés préféreront peut-être suivre le flux de travaux avancé (qui utilise également l'assistant) décrit à la rubrique «Flux de travaux pour les utilisateurs avancés», à la page 313, ou réaliser une configuration plus détaillée à l'aide de la «Boîte de dialogue Configuration des examens», à la page 46.

- «Etape 1 : Configurer l'examen», à la page 26
- «Etape 2 : Exécuter l'examen», à la page 27
- «Etape 3 : Réviser les résultats de l'examen», à la page 27
- «Etape 4 : Communiquer les résultats», à la page 28

Tout au long de ce tutoriel, vous pouvez travailler à l'aide du site Web "AltoroMutual Bank", qui a été créé à des fins de démonstrations :

URL	https://demo.testfire.net/
Nom d'utilisateur	jsmith
Mot de passe	demo1234

Remarque : Si vous utilisez une version d'évaluation d'AppScan, le site Web AltoroMutual Bank est le *seul* site que vous pouvez examiner.

Remarque : Ce tutoriel n'est qu'un aperçu des étapes de base de l'exécution d'un examen. Pour obtenir des explications et des instructions complètes, voir Chapitre 4, «Configuration», à la page 31. Voir aussi «Flux de travaux pour les utilisateurs avancés», à la page 313.

Etape 1 : Configurer l'examen

Première étape du tutoriel

Pourquoi et quand exécuter cette tâche

L'assistant de configuration des examens permet de configurer facilement un examen, lorsque vous n'avez pas besoin de modifier de nombreux paramètres de configuration par défaut.

Procédure

1. Lancez AppScan pour ouvrir l'écran d'accueil ou, si AppScan est ouvert, cliquez sur **Fichier > Nouveau** pour ouvrir une boîte de dialogue similaire.
2. Vérifiez que la case à cocher **Lancer l'assistant de configuration des examens** est sélectionnée, puis sélectionnez le modèle **Examen standard**.

   L'écran d'accueil de l'assistant de configuration des examens s'affiche.
3. Sélectionnez le bouton d'option **Examen d'application Web**, puis cliquez sur **Suivant**.

   L'étape URL et serveurs de l'assistant apparaît.

   Remarque : Si vous sélectionnez l'option d'examen des *Services* Web, le flux est légèrement différent et lorsque l'assistant se ferme, GSC s'ouvre pour vous permettre d'entrer des paramètres qui seront utilisés par AppScan pour l'étape de test de son examen. (Pour plus d'informations, voir «Assistant pour exploration avec GSC», à la page 43.)
4. Entrez l'URL de votre application dans la zone de saisie, puis cliquez sur **Suivant**.

   L'étape Gestion de connexion apparaît.
5. Cliquez sur **Enregistrer la connexion**.

   Le navigateur AppScan s'ouvre sur l'URL de départ définie à l'étape précédente. Votre choix de navigation est maintenant enregistré par AppScan.
6. Connectez-vous à votre application avec un nom d'utilisateur et un mot de passe autorisés.
7. Une fois la connexion effectuée, fermez le navigateur.

   La "Séquence de connexion" (séquence de liens ayant atteint l'état connecté) s'affiche (voir «Enregistrement d'une connexion», à la page 53 pour plus d'informations) et l'icône Clé grise devient verte, indiquant que la détection En session est active.

    devient : 
8. Cliquez sur **Suivant**.

   L'étape Stratégie de test apparaît.
9. Cliquez sur **Suivant**.

   L'étape Optimisation du test apparaît. Laissez le paramètre par défaut pour un examen standard.
10. Cliquez sur **Suivant**.

    L'étape finale de l'assistant apparaît. Vous êtes maintenant prêt à exécuter l'examen (voir «Etape 2 : Exécuter l'examen», à la page 27).

    Remarque : Bien qu'il soit possible de démarrer l'examen automatique à ce stade, vous obtiendrez généralement de meilleurs résultats en commençant par explorer manuellement l'application, comme un utilisateur standard (voir «Utilisation d'AppScan», à la page 143).

Etape 2 : Exécuter l'examen

Deuxième étape du tutoriel

Pourquoi et quand exécuter cette tâche

Une fois la configuration terminée vous pouvez exécuter l'examen.

Procédure

1. Sélectionnez **Démarrer un examen automatique complet** et cliquez sur **Terminer**.

   L'assistant se ferme et le panneau Scan Expert commence à évaluer la configuration actuelle de votre site. Une fois l'évaluation terminée, une liste de contrôle des modifications de configuration suggérées apparaît.

   Remarque : Si certaines modifications requièrent une entrée de l'utilisateur, leurs cases à cocher sont grisées ou désélectionnées. Pour fournir l'entrée requise pour ces modifications, cliquez sur le lien relatif à ces modifications.

2. Cliquez sur **Appliquer les recommandations**.

   Les modifications de configuration sélectionnées sont appliquées et l'examen commence. Le panneau de progression s'ouvre et les données d'application et problèmes sont mis à jour en temps réel.

   Pendant l'étape d'exploration, AppScan explore votre application Web pour reconnaître ses pages et son contenu. L'arborescence des **Données d'application** est mise à jour au fur et à mesure de l'exploration et finit par afficher l'arborescence complète du site. Ensuite, lors de l'étape de test, AppScan exécute des milliers de tests sur le site et rapporte les problèmes trouvés et les recommandations de correction. Pendant cette partie de l'examen, la vue Problèmes de sécurité est automatiquement sélectionnée et la Liste des résultats affiche une liste mise à jour de façon dynamique des problèmes trouvés.

   Un examen peut comprendre plusieurs phases (une phase est un cycle d'exploration suivi d'un test). Ceci se produit lorsque AppScan reconnaît de nouveaux liens pendant l'étape de test et a besoin d'un examen ; il crée de nouveaux tests en fonction de ces liens et exécute une étape d'examen supplémentaire. La phase suivante est généralement plus courte que la précédente, car seuls les nouveaux liens sont analysés. AppScan ajoutera des phases tant qu'il trouve de nouvelles URLs, ou jusqu'à ce qu'il ait atteint la "limite de balayage" configurée. Par défaut, le nombre de phases est limité à quatre.

   Une fois l'examen terminé, le panneau de progression se ferme et vous pouvez consulter les résultats (voir «Etape 3 : Réviser les résultats de l'examen»).

Etape 3 : Réviser les résultats de l'examen

Troisième étape du tutoriel

Pourquoi et quand exécuter cette tâche

Une fois l'examen terminé, les résultats sont affichés dans trois zones de la fenêtre principale : l'Arborescence de l'application, la Liste des résultats et le Panneau des détails. Le type d'informations présentées dans chacune de ces zones dépend de la vue sélectionnée (par défaut la vue Problèmes de sécurité).

Procédure

Pour accéder à une vue, cliquez sur l'icône appropriée dans le sélecteur de vue situé à gauche de l'écran.

Afficher	Description
	La **vue Données** fournit la liste des éléments de contenu trouvés dans votre application. Ceci permet de vérifier que l'examen est configuré de manière à couvrir l'application *avant* de commencer l'étape de test. • **Arborescence de l'application :** affiche les noeuds d'URL et de dossier. • **Liste de résultats :** affiche les données d'application, triées par résultats d'examen (voir «Données d'application : Liste de résultats», à la page 199). Par exemple, vous pouvez choisir de visualiser une liste de liens rompus, de JavaScript, de cookies, etc. • **Sous-fenêtre Détail :** affiche la demande envoyée à une page et la réponse reçue. Pour obtenir plus d'informations sur la vue Données d'application, voir Chapitre 7, «Résultats : Données d'application», à la page 199.
	La **vue Problèmes** fournit des données détaillées des problèmes de sécurité rencontrés lors de l'examen. • **Arborescence de l'application :** affiche les dossiers, URL et fichiers trouvés par AppScan dans votre application et les répertorie. Le numéro en regard de chaque noeud dans l'arborescence indique le nombre de problèmes trouvés. • **Liste des résultats :** affiche une icône par problème, indiquant la valeur de gravité affectée à ce problème (voir «Problèmes de sécurité : Liste de résultats», à la page 208). Chaque problème contient également une consolidation des URL qui lui sont vulnérables. Sous chaque URL, une liste des données vulnérables est présentée. • **Sous-fenêtre Détail :** Affiche des informations permettant de comprendre pourquoi il s'agit d'un problème, ce qu'il peut occasionner s'il n'est pas traité, des recommandations de correctifs, les variantes des demandes de test qui ont été envoyées, la réponse de votre application pour laquelle AppScan a marqué le test comme problème, et encore plus d'informations. Pour plus d'informations sur la vue Problèmes, voir Chapitre 8, «Résultats : Problèmes de sécurité», à la page 207.
	La **vue Tâches** affiche les résolutions conçues pour résoudre et empêcher les problèmes de sécurité. Elle vous permet de communiquer facilement et efficacement avec le personnel sur les problèmes de votre application et d'indiquer, dans un langage précis et concis, comment corriger la conception de votre application. • **Arborescence de l'application :** affiche le numéro situé en regard de chaque noeud dans l'arborescence et indique le nombre de tâches de résolution approprié à chaque élément. • **Liste des résultats :** affiche une icône par tâche de résolution, indiquant la valeur de priorité affectée à cette tâche (voir «Tâches de résolution : Liste de résultats», à la page 229). • **Sous-fenêtre Détail :** affiche les détails de la tâche de résolution et répertorie les problèmes qui seront résolus par cette tâche. Pour plus d'informations sur la vue Résolutions, voir Chapitre 9, «Résultats : Tâches de résolution», à la page 229.

Voir «Etape 4 : Communiquer les résultats».

Etape 4 : Communiquer les résultats

Quatrième étape du tutoriel

Pourquoi et quand exécuter cette tâche

Il existe deux façons de communiquer les résultats d'examen à vos équipes :

Rapports :
Vous pouvez choisir un modèle de rapport basé sur le rapport prévu : demander un rapport pour le contrôle qualité, un pour les cadres, un pour les développeurs, etc. Plus vous avancerez dans le cycle de vie de développement de votre application, plus les rapports de conformité seront essentiels. Vous pouvez obtenir un rapport complet sur la manière dont votre application répond aux réglementations et normes publiques et de l'industrie sélectionnées. Pour plus d'informations, voir Chapitre 10, «Rapports», à la page 233.

Problèmes individuels :
S'il existe un problème spécifique qui doit être résolu par une équipe ou une personne particulière, vous pouvez envoyer les tests et leurs résultats à la partie appropriée. Voir «Rapport Faux positif des résultats de test», à la page 222.

Exemples d'examen

Les exemples d'examen fournis illustrent l'utilisation d'AppScan et les types de résultats générés.

Quatre exemples d'examen sont enregistrés sur votre machine à l'installation d'AppScan. Vous pouvez les ouvrir pour voir comment ils sont configurés et comment les résultats sont affichés dans AppScan. Vous trouverez ces exemples d'examen dans le dossier AppScan Standard principal, dont l'emplacement par défaut est :

```
C:\Program Files (x86)\IBM\AppScan Standard
```

Ces examens sont les suivants :

demo.testfire.net.scan
Examen du site de test de la démonstration AppScan. Vous pouvez consulter la configuration et les résultats. Vous pouvez également envoyer des demandes supplémentaires au site et continuer l'examen avec les nouvelles données.

Glass_Box_DotNet_Demo.scan et Glass_Box_Java_Demo.scan
Ces deux examens sont des exemples d'examen glass box utilisant respectivement un serveur d'applications .NET et un serveur Java. Vous pouvez consulter la configuration et explorer les problèmes individuellement. Lorsque glass box détecte des problèmes, les informations incluent le code source concerné.

Remarque : L'examen glass box nécessite l'accès à un agent situé sur le serveur de l'application en cours d'examen, et vous n'avez pas accès à l'agent qui a été utilisé pour cet examen. Vous ne pouvez pas continuer cet examen.

GSC_demo.testfire.scan
Examen des services Web du site de test de la démonstration AppScan. Vous pouvez consulter la configuration et les résultats. Si vous avez installé GSC (Generic Service Client), vous pouvez l'utiliser pour envoyer des demandes supplémentaires au site et continuer l'examen avec les nouvelles données.

Chapitre 4. Configuration

Vous configurez un examen en choisissant les paramètres qui décrivent le mieux votre application ainsi que le type de test souhaité.

Vous avez le choix entre deux méthodes de configuration d'examens standard :

- «Assistant de configuration des examens» si :
  - vous utilisez AppScan pour la première fois ;
  - la plupart des paramètres requis sont standards ;
  - vous n'avez pas besoin de modifier des paramètres entre des examens et avez déjà enregistré un modèle d'examen avec vos propres spécifications.
- «Boîte de dialogue Configuration des examens», à la page 46 si :
  - vous devez personnaliser de nombreux paramètres d'un examen ;
  - vous souhaitez créer et sauvegarder un modèle d'examen personnalisé.

Dans les deux cas, commencez par un modèle d'examen (voir «Modèles d'examen», à la page 137) et, éventuellement, modifiez des paramètres. Cependant, certains paramètres avancés ne peuvent pas être modifiés à l'aide de l'assistant, mais uniquement à l'aide de la boîte de dialogue.

Vous pouvez baser votre examen sur le **modèle d'examen standard** ou charger un modèle que vous avez précédemment sauvegardé. (Un *"modèle d'examen"* est un ensemble de paramètres de configuration d'examen qui ont été sauvegardés.) La sauvegarde et le chargement de vos propres modèles d'examen est la méthode la plus efficace lorsque vous utilisez régulièrement les mêmes paramètres pour vos examens.

Remarque : Après avoir configuré l'examen, mais avant de le démarrer, vous pouvez utiliser «Scan Expert», à la page 164 pour évaluer la configuration de votre application, et suggérer des modifications pour l'optimiser.

Voir aussi : «Description du flux de travaux», à la page 18

Assistant de configuration des examens

Vous pouvez configurer rapidement des examens de base à l'aide de l'assistant.

L'**assistant de configuration des examens** représente la méthode la plus simple pour configurer et démarrer un examen si vous n'avez pas besoin de modifier de nombreuses options par défaut. Toutefois, si vous devez modifier des options avancées, il est préférable d'utiliser la «Boîte de dialogue Configuration des examens», à la page 46.

L'assistant permet d'accéder aux options de configuration les plus courantes, la principale différence étant la manière dont les options sont organisées. (Dans le tableau ci-dessous ainsi que dans les sections suivantes, des références croisées relatives aux options identiques dans l'assistant et dans la boîte de dialogue pointent vers la section boîte de dialogue de cette section.)

Explorer avec	Description
AppScan (automatiquement ou manuellement)	Sélectionnez cette option pour la plupart des examens d'application Web. L'exploration s'effectue manuellement et/ou automatiquement avec des demandes envoyées à l'application par AppScan.

Explorer avec	Description
Périphérique externe/client (avec AppScan comme proxy d'enregistrement)	Sélectionnez cette option pour utiliser l'enregistreur de trafic externe d'AppScan comme un proxy d'enregistrement, et explorer manuellement des services RESTful ou d'autres services Web non-SOAP - ou des services SOAP ne nécessitant pas d'enveloppes de sécurité - avec un téléphone mobile, un simulateur ou un émulateur. AppScan affiche les domaines et les demandes dans son enregistreur de trafic externe et crée les tests appropriés en fonction de l'entrée.
Client de service générique (WSDL)	Sélectionnez cette option pour les services Web avec un fichier WSDL. GSC (Generic Service Client) utilise le fichier WSD de votre service Web pour fournir une interface simple qui affiche les services disponibles et permet d'entrer des paramètres et de visualiser les résultats. Utilisez l'interface GSC pour explorer votre service Web manuellement afin qu' AppScan puisse utiliser vos entrées pour créer les tests appropriés. **Remarque :** Cette option est disponible uniquement si GSC (Generic Service Client) est installé sur votre machine. Vous pouvez cliquer sur le lien en bleu pour télécharger GSC sur votre ordinateur, puis cliquer deux fois sur le fichier .EXE pour l'installer.

Lancer l'assistant de configuration des examens

Pourquoi et quand exécuter cette tâche

Vous pouvez lancer l'**Assistant de configuration des examens** depuis l'écran d'accueil AppScan (qui s'affiche lorsque vous lancez AppScan), ou en cliquant sur l'icône Nouvel examen dans la barre d'outils.

Remarque : Si l'écran **Bienvenue** ne s'affiche pas lorsqu'AppScan démarre, c'est que vos paramètres de **Préférences** ont été modifiés. Pour les remettre dans l'état d'origine, voir «Onglet Général», à la page 264. (Vous pouvez également ouvrir l'écran d'accueil à tout moment à partir du menu *Afficher*.)

Procédure

1. Pour lancer l'assistant, procédez de l'une des façons suivantes :
   - Dans l'écran d'accueil, cliquez sur **Créer un examen**.
   - Si AppScan est déjà ouvert, cliquez sur l'icône **Nouvel examen** dans la barre d'outils.
2. Dans la boîte de dialogue Nouvel examen, vérifiez que la case **Lancer l'assistant de configuration des examens** est cochée.

3. Dans la liste Modèles prédéfinis, sélectionnez un modèle d'examen en cliquant dessus. Si vous n'avez pas besoin d'un modèle *spécifique* , sélectionnez le module d' **examen standard** (pour plus de détails, voir «Modèles prédéfinis», à la page 138).

   L'écran d'accueil de l'assistant de configuration des examens s'affiche.
4. Dans l'écran d'accueil de l'**Assistant de configuration des examens**, sélectionnez l'option d'examen requise.

Explorer avec	Description
AppScan (automatiquement ou manuellement)	Sélectionnez cette option pour la plupart des examens d'application Web. L'exploration s'effectue manuellement et/ou automatiquement avec des demandes envoyées à l'application par AppScan.
Périphérique externe/client (avec AppScan comme proxy d'enregistrement)	Sélectionnez cette option pour utiliser l'enregistreur de trafic externe d'AppScan comme un proxy d'enregistrement, et explorer manuellement des services RESTful ou d'autres services Web non-SOAP - ou des services SOAP ne nécessitant pas d'enveloppes de sécurité - avec un téléphone mobile, un simulateur ou un émulateur. AppScan affiche les domaines et les demandes dans son enregistreur de trafic externe et crée les tests appropriés en fonction de l'entrée.
Client de service générique (WSDL)	Sélectionnez cette option pour les services Web avec un fichier WSDL. GSC (Generic Service Client) utilise le fichier WSD de votre service Web pour fournir une interface simple qui affiche les services disponibles et permet d'entrer des paramètres et de visualiser les résultats. Utilisez l'interface GSC pour explorer votre service Web manuellement afin qu' AppScan puisse utiliser vos entrées pour créer les tests appropriés. **Remarque :** Cette option est disponible uniquement si GSC (Generic Service Client) est installé sur votre machine. Vous pouvez cliquer sur le lien en bleu pour télécharger GSC sur votre ordinateur, puis cliquer deux fois sur le fichier .EXE pour l'installer.

Assistant pour exploration avec AppScan

Répertorie les étapes de cet assistant.

1. «Adresses URL et serveurs»
2. (Facultatif :) «Paramètres de connexion», à la page 34
3. «Gestion de connexion», à la page 35
4. (Facultatif :) «Gestion de connexion - Détails», à la page 36
5. «Stratégie de test», à la page 36
6. «Optimisation du test», à la page 37
7. «Complet», à la page 38

Adresses URL et serveurs

Définissez l'URL de départ pour l'examen, ainsi que des serveurs et des domaines supplémentaires qui doivent être inclus.

Pourquoi et quand exécuter cette tâche

Si vous avez sélectionné **Examen d'application Web** à l'étape de bienvenue, la première étape de l'assistant consiste à définir l'URL de départ et les paramètres du serveur pour l'examen.

Procédure

1. **Adresse URL de départ :** saisissez l'URL de votre application. L'examen démarrera à cette URL.

   AppScan tente d'atteindre l'URL et, en cas de succès, une coche de couleur verte et le message de confirmation "Connecté au serveur" apparaissent sous l'URL de départ. Si le problème peut être

corrigé en modifiant la configuration, AppScan suggère la modification nécessaire et établit un lien à la vue appropriée dans la boîte de dialogue de configuration.

 ouvre la page que vous venez d'entrer dans un navigateur. Si nécessaire, vous pouvez accéder à une autre URL et utiliser la barre d'outils pour définir la nouvelle page comme URL de départ pour l'examen. Fermez le navigateur pour poursuivre la configuration de l'examen.

 Teste une nouvelle fois l'URL de départ. Cliquez sur ce bouton si le serveur était arrêté lors de la configuration et qu'il a repris ultérieurement.

Conseil : Si vous modifiez le domaine, le schéma ou le port de l'URL de départ *après la configuration de l'examen*, il peut être nécessaire de modifier la configuration. Le système vous demandera si vous souhaitez qu'AppScan tente d'effectuer cette opération automatiquement. Pour plus de détails, voir «Modification de l'hôte de l'URL de départ», à la page 50

2. **Chemin d'accès sensible à la casse :** Lorsque cette case est cochée (par défaut), les liens présentant des casses différentes sont traités comme des pages distinctes. Par exemple, "ReadMe.as" serait considéré comme différent de "readme.as". Dans la plupart des cas, vous devez cocher la case pour les serveurs Unix et la désélectionner pour les serveurs Windows.
3. **Serveurs et domaines supplémentaires :** si votre application inclut des serveurs ou des domaines autres que ceux de l'URL de départ, *et que votre licence AppScan les inclut*, vous devez les ajouter ici pour qu'ils soient inclus à l'examen :
   a. Cliquez sur l'icône  pour ouvrir la boîte de dialogue d'ajout de serveurs et de domaines.
   b. Entrez le nom d'hôte et l'adresse IP du serveur, ou le nom de domaine (par exemple, sitetoscan.com) puis cliquez sur **OK**.

   Le nouvel élément est ajouté à la liste.
4. **Je dois configurer des paramètres de connectivité supplémentaires :** Par défaut, AppScan utilise des paramètres de proxy Internet Explorer. Cochez cette case uniquement si vous souhaitez qu'AppScan utilise un autre proxy. Une étape supplémentaire s'ouvrira, «Paramètres de connexion», lorsque vous cliquerez sur le bouton Suivant.
5. Cliquez sur **Suivant** pour passer à l'étape suivante de l'assistant.

Que faire ensuite

«Gestion de connexion», à la page 35

Si vous avez sélectionné "Je dois configurer des paramètres de connectivité supplémentaires", poursuivez l'opération avec «Paramètres de connexion».

Paramètres de connexion

(Facultatif :) Configurez les paramètres de proxy et, le cas échéant, l'authentification au niveau serveur.

Pourquoi et quand exécuter cette tâche

Par défaut, AppScan utilise des paramètres de proxy Internet Explorer. Procédez à cette étape uniquement si vous cochez la case Paramètres de connexion supplémentaires lors de l'étape relative aux adresses URL et aux serveurs de l'assistant ; elle permet de configurer AppScan pour utiliser d'autres paramètres de proxy, ou ne pas en utiliser du tout.

Procédure

1. Sélectionnez l'une des trois options proxy :
   - **Utiliser les paramètres de proxy d'Internet Explorer :** (Par défaut) Lorsque cette option est sélectionnée, AppScan utilise l'adresse et le port de la connexion Internet Explorer lorsqu'il se connecte à l'application.

- **Ne pas utiliser de proxy :** sélectionnez cette option si vous ne souhaitez pas qu'AppScan utilise des paramètres de proxy.
- **Utiliser les paramètres de proxy personnalisés :** sélectionnez cette option si vous souhaitez utiliser une adresse et un port autres que ceux utilisés par Internet Explorer.

2. Si vous avez sélectionné l'une des options utilisant un proxy, vous pouvez éventuellement définir le nom d'utilisateur, le mot de passe et le domaine qu'utilisera AppScan lors de la connexion. Pour ce faire, cliquez sur le bouton **Configurer**.
3. Si votre plateforme requiert une authentification au niveau serveur, définissez le nom d'utilisateur, le mot de passe et le domaine dans la zone **Authentification HTTP**.
4. Cliquez sur **Suivant**.

Que faire ensuite

«Gestion de connexion»

Gestion de connexion

Configurez la méthode de connexion et, le cas échéant, enregistrez la procédure de connexion.

Pourquoi et quand exécuter cette tâche

L'étape Gestion de connexion de l'assistant permet de sélectionner l'une des trois méthodes utilisées par AppScan lorsqu'il rencontre des pages de connexion lors d'un examen :

- **Connexion enregistrée** : (méthode recommandée) : Si vous sélectionnez cette option, AppScan utilise une procédure de connexion que vous enregistrez en remplissant des zones et en cliquant sur des liens comme un utilisateur réel.

  Pour plus d'informations, voir «Enregistrement d'une connexion», à la page 53.

  Si la connexion nécessite l'intervention d'un utilisateur (comme l'authentification à deux facteurs, les mots de passe à usage unique ou CAPTCHA), sélectionnez l'option Invite.
- **Invite** : Dans ce cas, vous devez toujours enregistrer une procédure de connexion. Bien qu'AppScan ne tente pas de se connecter à l'aide de la procédure que vous enregistrez, il a besoin d'elle comme référence pour savoir à quel moment se déconnecter.
- **Connexion automatique :** Si AppScan parvient à se connecter au site uniquement à l'aide d'un nom et d'un mot de passe, sans procédure particulière, sélectionnez cette option et entrez un nom d'utilisateur et un mot de passe.
- **Aucune connexion :** Sélectionnez uniquement cette option si l'application ne nécessite pas d'être connectée ou si, pour une autre raison, vous ne souhaitez pas qu'AppScan se connecte.

Procédure

1. Sélectionnez le bouton radio pour la méthode de connexion requise.
2. Procédez de l'une des façons suivantes :
   - Pour Connexion enregistrée ou Invite, le fait de cliquer sur **Enregistrer** ou **Importer** définit une séquence de connexion (pour plus de détails, voir «Onglet Connexion», à la page 52).
   - Pour Connexion automatique, entrez simplement un **Nom d'utilisateur** et **Mot de passe**.

   Remarque : Si vous enregistrez une connexion, une boîte de dialogue peut s'ouvrir à la fin de l'enregistrement pour vous demander de confirmer que les données de connexion extraites par AppScan sont correctes. Si nécessaire, spécifiez ou corrigez les paramètres et les valeurs, puis cliquez sur **OK**.

   Si vous avez enregistré une séquence de connexion valide, l'icône représentant une clé passe de la couleur grise  à la couleur verte  , indiquant que la page En session a été identifiée.

Remarque : Si l'icône Clé devient rouge  , cela signifie qu'AppScan a tenté, sans y parvenir, d'identifier un schéma dans la page En session lors de l'examen pour vérifier qu'il n'était pas déconnecté. Pour y remédier, vous devez ouvrir l'étape supplémentaire de l'assistant et fournir manuellement un identificateur à AppScan (voir l'étape suivante).

3. Si vous cochez la case **Je souhaite configurer les options de détection en session**, une étape supplémentaire de l'assistant, «Gestion de connexion - Détails», s'ouvre lorsque vous cliquez sur **Suivant**. Sélectionnez-la uniquement si vous devez éditer la séquence de connexion (voir la note de l'étape précédente).
4. Cliquez sur **Suivant**.

Que faire ensuite

«Stratégie de test»

Si vous avez sélectionné "Je souhaite configurer les options de détection En session", poursuivez l'opération avec «Gestion de connexion - Détails»

Gestion de connexion - Détails

(Facultatif :) Révisez et éditez la séquence de connexion que vous avez enregistrée.

Pourquoi et quand exécuter cette tâche

La boîte de dialogue des paramètres supplémentaires de Gestion de connexion permet de réviser et d'éditer la séquence de connexion que vous avez enregistrée ainsi que le schéma qu'utilise AppScan lors de l'examen pour vérifier qu'il est connecté ("détection de schéma En session").

Procédure

1. Révisez et éditez la séquence de connexion et assurez-vous que le schéma de détection de session est valide. Les options sont décrites dans «Onglet Vérifier et valider», à la page 55
2. Cliquez sur **Suivant**.

Que faire ensuite

«Stratégie de test»

Stratégie de test

Le fait de limiter l'examen aux types de test souhaités permet de réduire la durée de l'examen.

Pourquoi et quand exécuter cette tâche

Le nombre de tests envoyés par AppScan lors d'un examen peut atteindre plusieurs milliers. Il est parfois préférable de réduire la durée de l'examen en le limitant à certains types uniquement. C'est la stratégie de test.

AppScan est livré avec une stratégie de test par défaut, ainsi qu'avec certaines configurations de stratégie de test supplémentaires que vous pouvez sélectionner. Vous pouvez également utiliser vos propres stratégies de test définies par l'utilisateur.

L'étape Stratégie de test de l'assistant présente le nom de la stratégie de test sur laquelle est basée la stratégie en cours, ainsi que sa description.

Procédure

1. Vérifiez que la stratégie de test correspond à vos besoins. (Dans le doute, conservez la stratégie de test par défaut.)

2. Pour charger une autre stratégie de test, cliquez sur l'une des stratégies prédéfinies ou des stratégies récentes dans le panneau **Fichiers de stratégies**. Pour plus d'informations, voir «Vue Stratégie de test», à la page 109.
3. **Envoyer les tests sur les pages de connexion et de déconnexion :** par défaut, AppScan teste vos pages de connexion et de déconnexion ainsi que le reste de l'application. Vous devez conserver cette configuration par défaut, sauf si :
   - votre application dispose de mesures de sécurité qui verrouillent l'accès aux utilisateurs qui fournissent une entrée illégale à ces pages,
   - le flux de votre application risque d'être altéré par le test de ces pages.

   Si vous n'êtes pas sûr de la réponse de votre application à ces tests, gardez cette option sélectionnée.
4. **Ne pas envoyer d'identificateurs de session lors des tests des pages de connexion :** (Cette case à cocher est active, et sélectionnée par défaut, uniquement si la case précédente est sélectionnée.) Il est recommandé de laisser cette case cochée, car les identificateurs de session peuvent limiter la réussite des tests des pages de connexion. Désactivez cette option uniquement si vous êtes certain que des jetons de session valides sont nécessaires pour tester vos pages de connexion.

   Si vous n'êtes pas sûr de la réponse de votre application, gardez cette option sélectionnée.
5. Cliquez sur **Suivant**.

Que faire ensuite

«Optimisation du test»

Optimisation du test

L'option Optimisation du test vous permet de profiter de l'apprentissage automatique pour réaliser un examen plus rapide.

Pourquoi et quand exécuter cette tâche

Généralement, un examen AppScan Standard complet standard envoie des milliers de tests et son exécution peut prendre plusieurs heures, voire plusieurs jours. Au cours des premières étapes de développement, ou pour avoir une évaluation globale rapide du contexte de sécurité actuel de votre produit, vous pouvez utiliser Optimisation du test pour obtenir les résultats requis dans un délai plus court.

Nos filtres de test intelligents s'appuient sur l'analyse statistique et filtrent certains tests (ou même des variantes de test spécifiques) pour générer un examen plus court qui identifie uniquement les vulnérabilités les plus fréquentes, graves et importantes. Les groupes de correctif et les correctifs iFixes AppScan permettent de vous maintenir à jour grâce aux filtres d'optimisation les plus récents. Grâce à l'option Optimisation du test, vous pouvez réduire considérablement la durée de l'examen, lorsque vous accordez davantage d'importance à la vitesse qu'à la profondeur de l'examen.

Procédure

1. Sélectionnez l'option dont vous avez besoin (en cas de doute, laissez l'option par défaut) :

Option	Description
Normal (par défaut)	Effectue un examen en profondeur, pour envoyer tous les tests appropriés au site, selon la configuration. Ce paramètre est recommandé lorsqu'un examen plus long ne va pas interrompre votre flux de développement.
Optimisé	Accélère l'examen en envoyant uniquement des tests pour les vulnérabilités les plus fréquentes, graves et importantes.

2. Cliquez sur **Suivant** pour passer à l'étape finale de l'assistant.

Que faire ensuite

«Complet»

Concepts associés:

«Compréhension de l'option Optimisation du test», à la page 325
Cette section décrit comment l'option Optimisation du test fonctionne et comment mieux l'intégrer au cycle de vie de votre développement.

Complet

Après avoir effectué les étapes de l'assistant, vous décidez comment et quand démarrer l'examen que vous avez configuré.

Pourquoi et quand exécuter cette tâche

Si vous sélectionnez l'une des options démarrant immédiatement un examen, vous pouvez également choisir d'exécuter *Scan Expert* avant l'examen principal. Scan Expert se connecte à votre application et exécute un rapide examen préliminaire qui permet d'évaluer les paramètres configurés. Il suggère ensuite des modifications de configuration, le cas échéant. L'incorporation de ces suggestions (automatique ou manuelle) peut augmenter l'efficacité de l'examen principal de façon significative.

Procédure

1. Sélectionnez l'une des options :
   - **Démarrer un examen automatique intégral :** Démarre un examen intégral de l'application (exploration suivie du test).
   - **Ne commencer qu'avec l'exploration automatique :** Explore l'application sans procéder à l'étape de test. (Vous pouvez exécuter l'étape de test ultérieurement.)
   - **Commencer avec l'exploration manuelle :** Le navigateur s'ouvre et vous pouvez manuellement explorer votre site en cliquant sur les liens et en remplissant les zones. AppScan enregistre les résultats à utiliser à l'étape de test.
   - **Je démarrerai l'examen ultérieurement :** Ferme l'assistant sans démarrer d'examen. Ce modèle sera utilisé la prochaine fois que vous démarrerez un examen.
2. **Démarrer Scan Expert lorsque l'assistant de configuration des examens a été exécuté :** (Cette option est active uniquement si l'une des trois premières options d'examen a été sélectionnée.) Cochez cette case si vous souhaitez que Scan Expert évalue votre configuration avant de démarrer l'examen principal.

Que faire ensuite

Voir : «Progression de l'examen», à la page 159

Voir aussi :

«Démarrer des examens», à la page 157

Chapitre 8, «Résultats : Problèmes de sécurité», à la page 207

Assistant pour exploration avec un périphérique externe ou un client

Répertorie les étapes de cet assistant.

1. «Enregistrement du proxy», à la page 39
2. (Facultatif :) «Paramètres de connexion», à la page 39
3. «Certificat SSL», à la page 40
4. «Gestion de connexion», à la page 40

5. (Facultatif :) «Gestion de connexion - Détails», à la page 41
6. «Stratégie de test», à la page 41
7. «Complet», à la page 42

Enregistrement du proxy

Configuez le port du proxy et le type de client.

Procédure

1. **Port du proxy d'enregistrement :** Configurez le port sur lequel AppScan recevra les demandes d'exploration manuelle envoyées depuis le périphérique distant ou le client externe. Vous pouvez laisser AppScan choisir automatiquement un port disponible.

   Conseil : Il est préférable que vous choisissiez le port vous-même car le port choisi automatiquement peut changer d'une session à l'autre. En revanche, ne sélectionnez pas de port si vous devez ouvrir plusieurs instances d'AppScan en même temps. Dans ce cas, configurez AppScan de sorte que le port soit choisi automatiquement.
2. **Enregistrer depuis :** Indiquez si vous enregistrerez depuis un client externe de la même machine qu'AppScan (par exemple, un simulateur ou un émulateur) ou depuis un périphérique distant (par exemple, un téléphone portable).
3. Configurez votre périphérique distant ou votre client externe de sorte qu'il utilise l'adresse IP et le port indiqués dans la sous-fenêtre d'informations.
4. **Je dois configurer des paramètres de connectivité supplémentaires :** Par défaut, AppScan utilise des paramètres de proxy Internet Explorer. Cochez cette case uniquement si vous souhaitez qu'AppScan utilise un autre proxy. Une étape supplémentaire s'ouvrira lorsque vous cliquerez sur le bouton Suivant.
5. Cliquez sur **Suivant** pour passer à l'étape suivante de l'assistant.

Que faire ensuite

«Certificat SSL», à la page 40

Si vous avez sélectionné "Je dois configurer des paramètres de connectivité supplémentaires", poursuivez l'opération avec «Paramètres de connexion»

Paramètres de connexion

(Facultatif :) Configurez les paramètres de proxy et, le cas échéant, l'authentification au niveau serveur.

Procédure

1. Sélectionnez l'une des trois options proxy :
   - **Utiliser les paramètres de proxy d'Internet Explorer :** (Par défaut) Lorsque cette option est sélectionnée, AppScan utilise l'adresse et le port de la connexion Internet Explorer lorsqu'il se connecte à l'application.
   - **Ne pas utiliser de proxy :** sélectionnez cette option si vous ne souhaitez pas qu'AppScan utilise des paramètres de proxy.
   - **Utiliser les paramètres de proxy personnalisés :** sélectionnez cette option si vous souhaitez utiliser une adresse et un port autres que ceux utilisés par Internet Explorer.
2. Si vous avez sélectionné l'une des options utilisant un proxy, vous pouvez éventuellement définir le nom d'utilisateur, le mot de passe et le domaine qu'utilisera AppScan lors de la connexion. Pour ce faire, cliquez sur le bouton **Configurer**.
3. Si votre plateforme requiert une authentification au niveau serveur, définissez le nom d'utilisateur, le mot de passe et le domaine dans la zone **Authentification HTTP**.
4. Cliquez sur **Suivant**.

Que faire ensuite

«Certificat SSL»

Certificat SSL

Si le serveur utilise HTTPS, vous devez ajouter le certificat racine SSL AppScan (afin que les demandes envoyées en utilisant AppScan comme proxy soient acceptées).

Procédure

1. Cliquez sur **Installer le certificat AppScan localement**, puis sur **Oui** dans la boîte de dialogue Windows qui apparaît pour effectuer la modification.

   Remarque : Lorsque le certificat est installé, le bouton est remplacé par un message de confirmation ; ce bouton n'apparaîtra plus la prochaine fois que vous utiliserez l'assistant (sauf si le certificat a été désinstallé).

   Remarque : Vous pouvez procéder à la désinstallation via **Outils > Options> Enregistrement du proxy** et cliquez sur **Supprimer**.
2. Si vous procédez à l'exploration à partir d'un périphérique distant (par exemple, un téléphone portable ou un émulateur), vous devez également installer le certificat sur ce périphérique :
   a. Sur le périphérique mobile, accédez au répertoire `http://appscan`
   b. Sur le périphérique, cliquez sur **Installer le certificat SSL AppScan**.

   Vous êtes prêt pour enregistrer la connexion à partir de votre périphérique, avec AppScan en tant que proxy d'enregistrement.
3. Cliquez sur **Suivant**.

Que faire ensuite

«Gestion de connexion»

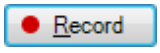
Gestion de connexion

Enregistrez la procédure de connexion.

Avant de commencer

L'icône de clé orange  indique que la connexion n'a pas encore été enregistrée.

Procédure

1. Sur votre périphérique, naviguez vers la page de connexion de l'application.
2. Dans AppScan, cliquez sur 

.
   L'enregistreur de connexion externe s'ouvre et indique qu'il est connecté à votre périphérique externe.
3. Sur votre périphérique, connectez-vous à l'application.
   Les demandes de connexion sont listées dans l'enregistreur de connexion externe.
4. Lorsque vous êtes connecté à l'application, cliquez sur **Arrêter l'enregistrement** (dans l'enregistreur de connexion externe).
5. (Facultatif) Recherchez dans la liste les demandes inutiles (par exemple, destinées à un domaine différent) et supprimez-les en les sélectionnant et en cliquant sur .
6. Cliquez sur **OK** pour fermer l'enregistreur.

L'icône de clé verte  indique que l'état En session a été détecté.

7. Si vous cochez la case **Je souhaite configurer les options de détection en session**, une étape supplémentaire de l'assistant, «Gestion de connexion - Détails», s'ouvre lorsque vous cliquez sur **Suivant**. Sélectionnez-la uniquement si vous devez éditer la séquence de connexion ou activer/désactiver la détection En session (voir la note de l'étape précédente).
8. Dans l'assistant, cliquez sur **Suivant**.

   Rubrique associée :

   «Enregistreur de connexion externe», à la page 151

Que faire ensuite

«Stratégie de test»

Si vous avez sélectionné "Je souhaite configurer les options de détection En session", poursuivez l'opération avec «Gestion de connexion - Détails», à la page 36

Gestion de connexion - Détails

(Facultatif :) Révisez et éditez la séquence de connexion que vous avez enregistrée.

Procédure

1. Révisez et éditez la séquence de connexion et assurez-vous que le schéma de détection de session est valide. Les options sont décrites dans «Onglet Vérifier et valider», à la page 55
2. Cliquez sur **Suivant**.

Que faire ensuite

«Stratégie de test»

Stratégie de test

Le fait de limiter l'examen aux types de test souhaités permet de réduire la durée de l'examen.

Pourquoi et quand exécuter cette tâche

Le nombre de tests envoyés par AppScan lors d'un examen peut atteindre plusieurs milliers. Il est parfois préférable de réduire la durée de l'examen en le limitant à certains types uniquement. C'est la stratégie de test.

AppScan est livré avec une stratégie de test par défaut, ainsi qu'avec certaines configurations de stratégie de test supplémentaires que vous pouvez sélectionner. Vous pouvez également utiliser vos propres stratégies de test définies par l'utilisateur.

L'étape Stratégie de test de l'assistant présente le nom de la stratégie de test sur laquelle est basée la stratégie en cours, ainsi que sa description.

Procédure

1. Vérifiez que la stratégie de test correspond à vos besoins. (Dans le doute, conservez la stratégie de test par défaut.)
2. Pour charger une autre stratégie de test, cliquez sur l'une des stratégies prédéfinies ou des stratégies récentes dans le panneau **Fichiers de stratégies**. Pour plus d'informations, voir «Vue Stratégie de test», à la page 109.

3. **Envoyer les tests sur les pages de connexion et de déconnexion :** par défaut, AppScan teste vos pages de connexion et de déconnexion ainsi que le reste de l'application. Vous devez conserver cette configuration par défaut, sauf si :
   - votre application dispose de mesures de sécurité qui verrouillent l'accès aux utilisateurs qui fournissent une entrée illégale à ces pages,
   - le flux de votre application risque d'être altéré par le test de ces pages.

   Si vous n'êtes pas sûr de la réponse de votre application à ces tests, gardez cette option sélectionnée.
4. **Ne pas envoyer d'identificateurs de session lors des tests des pages de connexion :** (Cette case à cocher est active, et sélectionnée par défaut, uniquement si la case précédente est sélectionnée.) Il est recommandé de laisser cette case cochée, car les identificateurs de session peuvent limiter la réussite des tests des pages de connexion. Désactivez cette option uniquement si vous êtes certain que des jetons de session valides sont nécessaires pour tester vos pages de connexion.

   Si vous n'êtes pas sûr de la réponse de votre application, gardez cette option sélectionnée.
5. Cliquez sur **Suivant**.

Que faire ensuite

«Complet»

Complet

AppScan est désormais configuré en tant que proxy d'enregistrement de sorte que votre périphérique puisse envoyer des demandes à l'application. Vous êtes maintenant prêt à lancer l'explorateur manuel de l'application.

Procédure

1. Cliquez sur **Fin**.

   L'enregistreur de trafic externe s'ouvre et affiche un message d'état indiquant qu'il est connecté à votre périphérique.
2. Lorsque l'enregistreur du trafic externe s'affiche à l'état "En attente des connexions entrantes", explorez manuellement le service Web à partir de votre périphérique/application :
   a. A l'aide de votre périphérique ou application, explorez le service Web.

      Au cours de l'exploration, les domaines détectés s'affichent dans la sous-fenêtre de gauche de l'enregistreur et les adresses URL dans la sous-fenêtre de droite.
   b. Ensuite, dans AppScan, cliquez sur **Arrêter l'enregistrement**.
3. Révisez et éditez les données d'exploration manuelle :

   Domaines détectés

   Tous les domaines auxquels des demandes ont été envoyées sont listés et sélectionnés par défaut pour être ajoutés à la liste des serveurs et domaines supplémentaires (Configuration > URL et serveurs > Serveurs et domaines supplémentaires) afin qu'il soient inclus dans l'examen. Désélectionnez ceux que vous ne voulez pas inclure dans l'examen.

   Conseil : Désélectionnez les domaines qui appartiennent à d'autres sociétés.

   Demandes envoyées

   Toutes les demandes envoyées par le périphérique à des domaines *sélectionnés* (dans la sous-fenêtre de gauche), sont listées. Si vous sélectionnez/désélectionnez des domaines dans la sous-fenêtre de gauche, la liste des demandes est mise à jour. Vous pouvez supprimer des demandes spécifiques si elles ne sont pas requises.

   Conseil : Si le nombre total de demandes filtrées dépasse 200, l'examen sera plus efficace si vous en supprimez certaines.

Remarque : A ce stade, vous pouvez cliquer sur **Exporter** pour enregistrer les données d'exploration à utiliser sur une autre machine.

4. Cliquez sur OK pour fermer l'enregistreur.

   AppScan met un certain temps à traiter et à afficher les données.

5. Pour démarrer l'étape de test, cliquez sur **Examen > Test uniquement**.

   L'étape de test commence et les résultats de l'examen s'affichent une fois celle-ci terminée.

   Rubriques connexes :

   •
   • «Onglet Enregistrement du proxy», à la page 261
   • Chapitre 8, «Résultats : Problèmes de sécurité», à la page 207

Assistant pour exploration avec GSC

Répertorie les étapes de cet assistant.

1. «Adresses URL et serveurs»
2. (Facultatif :) «Paramètres de connexion», à la page 44
3. «Stratégie de test», à la page 44
4. «Complet», à la page 45

Adresses URL et serveurs

Indiquez l'URL du fichier WSDL du service et définissez des serveurs et domaines supplémentaires à inclure dans l'examen.

Procédure

1. **URL WSDL :** saisissez l'URL du fichier WSDL pour le service.

   Exemple : `http://www.sitetoscan.com/Service1.asmx?wsdl`

2. Pour vérifier que vous avez correctement entré l'URL, vous pouvez la visualiser dans le navigateur AppScan :

   a. Cliquez sur  (Activée uniquement lorsque vous avez entré l'adresse URL dans la zone de saisie.) Le navigateur intégré s'ouvre à l'adresse URL entrée.
   b. Si nécessaire, corrigez l'URL.
   c. Fermez le navigateur pour poursuivre la configuration de l'examen.

3. **Chemin d'accès sensible à la casse :** Lorsque cette case est cochée (par défaut), les liens présentant des casses différentes sont traités comme des pages distinctes. Par exemple, "ReadMe.as" serait considéré comme différent de "readme.as". Dans la plupart des cas, vous devez cocher la case pour les serveurs Unix et la désélectionner pour les serveurs Windows.

4. **Serveurs et domaines supplémentaires :** si votre application inclut des serveurs ou des domaines autres que ceux de l'URL de départ, *et que votre licence AppScan les inclut*, vous devez les ajouter ici pour qu'ils soient inclus à l'examen :

   a. Cliquez sur  pour ouvrir la boîte de dialogue d'*ajout de serveurs et de domaines*.
   b. Entrez le nom d'hôte et l'adresse IP du serveur, ou le nom de domaine (par exemple, sitetoscan.com), puis cliquez sur **OK**

   Le nouvel élément est ajouté à la liste.

5. **Je dois configurer des paramètres de connectivité supplémentaires :** Par défaut, AppScan utilise des paramètres de proxy Internet Explorer. Cochez cette case uniquement si vous souhaitez qu'AppScan utilise un autre proxy. Une étape supplémentaire s'ouvrira lorsque vous cliquerez sur le bouton Suivant.

6. Cliquez sur **Suivant** pour passer à l'étape suivante de l'assistant.

Que faire ensuite

«Stratégie de test»

ou si vous avez coché la case **Je souhaite configurer...** :

«Paramètres de connexion»

Paramètres de connexion

(Facultatif :) Configurez les paramètres de proxy et, le cas échéant, l'authentification au niveau serveur.

Pourquoi et quand exécuter cette tâche

Par défaut, AppScan utilise des paramètres de proxy Internet Explorer. La boîte de dialogue supplémentaire URL et serveurs permet de configurer AppScan pour utiliser d'autres paramètres de proxy, ou ne pas en utiliser du tout.

Procédure

1. Sélectionnez l'une des trois options proxy :
   - **Utiliser les paramètres de proxy d'Internet Explorer :** (Par défaut) Lorsque cette option est sélectionnée, AppScan utilise l'adresse et le port de la connexion Internet Explorer lorsqu'il se connecte à l'application.
   - **Ne pas utiliser de proxy :** sélectionnez cette option si vous ne souhaitez pas qu'AppScan utilise des paramètres de proxy.
   - **Utiliser les paramètres de proxy personnalisés :** sélectionnez cette option si vous souhaitez utiliser une adresse et un port autres que ceux utilisés par Internet Explorer.
2. Si vous avez sélectionné l'une des options utilisant un proxy, vous pouvez éventuellement définir le nom d'utilisateur, le mot de passe et le domaine qu'utilisera AppScan lors de la connexion. Pour ce faire, cliquez sur le bouton **Configurer**.
3. Si votre plateforme requiert une authentification au niveau serveur, définissez le nom d'utilisateur, le mot de passe et le domaine dans la zone **Authentification HTTP**.
4. Cliquez sur **Suivant** pour passer à l'étape Paramètres de la stratégie de test.

Que faire ensuite

«Stratégie de test»

Stratégie de test

Définissez les types de test qui seront envoyés par AppScan au service une fois votre exploration manuelle terminée.

Procédure

1. Dans la boîte de dialogue **Assistant de configuration des examens WSDL > Authentification de la plateforme**, cliquez sur **Suivant**.

   L'**étape Stratégie de test WSDL** de l'assistant apparaît (identique à «Stratégie de test», à la page 36).
2. Vérifiez que la stratégie de test correspond à vos besoins. (Sauf si vous avez défini une stratégie personnalisée, la stratégie de test des services web est recommandée.)
   - Pour charger une autre stratégie de test, cliquez sur **Charger**.

     La boîte de dialogue **Charger une stratégie de test** s'ouvre, vous permettant de sélectionner l'une des stratégies prédéfinies ou définies par l'utilisateur.
   - Pour éditer la stratégie de test en cours, cliquez sur **Editer**.

     Le **Gestionnaire de stratégies de test** s'ouvre, vous permettant de configurer exactement les tests qui sont inclus à l'examen.

Pour plus de détails, voir «Importer une stratégie de test», à la page 111.

3. Si nécessaire, vous pouvez cliquer sur le bouton Paramètres de test **avancés** pour configurer des options supplémentaires. Pour plus d'informations, voir «Importer une stratégie de test», à la page 111. Sinon, cliquez sur **Suivant** pour procéder à l'étape finale de l'assistant.

Que faire ensuite

{ 1 > < 1 } { { 1 > < 1 } 1 { 1 > < 1 } > { 1 > < 1 } < { 1 > < 1 } 1 { 1 > < 1 } } { 1 > < 1 } { { 1 > < 1 } { { 1 >
< 1 } 1 { 1 > < 1 } > { 1 > < 1 } < { 1 > < 1 } 1 { 1 > < 1 } } { 1 > < 1 } 1 { 1 > < 1 } { { 1 > < 1 } 1 { 1 > < 1 }
> { 1 > < 1 } < { 1 > < 1 } 1 { 1 > < 1 } } { 1 > < 1 } > { 1 > < 1 } { { 1 > < 1 } 1 { 1 > < 1 } > { 1 > < 1 } < { 1
> < 1 } 1 { 1 > < 1 } } { 1 > < 1 } < { 1 > < 1 } { { 1 > < 1 } 1 { 1 > < 1 } > { 1 > < 1 } < { 1 > < 1 } 1 { 1 > <
1 } } { 1 > < 1 } 1 { 1 > < 1 } { { 1 > < 1 } 1 { 1 > < 1 } > { 1 > < 1 } < { 1 > < 1 } 1 { 1 > < 1 } } { 1 > < 1 } } {
1 > < 1 } { { 1 > < 1 } 1 { 1 > < 1 } > { 1 > < 1 } < { 1 > < 1 } 1 { 1 > < 1 } } { 1 > < 1 } { { 1 > < 1 } { { 1 > <
1 } 1 { 1 > < 1 } > { 1 > < 1 } < { 1 > < 1 } 1 { 1 > < 1 } } { 1 > < 1 } { { 1 > < 1 } { { 1 > < 1 } 1 { 1 > < 1 } >
{ 1 > < 1 } < { 1 > < 1 } 1 { 1 > < 1 } } { 1 > < 1 } 1 { 1 > < 1 } { { 1 > < 1 } 1 { 1 > < 1 } > { 1 > < 1 } < { 1 >
< 1 } 1 { 1 > < 1 } } { 1 > < 1 } > { 1 > < 1 } { { 1 > < 1 } 1 { 1 > < 1 } > { 1 > < 1 } < { 1 > < 1 } 1 { 1 > < 1 }
} { 1 > < 1 } < { 1 > < 1 } { { 1 > < 1 } 1 { 1 > < 1 } > { 1 > < 1 } < { 1 > < 1 } 1 { 1 > < 1 } } { 1 > < 1 } 1 { 1
> < 1 } { { 1 > < 1 } 1 { 1 > < 1 } > { 1 > < 1 } < { 1 > < 1 } 1 { 1 > < 1 } } { 1 > < 1 } } { 1 > < 1 } { { 1 > < 1
} 1 { 1 > < 1 } > { 1 > < 1 } < { 1 > < 1 } 1 { 1 > < 1 } } { 1 > < 1 } 1 { 1 > < 1 } { { 1 > < 1 } 1 { 1 > < 1 } > {
1 > < 1 } < { 1 > < 1 } 1 { 1 > < 1 } } { 1 > < 1 } { { 1 > < 1 } { { 1 > < 1 } 1 { 1 > < 1 } > { 1 > < 1 } < { 1 > <
1 } 1 { 1 > < 1 } } { 1 > < 1 } 1 { 1 > < 1 } { { 1 > < 1 } 1 { 1 > < 1 } > { 1 > < 1 } < { 1 > < 1 } 1 { 1 > < 1 } }
{ 1 > < 1 } > { 1 > < 1 } { { 1 > < 1 } 1 { 1 > < 1 } > { 1 > < 1 } < { 1 > < 1 } 1 { 1 > < 1 } } { 1 > < 1 } < { 1 >
< 1 } { { 1 > < 1 } 1 { 1 > < 1 } > { 1 > < 1 } < { 1 > < 1 } 1 { 1 > < 1 } } { 1 > < 1 } 1 { 1 > < 1 } { { 1 > < 1 }
1 { 1 > < 1 } > { 1 > < 1 } < { 1 > < 1 } 1 { 1 > < 1 } } { 1 > < 1 } } { 1 > < 1 } { { 1 > < 1 } 1 { 1 > < 1 } > { 1
> < 1 } < { 1 > < 1 } 1 { 1 > < 1 } } { 1 > < 1 } > { 1 > < 1 } { { 1 > < 1 } 1 { 1 > < 1 } > { 1 > < 1 } < { 1 > <
1 } 1 { 1 > < 1 } } { 1 > < 1 } { { 1 > < 1 } { { 1 > < 1 } 1 { 1 > < 1 } > { 1 > < 1 } < { 1 > < 1 } 1 { 1 > < 1 } } {
1 > < 1 } 1 { 1 > < 1 } { { 1 > < 1 } 1 { 1 > < 1 } > { 1 > < 1 } < { 1 > < 1 } 1 { 1 > < 1 } } { 1 > < 1 } > { 1 >
< 1 } { { 1 > < 1 } 1 { 1 > < 1 } > { 1 > < 1 } < { 1 > < 1 } 1 { 1 > < 1 } } { 1 > < 1 } < { 1 > < 1 } { { 1 > < 1 }
1 { 1 > < 1 } > { 1 > < 1 } < { 1 > < 1 } 1 { 1 > < 1 } } { 1 > < 1 } 1 { 1 > < 1 } { { 1 > < 1 } 1 { 1 > < 1 } > { 1
> < 1 } < { 1 > < 1 } 1 { 1 > < 1 } } { 1 > < 1 } } { 1 > < 1 } { { 1 > < 1 } 1 { 1 > < 1 } > { 1 > < 1 } < { 1 > < 1
} 1 { 1 > < 1 } } { 1 > < 1 } < { 1 > < 1 } { { 1 > < 1 } 1 { 1 > < 1 } > { 1 > < 1 } < { 1 > < 1 } 1 { 1 > < 1 } } {
1 > < 1 } { { 1 > < 1 } { { 1 > < 1 } 1 { 1 > < 1 } > { 1 > < 1 } < { 1 > < 1 } 1 { 1 > < 1 } } { 1 > < 1 } 1 { 1 > <
1 } { { 1 > < 1 } 1 { 1 > < 1 } > { 1 > < 1 } < { 1 > < 1 } 1 { 1 > < 1 } } { 1 > < 1 } > { 1 > < 1 } { { 1 > < 1 } 1
{ 1 > < 1 } > { 1 > < 1 } < { 1 > < 1 } 1 { 1 > < 1 } } { 1 > < 1 } < { 1 > < 1 } { { 1 > < 1 } 1 { 1 > < 1 } > { 1 >
< 1 } < { 1 > < 1 } 1 { 1 > < 1 } } { 1 > < 1 } 1 { 1 > < 1 } { { 1 > < 1 } 1 { 1 > < 1 } > { 1 > < 1 } < { 1 > < 1 }
1 { 1 > < 1 } } { 1 > < 1 } } { 1 > < 1 } { { 1 > < 1 } 1 { 1 > < 1 } > { 1 > < 1 } < { 1 > < 1 } 1 { 1 > < 1 } } { 1
> < 1 } 1 { 1 > < 1 } { { 1 > < 1 } 1 { 1 > < 1 } > { 1 > < 1 } < { 1 > < 1 } 1 { 1 > < 1 } } { 1 > < 1 } { { 1 > < 1
} { { 1 > < 1 } 1 { 1 > < 1 } > { 1 > < 1 } < { 1 > < 1 } 1 { 1 > < 1 } } { 1 > < 1 } 1 { 1 > < 1 } { { 1 > < 1 } 1 {
1 > < 1 } > { 1 > < 1 } < { 1 > < 1 } 1 { 1 > < 1 } } { 1 > < 1 } > { 1 > < 1 } { { 1 > < 1 } 1 { 1 > < 1 } > { 1 >
< 1 } < { 1 > < 1 } 1 { 1 > < 1 } } { 1 > < 1 } < { 1 > < 1 } { { 1 > < 1 } 1 { 1 > < 1 } > { 1 > < 1 } < { 1 > < 1 }
1 { 1 > < 1 } } { 1 > < 1 } 1 { 1 > < 1 } { { 1 > < 1 } 1 { 1 > < 1 } > { 1 > < 1 } < { 1 > < 1 } 1 { 1 > < 1 } } { 1
> < 1 } } { 1 > < 1 } { { 1 > < 1 } 1 { 1 > < 1 } > { 1 > < 1 } < { 1 > < 1 } 1 { 1 > < 1 } } { 1 > < 1 } } { 1 > < 1
} { { 1 > < 1 } 1 { 1 > < 1 } > { 1 > < 1 } < { 1 > < 1 } 1 { 1 > < 1 } } { 1 > < 1 } { { 1 > < 1 } { { 1 > < 1 } 1 { 1
> < 1 } > { 1 > < 1 } < { 1 > < 1 } 1 { 1 > < 1 } } { 1 > < 1 } 1 { 1 > < 1 } { { 1 > < 1 } 1 { 1 > < 1 } > { 1 > <
1 } < { 1 > < 1 } 1 { 1 > < 1 } } { 1 > < 1 } > { 1 > < 1 } { { 1 > < 1 } 1 { 1 > < 1 } > { 1 > < 1 } < { 1 > < 1 } 1
{ 1 > < 1 } } { 1 > < 1 } < { 1 > < 1 } { { 1 > < 1 } 1 { 1 > < 1 } > { 1 > < 1 } < { 1 > < 1 } 1 { 1 > < 1 } } { 1 >
< 1 } 1 { 1 > < 1 } { { 1 > < 1 } 1 { 1 > < 1 } > { 1 > < 1 } < { 1 > < 1 } 1 { 1 > < 1 } } { 1 > < 1 } } { 1 > < 1 }
{ { 1 > < 1 } 1 { 1 > < 1 } > { 1 > < 1 } < { 1 > < 1 } 1 { 1 > < 1 } } { 1 > < 1 }

Complet

Vous êtes maintenant prêt à lancer manuellement l'exploration du service à l'aide de GSC.

Procédure

Cliquez sur **Terminer**.
Une invite vous informant que GSC (Generic Service Client) est sur le point de s'ouvrir s'affiche (si c'est le cas, cliquez sur **OK**), puis le programme s'ouvre.

Que faire ensuite

«Utilisation de GSC», à la page 153

Boîte de dialogue Configuration des examens

Pourquoi et quand exécuter cette tâche

La boîte de dialogue Configuration des examens fournit diverses options permettant de configurer vos examens. Les options principales sont également disponibles via l'assistant de Configuration des examens, mais l'utilisation de la boîte de dialogue est recommandée lorsque vous souhaitez modifier la plupart des paramètres par défaut ou lorsque vous souhaitez régler une configuration existante.

Procédure

Pour ouvrir la boîte de dialogue Configuration des examens, cliquez sur l'icône **Configuration**  sur la barre d'outils (ou appuyez sur **F10**).
La boîte de dialogue Configuration des examens contient différentes vues, divisées en quatre groupes, qui sont accessibles en cliquant sur l'élément approprié dans le panneau de sélection de la vue, sur le côté gauche.

Remarque : Si vous arrêtez un examen et modifiez la configuration, les modifications n'affecteront pas les demandes déjà envoyées. Pour appliquer les modifications à tout l'examen, vous devez démarrer un nouvel examen.

Conseil : Vous pouvez modifier les options de configuration dans plusieurs vues, puis cliquer sur OK pour sauvegarder toutes les modifications. (Vos modifications sont conservées lorsque vous naviguez entre les vues, mais sont uniquement sauvegardées lorsque vous cliquez sur OK.)

Afficher	**Sélectionner pour configurer :**
Explorer	
«Vue URL et serveurs», à la page 47	URL de départ, type de système et serveurs supplémentaires
«Vue Gestion de connexion», à la page 51	Définir la méthode de connexion, enregistrer une séquence de connexion (facultatif) et configurer la détection En session
«Vue Définition de l'environnement», à la page 64	Fournir des informations sur l'environnement d'application
«Vue Exclusion de chemins et de fichiers», à la page 65	Chemins d'accès et types de fichier à exclure de l'examen
«Vue Options d'exploration», à la page 71	Limites de l'examen, méthodes d'extraction des liens et méthode d'exploration générale
«Vue Paramètres et cookies», à la page 76	Identifier les ID session et répertorier les paramètres à exclure de l'examen

Afficher	Sélectionner pour configurer :
«Vue Remplissage automatique de formulaires», à la page 90	Fournir à AppScan des valeurs de paramètre valides pour le remplissage des formulaires
«Vue Pages d'erreur», à la page 93	Ajouter des chaînes, des expressions régulières et des URL pour identifier des pages d'erreur personnalisées
«Vue Opérations en plusieurs étapes», à la page 95	Enregistrer et gérer des opérations en plusieurs étapes requises pour atteindre des parties de l'application
«Vue Résultats basés sur le contenu», à la page 103	Pour des applications sans structure d'URL hiérarchique, telles que des applications de point d'entrée unique, définir comment AppScan organise l'arborescence du site.
«Vue Glass box», à la page 105	Si l'agent glass box d'AppScan est installé sur votre serveur d'applications, configurez l'examen glass box ici.
Connexion	
«Vue Communication et Proxy», à la page 107	Configurer les paramètres de délai d'attente de communication et de serveur proxy
«Vue Authentification HTTP» , à la page 107	Ajouter une authentification de niveau serveur et des certificats côté client, si cela est requis par l'application
Test	
«Vue Stratégie de test», à la page 109	Définir et éditer la stratégie de test (quels tests sont envoyés à l'application)
«Vue Optimisation du test», à la page 113	Appliquez Optimisation de test dans le cycle de vie du produit lorsque vous accordez plus d'importance à la rapidité de l'examen qu'à sa profondeur.
«Vue Options de test», à la page 114	Options supplémentaires de test
«Vue Escalade des droits d'accès», à la page 117	AppScan peut faire référence à des exécutions d'examens à l'aide de droits utilisateur différents afin de reconnaître les ressources privilégiées accessibles aux utilisateurs dont les droits d'accès sont insuffisants.
«Vue Logiciels malveillants», à la page 118	Test des liens malveillants.
Général	
«Vue Scan Expert», à la page 118	Configurer le comportement et les modules Scan Expert
«Vue Configuration avancée» , à la page 120	Configurer les options d'examen avancées

Vue URL et serveurs

Vue URL et serveurs de la boîte de dialogue Configuration des examens.

Vous *devez* définir l'URL à partir de laquelle l'examen doit être démarré. Les autres paramètres sont facultatifs.

Paramètre	Détails
Adresse URL de départ	Spécifiez l'URL de votre application comme point de départ de l'examen. AppScan tente d'atteindre l'URL et en cas de succès, une coche de couleur verte et le message de confirmation "Connecté au serveur" apparaît sous l'URL de départ. Si le problème peut être corrigé en modifiant la configuration, AppScan suggère la modification nécessaire et établit un lien à la vue appropriée dans la boîte de dialogue de configuration.  ouvre la page que vous venez d'entrer dans un navigateur. Si nécessaire, vous pouvez accéder à une autre URL et utiliser la barre d'outils pour définir la nouvelle page comme URL de départ pour l'examen. Fermez le navigateur pour poursuivre la configuration de l'examen. **Remarque :** Le navigateur par défaut est utilisé. Vous pouvez sélectionner le navigateur par défaut comme étant soit l'un des deux navigateurs intégrés (IE ou Chromium), soit un navigateur externe pris en charge, dans Outils > Options > Onglet Préférences  Teste une nouvelle fois l'URL de départ. Cliquez sur ce bouton si le serveur était arrêté lors de la configuration et qu'il a repris ultérieurement. **Conseil :** Si vous modifiez le domaine, le schéma ou le port de l'URL de départ *après la configuration de l'examen*, il peut être nécessaire de modifier la configuration. Le système vous demandera si vous souhaitez qu'AppScan tente d'effectuer cette opération automatiquement. Pour plus de détails, voir «Modification de l'hôte de l'URL de départ», à la page 50
Examiner uniquement les liens dans et sous ce répertoire.	Lorsque cette option est sélectionnée, l'examen se limite aux pages situées sous l'URL de départ. Les liens aux autres URL ne seront pas analysés, même s'ils sont inclus dans la liste des Serveurs et domaines supplémentaires (ci-dessous). Pour plus de détails, voir «Limitation d'un examen au dossier de l'URL de départ»
Traiter tous les chemins d'accès comme sensibles à la casse	Lorsque cette option est sélectionnée, les liens qui diffèrent les uns des autres sont considérés comme des pages différentes. Par exemple, "ReadMe.as" serait considéré comme différent de "readme.as". Lorsqu'elle est désélectionnée, toutes les URL apparaissent en minuscules. Cochez cette case si le système de fichiers de votre hôte d'applications est sensible à la casse. Dans la plupart des cas, vous pouvez cocher la case pour les serveurs basés sur Unix et décocher la case pour les serveurs basés sur Windows.
Serveurs et domaines supplémentaires	Si votre application inclut des liens vers des domaines autres que le domaine de l'URL de départ, vous devez les ajouter pour qu'ils soient inclus dans l'examen. **Remarque :** Vous pouvez uniquement ajouter les serveurs ou domaines inclus dans votre licence AppScan. Pour plus de détails, voir «Serveurs et domaines supplémentaires», à la page 50

Limitation d'un examen au dossier de l'URL de départ

Vous pouvez aisément limiter un examen au dossier de l'URL de départ et à ses dossiers enfant.

Pourquoi et quand exécuter cette tâche

La case à cocher sous la zone de l'URL de départ crée les filtres nécessaires pour limiter votre examen à un répertoire particulier et à ses répertoires enfant.

Procédure

1. Sélectionnez **Configuration des examens > URL et Serveurs**.
2. Tapez ou collez l'URL du répertoire auquel vous voulez limiter l'examen.
3. Cochez la case **Examiner uniquement les liens dans ce répertoire et ses sous-répertoires** .

   Cet examen sera ainsi limité aux chemins sous cette adresse URL. Les liens situés hors de cette plage ne seront pas examinés.

Exemple

Si l'URL de départ définie est `http://main/bank/`

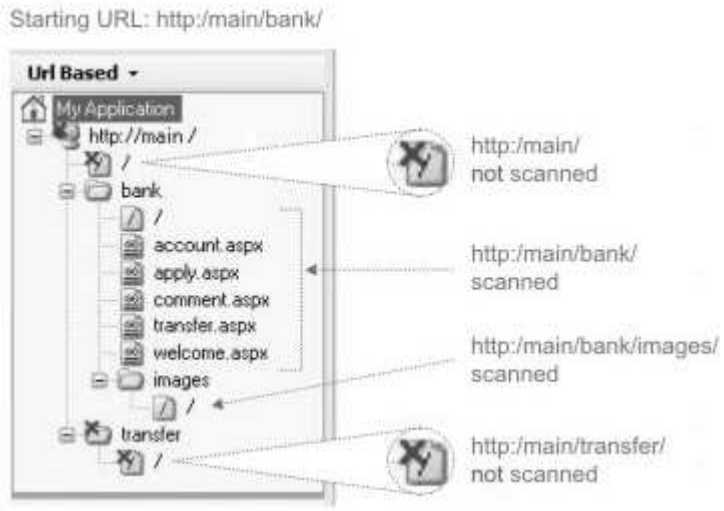
- Les liens vers les adresses suivantes seront examinés :
  - `http://main/bank/transfer.aspx/`
  - `http://main/bank/transfer/page_1.aspx/`
- Les liens vers les adresses suivantes seront ignorés :
  - `http://main/transfer.aspx/`
  - `http://main/transfer/page_1.aspx/`

Lorsque vous configurez l'adresse URL de départ et sélectionnez cette case à cocher, les deux éléments suivants sont ajoutés en haut de la table Exclusion de chemins et de fichiers (Configuration des examens > Exclusion de chemins et de fichiers) :

Type d'élément	Chemin d'accès	Correspondance	Comportement
Exclure (URL de départ)	.*	Expression régulière	Toujours en première position dans la table. Ne peut pas être rétrogradé. Ne peut pas être modifié ou supprimé. Cependant, si l'élément suivant (Exception) est supprimé, celui-ci l'est également.
Exception (URL de départ)	http://main/bank	Chemin d'accès complet	Toujours en deuxième position dans la table. Ne peut pas être remonté ni rétrogradé. *Peut* être modifié. (Ceci permet de modifier l'exception dans les rares cas où AppScan ne parvient pas à identifier le répertoire de l'URL de départ.) Si cet élément est supprimé, l'élément précédent (Exclure) l'est également et la case à cocher URL de départ est désélectionnée.

Remarque : A la différence d'autres exclusions et exceptions, ces éléments s'affichent sur fond gris, ce qui indique leur statut spécial.

Lorsque l'examen commence et que l'Arborescence de l'application s'affiche dans la sous-fenêtre de gauche, les liens vers les parties de l'application qui se trouvent maintenant sous l'URL de départ sont marqués d'une croix (X) rouge indiquant qu'ils n'ont pas été examinés.



Que faire ensuite

Vous pouvez vérifier que l'exception ajoutée est correcte, ou la modifier dans la vue **Exclure des chemins d'accès et des fichiers** (voir «Limitation d'un examen à un dossier spécifique», à la page 69).

Serveurs et domaines supplémentaires

Vous pouvez inclure des domaines autres que celui de l'URL de départ de l'examen.

Pourquoi et quand exécuter cette tâche

Si votre application inclut des liens vers des domaines autres que le domaine de l'URL de départ, vous devez les ajouter pour qu'AppScan les inclue dans l'examen.

Remarque : Vous pouvez uniquement ajouter les serveurs ou domaines inclus dans votre licence AppScan.

Procédure

- Pour ajouter un serveur, cliquez sur  et entrez le nom de serveur/domaine.
  Exemple : `demo.testfire.net` ou `65.61.137.117`
  Le serveur est ajouté à la liste.
- Pour éditer un serveur dans la liste, sélectionnez-le et cliquez sur  .
- Pour supprimer un serveur de la liste, sélectionnez-le et cliquez sur  .

Modification de l'hôte de l'URL de départ

Vous pouvez modifier l'hôte, le schéma ou le port dans l'URL de départ d'un examen configuré sans réenregistrer la procédure de connexion, les opérations en plusieurs étapes ou les données d'exploration manuelle.

Pourquoi et quand exécuter cette tâche

Si vous avez déjà enregistré une procédure de connexion, des opérations en plusieurs étapes et/ou une exploration manuelle et que l'hôte, le schéma ou le port de l'URL de départ est modifié, les demandes et les réponses de ces enregistrements doivent être mises à jour et vérifiées. Cliquez sur **Examiner >**

Modifier hôte/schéma/port pour ouvrir une boîte de dialogue dans laquelle vous pouvez modifier l'URL et demander à AppScan de mettre à jour, de vérifier et de confirmer automatiquement les modifications nécessaires.

La boîte de dialogue affiche les étapes en cours d'exécution et indique quand chaque étape aboutit. Si la procédure de mise à jour échoue, la boîte de dialogue vous indique quelle étape a échoué et vous permet de sauvegarder les modifications et de continuer la procédure manuellement ou d'annuler toutes les modifications.

Important : Dans certains cas, il est possible qu'AppScan ne mette pas à jour les réponses correctement et que ce dysfonctionnement entraîne l'échec partiel ou total de l'examen. Dans ce cas, vous devez réenregistrer les procédures qui posent problème.

Remarque : Bien que les données d'exploration *manuelle* soient mises à jour, les données d'exploration *automatique* et les résultats de l'examen sont supprimés lorsque vous modifiez l'URL de départ.

Remarque : Cette option peut être utilisée pour modifier *uniquement* l'hôte, le schéma ou le port de l'URL de départ. Si vous devez apporter *d'autres* modifications à l'URL de départ ou modifier l'hôte, le schéma ou le port pour l'un des domaines *supplémentaires* dans l'examen, vous ne pouvez pas utiliser cette option. A la place, sauvegardez l'examen en tant que modèle et utilisez le modèle pour créer un examen.

Procédure

1. Ouvrez le fichier d'examen (.scan) ou le fichier du modèle d'examen (.scant), puis effectuez les opérations suivantes :
   - **Pour un modèle d'examen :** dans la barre d'outils, cliquez sur **Configuration des examens > URL et serveurs**.
   - **Pour un examen configuré :** dans la barre de menus, cliquez sur **Examiner > Modifier hôte/schéma/port**.
2. Modifiez l'hôte, le schéma ou le port de l'URL de départ en fonction de vos besoins.

   AppScan tente de se connecter au serveur et une coche verte signale que cette procédure a abouti.
3. Cliquez sur **OK**.

   AppScan tente de mettre à jour la configuration et une coche verte signale que chaque étape a abouti.
4. **Si toutes les étapes aboutissent :** Cliquez sur **OK** pour sauvegarder les modifications de configuration.

   Si l'une des étapes échoue :
   - Pour sauvegarder les modifications de configuration, exécutez manuellement les étapes qui ont échoué, faites une nouvelle tentative et cliquez sur **OK**.
   - Pour annuler toutes les modifications et rétablir l'URL de départ d'origine, cliquez sur**Annuler**.

   Important : Dans certains cas, il est possible qu'AppScan ne mette pas à jour les réponses correctement et que ce dysfonctionnement entraîne l'échec partiel ou total de l'examen. Dans ce cas, vous devez réenregistrer les procédures qui posent problème.

Vue Gestion de connexion

Vue Gestion de connexion de la boîte de dialogue Configuration des examens.

La vue **Gestion de connexion** de la boîte de dialogue **Configuration des examens** permet de définir la manière dont AppScan se connecte à votre application, et la manière dont il reconnaît qu'il a été déconnecté.

AppScan peut automatiquement détecter des demandes de connexion et remplir les paramètres de nom d'utilisateur et de mot de passe. Si votre application a une séquence d'actions de connexion non standard, vous pouvez enregistrer ces actions pour qu'AppScan les utilise.

La vue Gestion de connexion comporte ces onglets :

- Connexion
- Vérifier et valider
- ID session
- Avancé

Onglet Connexion

Configuration des examens > Gestion de connexion > onglet Connexion.

La vue **Gestion de connexion** de la boîte de dialogue **Configuration des examens** permet de définir la manière dont AppScan se connecte à votre application, et la manière dont il peut reconnaître qu'il a été déconnecté.

AppScan peut automatiquement détecter des demandes de connexion et remplir les paramètres de nom d'utilisateur et de mot de passe. Si votre application a une séquence d'actions de connexion non standard, vous pouvez enregistrer ces actions pour qu'AppScan les utilise.

Paramètre	**Détails**
Sélectionner la méthode de connexion	
Enregistrée (recommandé)	(Méthode par défaut) Sélectionnez cette méthode pour ouvrir le navigateur et enregistrer une séquence de connexion (les demandes HTTP et les actions de l'utilisateur sont enregistrées). AppScan utilise cette séquence chaque fois qu'il doit se connecter à l'application.  permet d'enregistrer la séquence. Pour les applications Web, voir «Enregistrement d'une connexion», à la page 53. Pour RESTful (et d'autres services Web), voir «Exploration à l'aide de l'enregistreur du trafic externe», à la page 150
Connexion automatique	Sélectionnez cette méthode pour qu'AppScan puisse détecter automatiquement le formulaire de connexion de votre application et utiliser le nom d'utilisateur et le mot de passe que vous avez fournis. (Cette méthode peut être moins fiable que la méthode Connexion enregistrée.)
Invite	Sélectionnez cette méthode si la connexion nécessite à chaque fois l'intervention d'un utilisateur (comme l'authentification à deux facteurs, les mots de passe à usage unique ou CAPCHA). Notez que même si vous sélectionnez cette option, **vous devez enregistrer une séquence de connexion**. Ceci, afin de fournir à AppScan une page en-session pouvant être ensuite utilisée pour vérifier qu'il est connecté. Pour plus de détails, voir «Enregistrement d'une connexion», à la page 53
Aucun	Sélectionnez cette option si l'application ne nécessite pas que les utilisateurs se connectent.
Indicateur du statut de validation de la connexion	

Paramètre	Détails
Icône Clé	L'icône Clé indique l'état de la Détection En session :  Activée et configurée. (Une page En session a été identifiée dans la séquence de connexion, automatiquement ou par l'utilisateur.)  Activée, mais pas totalement configurée.  Activée, mais pas configurée.  Désactivée. Pour plus de détails, voir «Boîte de dialogue Sélectionner un schéma de détection», à la page 61.
Importer ou exporter des paramètres de connexion	
Importer	Lorsque vous enregistrez une séquence de connexion, celle-ci est sauvegardée dans le cadre de l'examen. Si vous enregistrez l'examen comme modèle, la séquence de connexion est sauvegardée en tant que partie du modèle. Pour importer une séquence de connexion qui a été précédemment enregistrée comme fichier `*.login`, cliquez sur le bouton **Importer**.
Exporter	Pour exporter la séquence de connexion à part, pour l'utiliser lors d'examens futurs, cliquez sur le bouton **Exporter**. La séquence est enregistrée sous format `*.login`.

Enregistrement d'une connexion :
Avant de commencer

Avant de pouvoir enregistrer une séquence de connexion, l'URL de départ doit être définie (dans la vue Configuration > URL et serveurs ou dans l'assistant).

Pourquoi et quand exécuter cette tâche

La connexion enregistrée permet d'indiquer à AppScan la procédure de connexion à votre site : sur quels liens cliquer, quel texte entrer dans les formulaires et l'ordre dans lequel effectuer ces opérations. Dès que vous avez terminé l'enregistrement, AppScan tente d'identifier un schéma En session pouvant servir ultérieurement pour vérifier sa connexion. Ensuite, AppScan peut utiliser la séquence de connexion pour se reconnecter pendant l'examen, chaque fois qu'il détecte qu'il a été déconnecté.

AppScan doit savoir, à tout moment, s'il est connecté ou déconnecté du site afin de pouvoir évaluer correctement les réponses du site. Lors de l'examen, AppScan envoie la demande de détection En session de façon répétitive et vérifie que la réponse contient le schéma de détection En session afin de vérifier qu'il est toujours connecté. Si AppScan ne trouve pas le schéma dans la réponse de la page, AppScan suppose qu'il a été déconnecté et tente de se reconnecter en rejouant la séquence de connexion. La séquence de connexion est, en général, exécutée plusieurs fois pendant l'examen. Il est donc préférable qu'elle contienne un nombre d'étapes aussi réduit que possible. Il est également utile que la page En session soit de petite taille et qu'elle ne contienne pas de paramètres suivis ou de cookies, car ces derniers peuvent prolonger considérablement la durée de l'examen.

Procédure

1. Dans l'onglet **Configuration des examens > Gestion de connexion > Connexion**, sélectionnez **Enregistré**.
2. Cliquez sur 

> Utiliser le navigateur AppScan IE.
   Le navigateur ouvre l'URL de départ et commence à enregistrer vos actions.

   Remarque : Si la connexion à votre site Web ne prend pas en charge Internet Explorer, cliquez sur > **Utiliser le navigateur Chromium d'AppScan** à la place.

   Remarque : Si l'URL de départ n'a pas encore été définie, vous êtes invité à le faire avant de pouvoir poursuivre (voir «Vue URL et serveurs», à la page 47).

   Remarque : Si une procédure de connexion a précédemment été enregistrée, vous êtes averti que le nouvel enregistrement écrasera l'existant.

   Remarque : Si vous avez configuré AppScan de sorte qu'il utilise un navigateur externe pour les examens (Outils > Options > Utiliser le navigateur externe > Sélectionner un navigateur), vous avez la possibilité d'enregistrer la connexion avec le navigateur d'AppScan ou le navigateur externe. Dans la mesure du possible, nous recommandons d'utiliser le navigateur d'AppScan pour l'enregistrement de la connexion (même si un autre navigateur est utilisé pour les examens), car il permet d'enregistrer des informations supplémentaires qui favorisent le succès des connexions lors des examens. Si l'enregistrement de la connexion avec le navigateur d'AppScan ne fonctionne pas pour votre application, utilisez le navigateur externe.

   Remarque : Si votre application ne prend pas en charge Internet Explorer, vous devez configurer AppScan pour qu'il fonctionne avec un navigateur externe.
3. Connectez-vous au site, en remplissant les formulaires et en cliquant sur les liens requis.

   Conseil : La page à laquelle vous accédez lorsque vous vous êtes connecté sera utilisée par défaut comme URL En session par AppScan. AppScan envoie cette URL à un intervalle de quelques secondes lors de l'examen pour vérifier qu'il est toujours connecté. Si la page renvoie un grand nombre de réponses, ou si elle inclut des paramètres suivis ou des cookies, vous pouvez améliorer les performances de l'examen en cliquant sur un ou plusieurs liens complémentaires jusqu'à ce que vous atteigniez une page avec un plus petit nombre de réponses (en restant connecté) et n'incluant aucun paramètre suivi ni cookie. Après avoir fermé votre navigateur, allez dans l'onglet **Vérifier et valider** et sélectionnez la page *ultérieure* comme "URL En session".
4. Une fois connecté avec succès au site, cliquez sur **Je suis connecté au site**.
   AppScan tente d'extraire les informations de connexion de votre demande de connexion de façon à les utiliser lors de l'examen.

   Remarque : Parfois, la page de connexion ne fournit pas suffisamment d'informations, et AppScan peut vous demander de cliquer sur une étape supplémentaire après la connexion ou de vous déconnecter.

   Remarque : Si le mécanisme de connexion manipule les données de connexion à l'aide de JavaScript, une boîte de dialogue peut s'ouvrir pour vous demander de confirmer que les données de connexion extraites par AppScan sont correctes. Si nécessaire, spécifiez ou corrigez les paramètres et les valeurs, puis cliquez sur **OK**.
   La boîte de dialogue Informations sur la session s'ouvre et affiche les demandes de connexion que vous avez enregistrées.  devient  , indiquant que la détection En session est active.

Remarque : Si l'icône Clé devient rouge  , cela signifie qu'AppScan a tenté, sans y parvenir, d'identifier un schéma dans la page En session lors de l'examen pour vérifier qu'il n'était pas déconnecté. Dans ce cas, vous devez identifier le "schéma en session" de AppScan. Pour plus d'informations, voir «Boîte de dialogue Sélectionner un schéma de détection», à la page 61. Dans certains cas un message plus spécifique s'affiche avec un lien vers une page de la présente aide pour traiter le problème. Voir «Traitement des incidents liés à la connexion», à la page 336.

5. Pour modifier la séquence enregistrée (par exemple pour supprimer les étapes inutiles), voir «Onglet Vérifier et valider».

   Conseil : En général, l'adresse URL de connexion de l'utilisateur (et dont la réponse est la première à inclure un schéma En session) doit être celle marquée En session. Toutefois, il est parfois nécessaire de sélectionner une autre adresse URL qui comprend aussi le schéma En session, mais qui a l'avantage de correspondre à une page plus petite et de ne pas inclure de paramètres suivis ou de cookies. En outre, la demande POST contenant les données d'identification de l'utilisateur est parfois la demande qui vous permet de vous connecter et qui contient d'abord le schéma En session. Ce n'est pas le meilleur choix pour la page En session, car la vérification En session enverra les données d'identification chaque fois, entraînant un faux positif dans la réponse de la session. Voir «Optimisation de la détection en session», à la page 62.

6. Pour enregistrer la nouvelle séquence de connexion, cliquez sur **OK**.

   Conseil : Si vous êtes sûr que la page En session ne contient aucun paramètre suivi ou cookie, améliorez les performances de l'examen en définissant le paramètre **Configuration avancée > Gestion de session : Analyser la page En session** sur "False". Voir «Vue Configuration avancée», à la page 120.

Onglet Vérifier et valider

Configuration des examens > Gestion de connexion > onglet Vérifier et valider.

Lorsque vous enregistrez une séquence de connexion, AppScan enregistre les actions et les demandes. Ces éléments sont affichés dans les deux sous-onglets : Actions et Demandes Lors de la réexécution de la séquence de connexion, AppScan tente (par défaut) de reproduire la connexion basée sur les actions. En cas d'échec, il revient à la connexion basée sur les demandes.

Cet onglet permet de réviser et d'éditer :

- la version basée sur les actions de la séquence de connexion
- la version basée sur les demandes de la séquence de connexion
- la demande de la détection En session
- le schéma de détection en session (ou hors session)

Il est également utilisé pour :

- Valider les paramètres définis

Tableau 1. Paramètres "Onglet Vérifier et valider"

Paramètre	Détails
Lecture de la connexion	*Cette section apparaît uniquement si Connexion enregistrée est la méthode de connexion sélectionnée*

Tableau 1. Paramètres "Onglet Vérifier et valider" (suite)

Paramètre	Détails
Méthode de lecture de la connexion	AppScan enregistre deux versions de la séquence de connexion que vous avez enregistrée : une basée sur les actions que vous avez effectuées, et l'autre sur les demandes HTTP réellement envoyées. • **Basés sur les actions :** (Utilisée par défaut lorsque cela est possible :) AppScan tente de se connecter via la séquence de connexion basée sur les actions, en réexécutant les clics et les frappes de l'utilisateur. –  **Rejouer :** Ouvre le lecteur Basée sur les actions et rejoue la séquence de connexion enregistrée dans son navigateur. – **Editer :** Ouvre l'éditeur Basée sur les actions pour voir et éditer les détails de l'enregistrement de connexion. • **Basée sur les demandes :** Si cette méthode échoue, AppScan utilise la version basée sur les demandes, laquelle renvoie les demandes HTTP brutes à partir de l'enregistrement de connexion. – **Editer :** Ouvre l'éditeur Basée sur les demandes pour voir et éditer les détails de l'enregistrement de connexion. Si un message indique l'échec d'une de ces méthodes, faites appel à l'autre méthode. **Remarque :** Si vous sélectionnez la connexion Basée sur les actions et qu'elle échoue, AppScan essaiera la connexion Basée sur les demandes. En cas de réussite, le paramètre ici sera automatiquement remplacé par Basée sur les demandes.
Connexion automatique	*Cette section apparaît uniquement si Connexion automatique est la méthode de connexion sélectionnée*
Bouton **Configuration de la détection automatique en session**	Cliquez pour qu'AppScan effectue les actions suivantes : • Tentative de connexion au site à l'aide des données d'identification que vous avez fournies • Identification d'un schéma de détection en session sur la page de connexion (voir ci-dessous) • Configuration d'identificateurs de session (voir «Onglet ID session», à la page 63)
Détection de session	AppScan doit savoir, à tout moment, s'il est connecté ou déconnecté du site afin de pouvoir évaluer correctement les réponses du site. Lors de l'examen, AppScan envoie la demande de détection En session de façon répétitive et vérifie que la réponse contient le schéma de détection En session afin de vérifier qu'il est toujours connecté. Si AppScan ne trouve pas le schéma dans la réponse de la page, AppScan suppose qu'il a été déconnecté et tente de se reconnecter en rejouant la séquence de connexion. La séquence de connexion est, en général, exécutée plusieurs fois pendant l'examen. Il est donc préférable qu'elle contienne un nombre d'étapes aussi réduit que possible. Il est également utile que la page En session soit de petite taille et qu'elle ne contienne pas de paramètres suivis ou de cookies, car ces derniers peuvent prolonger considérablement la durée de l'examen.
la demande de la détection En session	Il s'agit de la demande utilisée par AppScan pour vérifier qu'il est toujours En session. Cette demande doit être une requête produisant différentes réponses en fonction du statut de connexion de l'utilisateur. AppScan tente d'identifier des demandes En session valides, et vous pouvez sélectionner l'une d'elles dans la liste déroulante. Si aucune demande n'est trouvée, ou adaptée, vous pouvez sélectionner votre propre demande à l'aide du bouton **Sélection de demande avancée**.
Bouton **Sélection de demande avancée**	Ce bouton permet d'ouvrir une boîte de dialogue dans laquelle vous pouvez consulter les demandes dans la séquence de connexion, et sélectionner une demande de la détection En session. Pour plus de détails, voir «Boîte de dialogue de sélection de demande En session avancée», à la page 60

Tableau 1. Paramètres "Onglet Vérifier et valider" (suite)

Paramètre	Détails
Schéma de détection En session	(Actif uniquement lorsqu'une demande de la détection En session est sélectionnée :) Ce champ affiche un schéma trouvé dans la demande de la détection En session sélectionnée, qui indique que l'utilisateur est En session (ou Hors session si cette option est sélectionnée). La liste déroulante vous permet de sélectionner un schéma de détection parmi les candidats qu'AppScan a identifié dans l'enregistrement de connexion, tandis que le message vert ou rouge sous le schéma indique si le schéma actuel est valide ou non. **Remarque :** Il est préférable d'utiliser un schéma *En session*. Toutefois, dans les rares cas où le schéma En session n'est pas toujours renvoyé à la suite d'une demande En session, ou lorsqu'il est compliqué de le définir, vous pouvez utiliser un schéma *Hors session* à la place.Si AppScan n'a pas été en mesure d'identifier un schéma valide, ou si vous devez en sélectionner un autre, utilisez le bouton **Sélection de schéma avancée** (rangée suivante de ce tableau). **Expression régulière :** Cochez cette case pour entrer une expression régulière afin d'identifier le schéma.
Bouton **Sélection de schéma avancée**	(Actif uniquement lorsqu'une demande de la détection En session est sélectionnée :) Ce bouton ouvre la boîte de dialogue **Sélectionner le schéma de détection**, affichant le contenu des réponses En session et Hors session aux demandes dans la Séquence de connexion que vous avez enregistrée (en fonction du schéma de détection sélectionné). Cela vous permet de voir le schéma de détection sélectionné dans le contexte de la réponse, et de définir un schéma de détection qui n'est *pas* répertorié dans la zone de liste déroulante. La boîte de dialogue vous permet de parcourir toutes les réponses enregistrées. Dans la partie supérieure de la boîte, vous pouvez également voir les demandes En session et Hors session envoyées par AppScan.
Validation	
Validate bouton	(Actif uniquement si la séquence de connexion actuelle n'a pas encore été vérifiée :) Cliquez pour valider la séquence et le schéma de détection de session.
Icône Clé	L'icône Clé indique l'état de configuration de la Détection En session :  Activée et configurée. (Une page En session a été identifiée dans la séquence de connexion, automatiquement ou par l'utilisateur.)  Activée, mais pas totalement configurée.  Activée, mais pas configurée.  Désactivée. Pour plus de détails, voir «Boîte de dialogue Sélectionner un schéma de détection», à la page 61.

Boîte de dialogue Éditer la connexion basée sur les actions :

Boîte de dialogue s'ouvrant depuis **Config. > Connexion > Vérifier et valider > Éditer (Basée sur les actions)**, peut être utilisé pour dépanner la procédure de connexion si la validation échoue.

Même si la connexion basée sur les demandes a réussi, il est préférable de dépanner la connexion basée sur les actions si possible. Dans cette boîte de dialogue, vous pouvez :

- Cliquer sur **Rejouer** pour rejouer la connexion dans le navigateur sélectionné.

- Changer le navigateur sélectionné et **Rejouer** dans un navigateur différent.
- Cliquer sur **Sélectionner > Actions d'attente**, et augmenter le temps d'attente entre les demandes.
- Vérifier le "Type" des demandes spécifiques dans la procédure et les modifier si nécessaire.
- Cliquer sur **Éditer les actions de lecture** pour voir et éditer au format XML.
- Augmenter le délai d'attente pour la tentative de connexion.

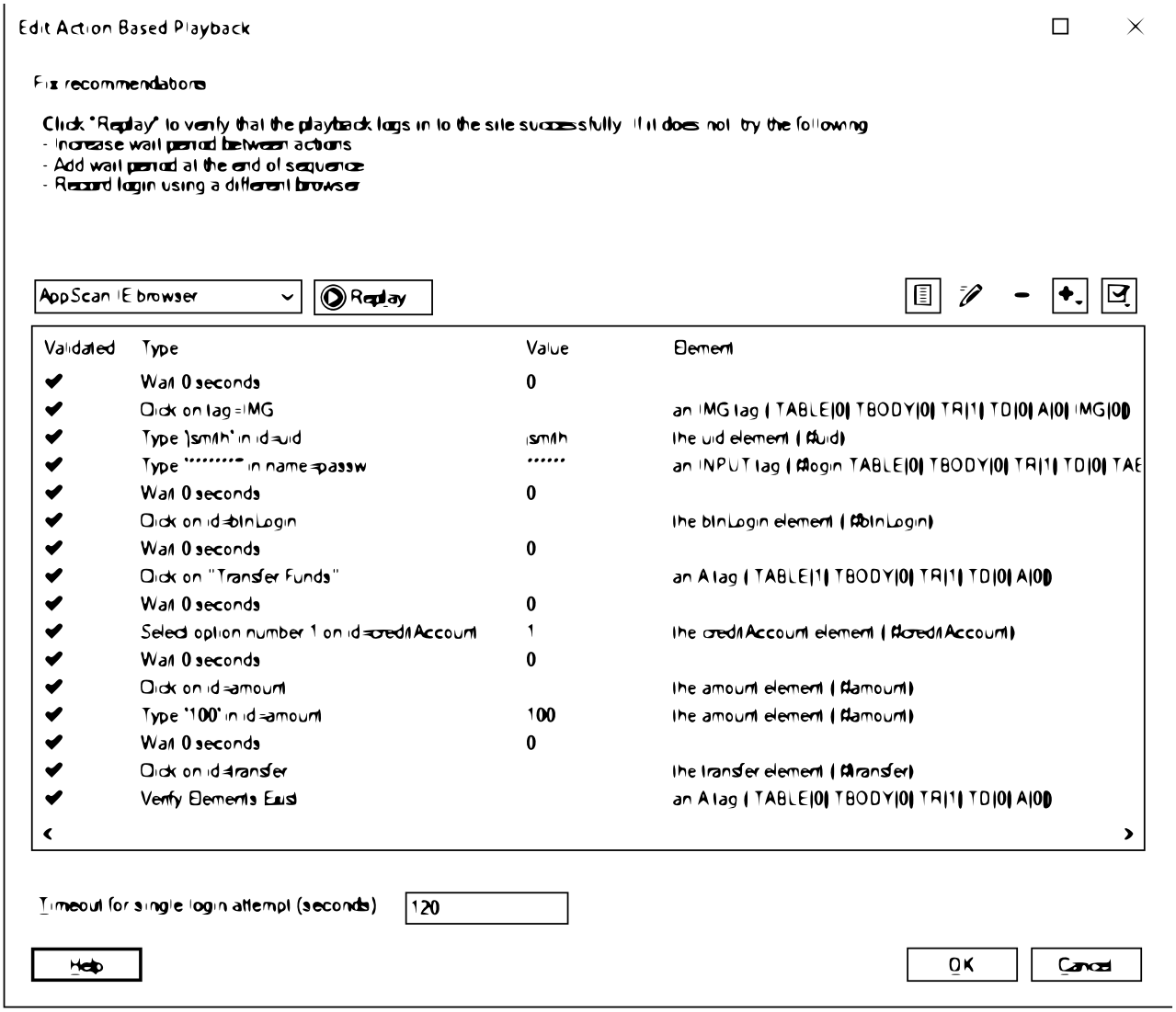


Figure 1. Boîte de dialogue Editer la lecture basée sur les actions

Tableau 2. Paramètres "Éditer la lecture basée sur les actions"

Elément	**Description**
Champ de navigateur	Affiche le navigateur actuellement sélectionné pour la lecture de la connexion. Vous pouvez le modifier depuis la liste déroulante.
Bouton **Rejouer**	Rejoue la procédure de connexion enregistrée dans le navigateur sélectionné.

Tableau 2. Paramètres "Éditer la lecture basée sur les actions" (suite)

Elément	Description
Liste de demandes et temps d'attente entre les demandes.	Affiche les éléments suivants pour chaque action : • **Validée :** Coche verte pour les actions correctement réalisées, croix rouge pour les actions ayant échoué • **Type :** Description de l'action (telle que "attendre", "cliquer" ou "définir" (valeur) • **Valeur :** Pour les actions d'attente : temps en secondes ; pour les actions d'utilisateur : nom de l'action • **Elément :** Elément HTML sur lequel l'action est effectuée Pour toute action sélectionnée, les icônes au-dessus du tableau vous permettent : • Voir et éditer les actions de lecteur au format XML • : D'éditer la valeur d'action • : De supprimer l'action • : D'ajouter un temps d'attente entre les actions • : D'ajouter une action "attente" avant ou après l'action sélectionnée
Délai d'attente (minutes) pour une tentative de connexion unique	Si votre procédure de connexion a besoin de plus de temps, vous pouvez augmenter ce paramètre.

Boîte de dialogue Éditer la connexion basée sur les demandes :

Boîte de dialogue s'ouvrant depuis **Config. > Connexion > Vérifier et valider > Éditer (Basée sur les demandes)**, peut être utilisé pour dépanner la procédure de connexion si la validation échoue.

Il s'agit d'une version simplifiée de la Boîte de dialogue de sélection de la demande En session avancée.

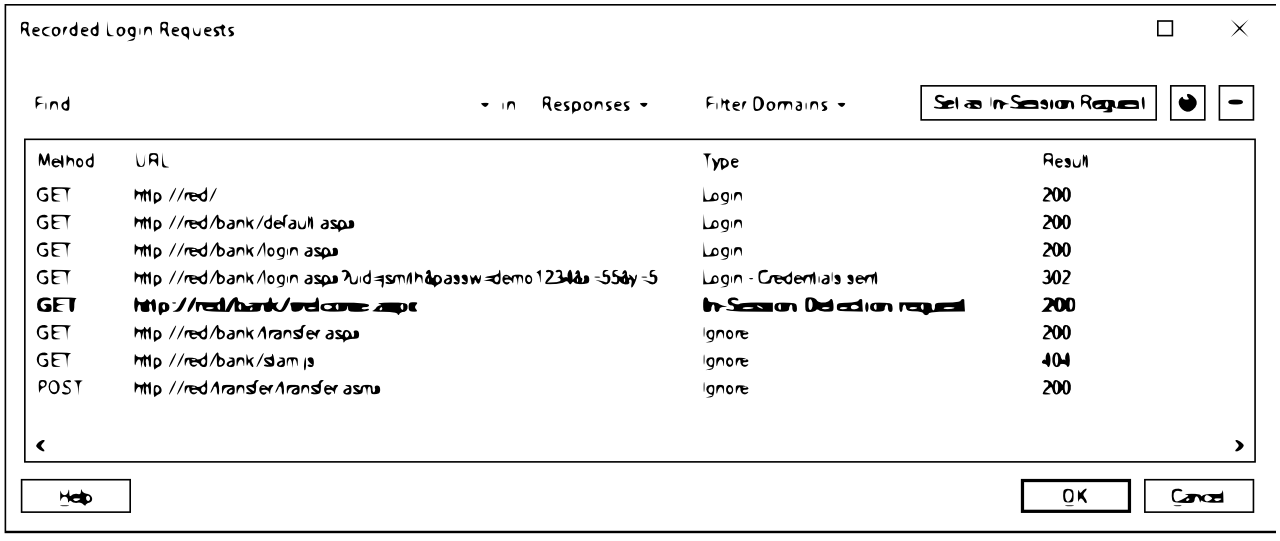


Figure 2. Boîte de dialogue Editer la lecture basée sur les demandes

Tableau 3. Paramètres "Demandes de connexion enregistrées"

Paramètre	Détails
Liste principale	Affiche toutes les demandes de la procédure de connexion enregistrées.
Rechercher	Affiche seulement les demandes qui contiennent la chaîne de texte que vous avez saisi, dans URL, Demande, Réponse ou Tous.
Filtrer les domaines	Affiche uniquement les demandes des domaines sélectionnés dans la liste déroulante.Cliquez pour qu'AppScan effectue les actions suivantes :
Bouton **Définir comme demande En session**	Définit la demande sélectionnée comme la Demande En session qui sera utilisée par AppScan au cours de l'analyse pour vérifier qu'il est toujours connecté. Vous pouvez également faire cela en effectuant un clic droit sur une demande dans la liste.
	Affiche la réponse reçue pour la demande sélectionnée lorsque la connexion a été enregistrée. La fenêtre qui s'ouvre présente deux onglets : L'onglet Navigateur affiche la réponse reçue, et l'onglet Demande/Réponse affiche les données brutes pour la demande et la réponse.
	Supprime la demande sélectionnée de la séquence de connexion.

Boîte de dialogue de sélection de demande En session avancée :

Boîte de dialogue de sélection de demande En session avancée, qui s'ouvre depuis **Config. > Connexion > Vérifier et valider > Sélection de demande avancée**

Il s'agit d'une version de la Boîte de dialogue Éditer la connexion basée sur les demandes avec davantage d'options. Dans cette boîte de dialogue, vous pouvez :

- Voir la séquence des demandes que vous avez envoyées lors de la connexion.
- Voir la demande de la détection En session

  Remarque : La page marquée "En session" doit correspondre à la première page à surligner. Si une page précédente à la page "Connexion" est surlignée, alors soit le schéma En session est incorrect, soit une page incorrecte est marquée "En session".
- Voir tous les URL de la séquence dans un navigateur.
- Définir une demande *différente* de la demande En session et sélectionner un nouveau schéma de détection En session depuis cette nouvelle demande.
- Supprimer les demandes qui ne sont pas nécessaires *avant* l'URL "En session", pour éviter à AppScan de répéter ces demandes inutiles de nombreuses fois pendant un examen.
- Voir les demandes envoyées *après* la demande de détection En session qui contiennent le schéma de détection En session et sont marquées comme "Ignorer".
- Rechercher les demandes dans la séquence
- Afficher uniquement les demandes de domaines spécifiques
- Ouvrir la boîte de dialogue Sélection du schéma de détection pour sélectionner un schéma qui n'est pas suggéré par AppScan

Tableau 4. Paramètres "Sélection de demande En session avancée"

Paramètre	Détails
Liste principale	Affiche toutes les demandes de la procédure de connexion enregistrées.
Rechercher	Affiche seulement les demandes qui contiennent la chaîne de texte que vous avez saisi, dans URL, Demande, Réponse ou Tous.

Tableau 4. Paramètres "Sélection de demande En session avancée" (suite)

Paramètre	Détails
Afficher les domaines	Affiche uniquement les demandes des domaines sélectionnés dans la liste déroulante.Cliquez pour qu'AppScan effectue les actions suivantes :
Bouton **Définir comme demande En session**	Définit la demande sélectionnée comme la Demande En session qui sera utilisée par AppScan au cours de l'analyse pour vérifier qu'il est toujours connecté. Vous pouvez également faire cela en effectuant un clic droit sur une demande dans la liste.
Bouton **Sélection de schéma avancée**	Ouvre la boîte de dialogue **Sélectionner le schéma de détection**, affichant le contenu des réponses En session et Hors session aux demandes dans la Séquence de connexion que vous avez enregistrée (en fonction du schéma de détection sélectionné). Cela vous permet de voir le schéma de détection sélectionné dans le contexte de la réponse, et de définir un schéma de détection qui n'est *pas* répertorié dans la zone de liste déroulante. La boîte de dialogue vous permet de parcourir toutes les réponses enregistrées. Dans la partie supérieure de la boîte, vous pouvez également voir les demandes En session et Hors session envoyées par AppScan. Vous pouvez également faire cela en effectuant un clic droit sur une demande dans la liste.
	Affiche la réponse reçue pour la demande sélectionnée lorsque la connexion a été enregistrée. La fenêtre qui s'ouvre présente deux onglets : L'onglet Navigateur affiche la réponse reçue, et l'onglet Demande/Réponse affiche les données brutes pour la demande et la réponse.
	Supprime la demande sélectionnée de la séquence de connexion.
Schéma de détection	Ce champ affiche un schéma trouvé dans la demande de la détection En session sélectionnée, qui indique que l'utilisateur est En session (ou Hors session si cette option est sélectionnée). La liste déroulante vous permet de sélectionner un schéma de détection parmi les candidats qu'AppScan a identifié dans l'enregistrement de connexion, tandis qu'une couleur verte ou rouge indique si le schéma est valide ou non. **Remarque :** En général, il est préférable d'utiliser un schéma *En session*. Toutefois, dans les rares cas où le schéma En session n'est pas toujours renvoyé à la suite d'une demande En session, ou lorsqu'il est compliqué de le définir, vous pouvez utiliser un schéma *Hors session* à la place.Si AppScan n'a pas été en mesure d'identifier un schéma valide, ou si vous devez en sélectionner un autre, utilisez le bouton **Sélection de schéma avancée** pour sélectionner le vôtre.

Boîte de dialogue Sélectionner un schéma de détection :

Utilisez cette boîte de dialogue pour comparer les réponses En session et Hors session aux demandes de connexion, afin de vous aider à décider du meilleur schéma de détection pour votre application. Ouvert en cliquant

Pourquoi et quand exécuter cette tâche

Cette boîte de dialogue s'ouvre lorsque vous cliquez sur **Config. > Gestion de connexion > Vérifier et valider > Sélection de schéma avancée**.

Dans cette boîte de dialogue, vous pouvez voir :

- Le schéma de détection de session actuel, et son statut
- Quatre sous-fenêtres affichant la demande et la réponse actuelles En session et Hors session
- La différence entre les demandes est surlignée en vert
- Dans la Réponse En session, le schéma sélectionné est surligné en vert
- Le bouton **Enregistrer le schéma** vous permet de sélectionner un schéma différent et de le définir

- La fonction de basculement de page dans le coin supérieur droit de la boîte de dialogue vous permet de basculer entre les demandes

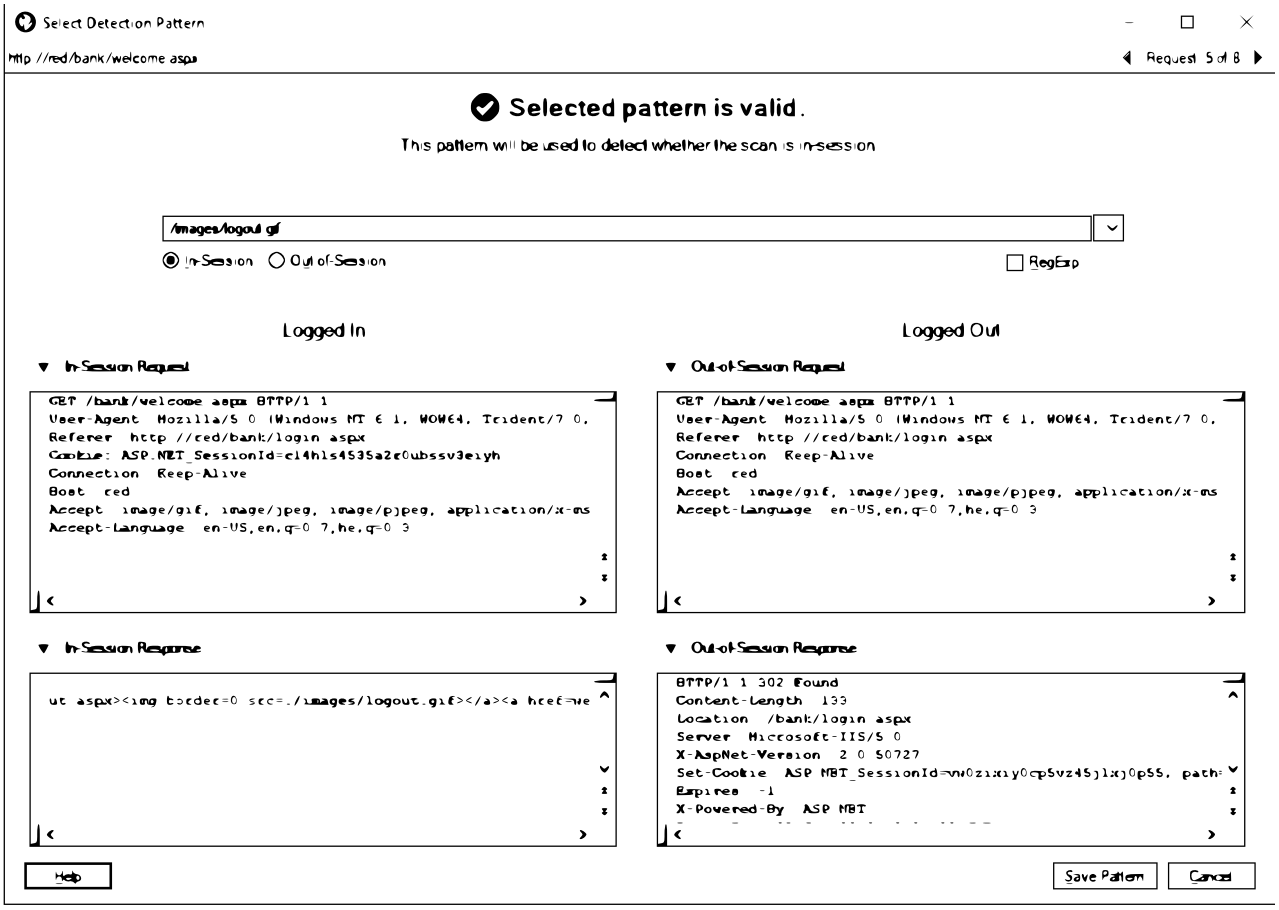


Figure 3. Boîte de dialogue Sélectionner un schéma de détection

Procédure

1. Vérifiez le schéma sélectionné lorsqu'il survient dans la réponse En session (ou Hors session).
2. Consultez et comparez les deux réponses pour trouver d'autres schémas valides.
3. Consultez et comparez les *demandes* En session et Hors session (au-dessus des champs de réponse) qui ont généré ces réponses.
4. Basculez entre les demandes et les réponses pour *toutes* les demandes dans la connexion enregistrée à l'aide des flèches dans le coin supérieur droit de la boîte de dialogue.
5. Sélectionnez et sauvegardez un nouveau schéma de votre choix.

Optimisation de la détection en session :

Réviser la séquence de connexion dans l'onglet Demandes permet d'identifier les incidents et d'optimiser la détection En session.

Pourquoi et quand exécuter cette tâche

AppScan tente d'identifier automatiquement un "Schéma de détection En session" qui se produit sur cette page et qu'il peut utiliser pendant l'examen pour vérifier qu'il est toujours connecté. Il doit s'agir d'un schéma qui se produit au format HTML *uniquement* lorsque vous êtes connecté. Par exemple, un texte qui dit : "Cliquez ici pour vous déconnecter."

Pendant l'examen, AppScan envoie la demande En session à plusieurs reprises, et vérifie que la réponse contient le Schéma de détection En session. Si AppScan ne trouve pas le schéma dans la réponse de la page, AppScan suppose qu'il a été déconnecté et tente de se reconnecter en rejouant la séquence de connexion. La séquence de connexion est, en général, exécutée plusieurs fois pendant l'examen. Il est donc préférable qu'elle contienne un nombre d'étapes aussi réduit que possible. Il est également utile que la page En session soit de petite taille et qu'elle ne contienne pas de paramètres suivis ou de cookies, car ces derniers peuvent prolonger considérablement la durée de l'examen.

Lorsque le schéma En session défini est détecté dans la demande En session, (la demande qui suit immédiatement la requête POST), il est mis en évidence en vert.

Procédure

1. Vérifiez que le Schéma de détection En session qui a été sélectionné automatiquement indique en fait que l'utilisateur est connecté. Si nécessaire, changez-le.
2. Vérifiez qu'il n'existe pas d'étapes inutiles dans la procédure de connexion. Si c'est le cas, supprimez-les.
3. Vérifiez que la réponse En session n'est pas de grande taille, et si possible, qu'elle ne comprend pas de paramètres suivis ou de cookies. Si nécessaire, ajoutez une ou plusieurs étapes jusqu'à atteindre une page plus petite ou ne comportant pas d'éléments suivis.
4. Si vous réussissez à sélectionner une page En session sans paramètres suivis ni cookies, il n'est pas nécessaire qu'AppScan les vérifie à chaque fois qu'il se connecte. Allez dans **Configuration avancée > Gestion de session : Analysez la page En session**, et définissez le paramètre sur False.
5. Si aucune de ces actions n'aboutit, vous pouvez tenter d'identifier un schéma Hors session à la place, puis de changer la méthode de détection.

Onglet ID session

Configuration des examens > Gestion de connexion > onglet ID session

L'onglet **ID session** de la vue **Gestion de connexion** permet de réviser et de gérer le suivi des variables (ID session) reçues au cours de la connexion enregistrée.

L'onglet répertorie toutes les variables reçues lors de la séquence de connexion et désigne automatiquement des ID session comme suivis (une coche apparaît à côté de la variable dans la colonne Suivi).

Vous pouvez sélectionner des variables dans cette liste et cliquer sur les boutons **Rechercher** et **Arrêter la recherche** pour changer leur statut. Tous les paramètres "suivis" sont ajoutés à la liste globale de paramètres et de cookies dont l'état est suivi lors de l'examen (voir «Vue Paramètres et cookies», à la page 76).

Conseil : Si vous n'êtes pas certain de connaître les ID session et que l'examen passe hors session, demandez aux développeurs de l'application de vous fournir une liste de paramètres et de cookies qui seront utilisés par l'application pour gérer la session.

Onglet Avancé

Configuration des examens > Gestion de connexion > onglet Avancé.

L'onglet **Avancé** de la vue **Gestion de connexion** est utilisé pour les paramètres de connexion avancés et pour la détection de page de déconnexion.

Paramètre	Détails
Paramètres de connexion avancés	**Autoriser la connexion même si l'application est déjà connectée :** Pour gagner du temps, AppScan envoie plusieurs demandes de connexion sans déconnexion entre chacune d'elles. Si votre application ne le permet pas, décochez cette case. **Nombre d'échecs de connexion admis par le serveur avant le verrouillage du compte utilisateur :** Si votre application verrouille un compte utilisateur à l'issue d'un certain nombre d'échecs de connexion, cochez cette case et indiquez un nombre. AppScan Enterprise envoie des demandes de connexion valides entre les échecs de connexion pour s'assurer que ce seuil ne soit jamais atteint, ce qui rendrait les examens ultérieurs impossibles.
Détection de page de déconnexion	AppScan utilise une expression régulière pour identifier les pages de déconnexion. Cela lui permet d'effectuer un examen plus efficace en essayant de ne pas être déconnecté trop souvent et de ne pas avoir à se connecter de nouveau. Cela permet également d'identifier les pages de déconnexion lorsque vous configurez l'examen pour ne pas tester les pages de connexion/déconnexion (voir «Vue Options de test», à la page 114), et pour vous déconnecter au besoin dans le cadre de certains tests de sécurité. Il s'agit de l'expression régulière par défaut : `(logout|signout|logoff|signoff|exit|quit|invalidate)` Si aucun des indicateurs de cette expression régulière n'apparaît dans l'URL, AppScan suppose que la page est une page de déconnexion et qu'elle est donc connectée à l'application. **Remarque :** AppScan peut ajouter cette expression lorsque vous enregistrez une procédure de connexion, s'il identifie des indicateurs supplémentaires. Vous pouvez ajouter d'autres indicateurs, si nécessaire, mais veillez bien à respecter les règles de syntaxe des expressions régulières. **Remarque :** L'outil Expression Test PowerTool (**Outils > Test d'expression**) peut être utile pour vérifier la syntaxe de vos expressions régulières. Si vous avez besoin d'une aide supplémentaire, reportez-vous au lien suivant : http://www.regular-expressions.info/quickstart.html

Vue Définition de l'environnement

Vue Définition de l'environnement de la boîte de dialogue Configuration.

La définition de l'environnement n'est pas essentielle mais permet à AppScan de ne pas envoyer de tests inappropriés lors de l'examen, ce qui le rend plus rapide et plus efficace.

Remarque : Si nécessaire, certaines zones de liste permettent de choisir plusieurs options en appuyant sur la touche **Ctrl** lors de la sélection d'éléments dans une liste.

Mesure	Commentaires
Système d'exploitation	Système d'exploitation de l'application en cours d'examen.
Serveur Web	Sélectionne *toutes* les réponses applicables. Pour sélectionner plusieurs options, appuyez sur la touche [Ctrl] tout en cliquant.
Serveur d'applications (le cas échéant)	Sélectionne *toutes* les réponses applicables. Pour sélectionner plusieurs options, appuyez sur la touche [Ctrl] tout en cliquant.
Type de base de données (le cas échéant)	Sélectionne *toutes* les réponses applicables. Pour sélectionner plusieurs options, appuyez sur la touche [Ctrl] tout en cliquant.
Composant tiers (le cas échéant)	Sélectionne *toutes* les réponses applicables. Pour sélectionner plusieurs options, appuyez sur la touche [Ctrl] tout en cliquant.
Emplacement du site	Indique si le site est distant ou local.

Mesure	Commentaires
Type de site	Indique s'il s'agit d'un site de test ou d'un site de production opérationnel.
Méthode de déploiement	Indique si le site est déployé en interne (site privé) ou en externe (sur Internet).
Dommage collatéral potentiel	Dommage ou vol potentiel si l'application est vulnérable.
Distribution cible	Proposition des systèmes dans l'environnement qui sont des cibles potentielles.
Exigence de disponibilité	Importance relative de la disponibilité (des informations).
Exigence de confidentialité	Importance relative de la confidentialité (des informations utilisateur).
Exigence d'intégrité	Importance relative de l'intégrité (précision) des informations.

Remarque : Les cinq derniers éléments sont des mesures environnementales CVSS pour le site. Si vous définissez l'importance relative de ces mesures sur l'environnement de votre application, AppScan prend en compte ces définitions lors de l'attribution des valeurs de gravité aux vulnérabilités trouvées lors de l'examen. Ces définitions sont globales. (Vous pouvez ajuster les mesures environnementales d'un problème *particulier* à partir du Panneau des détails > Gravité > Open CVSS Panel, voir «Paramètres CVSS», à la page 214.)

Vue Exclusion de chemins et de fichiers

Vue Exclusion de chemins et de fichiers de la boîte de dialogue Configuration.

Vous pouvez configurer AppScan pour qu'il ignore certains chemins de l'application ou des types de fichier spécifiques. Toutefois, vous devez appliquer les exclusions avec prudence car elles peuvent avoir des conséquences importantes. Ici, les changements s'appliquent uniquement à une exploration basée sur les demandes, et non à une exploration basée sur les actions (tel que configuré dans Configuration > Options d'exploration > Méthode d'exploration).

Paramètre	Détails
Exclusion de chemins d'accès	Vous pouvez filtrer sur la portée de l'étape d'exploration automatique en ajoutant des URL (chemins complets pouvant inclure des requêtes) ou des expressions régulières à la liste **Exclure ou inclure des chemins d'accès**. Pour plus de détails, voir «Exclusion de chemins d'accès».
Types de fichier à exclure	Vous pouvez configurer AppScan pour qu'il ignore des types de fichier spécifiques lors de l'examen. Par exemple, vous pouvez raccourcir la durée de l'examen en excluant des fichiers graphiques. Toutefois, vous devez exclure les fichiers avec prudence car ils peuvent contenir des données importantes. Pour plus de détails, voir «Exclusion des types de fichier», à la page 70

«Limitation d'un examen au dossier de l'URL de départ», à la page 48

Exclusion de chemins d'accès

Vue Exclusion de chemins et de fichiers de la boîte de dialogue Configuration

Vous pouvez filtrer la portée de l'étape d'exploration automatique en ajoutant des URL (chemins complets pouvant inclure des requêtes) ou des expressions régulières à la liste **Exclure des chemins d'accès**. Vous pouvez le faire pour diverses raisons :

- Car elles sont toujours en développement et vous savez qu'elles sont problématiques et ne souhaitez pas procéder à un examen pour le moment.
- Car vous savez qu'elles ne sont *pas* problématiques mais souhaitez réduire le temps d'examen.

- Pour réduire le temps d'examen en le restreignant à certaines parties de l'application.

Pour tout chemin défini, vous pouvez éventuellement limiter le filtre à un ou plusieurs paramètres spécifiques. Ce choix peut être motivé par la raison suivante :

- Pour les applications avec mégascripts (applications contenues dans une URL et contrôlées par ses paramètres) dans lesquelles vous souhaitez exclure certains paramètres (par exemple, le paramètre de connexion ou de déconnexion) des examens.

Deux types d'entrées figurent dans ce tableau :

- **Exclure :** Les chemins répertoriés sont exclus de l'examen.

  Tout lien correspondant à un chemin configuré pour être une exclusion est filtré hors de l'examen.

  Remarque : Vous pouvez également exclure un chemin en cliquant dessus avec le bouton droit de la souris dans l'arborescence de l'application et en sélectionnant **Exclure de l'examen**.
- **Exception :** Utilisé pour inclure un répertoire spécifique d'un chemin ayant été exclu *plus haut dans la liste*.

  Remarque : La fonction **Exception** est nécessaire uniquement si vous souhaitez inclure un répertoire se trouvant dans un chemin que vous avez exclu. Par exemple, si vous avez exclu : http://demo.testfire.net/bank vous pouvez alors ajouter http://demo.testfire.net/bank/transfer.aspx comme inclusion, plus bas dans la liste, pour inclure ce sous-répertoire aux examens.

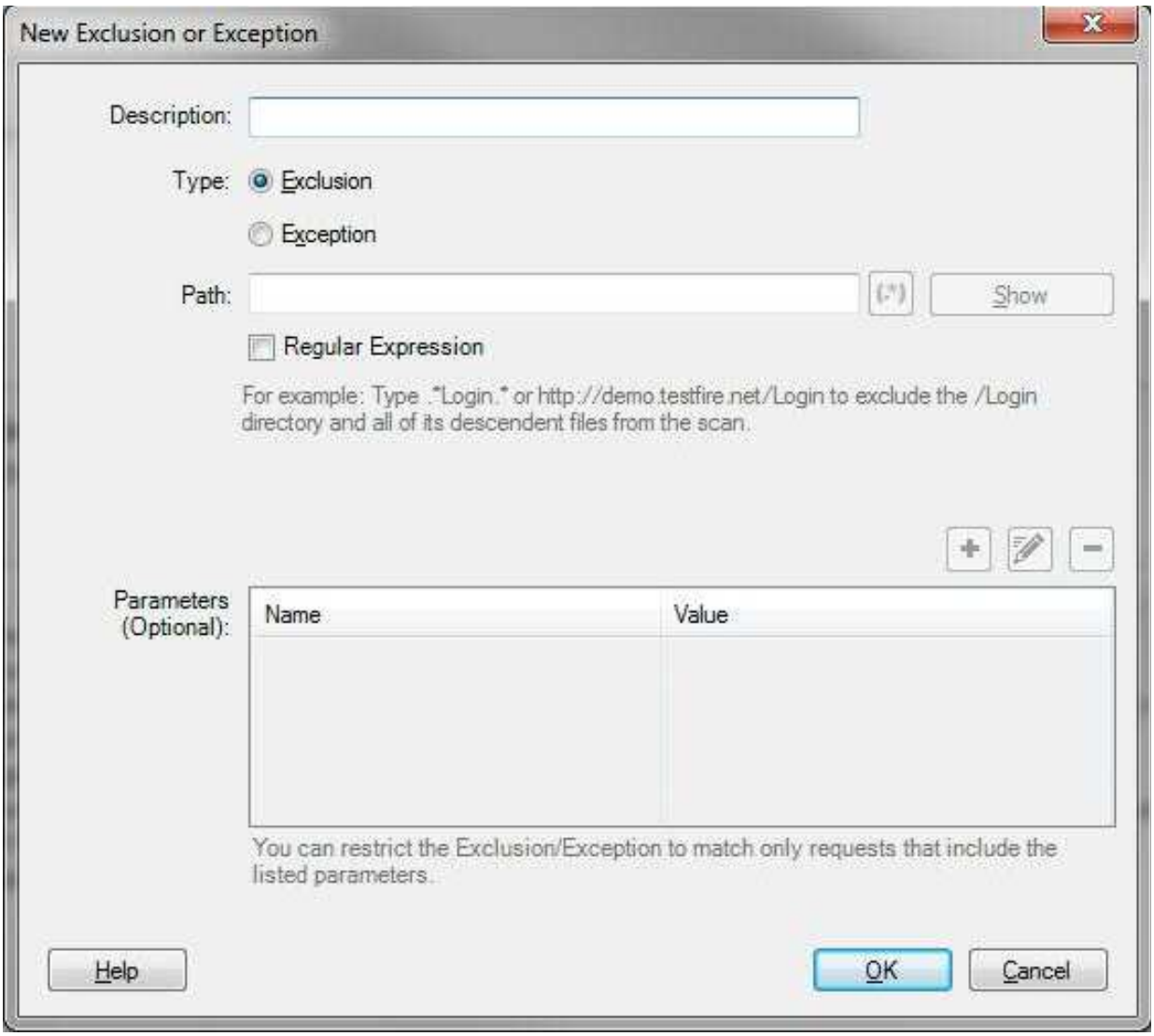
  Remarque : Si vous ajoutez des exclusions entre les étapes d'exploration et de test de l'examen, AppScan ne testera pas les chemins exclus même s'ils ont été explorés.

«Ajouter de nouvelles exclusions ou exceptions»

Ajouter de nouvelles exclusions ou exceptions :
Procédure

1. Dans la zone Exclure des chemins d'accès de l'onglet Exclure des chemins d'accès et des fichiers de la boîte de dialogue Configuration, cliquez sur  , sélectionnez Exclusion ou Exception, entrez le chemin d'accès complet ou l'expression régulière, puis cliquez sur **OK**. (Dans **Assistant de configuration des examens** > **URL de départ** > **Avancé**, cliquez sur **Explorer**.)

   La boîte de dialogue **Nouvelle exclusion ou exception** s'ouvre.



2. Cliquez sur le bouton radio correspondant au filtre que vous souhaitez créer :
   - **Exclusion :** Ne pas examiner les URL correspondant à cet élément.
   - **Exception :** Inclure les URL correspondant à cet élément, même si elles sont exclues par une exclusion figurant plus haut dans la liste.

   Remarque : La fonction **Exception** est nécessaire uniquement si vous souhaitez inclure un répertoire se trouvant dans un chemin que vous avez exclu. Par exemple, si vous avez exclu : http://demo.testfire.net/bank vous pouvez alors ajouter http://demo.testfire.net/bank/transfer.aspx comme inclusion, plus bas dans la liste, pour inclure ce sous-répertoire aux examens.

   Remarque : Si vous ajoutez des exclusions entre les étapes d'exploration et de test de l'examen, AppScan ne testera pas les chemins exclus même s'ils ont été explorés.
3. Eventuellement, ajoutez une description qui apparaîtra dans la liste Exclusion de chemins d'accès.
4. Entrez un chemin ou une expression régulière correspondant à un ensemble de répertoires dans la zone Chemin d'accès (voir les exemples dans le tableau suivant). Dans le cas d'une expression régulière, cochez la case.

Remarque : Une expression régulière (regexp.) est une chaîne décrivant un ensemble de chaînes selon une syntaxe précise. Cliquez sur le  qui ouvre l'outil Expression Test PowerTool afin de vous aider à vérifier la syntaxe de l'expression régulière.

Si vous avez besoin d'une aide supplémentaire pour écrire des expressions régulières, reportez-vous au lien suivant : http://www.regular-expressions.info/quickstart.html

5. Pour appliquer l'exclusion ou l'exception aux chemins d'accès qui incluent des paramètres spécifiques uniquement, cliquez sur  pour ajouter un ou plusieurs paramètres au panneau inférieur de la boîte de dialogue.

   Remarque : Cette fonction est conçue pour les applications avec mégascripts, où l'application entière est contenue dans une URL et contrôlée par ses paramètres. Le processus de filtrage de l'URL risque de désactiver l'examen, mais vous pouvez filtrer des paramètres spécifiques ou des valeurs de paramètre (comme les paramètres de connexion ou de déconnexion).
6. Cliquez sur **OK**.
   Le nouvel élément est ajouté au bas de la liste.

   Remarque : Lorsqu'il y a un conflit entre deux éléments de la liste, l'élément le *plus bas* est prioritaire. Utilisez les boutons **Haut/Bas** pour ajuster l'ordre des éléments, le cas échéant. Si une exclusion ou une inclusion est redondante avec une autre exclusion ou inclusion de niveau supérieur dans la liste, l'élément redondant sera supprimé de la liste lorsque vous cliquerez sur OK.

Exemple

Type	Exemple et fonction
Exclude	**http://demo.testfire.net/transfer** ou **http://demo.testfire.net/transfer/** Filtre l'URL spécifiée ainsi que tous les sous-répertoires et fichiers.
Exclude	**.*private.*** Exclut toutes les URL contenant la chaîne **private**.
Exclude	.*_bk.aspx Exclut toutes les URL se terminant par **_bk.aspx**
Exception	**http://demo.testfire.net/transfer/customize.aspx** Lorsqu'une exclusion précédente (telle que la première du tableau) exclut des sous-répertoires et des fichiers, cette exception inclut ce chemin spécifique dans l'examen. Notez que l'exception doit apparaître *sous* l'exclusion pour prendre effet.

Editer des exclusions ou des inclusions :
Procédure

1. Sélectionnez un élément dans la liste **Exclure ou inclure des chemins d'accès**.
2. Cliquez sur **Editer**.
   La boîte de dialogue **Éditer l'exclusion ou la restriction** apparaît, affichant les propriétés de l'élément sélectionné.
3. Modifiez comme vous le souhaitez puis cliquez sur **OK**.

Que faire ensuite

Voir aussi : «Limitation d'un examen à un dossier spécifique»

«Limitation d'un examen au dossier de l'URL de départ», à la page 48

Limitation d'un examen à un dossier spécifique

Utilisation des exclusions et des exceptions pour limiter la portée d'un examen.

Pourquoi et quand exécuter cette tâche

Vous pouvez limiter l'examen automatique à un ou plusieurs dossiers *spécifiques* en excluant toutes les adresses URL, puis en incluant le ou les répertoires requis. (Pour limiter l'examen au *dossier d'adresses URL de départ*, voir «Limitation d'un examen au dossier de l'URL de départ», à la page 48.)

Procédure

1. Ouvrez **Configuration des examens > Exclusion de chemins et de dossiers**.
2. Ajoutez un élément **Exclure** au chemin d'accès de votre site, tel que **http://www.mysite.com/** (voir «Exclusion de chemins d'accès», à la page 65).
3. Ajoutez un ou plusieurs éléments **Exception** *sous* l'élément **Exclure** avec le ou les chemins que vous voulez examiner.

   Remarque : Le ou les éléments **Exception** doivent apparaître *sous* l'élément **Exclure** pour qu'ils prennent effet. Si nécessaire, utilisez les boutons **Haut/Bas** pour ajuster l'ordre avant de fermer.
4. Vérifiez que l'URL de départ (voir «Vue URL et serveurs», à la page 47) ne se trouve pas dans l'un des chemins exclus. (Si c'est le cas, l'examen ne parviendra pas à démarrer !)
5. Cliquez sur **OK** pour sauvegarder les modifications et fermer la liste.

Exemple 1 :
Pourquoi et quand exécuter cette tâche

Imaginons un cas dans lequel l'URL de départ pour l'examen (voir «Vue URL et serveurs», à la page 47) est : **http://www.mysite.com/index.aspx** et pour lequel nous souhaitons restreindre l'examen au dossier : **http://www.mysite.com/myfolder/**

Procédure

1. Ajoutez un élément **Exclure** au chemin d'accès `http://www.mysite.com/` (voir «Exclusion de chemins d'accès», à la page 65).
2. Ajoutez un élément **Inclure** *sous* l'élément **Exclure** avec le chemin d'accès de l'URL de départ : `http://www.mysite.com/index.aspx`
3. Ajoutez un *second* élément **Inclure** sous l'élément **Exclure** avec le chemin du dossier à examiner : `http://www.mysite.com/myfolder/`

Exemple 2 :
Pourquoi et quand exécuter cette tâche

Imaginons un cas dans lequel l'URL de départ pour l'examen se trouve dans le dossier à examiner. L'URL de départ est : `http://www.mysite.com/myfolder/index.aspx` et nous voulons limiter l'examen au dossier : `http://www.mysite.com/myfolder/`

Dans le cas présent, le dossier à examiner et l'URL de départ sont ajoutés à l'examen dans un seul élément **Inclure**.

Procédure

1. Ajoutez un élément **Exclure** au chemin d'accès `http://www.mysite.com/`
2. Ajoutez un élément **Inclure** *sous* l'élément **Exclure** avec le chemin du dossier à examiner : `http://www.mysite.com/myfolder/`

Exclusion des types de fichier

Exclure certains types de fichier de l'examen.

Pourquoi et quand exécuter cette tâche

Vous pouvez configurer le logiciel AppScan pour qu'il ignore des types de fichiers spécifiques, plutôt que des pages complètes, comme dans les paramètres Exclusion de chemins d'accès. Par exemple, vous pouvez raccourcir la durée de l'examen en excluant des graphiques. Toutefois, vous devez exclure les fichiers avec prudence car ils peuvent contenir des données importantes.

Procédure

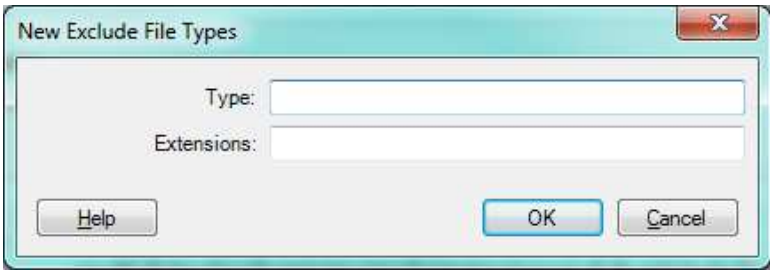
1. Ouvrez la boîte de dialogue **Configuration des examens**, puis la vue **Paramètres d'exploration**.
2. Dans le volet **Types de fichiers à exclure**, vérifiez que les cases à cocher des types de fichiers que vous ne souhaitez pas examiner sont sélectionnées.

Exclusion de types de fichier supplémentaires :
Pourquoi et quand exécuter cette tâche

Si une extension de fichier n'est pas répertoriée dans la boîte de dialogue **Types de fichier à exclure** de votre application, vous pouvez l'ajouter à la liste.

Procédure

1. Dans la zone **Types de fichier à exclure**, cliquez sur  .
   La boîte de dialogue **Nouveaux types de fichier à exclure** s'affiche.



2. Dans la zone de saisie **Type**, entrez un mot ou une phrase pour décrire un ensemble d'extensions de fichier.
3. Dans la zone de saisie **Extensions**, entrez la liste des extensions appartenant à ce type de fichier. (Séparez les extensions par des virgules, sans espace.)
4. Cliquez sur **OK**.

Edition de la liste des types de fichier exclus :
Procédure

1. Sélectionnez une ligne dans la boîte de dialogue **Types de fichier à exclure**.
2. Cliquez sur **Editer**.
   La boîte de dialogue **Éditer les types de fichier à exclure** apparaît, affichant les extensions associées à l'exclusion sélectionnée.

3. Modifiez le nom du type ou la liste des extensions, comme nécessaire.
4. Cliquez sur **OK**.

Vue Options d'exploration

Vue Options d'exploration de la boîte de dialogue Configuration.

La vue Options d'exploration comporte ces onglets :

- L'onglet Principal permet de sélectionner la méthode utilisée par AppScan pour explorer le site.
- L'onglet Basée sur les actions permet de configurer les paramètres spécifiques à l'exploration basée sur les actions.
- L'onglet Basée sur les demandes permet de configurer les paramètres spécifiques à l'exploration basée sur les demandes.

Onglet Principal

Configuration des examens > Options d'exploration > Onglet Principal.

Cet onglet permet de sélectionner la méthode d'exploration qu'AppScan doit utiliser pour l'examen et de configurer les options applicables aux deux méthodes.

Méthode d'exploration
AppScan utilise deux méthodes distinctes pour l'étape d'exploration de l'analyse. Vous pouvez sélectionner l'une des deux, ou les deux. Des deux méthodes disponibles, l'exploration basée sur les demandes est généralement plus rapide que l'exploration basée sur les actions. Lorsque ces deux méthodes sont sélectionnées (valeur par défaut recommandée), l'exploration basée sur les actions s'exécute en premier avec un délai maximal de 30 minutes, suivie de l'exploration basée sur les demandes.

Filtrage sur la structure de page (DOM)
Cette option permet de réduire *considérablement* la durée de l'examen en identifiant les pages qui présentent un niveau de similarité suffisant avec les pages déjà explorées, ce qui permet à AppScan de les ignorer en toute sécurité.

Limites de l'examen
Cette option permet de déterminer la profondeur (ou la vitesse) à laquelle AppScan explore votre application.

Autres paramètres
Cette option permet de configurer le client pour reconnaître un codage de serveur spécifique et envoyer un en-tête d'agent d'utilisateur spécifique.

Paramètre	Détails
Méthode d'exploration	
Basée sur les actions	Une version du navigateur Google Chrome est utilisée pour examiner le site comme le ferait un utilisateur en cliquant sur les liens visibles dans le navigateur. Cette méthode est particulièrement efficace lorsque de nouvelles technologies, comme JavaScript et le stockage de session, et des sites de type RIA, SPA (Single-Page Application) ou AngularJS sont utilisés.
Basée sur les demandes	Les demandes sont envoyées en fonction de l'ensemble du contenu des pages reconnu par AppScan. Cette procédure inclut le contenu qui n'est pas visible pour les utilisateurs d'un navigateur mais qu'un pirate pourrait détecter, comme des liens dans des commentaires.
Filtrage sur la structure de page (DOM)	

Paramètre	Détails
Filtrer les pages identiques en fonction de leur structure (DOM)	AppScan compare les nouvelles pages aux pages déjà explorées à la recherche d'une similitude structurelle (DOM) pour indiquer qu'elles ne contiennent pas de nouveaux liens ou de nouveaux contenus nécessitant des tests supplémentaires. Par exemple, sur un site commercial, il peut y avoir un catalogue composé de différentes pages individuelles pour un millier de produits différents, identiques dans tous les autres aspects. Il est généralement inutile d'examiner toutes ces pages. Le filtrage basé sur la similitude DOM peut réduire *considérablement* la durée de l'examen. Par défaut, les deux options sont sélectionnées. Après l'examen, vous devez contrôler l'onglet Filtré des résultats de l'examen afin de vérifier si certaines demandes n'ont pas été exclues de l'examen par erreur. Si c'est le cas, essayez d'utiliser l'option "Filtrer moins de pages", qui maintient un niveau inférieur constant de filtrage, ou désactivez en même temps l'option Filtrage en fonction de la structure de page (DOM). L'onglet Filtré des résultats contient trois types d'éléments filtrés : • **DOM identique** : Cela signale une page qui a été éliminée de l'examen parce que sa structure (DOM) est similaire à celle d'une page déjà explorée, et qu'elle ne contient probablement pas de nouveaux éléments à tester. • **DOM probablement identique** : Une requête n'a pas été envoyée car AppScan estime que la réponse présente une structure (DOM) identique à celle d'une page déjà explorée et qu'elle ne contient probablement aucun élément à tester. • **Corps similaire** : Demande (provenant d'une page qui n'a *pas* été filtrée en raison d'un élément DOM similaire) exclue de l'examen car le contenu du corps de la réponse est identique à celui d'une demande précédemment explorée. Après l'examen, vous devez contrôler l'onglet Filtré des résultats de l'examen afin de vérifier si certaines demandes n'ont pas été exclues de l'examen par erreur. Si tel est le cas, vous devez décocher l'option de filtrage des pages probablement en double (option suivante) ou désactiver en même temps l'option Filtrage en fonction de la structure de page DOM.
Filtrer les pages susceptibles d'être identiques en fonction de leur structure (DOM)	Ce paramètre filtre les pages avec un "DOM probablement identique" lors de l'examen (voir description ci-dessus). Si des demandes uniques sont filtrées par erreur en dehors de l'examen, vous devez désactiver cette option.
Limites de l'examen	
Limite pour les chemins d'accès redondants	AppScan n'accède pas au même chemin plus que le nombre de fois indiqué. Un chemin particulier peut être visité plusieurs fois s'il apparaît avec différents paramètres. Cette limite est principalement utile pour les scripts. Cette option est désélectionnée par défaut, car dans la plupart des cas, la sélection de la case à cocher ci-dessus, **Filtrage en fonction de la structure de page (DOM)**, permet de contrôler la durée de l'examen de façon satisfaisante.
Limite de profondeur de clic	AppScan n'examine pas les pages qui sont accessibles en cliquant sur un nombre de liens supérieur à la valeur indiquée.
Limite du total de pages	Si cette option est sélectionnée, AppScan n'accède pas à plus de pages que ce nombre maximal défini. Remarquez que chaque page peut contenir de nombreuses URL.
Autres paramètres	
Codage	En général, AppScan détecte automatiquement la méthode de codage de l'application ; par conséquent, la fonction de **détection automatique** est sélectionnée par défaut. Si le contenu des réponses figurant dans les résultats de l'examen semble erroné, cela peut signifier que la méthode de codage n'a pas été correctement identifiée. Pour résoudre ce problème, sélectionnez la méthode de codage appropriée dans la liste déroulante.

Paramètre	Détails
Agent d'utilisateur	L'en-tête agent d'utilisateur dans une requête HTTP indique au serveur quel type de client envoie la requête, ce qui peut affecter le contenu renvoyé par le serveur. Par exemple, certains contenus spécifiques aux téléphones mobiles ne sont envoyés que lorsque l'agent d'utilisateur est un navigateur de téléphone mobile. Pour qu'AppScan puisse tester ce type de contenu, vous devez le configurer pour qu'il envoie l'en-tête agent d'utilisateur approprié. En général, AppScan détecte automatiquement l'agent d'utilisateur ; par conséquent, la fonction de **détection automatique** est sélectionnée par défaut. Cependant, si vous utilisez un navigateur différent du navigateur intégré, et si vous n'enregistrez pas de procédure de connexion, d'opération en plusieurs étapes ou d'exploration manuelle, AppScan ne peut pas détecter l'agent d'utilisateur automatiquement, et vous devez le sélectionner manuellement. Pour modifier l'agent d'utilisateur, sélectionnez un agent dans la liste déroulante. Pour entrer du contenu personnalisé, cliquez sur le bouton **Editer** et saisissez le contenu. A la fermeture de la boîte de dialogue, le nom du bouton devient **Agent d'utilisateur personnalisé**. **Remarque :** Si vous modifiez le navigateur par défaut, consultez les conditions décrites à la rubrique «Modification du navigateur par défaut», à la page 334.

En-tête agent d'utilisateur :

La présente section décrit l'en-tête agent d'utilisateur envoyé pour chaque agent d'utilisateur, et l'utilisation de la "détection automatique".

Si nécessaire, vous pouvez éditer le contenu des en-têtes d'agent d'utilisateur en cliquant sur le bouton Editer. L'agent d'utilisateur mis à jour apparaît ensuite comme "agent d'utilisateur personnalisé".

Vous pouvez sélectionner un en-tête en cliquant sur le bouton Agent d'utilisateur, et éditer son contenu en cliquant sur le bouton Editer. Une fois que vous éditez son contenu, le nom du bouton devient "Agent d'utilisateur personnalisé". Le contenu de l'agent d'utilisateur personnalisé n'est enregistré avec l'examen (et transféré aux autres ordinateurs avec l'examen) que s'il est l'agent d'utilisateur sélectionné au moment où l'examen est enregistré.

Onglet Basée sur les actions

Configuration des examens > Options d'exploration > Onglet Basée sur les actions.

Dans cet onglet, vous pouvez configurer les paramètres ayant un impact sur l'exploration basée sur les actions. Cet onglet est actif si la méthode d'exploration basée sur les actions est sélectionnée dans l'onglet principal.

Paramètre	Détails
Général	
Dépassement du délai d'exploration (minutes)	La limite de temps par défaut pour l'exploration basée sur les actions d'un site est de 30 minutes. Après ce délai, l'étape d'exploration s'arrête même si le site n'a pas été entièrement couvert. Si AppScan omet des parties importantes du site pendant cette période, vous pouvez augmenter ce délai.

Paramètre	Détails
Attente minimum avant l'appel d'actions sur une page (millisecondes)	AppScan tente d'identifier qu'une page a chargé complètement avant de commencer à l'explorer. Si vous ajoutez une période d'attente minimale ici, AppScan utilise toujours *ce* paramètre comme période d'attente minimale (même s'il détecte que page a chargé), mais attendra plus longtemps que cette période s'il détecte que la page n'a *pas* chargé. **Conseil :** Si, lorsque vous vérifiez les Données d'exploration, vous voyez qu'AppScan n'a pas réussi à exécuter toutes les actions possibles sur une page, cela peut indiquer que son temps d'attente dynamique était trop court. Vous pouvez également le voir pendant l'analyse si vous autorisez le navigateur : 1. Allez dans **Outils > Options > Avancé** 2. Repérez `SessionManagement:ShowActionBasedPlayerWindow`, et définissez son paramètre sur `True`. 3. Effectuez une analyse. Le navigateur s'ouvre pendant l'analyse, et vous pouvez regarder pendant que AppScan explore votre site. Si vous remarquez qu'il passe à une nouvelle page avant que la page actuelle soit complètement chargée, l'augmentation du temps d'attente peut résoudre le problème. **Remarque :** La modification de ce paramètre peut avoir un impact sur le Temps d'exploration. Il sera alors peut-être pertinent d'augmenter le Dépassement du délai d'exploration (ci-dessus).
Détection automatique du chargement de page dynamique	Par défaut, AppScan détecte activement le contenu de page dynamique et traite la page comme telle. Dans de rares occasions, cela peut empêcher la page de charger correctement et, par conséquent, avoir un impact sur la couverture de l'analyse. **Conseil :** Pour identifier ce problème : 1. Allez dans **Outils > Options > Avancé** 2. Repérez `SessionManagement:ShowActionBasedPlayerWindow`, et définissez son paramètre sur `True`. 3. Effectuez une analyse. Le navigateur s'ouvre pendant l'analyse, et vous pouvez regarder pendant que AppScan explore votre site. Si vous remarquez que des pages qui chargent correctement dans un navigateur classique ne chargent pas correctement pendant l'analyse, décochez cette case pour éventuellement résoudre le problème.
Filtres	
Ignorer des actions sur des éléments DOM identiques	AppScan identifie les actions qu'il a déjà exécutées sur une page précédente en fonction de divers critères. Si votre site comprend *différentes* actions qui peuvent sembler identiques en raison de leur élément DOM, AppScan peut les ignorer de manière erronée. Si cela se produit, décochez cette case. **Remarque :** AppScan effectue *plusieurs fois* des actions identiques, pour vérifier qu'elles sont bien identiques, avant de décider d'ignorer de futures itérations.
Analyser et ignorer des actions redondantes	Lorsqu'AppScan identifie des actions qui semblent similaires, il compare leurs pages générées. Si, après quelques itérations, les résultats semblent tous similaires AppScan ignore les futures actions similaires en les considérant comme redondantes. Si votre site comprend plusieurs pages dont la seule différence est leur contenu, comme un nouveau site, cette fonction peut considérablement réduire la durée de l'examen et nous vous invitons à cocher cette case.
Actions à ignorer	Il s'agit d'une liste d'actions qu'AppScan va ignorer puisqu'elles peuvent avoir un impact négatif sur l'analyse, ou même sur l'application. Les actions à ignorer sont identifiées en fonction des attributs `Id`, `name` ou `ng-model` de l'élément DOM pour l'action. Toute action dont les attributs `Id`, `name` ou `ng-model` de l'élément DOM contiennent un des mots de la liste sera éliminée de l'analyse. Vous pouvez **Ajouter**, **Editer** et **Supprimer** des éléments dans cette liste.

Onglet Basée sur les demandes

Configuration des examens > Options d'exploration > Onglet Basée sur les demandes.

Dans cet onglet, vous pouvez configurer les paramètres ayant un impact sur l'exploration basée sur les demandes. Cet onglet est actif si la méthode d'exploration basée sur les demandes est sélectionnée dans l'onglet principal.

- Les options **JavaScript** et **Flash** déterminent si AppScan doit ignorer ou examiner ces scripts.
- L'option **Mode d'exploration** détermine si AppScan explore tous les liens d'une page avant de passer à la page suivante ou s'il explore chaque nouveau lien au fur et à mesure qu'il est détecté.
- L'option **WebSphere Portal** permet de configurer le client pour reconnaître un codage de serveur spécifique et envoyer un en-tête d'agent utilisateur.
- **Flash**

Paramètre	Détails
JavaScript	
Faire une analyse syntaxique du code JavaScript pour reconnaître les adresses URL	AppScan fait une analyse syntaxique des codes JavaScript en tant que données de texte pour collecter des liens.
Exécuter JavaScript pour reconnaître les adresses URL et le contenu dynamique	AppScan exécute le code JavaScript et analyse les résultats pour collecter des liens, y compris les liens dynamiques qui ne peuvent pas toujours être détectés par une simple analyse syntaxique. (Cette option utilise davantage de ressources système que l'analyse syntaxique.) **Remarque :** Cette option est désormais désélectionnée par défaut, en raison de l'efficacité éprouvée de l'exécution JavaScript *basée sur les actions*.
Exécuter JavaScript lors de la reconnexion	Si la page de connexion de l'application utilise le code JavaScript, cette case doit être cochée pour permettre à AppScan de pouvoir se connecter lors de l'examen.
Mode d'exploration	
Largeur en premier	(Par défaut) AppScan effectue l'exploration page par page en explorant tous les liens d'une page avant de passer à la page suivante. Il est recommandé de ne pas modifier la sélection par défaut de cette option (Largeur en premier), sauf si vous avez connaissance de limitations dans votre application qui nécessitent de visiter les liens dans un ordre spécifique.
Profondeur en premier	AppScan effectue l'exploration lien par lien en explorant chaque nouveau lien au fur et à mesure qu'il est détecté. Si vous modifiez la méthode d'exploration en indiquant **Profondeur en premier**, vous devez également modifier AppScan pour qu'il n'utilise qu'une seule unité d'exécution lors de l'exploration (dans Configuration > Vue Communication et proxy).
Portail WebSphere	

Paramètre	Détails
Analyse de portail Enable WebSphere	Dans le cas d'un site WebSphere Portal, AppScan doit recevoir les informations de décodage d'adresse URL en provenance du site afin d'optimiser l'examen et de construire une arborescence d'application utile. Pour activer le décodage, sélectionnez **Activer l'examen WebSphere Portal**. Si l'adresse URL de la racine de contexte ne suit pas le format par défaut, cliquez sur **Ajouter l'adresse URL de la racine de contexte** pour ajouter une ou plusieurs adresses URL de racine de contexte. **Conseil :** Si vous n'êtes pas sûr de connaître l'adresse URL de racine de contexte de votre portail : 1. Sur l'ordinateur sur lequel WebSphere Portal est installé, ouvrez le fichier `wkplc.properties` dans le répertoire `wp_profile_root/ConfigEngine/properties`. 2. La valeur de la racine de contexte est indiquée dans la propriété `WpsContextRoot`. **Conseil :** Lors de l'examen d'un site WebSphere Portal, il est recommandé d'utiliser le modèle d'examen WebSphere Portal prédéfini qui est configuré à cette fin.
Flash	
Faire une analyse syntaxique du code Flash pour reconnaître les adresses URL	AppScan fait une analyse syntaxique des codes Flash en tant que données de texte pour collecter des liens.
Lire les fichiers Flash pour détecter les vulnérabilités potentielles	AppScan *lit* les fichiers Flash et analyse les résultats pour collecter les liens, y compris les liens dynamiques qui ne peuvent pas être reconnus par une simple analyse syntaxique. (Cette option utilise davantage de ressources système que l'analyse syntaxique.) Adobe Flash Player for Internet Explorer, Version 9.0.124.0 ou suivante est requis. Si aucune version prise en charge n'est installée, un avertissement s'affiche en regard de cette case lorsqu'elle est cochée et Flash ne peut pas s'exécuter. Voir «Contenus Flash», à la page 326. Si vous disposez d'Adobe Flash Player Version 10.1 ou suivante, vous risquez d'obtenir un message indiquant que ce produit doit être configuré pour pouvoir fonctionner avec AppScan. Voir «Configuration de Flash Player», à la page 7. Lorsque l'exécution Flash est sélectionnée, trois limites d'exécution Flash sont également configurables. Elles sont les suivantes : • **Limite de profondeur :** Nombre maximal de clics depuis l'écran initial qui peuvent être effectués avant que l'examen d'un film Flash spécifique s'arrête et que l'examen se poursuive. • **Limite de clic :** Nombre total maximal de clics qui peuvent être effectués avant que l'examen d'un film Flash spécifique s'arrête et que l'examen se poursuive. • **Limite d'écran :** Nombre maximal d'états Flash uniques autorisés avant que l'examen d'un film Flash spécifique s'arrête et que l'examen se poursuive.

Vue Paramètres et cookies

Vue Paramètres et cookies de la boîte de dialogue Configuration.

Cette vue permet de gérer quatre fonctions principales :

- Affectation d'un traitement spécial à certains paramètres et cookies
- Contrôle du traitement par défaut des paramètres et des cookies ("réglage de la redondance")
- Définition de paramètres et de cookies ayant un format spécial que AppScan risque de ne pas reconnaître de façon isolée
- Définition d'en-têtes personnalisés

Paramètre	Description	Voir
Onglet Paramètres et cookies	Permet d'afficher, d'ajouter, d'éditer et de supprimer des paramètres globaux nécessitant un traitement autre que le traitement par défaut. Par exemple, votre application peut avoir des paramètres et des cookies pour lesquels vous ne souhaitez pas qu'AppScan manipule les valeurs lors des tests. Afin de vous assurer que AppScan ne change pas ces paramètres et ces cookies, excluez-les des tests. Par exemple, votre application peut verrouiller une session utilisateur si certaines valeurs des cookies ou des paramètres sont modifiées. Vous pouvez exclure ces paramètres de la manipulation. Si vous ne les excluez pas, il est possible que AppScan ne parvienne pas à terminer l'examen car ces cookies verrouilleront AppScan hors de l'application. Lors de l'étape d'exploration, AppScan détecte automatiquement les cookies et les paramètres HTML pouvant être des ID session et les ajoute à cette liste dans cet onglet. Vous pouvez manuellement ajouter des cookies et des paramètres que vous savez être des ID session. Les colonnes de cet onglet sont définies dans le tableau ci-dessous. **Remarque :** Le bouton **Masquer/Afficher les éléments modèles** permet de filtrer les éléments provenant à l'origine du modèle de l'examen, et qui peuvent ne pas être pertinents pour l'examen en cours.	«Définition de paramètre», à la page 78
Onglet Paramètres personnalisés	Permet d'ajouter, d'éditer et de supprimer des paramètres ayant un format personnalisé que AppScan risque de ne pas reconnaître.	«Onglet Paramètres personnalisés», à la page 86
Onglet En-têtes personnalisés	Vous permet de définir des formats d'en-tête HTTP non standard (personnalisés). AppScan doit pouvoir identifier les paramètres du contenu de la réponse et les ajouter correctement dans les en-têtes qu'il envoie au site, afin d'être en mesure de tester le site de manière efficace.	«Onglet En-têtes personnalisés», à la page 88
Valeurs par défaut du réglage de la redondance	Ce lien (en bas de l'onglet Paramètres et cookies) vous permet d'accéder au réglage de redondance *par défaut* appliqué à tous les paramètres et de le modifier, qu'il ait été découvert par AppScan ou défini par l'utilisateur. **Remarque :** La modification du réglage de redondance spécifique à un paramètre individuel fait partie de la section «Définition de paramètre», à la page 78. Les modifications apportées aux valeurs par défaut ne s'appliquent pas rétroactivement aux paramètres ayant déjà été définis. Cela doit se faire manuellement pour chaque paramètre.	«Réglage de la redondance», à la page 83

Zones de l'onglet Paramètres et cookies

Le tableau suivant récapitule les zones de cet onglet.

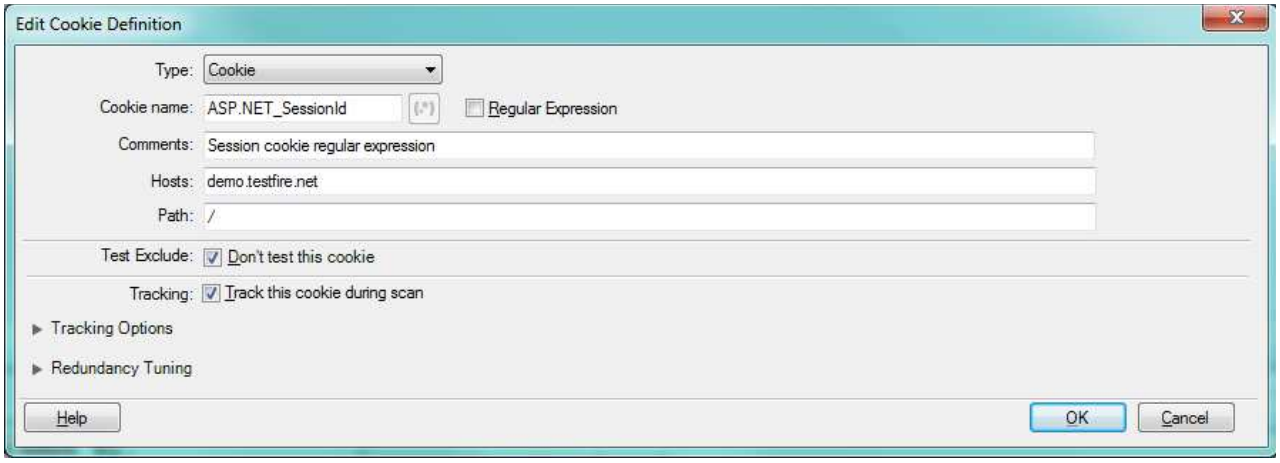
En-tête	Options et description
Type	Paramètre /cookie/ paramètre personnalisé
Nom	

En-tête	Options et description
Suivi	Comment suivre ce paramètre ou cookie : • En tant que valeur de connexion • En tant que valeur dynamique • En tant que valeur fixe • Aucun suivi Pour plus d'informations, voir «ID session», à la page 81.
Exclusion de test	Indique si ce paramètre/cookie doit être exclu du test pendant la phase de Test de l'examen.
Réglage de la redondance	• Valeur par défaut : Le réglage de la redondance par défaut est appliqué à cet élément. • Personnalisation : Le réglage de la redondance de cet élément est différent de la valeur par défaut en cours
Source	Indique à partir de quelle source AppScan s'est procuré cet élément : • Modèle d'examen : A pour origine le modèle d'examen • ID session de connexion : A partir de la séquence de connexion enregistrée par l'utilisateur • Séquence en plusieurs étapes variable : A partir d'une séquence enregistrée par l'utilisateur • Scan Expert [nom de module] : A partir du module Scan Expert indiqué • Optimiseur d'exploration : A partir de l'extension Optimiseur d'exploration • Défini par l'utilisateur

Définition de paramètre

Procédure

Pour ajouter une nouvelle définition, cliquez sur  (ou, pour éditer un paramètre existant, sélectionnez-le et cliquez sur ).
La boîte de dialogue **Ajouter une définition de paramètre** apparaît.



Paramètre	Description
Type	Sélectionnez un type de paramètre dans la liste déroulante : **Paramètre :** Tous les paramètres correspondant à ce nom sont inclus dans la définition. **Cookie :** Tous les cookies correspondant à ce nom sont inclus dans la définition. **Paramètre personnalisé :** Il s'agit d'un paramètre personnalisé (sélectionnez l'un des paramètres personnalisés dans la liste déroulante *Nom*).
Nom	Nom du paramètre ou du cookie. Cochez la case adjacente si le nom que vous entrez est une expression régulière. Si vous avez effectué cette opération, vous pouvez aussi ouvrir l'outil Expression Test PowerTool : pour ce faire, cliquez sur  , qui vous aide à vérifier la syntaxe de l'expression régulière. Pour plus de détails, voir «Noms des paramètres», à la page 81.
Commentaires	Vous pouvez éventuellement ajouter dans cette zone un commentaire sur le paramètre pour votre propre référence.
Hôtes	**Si un hôte est spécifié :** Utilisez ce paramètre uniquement pour l'hôte spécifié. **S'il est vide :** Utilisez cet ID session pour tous les hôtes.
Chemin d'accès	Si l'application fournit des cookies de même nom à partir de différents composants de l'application, vous pouvez les différencier en définissant le chemin d'accès à chacun d'eux. Si vous indiquez un blanc ou /, toutes les occurrences du cookie seront incluses.
Exclusion de test	Cochez cette case uniquement si vous êtes sûr de ne pas vouloir que AppScan teste ce paramètre.
Suivi	Ce paramètre indique à AppScan que ce paramètre ou cet ID session doit être mis à jour lors de l'examen chaque fois qu'une nouvelle valeur est définie par l'application, de sorte qu'un cookie/paramètre valide soit toujours envoyé à l'application.

Paramètre	Description
Options de suivi...	(Cliquez sur le lien pour ouvrir cette section supplémentaire de la boîte de dialogue.) Ces options vous permettent d'affiner le mode de traitement du paramètre ou cookie qui fait l'objet d'un suivi. **Type de suivi** • **Valeur de connexion :** (Par défaut et recommandé) Les demandes envoyées à l'application qui comprennent ce paramètre utilisent la dernière valeur du paramètre reçue à la fin du processus de connexion, à l'exception de la *demande En session*. **Conseil :** Pour effectuer le suivi du paramètre *dans la réponse En session*, vous devez définir son type sur **Dynamique**, *et non Valeur de connexion*, et vérifier que **Configuration > Avancée > Gestion de session : Analyser la page En session** est défini sur **True** (sa valeur par défaut). **Remarque :** Si vous enregistrez des étapes de connexion dans le cadre d'une séquence en plusieurs étapes, la définition d'un paramètre reçu en tant que valeur de connexion ne va pas affecter son mode d'utilisation. Il sera toujours considéré comme dynamique. • **Valeur dynamique :** Les demandes envoyées à l'application qui comprennent ce paramètre utilisent la valeur la plus récente reçue de l'application. • **Valeur fixe :** Les demandes envoyées à l'application qui comprennent ce paramètre utilisent toujours la valeur que vous entrez dans la zone Valeur. Pour plus d'informations, voir «ID session», à la page 81. **Envoyer un cookie sur toutes les demandes :** Lorsque ce paramètre est sélectionné, le cookie est inclus dans toutes les demandes, même si cela n'est pas indiqué explicitement par l'application. **Traiter comme groupe :** Si le nom de cookie est une expression régulière, indiquez si les autres noms de cookie qui correspondent à l'expression régulière doivent être traités en tant que groupe (et par conséquent, si une mise à jour du nom et de la valeur doit être effectuée en cas de modifications) ou en tant que cookies distincts. **Schéma de réponse :** En règle générale, AppScan met à jour les valeurs de paramètre ou de cookie en fonction du contenu de liens extrait de la réponse (paramètres) ou de l'en-tête de cookie (cookies). Si AppScan ne peut pas extraire la valeur sans aide, vous pouvez indiquer l'expression régulière dont AppScan pourra se servir pour extraire la valeur de la réponse brute. L'expression régulière doit contenir au moins un groupe, et AppScan peut extraire la première correspondance. • **Filtre URL :** Si vous savez que le paramètre/cookie n'apparaît que dans une URL spécifique, vous pouvez améliorer l'efficacité du scan en définissant ici le chemin URL complet. • **Codage :** Si la valeur extraite doit être codée lorsqu'elle est collée dans la demande, définissez la méthode ici. Si vous n'êtes pas certain du codage à utiliser, sélectionnez **En fonction du contexte**, sinon, il est préférable de sélectionner le codage *correct*. Les options sont les suivantes : Aucun, En fonction du contexte, URL, XML, JSON. • **Correspondance :** Sélectionnez **En-tête et corps** (par défaut) ou **Corps uniquement**.
Réglage de la redondance...	(Cliquez sur le lien pour ouvrir cette section supplémentaire de la boîte de dialogue.) Ces quatre cases à cocher permettent de régler de façon précise de quelle manière AppScan est associé aux modifications apportées au paramètre (ou son existence même) lors des étapes d'exploration et de test de l'examen. Voir «Réglage de la redondance», à la page 83.

Identificateurs définissant un paramètre ou un cookie

Un paramètre ou un cookie est reconnu comme unique en fonction de certains identificateurs. En conséquence, vous ne pouvez pas définir deux paramètres ou cookies ou plus avec les mêmes identificateurs. Le tableau ci-dessous indique les identificateurs pour chaque type d'entrée.

Paramètre	Nom du paramètre, indique s'il s'agit d'une expression régulière, hôte
Cookie	Nom du paramètre, indique s'il s'agit d'une expression régulière, hôte, chemin
Paramètre personnalisé	Nom extrait (le cas échéant), nom de référence, hôte, index d'occurrence

Noms des paramètres
Procédure

Dans la zone de saisie **Nom** entrez une expression régulière qui corresponde au nom du paramètre ou du cookie :

- Tout texte est sensible à la casse. Ajoutez `(?i)` à l'expression régulière pour qu'elle ne soit pas sensible à la casse.
- Toutes les chaînes de l'expression régulière sont considérées comme partielles. Vous n'avez pas à ajouter `(.*)`

Un nombre de définitions par défaut est fourni.

Type	Valeur	Includes
Paramètre	**__VIEWSTATE**	paramètres contenant cette chaîne dans leur nom
Paramètre et cookie	**^CFID**	paramètres et cookies dont le nom commence par CFID ou cfid
Paramètre et cookie	**Jeton**	paramètres et cookies dont le nom contient "Jeton"

Remarque : Une expression régulière (regexp) est une chaîne décrivant un ensemble de chaînes selon une syntaxe précise. L'Expression Test PowerTool (**Outils > Test d'expression**) peut être utile pour vérifier la syntaxe de vos expressions régulières.

Si vous avez besoin d'aide pour écrire des expressions régulières, reportez-vous au lien suivant : http://www.regular-expressions.info/quickstart.html

ID session
Si le site utilise des ID session restreints dans le temps (sous la forme de cookies ou de paramètres), il rejette les demandes contenant des jetons ayant expiré, occasionnant l'échec des tests du site.

Pour cette raison, AppScan doit pouvoir reconnaître et gérer les paramètres ou cookies HTML qui sont des *ID session* restreints dans le temps. AppScan attribue aux ID session les valeurs disponibles les plus récentes, empêchant ainsi l'expiration de la session de l'application.

Vous pouvez déterminer si AppScan doit automatiquement mettre à jour la valeur d'un ID session. Définissez le **Statut** d'un ID session :

- **Valeur de connexion :** (Recommandée) Lorsqu'une demande de test contenant ce paramètre est envoyée, AppScan met automatiquement à jour l'ID session avec la dernière valeur reçue de l'application une fois que la connexion a abouti avant la demande En session.

  Conseil : Pour effectuer le suivi du paramètre *dans la réponse En session*, vous devez définir son type sur **Dynamique**, *et non Connexion*, et vérifier que **Configuration > Avancée > Gestion de session : Analyser la page En session** est défini sur **True** (sa valeur par défaut).

  Ce statut est recommandé pour la plupart des paramètres et des cookies, à moins qu'il n'y ait un besoin particulier de définir une valeur spécifique. Toutefois, lorsque des ID session de valeur de connexion sont utilisés, la valeur peut expirer alors qu'elle se trouve dans la base de données.

Remarque : Si vous enregistrez des étapes de connexion dans le cadre d'une séquence en plusieurs étapes, la définition d'un paramètre reçu en tant que valeur de connexion ne va pas affecter son mode d'utilisation. Il sera toujours considéré comme dynamique. Pour plus d'informations, voir «Vue Opérations en plusieurs étapes», à la page 95.

Pour mettre à jour un ID session suivi dans la base de données : Avant d'exécuter l'examen, visitez l'URL où l'ID session est envoyé. Un nouvel ID session sera envoyé, avec une valeur mise à jour.

- **Dynamique :** AppScan met automatiquement à jour la valeur de l'ID session lors de l'étape de test, selon les nouvelles valeurs définies par l'application Web dans les tests précédents (par exemple, comme avec Shadow Cookies).

  Sélectionnez *Dynamique* uniquement si vous savez que votre application Web impose des mesures de sécurité exigeant qu'un ID session spécifique soit mis à jour lors de certaines procédures.

- **Fixe :** Conserve une valeur fixe. Définissez une valeur fixe pour l'ID session si la sécurité de votre application Web a besoin de cet ID session pour conserver cette valeur.

Lors de l'étape d'exploration, AppScan détecte automatiquement des cookies et des paramètres HTML pouvant être des ID session et les ajoute à une liste. Vous pouvez manuellement ajouter les cookies et les paramètres que vous savez être des ID session lorsque vous configurez l'examen.

ID session dans l'URL :

Comment suivre un ID session incorporé dans le chemin d'accès de l'URL.

Pourquoi et quand exécuter cette tâche

Si AppScan ne suit pas les ID session correctement, il risque de perdre fréquemment la session. Cette section explique comment suivre un ID session incorporé dans l'URL.

ID session : `abc34f3fa135`

URL contenant un ID session : `http://domain.name/dir/subdir/abc34f3fa135/anotherdir?param=val`

Procédure

1. Créer une règle pour reconnaître ce paramètre personnalisé :
   a. Sélectionnez **Configuration des examens > Paramètres et cookies > onglet Paramètres personnalisés**.
   b. Cliquez sur  pour ajouter un nouveau paramètre personnalisé.
   c. Dans le champ Nom de référence, entrez un nom pour la règle du paramètre personnalisé.
   d. Dans le champ Schéma, entrez une expression régulière décrivant le format du paramètre. Exemple : `(abc[a-zA-Z0-9]+)`
   e. Laissez l'index des groupes de valeurs et l'index des groupes de noms inchangés.
   f. Dans le champ Emplacement, sélectionnez **Chemin d'accès**.
   g. Cliquez sur **OK** pour enregistrer les modifications.
2. Configurer AppScan pour suivre ce paramètre personnalisé :
   a. Sélectionnez **Configuration des examens > Paramètres et cookies > onglet Paramètres et cookies**.
   b. Cliquez sur  pour ajouter un nouveau paramètre.
   c. Définissez le type sur **Paramètre personnalisé**.
   d. Sélectionnez le nom de référence que vous avez affecté à l'étape précédente.
   e. Sélectionnez la case à cocher **Suivre ce paramètre lors de l'examen**.

f. Définissez le type de suivi sur **Valeur de connexion** ou **Dynamique**, comme il convient.
g. Cliquez sur **OK** pour enregistrer les modifications.

3. Si la séquence de connexion enregistrée inclut une URL contenant cet ID session dans le chemin d'accès, vous devez réenregistrer la connexion pour permettre à AppScan de suivre l'ID session.
4. Effectuez un nouvel examen complet ou une nouvelle exploration, selon les besoins.

Réglage de la redondance

Un réglage précis de la redondance peut réduire de façon significative la durée de l'examen.

AppScan essaye de ne pas envoyer plus d'une demande lorsqu'il est clair qu'elles n'en dégageront pas d'informations supplémentaires. Dans de nombreux cas, la différence de valeur d'un paramètre est insignifiante et il n'est pas nécessaire d'envoyer plusieurs demandes alors que tous les autres paramètres sont identiques et que seule cette valeur diffère.

Prenez en compte les deux demandes suivantes :

```
.../doAction.pl?action=buy&timestamp=14:00&n=1

.../doAction.pl?action=buy&timestamp=15:30&n=1
```

La seule différence entre ces deux demandes est leur valeur d'horodatage.

Dans la plupart des cas, il suffit d'envoyer une seule demande à l'aide d'une des configurations et il n'est pas nécessaire d'envoyer les deux. Il est peu probable que la réponse à l'une des demandes révèle une faiblesse non révélée par l'autre. Vous devez donc configurer les paramètres de réglage de redondance pour le paramètre d'horodatage de sorte qu'en un tel cas une seule demande soit envoyée.

Voir aussi :

«Options du réglage de la redondance»

«Options par défaut du réglage de la redondance», à la page 84

«Modification des valeurs par défaut du réglage de la redondance», à la page 85

«Modification du réglage de la redondance pour un paramètre spécifique», à la page 85

Options du réglage de la redondance :

Réglage de la redondance pour les paramètres et les cookies avec les attributs spéciaux répertoriés dans la liste appelée en sélectionnant Configuration > Paramètres et Cookies.

Case à cocher	Lorsqu'elle est sélectionnée...

Explorer à nouveau l'URL chaque fois que le paramètre/cookie est ajouté ou supprimé.	Pendant l'étape d'exploration, traite les adresses URL qui se différencient uniquement par le fait que l'une inclut ce paramètre et l'autre non comme des adresses URL différentes et explore les deux.
	
	Par exemple, les *deux* adresses URL suivantes seront explorées :
	`...page.jsp`
	`...page.jsp?thisParam=Value`
	
	Si vous désélectionnez cette case à cocher, une seule demande sera envoyée dans ce type de situation, l'autre étant supprimée.

Case à cocher	Lorsqu'elle est sélectionnée...

Explorer à nouveau l'URL chaque fois que la valeur du paramètre/cookie change.	Pendant l'étape d'exploration, traite les adresses URL qui se différencient uniquement par le fait que l'une inclut ce paramètre et l'autre non comme des adresses URL différentes et explore les deux.
	
	Par exemple, les *deux* adresses URL suivantes seront explorées :
	`...page.jsp?thisParam=Value1`
	`...page.jsp?thisParam=Value2`
	
	Si vous désélectionnez cette case à cocher, une seule demande sera envoyée dans ce type de situation, l'autre étant supprimée.
	Remarque : Cette option ne s'applique pas lorsque le paramètre ou le cookie fait l'objet d'un suivi.

Répéter tous les tests de paramètre/cookie adjacent chaque fois que le paramètre/cookie est ajouté ou supprimé.	Pendant l'étape de test, traite les adresses URL qui se différencient uniquement par le fait que ce paramètre a été ajouté ou supprimé comme des adresses URL différentes et teste à nouveau les paramètres adjacents.
	
	Par exemple, dans le cas des deux adresses URL suivantes, *deux ensembles complets* de tests seront générés pour le paramètre adjacent, un pour chaque adresse URL.
	`...page.jsp?adjacentParam=<test_this>`
	`...page.jsp?adjacentParam=<test_this>&thisParam=Value`
	
	Si vous désélectionnez cette case à cocher, un seul ensemble de tests sera généré pour le paramètre adjacent.

Répéter tous les tests de paramètre/cookie adjacent chaque fois que la valeur du paramètre/cookie change.	Pendant l'étape de test, traite les adresses URL qui se différencient uniquement par la valeur de ce paramètre/cookie comme des adresses URL différentes et teste à nouveau les paramètres adjacents.
	
	Par exemple, dans le cas des deux adresses URL suivantes, *deux ensembles complets* de tests seront générés pour le paramètre adjacent, un pour chaque adresse URL.
	`...page.jsp?adjacentParam=<test_this>&thisParam=Value1`
	`...page.jsp?adjacentParam=<test_this>&thisParam=Value2`
	
	Si vous désélectionnez cette case à cocher, un seul ensemble de tests sera généré pour le paramètre adjacent.
	Remarque : Cette option ne s'applique pas lorsque le paramètre ou le cookie fait l'objet d'un suivi.

Voir aussi :

«Réglage de la redondance», à la page 83

Options par défaut du réglage de la redondance :

Réglage de la redondance pour les paramètres et les cookies avec les attributs spéciaux répertoriés dans la liste appelée en sélectionnant Configuration > Paramètres et Cookies.

Si le module Explore Optimization eXtension n'est pas exécuté, le réglage par défaut du réglage de la redondance est celui-ci :

Case à cocher	Valeur par défaut
Explorer à nouveau l'URL chaque fois que le paramètre/cookie est ajouté ou supprimé.	✓
Explorer à nouveau l'URL chaque fois que la valeur du paramètre/cookie change.	✓

Case à cocher	Valeur par défaut
Répéter tous les tests de paramètre/cookie adjacent chaque fois que le paramètre/cookie est ajouté ou supprimé.	
Répéter tous les tests de paramètre/cookie adjacent chaque fois que la valeur du paramètre/cookie change.	

Si le module Explore Optimization eXtension est activé et exécuté, le réglage de la redondance pour les paramètres de navigation est *augmenté*, tandis que le paramétrage par défaut (appliqué aux paramètres non navigationnels) est *décru*.

Case à cocher	Navigation	Par défaut
Explorer à nouveau l'URL chaque fois que le paramètre/cookie est ajouté ou supprimé.		
Explorer à nouveau l'URL chaque fois que la valeur du paramètre/cookie change.		
Répéter tous les tests de paramètre/cookie adjacent chaque fois que le paramètre/cookie est ajouté ou supprimé.		
Répéter tous les tests de paramètre/cookie adjacent chaque fois que la valeur du paramètre/cookie change.		

Voir aussi :

«Réglage de la redondance», à la page 83

Modification des valeurs par défaut du réglage de la redondance :

Le paramètre de réglage des redondances est appliqué à tous les ajouts à la liste dans Configuration > Paramètres et cookies, sauf s'ils ont été modifiés manuellement.

Procédure

1. En bas de l'onglet Paramètres et cookies, cliquez sur **Valeurs par défaut du réglage de la redondance**.

   La boîte de dialogue Valeurs par défaut du réglage de la redondance s'ouvre. Ses options sont décrites dans «Options du réglage de la redondance», à la page 83.
2. Réglez les paramètres selon les besoins (pour plus d'informations, voir «Options du réglage de la redondance», à la page 83).

   Les modifications effectuées ici sont appliquées à tous les nouveaux paramètres au fur et à mesure qu'ils sont découverts par AppScan ou définis par l'utilisateur.

   Remarque : Les modifications apportées aux valeurs par défaut ne s'appliquent *pas* rétroactivement aux paramètres ayant déjà été définis. Cela doit se faire manuellement pour chaque paramètre.

Que faire ensuite

Voir «Options du réglage de la redondance», à la page 83.

Modification du réglage de la redondance pour un paramètre spécifique :
Procédure

1. Dans l'onglet Paramètres et cookies, sélectionnez le paramètre et cliquez sur  .

La boîte de dialogue **Définition des paramètres** s'affiche (pour plus d'informations, voir «Définition de paramètre», à la page 78).

2. En bas de la boîte de dialogue, cliquez sur **Options supplémentaires**.

   Les options Réglage de la redondance s'ouvrent (pour plus d'informations, voir «Options du réglage de la redondance», à la page 83).

Que faire ensuite

Voir «Options du réglage de la redondance», à la page 83.

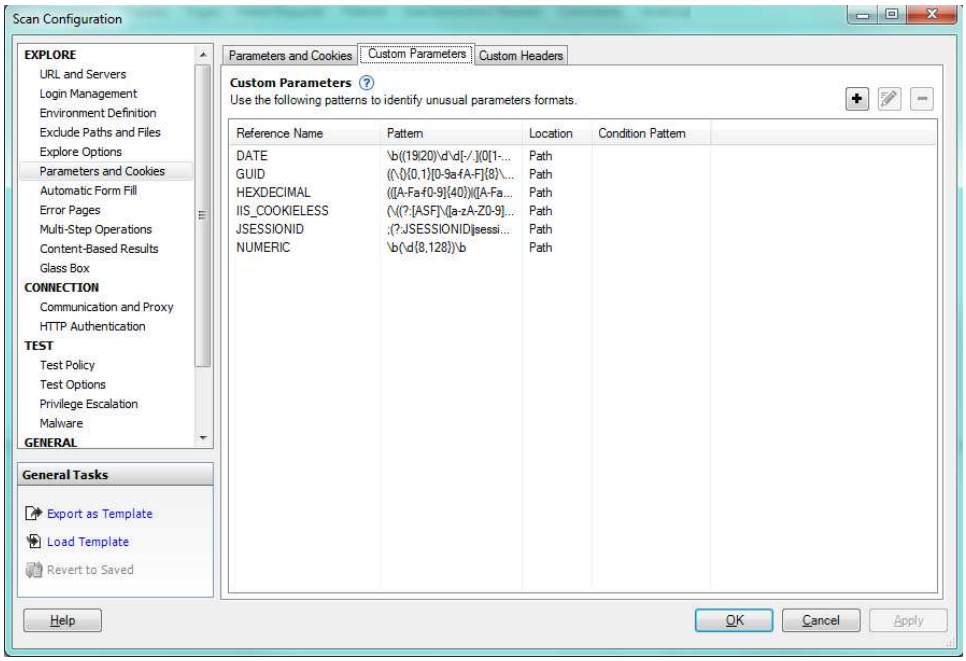
Onglet Paramètres personnalisés

Onglet Paramètres personnalisés de la vue Paramètres et cookies de la boîte de dialogue Configuration.

Pourquoi et quand exécuter cette tâche

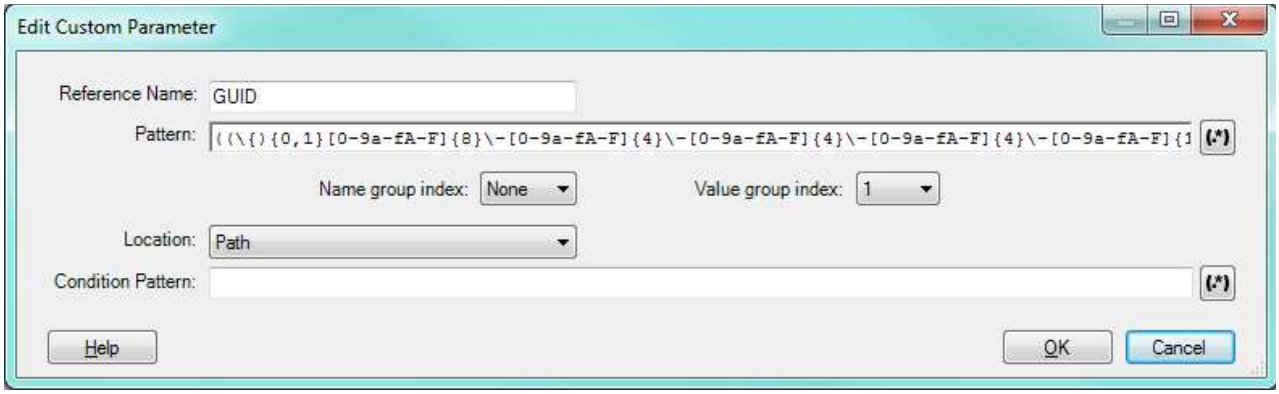
Le deuxième onglet de la vue Exploration : La vue Paramètres et cookies permet de créer et de gérer des paramètres personnalisés avec des formats qu'AppScan ne pourrait pas reconnaître automatiquement.

AppScan reconnaît automatiquement les paramètres au format HTML standard, mais si des paramètres en utilisent d'autres (par exemple, dans le chemin d'accès ou dans un autre paramètre), vous devez les définir à AppScan afin qu'il puisse les reconnaître, les suivre et les manipuler lors de l'examen.



Procédure

Pour définir un nouveau paramètre personnalisé, cliquez sur ; pour modifier une définition existante, sélectionnez le paramètre dans le tableau et cliquez sur .
La boîte de dialogue **Ajouter/Editer un paramètre personnalisé** s'ouvre. Ses zones et options sont décrites dans le tableau suivant.



Paramètre	Description
Nom de référence	Donnez au paramètre un nom facilement reconnaissable. Les paramètres personnalisés apparaissent dans l'arborescence des données d'application avec le préfixe "__patternParameter__" suivi du nom du paramètre.
Schéma	Expression régulière contenant un ou plusieurs groupes définissant le paramètre. Un "groupe" est une section de l'expression régulière délimitée par des parenthèses. L'un des groupes contient la valeur du paramètre. Un groupe peut aussi contenir le nom. Pour ouvrir l'outil Expression Test PowerTool, cliquez sur le (.*) qui vous aide à vérifier la syntaxe de l'expression régulière.
Index des groupes de noms	(Facultatif) Si le nom est inclus dans l'expression régulière, indiquez le groupe (1,2,3...) le contenant. AppScan utilise cette valeur pour "compter dans les groupes" et localiser le nom du paramètre (voir exemple suivant).
Index des groupes de valeurs	Indiquez quel groupe (1, 2, 3...) de l'expression régulière ci-dessus contient la valeur du paramètre. AppScan utilise cette valeur pour "compter dans les groupes" et localiser la valeur du paramètre (voir exemple suivant).
Localisation	Indiquez le composant de la demande contenant le paramètre : Corps / Chemin / Demande. **Remarque :** La sélection que vous effectuez s'applique à la fois au schéma et au schéma de condition (le cas échéant), mais pas au schéma de réponse.
Schéma de condition	(Facultatif) Vous pouvez entrer une expression régulière qui définit tout le composant (corps, chemin ou demande) contenant le paramètre. AppScan ne crée le paramètre que si tout le composant est conforme au schéma, ce qui réduit la durée de l'examen. Par exemple, si le paramètre se trouve dans le corps, et que le corps doit être au format XML, vous pouvez définir comme Schéma de condition une expression régulière qui vérifie que le corps commence et se termine par des balises XML. Si ce n'est pas le cas, AppScan ne crée pas le paramètre.

Remarque : Les zones exigeant ou acceptant une expression régulière comportent le bouton suivant : (.*), qui ouvre l'outil Expression Test PowerTool, afin de vous aider à vérifier la syntaxe de l'expression régulière.

Index de groupe

Pour comprendre le système d'indexation des groupes dans l'expression régulière Schéma, examinez l'exemple suivant :

```
Pattern: (abc)((def)(ghi))
```

Les groupes de cette expression seraient indexés comme suit :

```
Group 1: (abc)
Group 2: ((def)(ghi))
Group 3: (def)
Group 4: (ghi)
```

Utilisez les listes déroulantes **Index des groupes de noms** et **Index des groupes de valeurs** pour sélectionner les groupes appropriés pour le paramètre. Le groupe sélectionné apparaît dans la zone Schéma.

Remarque : Si vous modifiez le schéma une fois les index sélectionnés, et si l'index sélectionné n'existe plus dans le schéma, un avertissement s'affiche. La valeur n'est toutefois pas modifiée automatiquement, vous devez donc la modifier manuellement.

Onglet En-têtes personnalisés

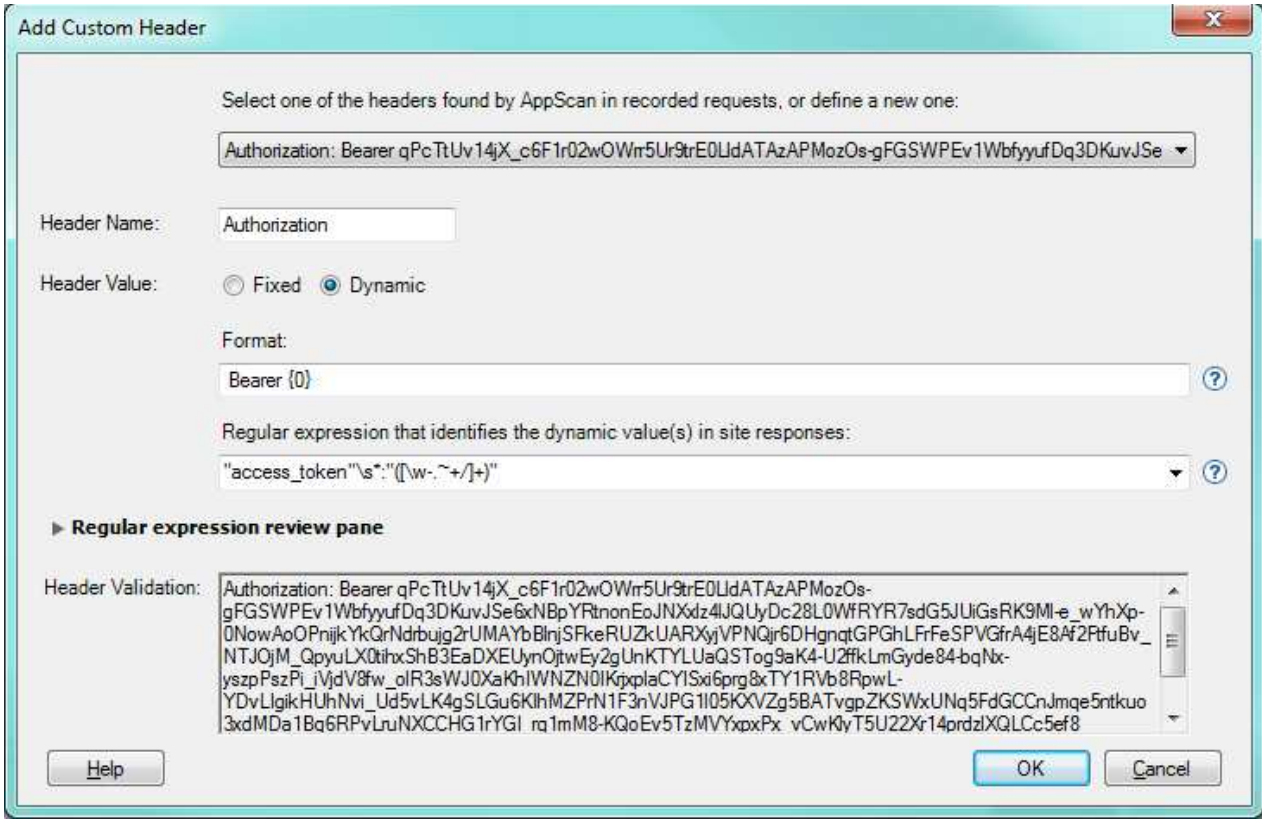
Onglet En-têtes personnalisés de la vue Paramètres et cookies de la boîte de dialogue Configuration.

Pourquoi et quand exécuter cette tâche

Le troisième onglet de la vue Exploration : La vue Paramètres et cookies permet de définir des formats d'en-tête HTTP non standard (personnalisés). AppScan doit pouvoir identifier les paramètres du contenu de la réponse et les ajouter correctement dans les en-têtes qu'il envoie au site, afin d'être en mesure de tester le site de manière efficace. AppScan tente de reconnaître automatiquement les en-têtes personnalisés, mais vous pouvez utiliser cet onglet pour ajouter et modifier les définitions. Vous pouvez également activer ou désactiver des définitions existantes (lorsqu'elle est désactivée, la définition est sauvegardée avec l'examen, mais n'est pas utilisée).

Procédure

Pour créer une définition, cliquez sur  ; pour modifier une définition existante, sélectionnez l'en-tête dans le tableau et cliquez sur  .
La boîte de dialogue **Ajouter/Editer un paramètre personnalisé** s'ouvre. Ses zones et options sont décrites dans le tableau suivant.

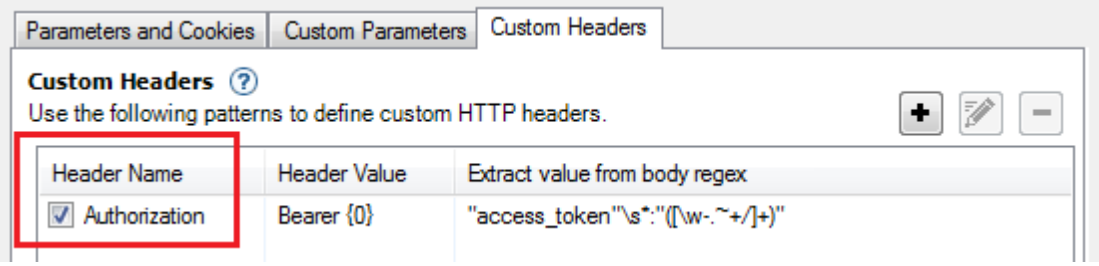


Paramètre	Description
Sélectionnez l'en-tête...	Si des demandes ont été enregistrées et qu'AppScan a identifié un en-tête personnalisé, celui-ci s'affiche dans une liste déroulante dans la partie supérieure de la boîte de dialogue. Si aucun en-tête personnalisé n'a été identifié, cette liste déroulante ne s'affiche pas. Si vous sélectionnez un en-tête dans cette liste, les autres zones sont renseignées automatiquement.
Nom d'en-tête	Nom de l'en-tête HTTP.
Type de suivi	
Connexion/ Dynamique/Fixe	• **Valeur de connexion :** (Par défaut et recommandé) Les demandes envoyées à l'application qui comprennent cet en-tête utilisent la valeur de l'en-tête reçue à la fin du processus de connexion. • **Valeur dynamique :** Les demandes envoyées à l'application qui comprennent cet en-tête utilisent la valeur la plus récente reçue de l'application. • **Valeur fixe :** Les demandes envoyées à l'application qui comprennent cet en-tête utilisent toujours la valeur que vous entrez dans la zone Valeur.
Valeur	(Fixe uniquement) Entrez la valeur.
Format	(Dynamique uniquement) Définissez le format de l'en-tête complet, comprenant un ou plusieurs groupes pour les valeurs dynamiques, en commençant à `{0}` pour le premier groupe, `{1}` pour le suivant et ainsi de suite.
Expression régulière	(Dynamique uniquement) Expression régulière définissant les valeurs dans la réponse du site. Cette expression doit inclure un groupe pour chaque valeur définie dans la zone Format.
Panneau d'aperçu des expressions régulières	(Dynamique uniquement) Cliquez pour développer. Utilisez ce panneau pour valider votre expression régulière. Entrez la réponse complète dans la zone située en haut du panneau. La zone située en bas du panneau affichera les groupes identifiés ainsi que leurs valeurs.

Paramètre	Description
Validation d'en-tête	Indique si la définition d'en-tête a été validée ou non avec succès en vue d'une utilisation lors de l'examen.

Résultats

Lorsque vous ajoutez une définition d'en-tête personnalisé, celle-ci s'affiche dans la liste des en-têtes personnalisés et la case en regard est cochée, indiquant que la définition est activée. Les entrées désactivées sont sauvegardées avec l'examen mais ne sont pas utilisées.



Vue Remplissage automatique de formulaires

La vue Remplissage automatique de formulaires de la boîte de dialogue Configuration contient les valeurs utilisées pour remplir les formulaires de votre application.

Les valeurs de Remplissage automatique de formulaires sont celles utilisées par AppScan pour remplir les formulaires de votre application. Pour la plupart d'entre elles, il existe des valeurs par défaut qui sont automatiquement mises à jour afin d'inclure les valeurs que vous entrez lors d'une «Enregistrement d'une connexion», à la page 53.

Vous pouvez visualiser, ajouter et modifier ces valeurs depuis cette vue de la boîte de dialogue Configuration des examens.

Paramètre	Détails
Activer le remplissage automatique de formulaires	Lorsque cette case est cochée (par défaut), AppScan tente de remplir automatiquement les formulaires d'entrée utilisateur de votre application lors de l'étape d'exploration.
Liste des propriétés de remplissage automatique de formulaires	Liste des valeurs utilisée par AppScan pour remplir automatiquement des formulaires lors de l'examen. Vous pouvez ajouter des valeurs à cette liste et la modifier. Pour plus de détails, voir «Propriétés des formulaires», à la page 91.
Paramètres du nom d'utilisateur et du mot de passe	Affiche les chaînes, séparées par des virgules, utilisées par AppScan pour reconnaître les zones dans lesquelles doivent être indiqués le nom d'utilisateur ou le mot de passe. Vous pouvez éditer cette chaîne si nécessaire. Ajoutez une virgule sans espace entre les chaînes.
Valeurs du nom d'utilisateur et du mot de passe	Affiche le nom et le mot de passe utilisés pour la connexion si Connexion automatique est sélectionnée dans la vue Connexion. Vous pouvez les éditer ici. (Pour plus de détails, voir «Onglet Connexion», à la page 52.)
Renseigner les zones inconnues avec	Vous pouvez entrer une chaîne qui sera utilisée par AppScan chaque fois qu'il rencontre une zone qu'il ne reconnaît pas (par défaut, la chaîne est 1234), ou faire en sorte qu'AppScan utilise une **Valeur aléatoire** à chaque fois.

Propriétés des formulaires

La vue Propriétés des formulaires de la boîte de dialogue Configuration recense les valeurs qui seront utilisées par AppScan pour renseigner automatiquement les formulaires.

Pourquoi et quand exécuter cette tâche

Vous pouvez ajouter ou éditer les **Propriétés des formulaires** utilisées par AppScan pour remplir automatiquement des formulaires lors de l'examen.

Procédure

Pour ajouter une nouvelle définition, cliquez sur  (ou, pour éditer une propriété de formulaire existante, sélectionnez-la et cliquez sur ).
La boîte de dialogue **Propriétés des formulaires** s'affiche.

Colonne	Description
Description	Nom décrivant le paramètre.
Paramètres	Nom ou partie du nom utilisé pour définir ce paramètre dans le fichier HTML. Lorsque AppScan trouve une zone avec ce nom de paramètre, il entre la valeur fournie. Pour entrer plusieurs noms de paramètre sur une seule ligne, utilisez une virgule sans espace. **Exemple :** Description : Code postal | Paramètres : zip,postal
Valeur	L'entrée utilisateur qui sera envoyée par AppScan pour ce paramètre.
Substitution	Parfois, le site rentre sa propre valeur par défaut pour une zone particulière. Dans ce cas, par défaut, AppScan utilisera la valeur suggérée par le site plutôt que celle entrée ici. Sélectionnez cette case à cocher si vous voulez que AppScan utilise la valeur définie ici *même si le site propose une autre valeur par défaut*.
Type de correspondance	Définit comment AppScan recherchera le paramètre défini ici, et comment il est en relation avec les options de remplissage de zones fournies par le site. Les options sont "Partiel" ou "Complet". **Complet :** la valeur constituera l'entrée *uniquement* pour les paramètres qui correspondent exactement à l'une des chaînes de texte de la zone Paramètres. (Par exemple, le paramètre défini en tant que `addr` ne sera pas utilisé pour une zone appelée `address`.) De plus, si la zone contient une liste d'options de recherche, cette valeur sera utilisée uniquement si elle correspond *exactement* à l'une des options. **Partiel :** cette valeur constituera l'entrée pour les paramètres qui correspondent *ou correspondent partiellement* à l'une des chaînes de paramètre répertoriées ici. (Par exemple, si le paramètre est défini en tant que `addr`, il sera également utilisé pour une zone appelée `address` ou `ADDR`.) De plus, si la zone contient une liste d'options de recherche, et qu'aucune des options ne correspond exactement à la valeur entrée ici, une correspondance proche sera utilisée à la place.
URL	Si cette zone est laissée vide, cette valeur sera utilisée pour ce paramètre, quelle que soit l'adresse URL. Si une adresse URL spécifique est fournie, cette valeur sera utilisée uniquement pour les paramètres qui font partie de cette URL. (Vous pouvez alors définir un paramètre pour une URL et un autre pour une autre URL.) Cependant, s'il n'y a pas d'autre ligne avec les mêmes paramètres et une adresse URL vide, la valeur de cette ligne est celle par défaut pour toutes les autres adresses URL également.

Exemple

«Exporter et importer des propriétés de formulaire»

«Importation d'un fichier ASFF sauvegardé»

Exporter et importer des propriétés de formulaire :
Pourquoi et quand exécuter cette tâche

Vous pouvez sauvegarder les propriétés de l'outil de remplissage des formulaires et les propriétés d'authentification pour un usage ultérieur en exportant votre tableau **Propriétés des formulaires** sous forme de fichier XML.

Procédure

1. Dans la vue **Exploration : Remplissage automatique de formulaires**, cliquez sur **Exporter**.

   La boîte de dialogue **Sauvegarder sous** qui s'affiche permet de sauvegarder les données sous forme de fichier ASFF (fichier de l'outil de remplissage des formulaires AppScan). Le contenu est au format XML.
2. Nommez votre fichier et cliquez sur **Sauvegarder**.

   Exemple de contenu d'un fichier ASFF :

```
<FormFiller Version="1.0" Enabled="True" DefaultValue="1234"
UseDefaultValue="True">
 <Group Name="InternalAppScanUserName" Value="" MatchType="Partial" Action="">
 <MatchNames>
 <MatchName>user</MatchName>
 <MatchName>name</MatchName>
 <MatchName>uid</MatchName>
 <MatchName>login</MatchName>
 <MatchName>usr</MatchName>
 </MatchNames>
 </Group>
```

Importation d'un fichier ASFF sauvegardé :
Procédure

1. Dans la vue **Exploration : Remplissage automatique de formulaires,** cliquez sur Importer.

   Un message apparaît, vous avertissant qu'en important un fichier ASFF, vous supprimez toute donnée en cours du tableau. Si vous souhaitez poursuivre, cliquez sur **OK**.
2. Accédez au fichier ASFF approprié et cliquez sur **Ouvrir**.

Propriétés des formulaires dans les fichiers Flash

Les propriétés des formulaires dans les fichiers Adobe Flash requièrent une attention particulière.

Pourquoi et quand exécuter cette tâche

L'une des actions importantes de la configuration des examens consiste à définir des valeurs valides pour les zones des formulaires, particulièrement lorsqu'ils ont des noms inhabituels. Par exemple, si une zone de courrier électronique a un nom inattendu, AppScan peut envoyer une entrée dont le format d'adresse électronique n'est pas valide, ce qui provoque l'échec des tests.

Dans le cas de fichiers Flash, le problème est plus important en raison de l'inaccessibilité des noms d'instance (zones de formulaire). Accès à ces noms et configuration des valeurs pour ces derniers dans la «Vue Remplissage automatique de formulaires», à la page 90 de la boîte de dialogue Configuration des examens.

Vue Pages d'erreur

Vue Pages d'erreur de la boîte de dialogue Configuration.

Lorsqu'AppScan obtient une page d'erreur 404 en réponse d'un test, il enregistre ce test comme un échec car cette réponse indique que le site a reconnu que la demande était illégale. Il peut aussi arriver le contraire, et la page d'erreur indique un résultat satisfaisant. Dans les deux cas, il est important que les pages d'erreur soient correctement définies de sorte qu'AppScan puisse les reconnaître comme telles.

Les applications et serveurs Web utilisent souvent des pages d'erreur 404 personnalisées ou générées de manière dynamique qui peuvent être difficiles à reconnaître automatiquement. AppScan tente de reconnaître les pages d'erreur 404 personnalisées, mais peut ne pas y arriver dans certains cas. S'il reçoit une page d'erreur personnalisée et ne la reconnaît pas comme telle, il enregistre le résultat comme positif, alors qu'il devrait être négatif, ou inversement. Par défaut, la liste Pages d'erreur comprend des définitions de pages d'erreur standard. Pour chaque définition, le type et la valeur sont indiqués.

Si les définitions de cette liste ne s'appliquent pas aux pages d'erreur de votre application, vous devez ajouter les chaînes, les expressions régulières et les URL nécessaires qui permettront à AppScan de les reconnaître. Vous pouvez alors réduire le nombre de "faux positifs" dans vos résultats d'examen. Il existe deux procédures :

- Vous pouvez définir manuellement l'erreur avant l'examen. Voir «Définition d'une nouvelle page d'erreur»
- Si vous avez exécuté l'étape d'exploration, vous pouvez définir une adresse URL découverte comme page d'erreur. Voir «Définition d'une page d'erreur», à la page 94

Important : Des définitions incorrectes de page d'erreur peuvent entraîner des résultats de type "faux positif" et "faux négatif". Par conséquent, lorsque vous ajoutez ou supprimez des pages d'erreur *après* l'étape Test d'un examen, il convient de mettre à jour les résultats de l'examen.

- Pour les tests dans lesquels la définition précédente indiquait un examen réussi, il est possible de mettre à jour les résultats en cliquant sur **Appliquer aux résultats en cours.**
- Pour les tests dans lesquels la définition précédente indiquait l'échec d'un test, vous devez exécuter le test une nouvelle fois.

Voir aussi :

«Application des modifications de page d'erreur», à la page 95

Définition d'une nouvelle page d'erreur

Procédure

1. Pour ajouter une nouvelle définition Page d'erreur personnalisée, cliquez sur  (ou, pour éditer un paramètre existant, sélectionnez-le et cliquez sur ).
   La boîte de dialogue **Page d'erreur personnalisée** s'affiche.
2. Dans la liste **Type**, sélectionnez :
   - **Chaîne :** Correspond à une chaîne trouvée dans le contenu HTML de vos pages d'erreur.
   - **Expression régulière :** Correspond à une expression régulière trouvée dans le contenu HTML de vos pages d'erreur. Pour ouvrir l'outil Expression Test PowerTool, cliquez sur le bouton  qui vous aide à vérifier la syntaxe de l'expression régulière.
   - **URL :** Correspond à l'adresse URL de la page de réponse.
   - **Page :** Correspond rigoureusement à la page de réponse. (Cette méthode est utilisée lorsque vous cliquez sur **Définir comme page d'erreur** pour une variante particulière dans l'«Onglet Demande/Réponse», à la page 220.)

3. Dans la zone de saisie **Valeur**, entrez la chaîne, l'expression régulière ou l'URL (chemin relatif et nom de fichier).

   Important : Des définitions incorrectes de page d'erreur peuvent entraîner des résultats de type "faux positif" et "faux négatif". Par conséquent, lorsque vous ajoutez ou supprimez des pages d'erreur *après* l'étape Test d'un examen, il convient de mettre à jour les résultats de l'examen.
   - Pour les tests dans lesquels la définition précédente indiquait un examen réussi, il est possible de mettre à jour les résultats en cliquant sur **Appliquer aux résultats en cours.**
   - Pour les tests dans lesquels la définition précédente indiquait l'échec d'un test, vous devez exécuter le test une nouvelle fois.
4. Cliquez sur **OK**.

   Toute réponse correspondant à la chaîne, à l'expression régulière ou à l'URL sera reconnue par AppScan comme une page d'erreur.

Exemple

«Exemples de filtrage de page personnalisé»

Exemples de filtrage de page personnalisé :

Le tableau suivant fournit des exemples d'ajout de pages à la liste Page d'erreur personnalisée.

Type	Valeur	Ajoute
URL	**/fileNotFound.aspx**	Fichier spécifique
Chaîne	**"page introuvable"**	N'importe quelle page avec cette chaîne
Expression régulière	**(?i)(URL|page) (.*) introuvable**	N'importe quelle page avec : "nom URL introuvable", "nom url introuvable", "Page page.ext introuvable", etc.

Remarque : Une expression régulière (regexp) est une chaîne décrivant un ensemble de chaînes selon une syntaxe précise. L'Expression Test PowerTool (**Outils > Test d'expression**) peut être utile pour vérifier la syntaxe de vos expressions régulières.

Si vous avez besoin d'aide pour écrire des expressions régulières, reportez-vous au lien suivant : http://www.regular-expressions.info/quickstart.html

Définition d'une page d'erreur

Vous pouvez définir une page listée dans les résultats de l'exploration comme page d'erreur personnalisée.

Pourquoi et quand exécuter cette tâche

Vous pouvez afficher la liste des adresses URL découvertes lors de la phase d'exploration dans Vue Données > Pages. Si l'une de vos pages d'erreur personnalisées y est listée par erreur, vous pouvez définir la page comme page d'erreur.

Procédure

1. Ouvrez les résultats d'exploration dans la Vue Données d'application (F2).
2. Dans le panneau Résultats, cliquez sur **Pages**.
3. Cliquez avec le bouton droit de la souris sur l'adresse URL et cliquez sur **Définir comme page d'erreur**.

   Vous êtes invité à confirmer la mise à jour des résultats afin d'incorporer la nouvelle définition.

4. Cliquez sur **Démarrer**.

   L'adresse URL est ajoutée à la liste Page d'erreur dans la configuration d'examen et les résultats sont mis à jour si nécessaire.

Application des modifications de page d'erreur

Pourquoi et quand exécuter cette tâche

Si vous éditez la liste des pages d'erreur après examen, vous devez mettre à jour les résultats de l'examen pour refléter les modifications (supprimer les "faux positifs").

Après cette édition, le bouton *Appliquer aux résultats Current*, au-dessus de la liste, est désormais activé.

Procédure

Cliquez sur **Appliquer aux résultats Current**.
Les résultats sont mis à jour pour que les nouvelles pages ou les pages mises à jour soient prise en compte en tant que pages d'erreur.

Vue Opérations en plusieurs étapes

La vue Opérations en plusieurs étapes de la boîte de dialogue Configuration permet de tester les parties du site accessibles uniquement en cliquant sur les liens dans un ordre spécifique.

Une opération à plusieurs étapes est requise pour l'exploration des parties du site accessibles uniquement en cliquant sur des liens *dans un ordre spécifique*, comme une boutique en ligne où l'utilisateur ajoute des articles dans un panier avant de les payer. Prenez en compte les trois pages suivantes :

1. L'utilisateur ajoute un ou plusieurs articles à un panier
2. L'utilisateur remplit les détails pour le règlement et la livraison
3. L'utilisateur reçoit la confirmation que la commande est terminée

La page 2 peut uniquement être atteinte via la page 1. La page 3 peut uniquement être atteinte via la page 1 suivie de la page 2. Il s'agit d'une séquence. Pour pouvoir tester les pages 2 et 3, AppScan doit envoyer la séquence correcte de demandes HTTP avant chaque test.

Dans le cas de l'exemple ci-dessus, vous enregistrez une seule séquence : Page 1 > Page 2 > Page 3. AppScan extrait les sous-séquences nécessaires de cette séquence, le cas échéant. (Lors du test de la page 2, il envoie tout d'abord une demande de page 1 ; lors du test de la page 3, il envoie une demande de la page 1 suivie de la page 2.)

Remarque : Il est recommandé de limiter le nombre d'opérations en plusieurs étapes à cinq, avec un maximum de 25 étapes par opération, et de 70 étapes en tout.

Remarque : La configuration des opérations en plusieurs étapes ne doit pas être confondue avec l'exploration manuelle, et ne doit être utilisée que dans les cas décrits ci-dessus. Pour plus de détails, voir Exploration manuelle à l'aide d'AppScan

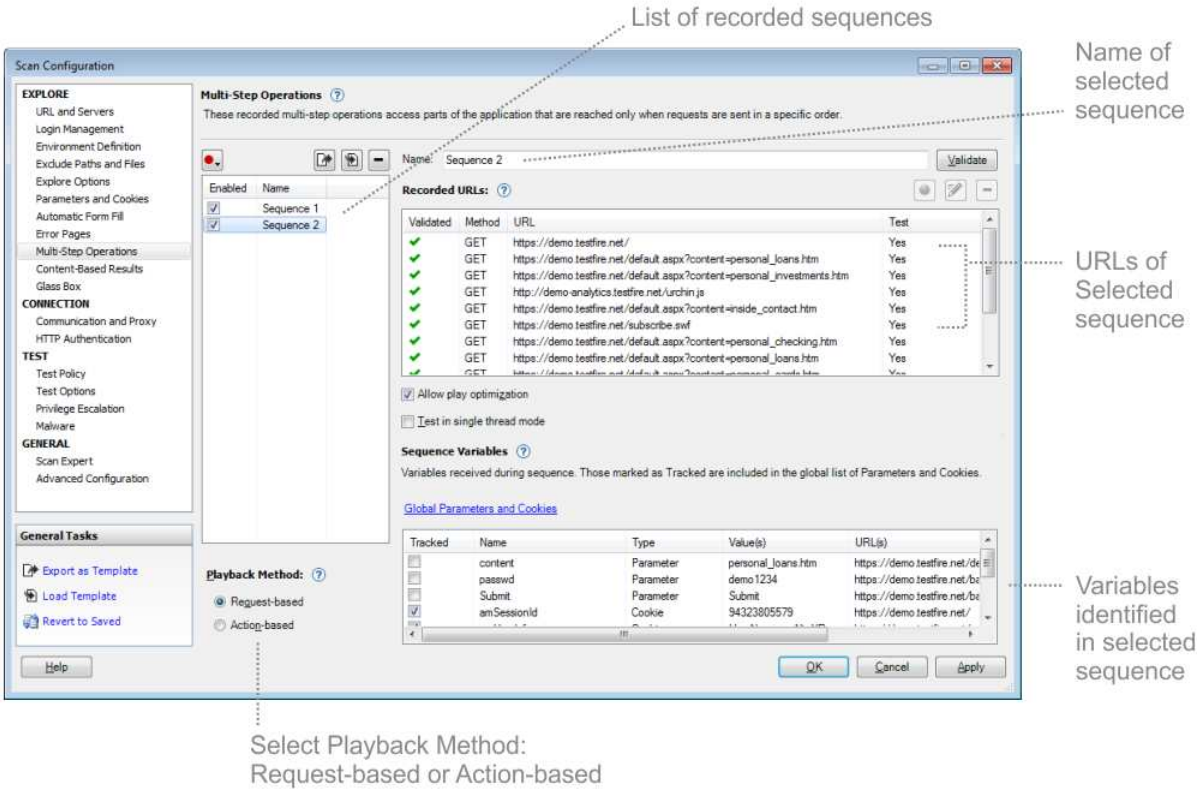

List of recorded sequences
Name of selected sequence
URLs of Selected sequence
Variables identified in selected sequence
Select Playback Method: Request-based or Action-based
Scan Configuration
EXPLORE
URL and Servers
Login Management
Environment Definition
Exclude Paths and Files
Explore Options
Parameters and Cookies
Automatic Form Fill
Error Pages
Multi-Step Operations
Content-Based Results
Glass Box
CONNECTION
Communication and Proxy
HTTP Authentication
TEST
Test Policy
Test Options
Privilege Escalation
Malware
GENERAL
Scan Expert
Advanced Configuration
General Tasks
Export as Template
Load Template
Revert to Saved
Multi-Step Operations
These recorded multi-step operations access parts of the application that are reached only when requests are sent in a specific order.
Enabled
Name
Sequence 1
Sequence 2
Name: Sequence 2
Validate
Recorded URLs:
Validated
Method
URL
Test
GET https://demo.testfire.net/ Yes
GET https://demo.testfire.net/default.aspx?content=personal_loans.htm Yes
GET https://demo.testfire.net/default.aspx?content=personal_investments.htm Yes
GET http://demo-analytics.testfire.net/urchin.js Yes
GET https://demo.testfire.net/default.aspx?content=inside_contact.htm Yes
GET https://demo.testfire.net/subscribe.swf Yes
GET https://demo.testfire.net/default.aspx?content=personal_checking.htm Yes
GET https://demo.testfire.net/default.aspx?content=personal_loans.htm Yes
Allow play optimization
Test in single thread mode
Sequence Variables
Variables received during sequence. Those marked as Tracked are included in the global list of Parameters and Cookies.
Global Parameters and Cookies
Tracked
Name
Type
Value(s)
URL(s)
content Parameter personal_loans.htm
passwd Parameter demo1234
Submit Parameter Submit
amSessionId Cookie 94323805579 https://demo.testfire.net/
Playback Method:
Request-based
Action-based
Help
OK
Cancel
Apply

Tableau 5. Options de vue Opérations multi-étapes

Paramètre	Détails
Enregistrement	Cliquez pour enregistrer une nouvelle séquence. Si les détails de connexion ont été configurés, vous pouvez cliquer sur la flèche vers le bas pour sélectionner une des actions suivantes : **Navigateur AppScan IE > Connecter, puis enregistrer** AppScan se connecte automatiquement à l'application (en utilisant la connexion que vous avez enregistrée) avant l'ouverture du navigateur. Vous pouvez ensuite enregistrer l'opération en plusieurs étapes *sans* enregistrer les demandes de connexion. L'avantage de cette méthode est que les demandes de connexion ne seront pas relayées à chaque exécution de cette séquence, mais uniquement si AppScan est hors session. **Remarque :** Les paramètres et les cookies présents dans la séquence en plusieurs étapes *et non dans la séquence de connexion* sont toujours suivis comme étant dynamiques, même si vous modifiez leur suivi en tant que Valeur de connexion. **Navigateur AppScan IE > Enregistrer sans connexion** AppScan commence l'enregistrement de la séquence sans se connecter. Lorsque le navigateur s'ouvre, vous enregistrez directement votre séquence en plusieurs étapes. Si vous devez vous connecter, la connexion fera partie de l'enregistrement et sera donc relayée à chaque exécution de la séquence, ce qui risque d'augmenter la durée d'examen de façon significative. Lorsqu'une connexion est requise, il est conseillé d'utiliser l'option précédente. **Remarque :** Si vous utilisez cette option *et que vous enregistrez ensuite les demandes de connexion dans le cadre de la séquence*, les paramètres et les cookies reçus sont toujours suivis comme étant dynamiques, même si vous modifiez leur suivi en tant que Valeur de connexion. **Navigateur AppScan Chromium** AppScan effectue l'enregistrement *en utilisant le navigateur intégré basé sur Chromium*, sans connexion. Lorsque le navigateur s'ouvre, vous pouvez vous connecter, le cas échéant, puis enregistrer votre séquence en plusieurs étapes. **Remarque :** Si vous utilisez cette option *et que vous enregistrez ensuite les demandes de connexion dans le cadre de la séquence*, les paramètres et les cookies reçus seront toujours traités comme étant dynamiques, même si vous modifiez leur suivi en tant que Valeur de connexion. Pour plus de détails, voir «Enregistrement d'une séquence», à la page 99
	Exportez une séquence (sous forme de fichier SEQ) à utiliser avec un autre examen ; importez une séquence (fichier SEQ) exportée à partir d'un autre examen ; supprimez de l'examen en cours la séquence sélectionnée.

Tableau 5. Options de vue Opérations multi-étapes (suite)

Paramètre	Détails
Méthode de lecture	Lorsque vous enregistrez une opération à plusieurs étapes, AppScan enregistre les actions et les demandes. Vous pouvez sélectionner la méthode qui sera utilisée pour l'examen : **Lecture basée sur les demandes** Envoie les demandes HTTP brutes à partir de l'enregistrement. Cette méthode est généralement plus rapide. **Lecture basée sur les actions** Exécute à nouveau les actions de clic et de frappe de l'utilisateur. Vous pouvez être amené à choisir cette méthode lorsque le site inclut un grand nombre d'éléments JavaScript ou lorsque certaines demandes de la lecture basée sur les demandes ont été marquées d'un caractère X rouge lors d'une tentative de validation. Cette méthode peut augmenter la durée de l'examen. La lecture basée sur les demandes constitue la méthode par défaut. **Remarque :** Si l'examen est configuré pour utiliser uniquement le navigateur intégré (Outils > Options > Utiliser un navigateur externe), la lecture basée sur les demandes est toujours utilisée. **Remarque :** Si vous chargez une séquence qui a été enregistrée dans une version d'AppScan qui ne prenait pas en charge la lecture basée sur l'action, la lecture basée sur les requêtes est utilisée *pour cette séquence*, même si la lecture basée sur l'action est sélectionnée. **Remarque :** Si vous sélectionnez Lecture par action pour une opération en plusieurs étapes, vous devez également sélectionner Lecture par action comme méthode de connexion. Si nécessaire, enregistrez à nouveau la séquence de connexion (voir «Vue Gestion de connexion», à la page 51).
Liste de la séquence	Répertorie toutes les opérations en plusieurs étapes pour cet examen.
Nom de la séquence	Nom de la séquence sélectionné dans la liste de séquences. La case à cocher en regard de chacune indique si la séquence est activée pour cet examen. **Validate** Cliquez pour vérifier que la séquence est valide. AppScan réexécute la séquence et toute demande recevant une réponse différente de la réponse d'origine est marquée d'un x rouge pour indiquer qu'elle ne sera pas testée. **Conseil :** Une raison habituelle expliquant la réception d'une réponse différente à une demande est la présence d'une variable de séquence dynamique (voir «Variables de la séquence», à la page 102). S'il ne s'agit pas du problème et que le site contient des éléments JavaScript, le fait d'utiliser la lecture basée sur les actions peut donner de meilleurs résultats.

Tableau 5. Options de vue Opérations multi-étapes (suite)

Paramètre	Détails
URL enregistrées	Affiche les liens ou les actions dans la séquence sélectionnée. **Validée** Une coche verte signale que l'URL a été validée. Une croix rouge apparaît à côté des URL qui n'ont pas été validées. **Test** Signale si cette URL est testée seule (ainsi que lors de l'opération en plusieurs étapes). Les options sont Oui/Non. Pour modifier le paramètre, cliquez avec le bouton droit de votre souris sur l'URL et sélectionnez **Tester/Ne pas tester**. Même si vous avez sélectionné Non, l'URL sera tout de même exécutée lors de l'opération en plusieurs étapes. **Exécuter la séquence :** (S'applique uniquement aux URL testées) Indique si les étapes précédentes de la séquence sont réexécutées à *chaque fois* que cette URL est testée. Les options sont Oui/Non. Pour modifier le paramètre, cliquez avec le bouton droit de votre souris et sélectionnez **Exécuter la séquence avant de tester la demande > Oui/Non**. • Visualisez n'importe quel lien de la séquence en le sélectionnant, puis en cliquant sur le bouton du navigateur (vous pouvez supprimer des demandes individuelles ouvertes en cliquant sur l'icône représentant une corbeille en haut à droite) • Supprimez n'importe quel lien de la séquence en le sélectionnant et en cliquant sur [-]. Une fois cette opération effectuée, cliquez sur **Valider** pour vérifier que la séquence mise à jour est toujours en session.
Se connecter avant l'exécution de la séquence	Si cette option est sélectionnée, chaque fois qu'une opération en plusieurs étapes est exécutée, AppScan se connecte en premier. Cette option est désélectionnée si vous enregistrez la connexion en tant qu'opération en plusieurs étapes.
Autoriser l'optimisation de la lecture	(Lecture basée sur les demandes uniquement) Lorsque cette option est sélectionnée (valeur par défaut), AppScan tente d'optimiser la durée de l'examen en évitant la lecture inutile. Vous ne devez pas désactiver ce paramètre, sauf si AppScan n'examine pas certaines parties de l'application à cause de l'optimisation de la lecture. Le «Journal d'examen», à la page 300 peut vous aider à le déterminer.
Tester en mode unité d'exécution unique	AppScan peut envoyer simultanément deux requêtes (ou plus) si elles ne nécessitent pas la relecture d'une séquence entre les requêtes. Si cela conduit à la mise à part de parties de l'application, cochez cette case.
Variables de la séquence	Répertorie les variables reçues lors de l'enregistrement de la ou des séquences, et indique celles qu'AppScan a déterminé comme devant faire l'objet d'un suivi. Il peut s'agir d'ID session ou d'autres variables. Vous pouvez modifier l'état des variables dans cette liste pour améliorer la manière dont AppScan les traite (pour plus d'informations, voir «Variables de la séquence», à la page 102).

Voir aussi :

Exploration manuelle à l'aide d'AppScan

«Examiner uniquement les opérations en plusieurs étapes», à la page 192

Enregistrement d'une séquence

Pourquoi et quand exécuter cette tâche

Si une séquence de connexion a été configurée (voir «Onglet Connexion», à la page 52), il existe deux options lors de l'enregistrement d'une opération en plusieurs étapes :

Navigateur AppScan IE > Connecter, puis enregistrer
AppScan se connecte automatiquement à l'application (en utilisant la connexion que vous avez enregistrée) avant l'ouverture du navigateur. Vous pouvez ensuite enregistrer l'opération en

plusieurs étapes *sans* enregistrer les demandes de connexion. L'avantage de cette méthode est que les demandes de connexion ne seront pas relayées à chaque exécution de cette séquence, mais uniquement si AppScan est hors session.

Remarque : Les paramètres et les cookies présents dans la séquence en plusieurs étapes *et non dans la séquence de connexion* sont toujours suivis comme étant dynamiques, même si vous modifiez leur suivi en tant que Valeur de connexion.

Navigateur AppScan IE > Enregistrer sans connexion
AppScan commence l'enregistrement de la séquence sans se connecter. Lorsque le navigateur s'ouvre, vous enregistrez directement votre séquence en plusieurs étapes. Si vous devez vous connecter, la connexion fera partie de l'enregistrement et sera donc relayée à chaque exécution de la séquence, ce qui risque d'augmenter la durée d'examen de façon significative. Lorsqu'une connexion est requise, il est conseillé d'utiliser l'option précédente.

Remarque : Si vous utilisez cette option *et que vous enregistrez ensuite les demandes de connexion dans le cadre de la séquence*, les paramètres et les cookies reçus sont toujours suivis comme étant dynamiques, même si vous modifiez leur suivi en tant que Valeur de connexion.

Navigateur AppScan Chromium
AppScan effectue l'enregistrement *en utilisant le navigateur intégré basé sur Chromium*, sans connexion. Lorsque le navigateur s'ouvre, vous pouvez vous connecter, le cas échéant, puis enregistrer votre séquence en plusieurs étapes.

Remarque : Si vous utilisez cette option *et que vous enregistrez ensuite les demandes de connexion dans le cadre de la séquence*, les paramètres et les cookies reçus seront toujours traités comme étant dynamiques, même si vous modifiez leur suivi en tant que Valeur de connexion.

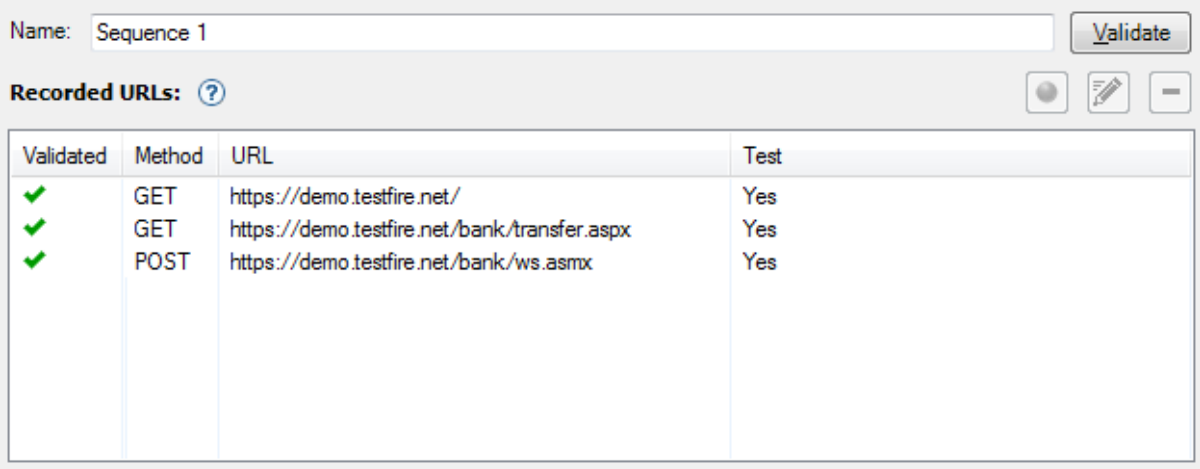
Si aucune séquence de connexion n'a été configurée, il n'y a qu'une seule option : **Enregistrer**.

Important : Lors de la lecture d'une opération en plusieurs étapes, la détection En session est désactivée (voir «Onglet Connexion», à la page 52). Cela signifie qu'AppScan ne vérifie pas qu'il est connecté. Par conséquent, si l'échec de l'opération en plusieurs étapes déconnecte l'utilisateur de l'application, il est important que la connexion soit enregistrée comme faisant partie de la séquence (pour qu'elle puisse être réexécutée à chaque exécution de la séquence). Si ce n'est pas le cas, l'opération en plusieurs étapes risque d'échouer.

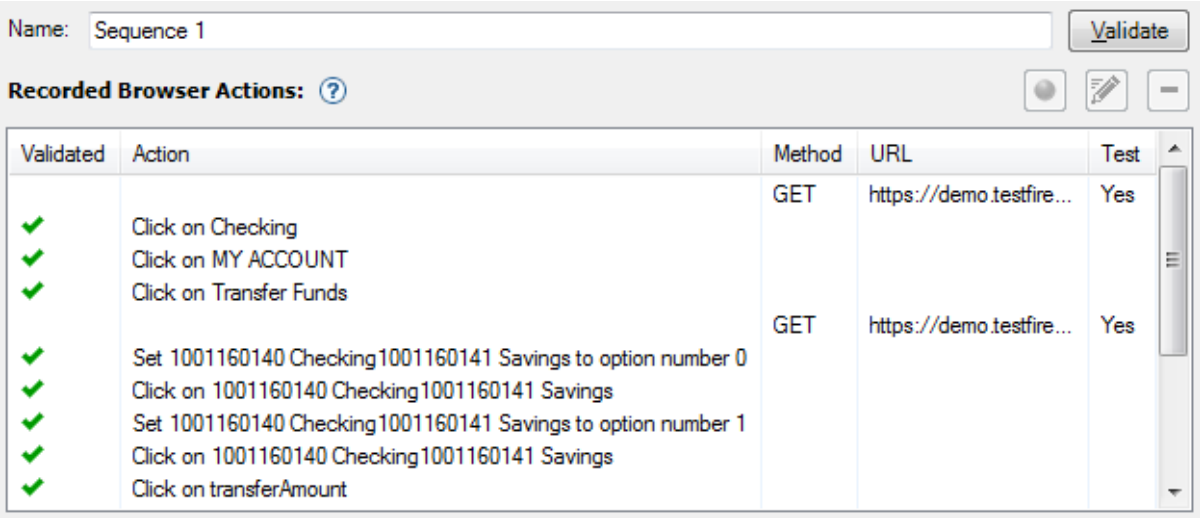
Remarque : Si votre site Web ne prend pas en charge Internet Explorer, cliquez sur **> Utiliser le navigateur AppScan Chromium** à la place.

Procédure

1. Cliquez sur  et sélectionnez l'une des options d'enregistrement (voir ci-dessus).
   Le navigateur s'ouvre et commence l'enregistrement.
2. Cliquez sur les liens et renseignez les zones pour atteindre les pages demandées. Vous pouvez utiliser le bouton **Pause**  si vous souhaitez cliquer sur des liens sans les enregistrer comme faisant partie de l'opération.
3. Fermez le navigateur.
   La séquence apparaît dans le panneau *Séquence* (partie supérieure droite). Les séquences sont automatiquement nommées dans l'ordre : "Séquence 1", "Séquence 2", etc., mais vous pouvez les renommer dans la zone de nom.
   Vous pouvez changer la méthode de lecture (partie inférieure gauche de la boîte de dialogue) :
   - La lecture **basée sur les demandes** (valeur par défaut) envoie les demandes HTTP brutes à partir de l'enregistrement. Cette méthode est généralement plus rapide.



- La lecture **basée sur les actions** exécute à nouveau les actions de clic et de frappe de l'utilisateur. Vous pouvez être amené à choisir cette méthode lorsque le site inclut un grand nombre d'éléments JavaScript ou lorsque certaines demandes de la lecture basée sur les demandes ont été marquées d'un caractère X rouge lors d'une tentative de validation. Cette méthode peut augmenter la durée de l'examen.



Remarque : Si l'examen est configuré pour utiliser un navigateur autre que le navigateur intégré (Outils > Options > Utiliser un navigateur externe), la méthode basée sur les demandes est toujours utilisée.

Remarque : Si votre site exige que les utilisateurs se connectent et que vous avez sélectionné Ouverture de session sur demande, vous *devez sélectionner* également Opérations multi-étapes sur demande, sinon les opérations multi-étapes ne seront pas envoyées.

4. Cliquez sur **Valider**.

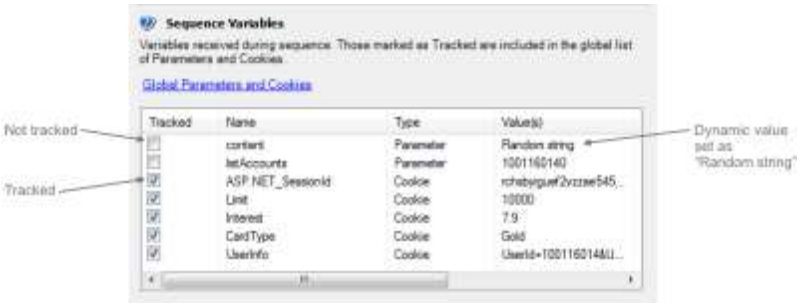
   AppScan réexécute la séquence et une coche verte s'affiche en regard de la demande ou de l'action dont la lecture a abouti. Si une demande ou une action n'aboutit pas, une coche X rouge s'affiche. Options possibles :

   - Affichez toutes les URL en les sélectionnant et en cliquant sur  .
   - Supprimez les étapes inutiles en les sélectionnant et en cliquant sur  . Une fois cette opération effectuée, cliquez sur le bouton **Valider** pour vérifier que la séquence est toujours en session.

- Cliquez avec le bouton droit de la souris sur une étape de la séquence et associez-la à l'option **Ne pas tester**. Les URL sont toujours incluses dans la lecture de la séquence, mais elles ne seront pas testées individuellement.
- Cliquez avec le bouton droit de la souris sur une étape configurée pour être testée individuellement, puis sélectionnez **Exécuter la séquence avant de tester la demande > Non** s'il n'est pas nécessaire d'exécuter les étapes précédentes de la séquence à chaque fois que cette URL est testée.

Variables de la séquence

Le panneau Variables de la séquence répertorie toutes les variables reçues lors des séquences enregistrées. Ces variables reconnues par AppScan comme ID session sont automatiquement ajoutées à la liste globale des paramètres et des cookies qui sont suivis lors de l'examen (voir «Vue Paramètres et cookies», à la page 76). De plus, elles sont marquées d'une coche dans la colonne "Suivi" afin d'indiquer qu'elles font l'objet d'un suivi.



Variables de suivi

Vous pouvez modifier l'état de chaque variable en la sélectionnant, puis en cochant ou décochant la case **Suivi**. Lorsqu'une variable est "suivie", AppScan envoie toujours la version reçue la plus récente, pour rester en session.

Notez que si vous désignez une variable comme "non suivie", elle est supprimée de la liste globale des paramètres et des cookies (voir «Vue Paramètres et cookies», à la page 76).

Définition d'un format de variable

Pour aider AppScan à envoyer, au cours de l'étape de test, des versions alternatives valides d'un paramètre qui varie, vous pouvez définir le format du paramètre. Cliquez avec le bouton droit de la souris sur le paramètre et sélectionnez une des options de "valeur dynamique" :

- Entier aléatoire (entre 1 et 1000)
- Entier décrémenté (commence à 999999 et soustrait 1 à chaque fois)
- Entier incrémenté (commence à 1 et ajoute 1 à chaque fois)
- Entier incrémenté avec zéros non significatifs (commence à 000001 et ajoute 1 à chaque fois)
- Chaîne aléatoire (5 caractères aléatoires)
- Chaîne alphabétique aléatoire (6 caractères alphabétiques aléatoires)
- Date et heure (MMjjaaHHmmss)
- Date, heure et millisecondes (MMjjaaHHmmssSSS)
- Adresse e-mail aléatoire

Si la séquence enregistre un nouvel utilisateur et que le processus requiert qu'une nouvelle adresse de courrier électronique soit entrée à chaque fois (de sorte que le site propose le processus d'inscription plutôt qu'une page "Utilisateur existant"), définissez la variable comme "Adresse électronique aléatoire". Chaque fois qu'une demande de test incluant cette variable est envoyée, une adresse électronique

différente est utilisée, ce qui permet à AppScan de tester les pages d'inscription.

Vue Résultats basés sur le contenu

Vue basée sur le contenu de la boîte de dialogue Configuration. Vous pouvez utiliser cette vue pour définir une structure logique pour l'arborescence de l'application, si AppScan ne peut pas le faire en fonction de la structure URL.

- Si le contenu de votre site est structuré de sorte que les URL reflètent une hiérarchie de type dossier, les résultats d'examen la refléteront automatiquement, la rendant plus facile à parcourir.
- Si votre site utilise la méthode de navigation "chemins de navigation", ou toute autre méthode "basée sur le contenu", et que les URL n'indiquent pas l'"emplacement" de l'utilisateur dans le site, nous vous recommandons d'"apprendre" à AppScan comment le site est organisé "logiquement" pour qu'il puisse présenter les résultats de l'examen dans un format simple et structuré plutôt que dans de longues listes sous une ou deux URL. Il n'est pas primordial de procéder ainsi, *mais cela facilite l'exploration des résultats.*

Par exemple, le code snippet ci-dessous a une structure logique **Home | Buy | Books** et il est utile de structurer les résultats pour que "Books" apparaisse sous "Buy" et "Buy" sous "Home".

```
<td class="navigation">
    <a href="http://www.onlineshop.com/">Home</a> &gt;
    <a href="http://hub.onlineshop.com/buy?ssPageName=h:h:cat:US">Buy</a> &gt;
    <b>Books<b>
</td>
```

Pour ce faire, définissez les règles qui permettront à AppScan d'identifier et d'extraire le contenu approprié (dans le cas présent, "Home", "Buy" et "Books") pour construire une arborescence basée sur le contenu.

Une fois les règles définies, vous pouvez sélectionner l'option "Basé sur le contenu" dans l'arborescence de l'application pour afficher les résultats à l'aide de ces informations. (Voir «Problèmes de sécurité : Arborescence de l'application», à la page 207.)

Remarque : Le nombre total de problèmes de sécurité (affiché en haut de la «Liste de résultats», à la page 23) est une mesure des emplacements vulnérables du site et dépend en partie de sa structure. Si vous définissez une structure basée sur le contenu, le nombre total de problèmes dans l'arborescence de l'application peut ne pas être identique à celui de l'arborescence de l'application basée sur l'URL (pour les mêmes résultats). Lorsque la structure du site est basée sur le contenu (plutôt que sur l'URL), et que la vue basée sur le contenu est correctement configurée, le nombre de problèmes de la vue basée sur le contenu représente plus précisément le nombre d'"emplacements vulnérables" existant dans le site. Le nombre total de *variantes* (en haut de la Liste des résultats entre parenthèses) est indépendant de la structure du site et ne change pas entre la vue basée sur le contenu et la vue basée sur l'URL.

Ajouter de nouvelles règles de vue basées sur le contenu

Instructions et exemples relatifs à l'ajout de règles en vue de définir la structure logique du site.

Avant de commencer

Dans la Vue basée sur le contenu de la boîte de dialogue Configuration des examens (Exploration > Basée sur le contenu), vous pouvez définir une structure basée sur le contenu à l'aide de deux types de définitions :

- Chemin d'accès au contenu logique (par exemple, des chemins de navigation)
- Personnalisé (utilisez des expressions régulières pour définir vos propres nœuds personnalisés)

Cela permet à AppScan d'afficher une arborescence d'applications logique, au lieu de lister de grandes parties du site sous un seul noeud. Lorsque plusieurs règles sont définies, AppScan tente de faire correspondre chaque URL aux règles dans l'ordre selon lequel elles sont listées. Lorsqu'une

correspondance est détectée, l'URL est incluse dans l'arborescence basée sur le contenu en fonction de cette règle, puis l'URL suivante est traitée.

Procédure

1. Ajoutez de nouvelles définitions en cliquant sur  (ou éditez des définitions existantes en sélectionnant une définition et en cliquant sur ). Pour connaître les descriptions des zones, reportez-vous au tableau ci-dessous.

Paramètre	Description
Nom	Nom de cette règle.
Description	(Facultatif) Description de cette règle.
Type de règle	Sélectionnez Chemin d'accès au contenu logique ou Personnalisé. Les zones restantes varient en fonction de votre sélection.
Chemin d'accès au contenu logique	
Chemin d'accès du contenu	Expression régulière correspondant au chemin d'accès du contenu dans le fichier HTML.
Séparateur	Expression régulière correspondant aux séparateurs de hiérarchie du chemin d'accès du contenu dans le fichier HTML.
Nom d'affichage du nœud	Expression régulière correspondant aux noms de noeuds (visibles pour l'utilisateur de l'application et qui seront utilisés dans l'arborescence de l'application).
Condition	(Facultatif) Expression régulière définissant les réponses devant être incluses à cet emplacement de noeud.
Personnalisé	
Emplacement du nœud	Utilisez le format URL standard pour indiquer à quel emplacement les noeuds remplissant les conditions pour cette règle doivent être placés dans l'arborescence de l'application (par exemple : /Home/Buy/Books). Si le chemin d'accès n'existe pas, il sera créé.
Condition	Expression régulière définissant les réponses devant être incluses à cet emplacement de noeud. Si le contenu de la page correspond à cette condition, il sera inclus dans l'arborescence basée sur le contenu.

   Remarque : Les zones exigeant ou acceptant une expression régulière comportent le bouton Expression Test :  , qui ouvre l'outil Expression Test PowerTool afin de vous aider à vérifier la syntaxe de l'expression régulière.

   Si vous avez besoin d'une aide supplémentaire, reportez-vous au lien suivant : http://www.regular-expressions.info/quickstart.html
2. Utilisez les flèches de défilement pour organiser les définitions dans l'ordre dans lequel elles doivent être appliquées.
3. Vérifiez que la case située en regard de chaque règle à appliquer est cochée.
4. Cliquez sur **OK** pour enregistrer les modifications.

Exemple

Le tableau suivant présente des exemples de contenu pour les deux types de règles.

Tableau 6. Règle de vue basée sur le contenu

Paramètre	Exemple	Signification
Chemin d'accès du contenu	**<title>(.*?)</title>**	Le texte placé entre les balises de titre sera utilisé comme base pour les noms de noeuds.
Séparateur	**[:\->|]**	Ces cinq caractères seront traités en tant que séparateurs. Par conséquent : **<title>Home:Accounts</title>** et **<title>Home:Plans</title>** apparaîtront dans l'arborescence de l'application en tant que noeud parent **Home** avec deux noeuds enfants : **Accounts** et **Plans**
Nom d'affichage du nœud	**^\s*(.*?)\s*$**	Les espaces avant et après le texte seront supprimés lorsqu'un nom sera attribué au noeud.
Condition	**Log out**	Seules les pages contenant les mots "Log out" seront incluses dans l'arborescence d'application sous cette règle.

Tableau 7. Règle personnalisée

Paramètre	Exemple	Signification
Emplacement du nœud	**/root/child/grandchild**	Toutes les pages qui remplissent la condition sont ajoutées à l'arborescence d'application sous **/root/child/grandchild** **Remarque :** Si les noeuds parents de la branche spécifiée n'existent pas, ils sont créés.
Condition		Cette zone étant vide, le contenu auquel la règle est appliquée sera ajouté à cet emplacement de noeud. Dès lors, si cette règle apparaît après la règle ci-dessus, toutes les pages ne contenant pas les mots "Log out" seront ajoutées sous le noeud **/root/child/grandchild**

Vue Glass box

Vue Glass box de la boîte de dialogue de configuration.

L'examen glass box utilise un agent installé sur le serveur d'applications. Cet agent surveille l'activité côté serveur pendant l'examen, en collectant les informations sur le code source et d'autres données. En conséquence, l'examen est plus rapide et plus précis. L'agent glass box correspondant à l'URL de départ est sélectionné par défaut, et les deux fonctions d'examen glass box sont activées.

L'examen glass box peut découvrir des URL masquées à l'étape d'exploration, ainsi que des problèmes et des informations complémentaires au cours de l'étape de test.

Paramètre	Détails
Utiliser cet agent glass box	Si l'agent glass box a été installé sur votre serveur d'applications, et s'il est défini dans AppScan, vous pouvez le sélectionner et l'utiliser dans l'examen. Si vous avez entré une URL de départ, AppScan tente de sélectionner l'agent adéquat automatiquement. Lorsqu'un agent est sélectionné, AppScan tente de s'y connecter, et indique s'il y a réussi. **Remarque :** Si vous sélectionnez un agent et que vous recevez le message "Données d'identification requises", vérifiez que les données d'identification fournies dans Outils > Gestion de Glass Box sont correctes. Si le serveur requis ne s'affiche pas dans la liste déroulante, vous pouvez le définir en cliquant sur le lien **Gestion de l'agent glass box**. **Restriction :** Un seul agent glass box peut être sélectionné pour être utilisé dans un examen. Si l'application à examiner utilise plusieurs serveurs, vous devez réaliser l'examen pour chaque serveur séparément à l'aide des agents respectifs.

Utiliser Glass Box dans l'étape d'exploration	(Sélectionné par défaut.)
	
	Cette fonction peut élargir la couverture du site en examinant le code source côté serveur pour rechercher les paramètres qui affectent le comportement du serveur, mais qui n'apparaissent pas dans la réponse.
	
	Exemple de code sur le serveur :
	`String debugOn = request.getParameter("debug");`
	`if (debugOn == "true"){`
	`response.getWriter().println(SECRET_SERVER_DATA);`
	`}`
	
	Dans cet exemple, le développeur a laissé le paramètre `"debug"` dans le code. Il n'apparaît dans aucun lien sur le site, mais si un cyber-attaquant envoyait une requête le contenant, il pourrait obtenir `SECRET_SERVER_DATA`.

Utiliser Glass Box dans l'étape de test	(Sélectionné par défaut.) Cochez cette case pour envoyer des tests glass box pendant l'étape de test de l'examen. Cette fonction peut vérifier la réussite ou l'échec de certains tests, par exemple les tests d'injection SQL en aveugle, avec plus de précision, et révéler l'existence de certains problèmes de sécurité qui ne sont pas détectables par les techniques de test de type boîte noire.
Ignorer les tests de boîte noire équivalents	(Désélectionné par défaut.) Cela signifie que les tests glass box et les tests de boîte noire de la même vulnérabilité (Classification des menaces par le consortium WASC) sont envoyés. En effet, même si les tests glass box sont généralement plus précis et fournissent des résultats plus détaillés, il arrive qu'un test glass box échoue et que le test de boîte noire équivalent aboutisse. Si les résultats pour votre application sont inchangés lorsque des tests de boîte noire sont ignorés, vous pouvez réduire le temps d'examen en cochant cette case.

Remarque : Par défaut, les deux cases principales sont sélectionnées. Les *désélectionner* toutes les deux revient à désactiver l'examen glass box.

Voir aussi :

«Examen glass box», à la page 165

«Installation de l'agent glass box», à la page 166

«Définition de l'agent glass box dans AppScan», à la page 178

«Examen à l'aide de glass box», à la page 181

Vue Communication et Proxy

Vue Communication et Proxy (si AppScan a besoin d'un proxy pour accéder à l'application testée) de la boîte de dialogue Configuration.

Paramètre	Détails
Communication	
Nombre d'unités d'exécution	Définissez le nombre de demandes qui seront envoyées simultanément. Par défaut, ce nombre est défini sur une valeur maximale possible de 10. Si votre site n'autorise pas les unités d'exécution simultanées, veuillez réduire ce nombre à 1.
Ajuster automatiquement le délai d'attente	Dans certains cas, vous serez en mesure de réduire la durée de l'examen en sélectionnant **Ajuster automatiquement le délai d'attente pendant l'examen**. Lorsque cette option est sélectionnée, AppScan révise et ajuste le délai d'attente automatiquement lors de l'examen, ce qui peut réduire significativement la durée de l'examen.
Dépassement du délai	Si la case à cocher ci-dessus est désélectionnée, définissez la durée maximale (en secondes) pendant laquelle AppScan doit attendre une réponse du serveur Web. Un délai d'attente de 10 secondes est sélectionné par défaut.
Limite de débit de demande	Par défaut, AppScan envoie ses demandes au site aussi rapidement que possible. Si l'examen envoie à votre réseau ou à votre serveur des demandes dépassant sa capacité, ou si votre site limite les utilisateurs à un taux de demande maximal, cochez cette case et réduisez la limite. • Si l'exploration basée sur les actions est utilisée (Configuration > Options d'exploration > Méthode d'exploration), ce paramètre affecte uniquement l'étape de test de l'analyse • Si l'exploration basée sur les demandes est utilisée, ce paramètre affecte à la fois l'étape d'exploration et de test de l'analyse
Proxy	
Paramètres du proxy	Si AppScan a besoin d'un proxy pour accéder à votre application, configurez-le ici. Par défaut, AppScan est configuré pour utiliser les paramètres de proxy Internet Explorer. **Utiliser les paramètres de proxy d'Internet Explorer** (Par défaut) Sélectionnez ce paramètre pour utiliser l'adresse et le port de la connexion Internet Explorer. Si l'authentification est requise, ajoutez le nom d'utilisateur, le mot de passe et le domaine ci-dessous. **Ne pas utiliser de proxy** Sélectionnez cette option si vous ne voulez pas autoriser AppScan à utiliser un proxy. **Utiliser des paramètres de proxy personnalisés** Sélectionnez cette option pour définir vos propres paramètres de proxy. Entrez l'adresse et le port du proxy. Si l'authentification est requise par le proxy, ajoutez le nom d'utilisateur, le mot de passe et le domaine ci-dessous.

Vue Authentification HTTP

Vue Authentification HTTP de la boîte de dialogue Configuration.

Utilisez cette vue pour configurer les informations d'authentification de la plateforme et le certificat côté client, le cas échéant. AppScan prend en charge plusieurs certificats du magasin personnel de l'utilisateur, ou un certificat unique (par examen) au format PKCS#12 (PFX).

Conseil : Les certificats PEM ne sont pas pris en charge, mais vous pouvez les convertir en PFX (voir «Conversion d'un certificat PEM au format PFX/P12», à la page 108).

Paramètre	Détails
Authentification HTTP	Si votre site requiert une authentification Basic, Digest, NTLM, Negotiate ou Kerberos HTTP, entrez ici le nom d'utilisateur, le mot de passe et le domaine à utiliser par AppScan lors de l'examen.
Certificat côté client	Si votre serveur de site utilise des certificats côté client pour vérifier l'identité de l'utilisateur, AppScan doit en disposer. **Ne pas utiliser de certificat** (Par défaut) **PFX/P12** Utiliser un certificat PFX ou P12 unique. Cliquez sur pour sélectionner **Fichier du certificat** et entrez le **mot de passe**. **Certificats installés (incluant une carte à puce)** Utiliser les certificats installés sur cette machine. • Si vous connaissez le certificat requis ou si vous utilisez une carte à puce, il est préférable de l'ajouter manuellement : 1. Laissez la case **Identifier automatiquement les certificats requis** décochée. 2. Cliquez sur **Ajouter**. 3. Sélectionnez le ou les certificats à partir du magasin de certificats personnels Windows (pour l'utilisateur en cours). 4. Cliquez sur **Ajouter**. Les certificats sont ajoutés à la table. 5. Si le certificat requiert un numéro personnel d'identification, cliquez deux fois dans la colonne et indiquez-le. • Si vous ne savez pas de quels certificats vous avez besoin : 1. Cochez la case **Identifier automatiquement les certificats requis**. 2. Si un code confidentiel est requis et que vous le connaissez, indiquez-le dans la zone correspondante. Sinon, vous serez invité à le saisir lors du lancement de l'examen. **Conseil :** Il est possible que les cartes à puce nécessitant un code confidentiel deviennent verrouillées. Lorsque cela est possible, ajoutez le certificat manuellement. **Remarque :** Pour la plupart des certificats de carte à puce, la carte doit être insérée dans le lecteur.
Etat de connexion	Indique l'état de la connexion avec l'URL de départ configurée dans «Vue URL et serveurs», à la page 47.

Conversion d'un certificat PEM au format PFX/P12

Les certificats sur PEM ne sont pas pris en charge, ils doivent être convertis au format PKCS#12 (PFX/P12).

Pourquoi et quand exécuter cette tâche

Cette conversion peut s'effectuer à l'aide d'un outil externe tel que OpenSSL, comme décrit ci-dessous.

Procédure

1. Aller à https://www.openssl.org/community/binaries.html
2. Téléchargez et installez la version 1.0.1p.
3. Exécutez la commande suivante à partir du dossier bin de l'installation OpenSSL.

```
openssl pkcs12 -export -out Cert.p12 -in cert.pem -inkey key.pem -passin pass:root -passout pass:root
```

Vue Stratégie de test

La vue Stratégie de test de la boîte de dialogue Configuration affiche les détails relatifs à la stratégie de test courante.

Nombre de tests AppScan possibles pour qu'un site puisse atteindre les milliers. Plutôt que de filtrer manuellement un grand nombre de tests et de variantes de test, vous pouvez définir une stratégie générale pour le type de test que vous effectuez (ou ne souhaitez pas effectuer) sur votre application.

Utilisez la vue Stratégie de test pour afficher, éditer et gérer les stratégies de test qui définissent les tests inclus dans les examens, et pour définir la stratégie de l'examen en cours.

Les tests sont groupés et répertoriés dans le panneau supérieur. Les conseils et recommandations de correction pour le test sélectionné apparaissent dans le panneau inférieur.

La vue Stratégie de test vous permet d'effectuer les actions suivantes :

- Afficher les détails sur la stratégie en cours
- Editer la stratégie en cours pour créer une stratégie de test définie par l'utilisateur qui vous est propre
- Importer une stratégie prédéfinie ou une stratégie définie par l'utilisateur et enregistrée précédemment

Zone/Panneau/Option	**Détails**
Stratégie de test	Affiche le nom de la stratégie de test en cours. Les tests sont groupés et répertoriés dans le panneau supérieur. Les conseils et recommandations de correction pour le test sélectionné apparaissent dans le panneau inférieur.
Méthode de regroupement	Utilisez la liste déroulante pour sélectionner une méthode de regroupement pour les tests dans le panneau supérieur.
Filtre	Utilisez la liste déroulante pour filtrer les tests dans le panneau supérieur. Vous avez le choix entre : Tous, DAST uniquement (analyse dynamique), IAST uniquement (analyse d'exécution glass box) ou SAST uniquement (analyse statique).
Recherche	Si vous entrez du texte dans la zone de recherche, seuls les tests contenant la chaîne recherchée s'afficheront. La liste déroulante Loupe vous permet de définir si vous devez rechercher la chaîne dans *toutes* les zones de test ou uniquement dans certaines zones (par exemple, Nom du test ou ID CVE).
Exporter	Cliquez pour sauvegarder la stratégie de test en cours afin de pouvoir la charger ultérieurement.
Importer	Cliquez pour charger une stratégie de texte prédéfinie ou définie par l'utilisateur (voir «Importer une stratégie de test», à la page 111).
Description de la stratégie	Le panneau supérieur droit affiche la description de la stratégie en cours. Pour les stratégies définies par l'utilisateur, cette zone peut être éditée.
Panneau Test	Le panneau principal supérieur répertorie tous les tests AppScan qui répondent aux critères de filtre/recherche. Pour chaque test, les informations suivantes sont affichées : nom, ID variante, ID CVE, ID CWE, niveau de gravité attribué au problème (et s'il est attribué par CVSS ou l'utilisateur), XFID (ID X-Force), type, invasivité et classification des menaces WASC. Vous pouvez **Trier** des tests en fonction de certaines de ces zones en cliquant sur l'en-tête de colonne. Les tests dont la case à cocher est sélectionnée sont inclus dans la stratégie en cours. Vous pouvez modifier la stratégie en sélectionnant/désélectionnant des tests (voir «Editer une stratégie de test», à la page 110).
Mettre à jour un lien de paramètres	Ce lien ouvre une boîte de dialogue qui permet de définir les types de test pouvant être ajoutés à cette stratégie lorsque de nouveaux tests sont ajoutés à la base de données. Pour plus de détails, voir «Paramètres de mise à jour de stratégie de test», à la page 112.

Zone/Panneau/Option	Détails
Onglets Conseils et recommandations de correction	Le panneau principal inférieur affiche les conseils et recommandations de correction pour le test sélectionné. Vous pouvez **éditer** tout conseil selon vos propres spécifications, ou **Rétablir les valeurs par défaut** d'un conseil ayant été édité (voir «Editer des conseils et des recommandations de correction», à la page 112).
Fichiers de stratégies	Chargez une stratégie de test existante en cliquant sur **Stratégies récentes** ou **Stratégies prédéfinies**, ou en cliquant sur **Parcourir...** et en accédant à la stratégie requise.

Editer une stratégie de test

La vue Stratégie de test peut être utilisée pour ajuster précisément votre stratégie de test sélectionnée.

Pourquoi et quand exécuter cette tâche

Vous pouvez ajuster la stratégie de test courante en ajoutant ou en supprimant des tests, et en exportant la configuration modifiée en tant que stratégie de test en vue d'une utilisation ultérieure.

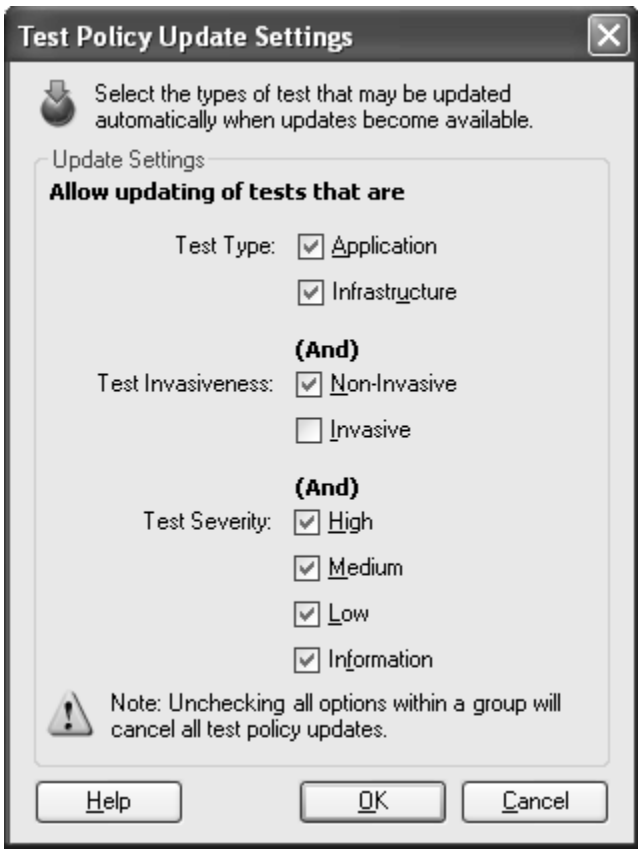
Procédure

1. Dans la boîte de dialogue Configuration des examens, cliquez sur **Stratégie de test** (ou dans **Assistant de configuration des examens > Stratégie de test**).

   La zone supérieure répertorie tous les tests AppScan et indique lesquels sont inclus à l'examen en cours (case cochée).
2. Vous pouvez alors inclure/exclure des tests ou des variantes en cochant/décochant des cases. (Pour visualiser des variantes individuelles, cliquez sur l'icône **+** en regard du nom du test.)

   Remarque : Pour chaque test, les informations suivantes sont affichées : nom, ID variante, ID CVE, ID CWE, niveau de gravité attribué au problème (et s'il est attribué par CVSS ou l'utilisateur), type, invasivité, classification des menaces WASC et XFID (ID X-Force). Vous pouvez **Trier** des tests à partir de chacune de ces zones, en cliquant sur l'en-tête de colonne.

   Remarque : La fonction **Rechercher** permet de rechercher des tests à l'aide de la recherche de texte libre.
3. Dans la zone Informations située dans la partie supérieure droite de la boîte de dialogue, vous pouvez éditer la description.
4. De nouveaux tests sont continuellement ajoutés à la base de données de tests d'AppScan. Par défaut, tous les nouveaux tests, à l'exception des tests invasifs, sont ajoutés à toutes les stratégies de tests définies par l'utilisateur. Vous pouvez toutefois définir quels groupes de votre stratégie seront mis à jour : cliquez sur **Mettre à jour les paramètres**, cochez/décochez les cases dans la boîte de dialogue **Paramètres de mise à jour des stratégies de test** comme nécessaire, puis cliquez sur **OK**.



On distingue trois groupes : Type de test, Invasivité du test et Gravité du test. Seuls les tests appartenant à une catégorie sélectionnée *dans les trois groupes à la fois* seront ajoutés à la stratégie en cours lorsque de nouveaux tests sont ajoutés à votre base de données de tests AppScan. Exemple : si vous sélectionnez **Gravité élevée** et que vous désélectionnez **Invasif**, les tests de gravité élevée et invasifs ne seront *pas* ajoutés à cette stratégie lorsque des mises à jour seront disponibles.

5. Vous pouvez éventuellement donnez un nom à l'examen et l'enregistrer pour une utilisation ultérieure (cliquez sur **Exporter** et sauvegardez au format **.policy**).
6. Cliquez sur **OK** pour sauvegarder les modifications dans la stratégie de test en cours.

Importer une stratégie de test

Pourquoi et quand exécuter cette tâche

Vous pouvez charger des stratégies de test récentes, prédéfinies et définies par l'utilisateur.

Procédure

Procédez de l'une des façons suivantes :

- Dans la zone Fichiers de stratégie, sélectionnez l'une des **Stratégies récentes** ou **Stratégies de test prédéfinies** répertoriées (voir «Stratégies de test prédéfinies», à la page 112)
- Pour ouvrir une stratégie définie par l'utilisateur non répertoriée dans la zone Fichiers de stratégies, cliquez sur le bouton **Importer** dans la partie supérieure de l'écran (ou cliquez sur **Parcourir** dans la zone Fichiers de stratégies).

Résultats

La stratégie sélectionnée se charge et son nom et sa description apparaissent dans la partie supérieure de la boîte de dialogue.

Stratégies de test prédéfinies

Le panneau Fichiers de stratégies situé dans la partie inférieure gauche de la vue Stratégie de test permet de sélectionner l'une des stratégies récemment utilisées ou l'une de celles prédéfinies. Les stratégies prédéfinies fournissent une large gamme de stratégies utiles pour les exigences courantes.

Nom de règle	Description
Par défaut	Inclut tous les tests sauf les tests invasifs et ceux du programme d'écoute des ports.
Application uniquement	Inclut tous les tests au niveau application, à l'exception des tests invasifs et de ceux du programme d'écoute des ports.
Infrastructure uniquement	Inclut tous les tests au niveau infrastructure, à l'exception des tests invasifs et de ceux du programme d'écoute de port.
Tiers uniquement	Inclut tous les tests de niveau tiers, à l'exception des tests invasifs et d'écouteur de port.
Invasif	Inclut tous les tests invasifs (tests pouvant affecter la stabilité du serveur).
Terminée	Inclut tous les tests AppScan.
Services Web	Inclut tous les tests associés à SOAP, à l'exception des tests invasifs et de ceux du programme d'écoute de port.
Le minimum indispensable	Inclut une sélection de tests présentant une forte probabilité de réussite. Peut être utile pour évaluer un site lorsque le temps disponible est limité.
Fondamentaux du développeur	Inclut une sélection de tests d'*application* présentant une forte probabilité de réussite. Peut être utile pour évaluer un site lorsque le temps disponible est limité.
Site de production	Exclut les tests invasifs susceptibles de dégrader le site ou les tests susceptibles d'entraîner un refus de service aux autres utilisateurs. **Remarque :** Pour plus d'informations sur l'examen d'un site opérationnel, voir «Examen des environnements de production opérationnels», à la page 323.

Paramètres de mise à jour de stratégie de test

Cette boîte de dialogue s'ouvre à partir de la vue Configuration d'examen > Stratégie de test.

Sélectionnez les types de test, le cas échéant, qui seront ajoutés à la stratégie de test en cours lors de l'intégration de nouveaux tests dans votre base de données de tests AppScan. Les tests sont mis à jour lorsque vous chargez un examen ou un modèle, ou lorsque vous importez un fichier de stratégie de test.

Il existe trois types : Type de test, Invasivité du test et Gravité du test. Notez que seuls les tests qui appartiennent à une catégorie sélectionnée *dans les trois groupes à la fois* seront ajoutés à la stratégie en cours lorsque de nouveaux tests sont mis à disposition. Par exemple : Si vous sélectionnez **Gravité élevée** et que vous désélectionnez **Invasif**, les tests de gravité élevée et invasifs ne seront pas ajoutés à cette stratégie lorsque des mises à jour seront disponibles.

Editer des conseils et des recommandations de correction

Pourquoi et quand exécuter cette tâche

Vous pouvez modifier le texte apparaissant dans les onglets Conseils et recommandations de correction des résultats de l'examen d'un test (voir «Onglet Conseils», à la page 217). (Dans ce cas, le fichier édité est sauvegardé au format .xml sur votre ordinateur. L'emplacement exact est configuré dans Outils | Options | onglet Préférences, voir «Onglet Préférences», à la page 261.) Le texte des conseils ainsi que celui des recommandations de correction est stocké dans le même fichier. (Vous pouvez restaurer le texte d'origine à tout moment à l'aide du bouton *Rétablir les valeurs par défaut*.)

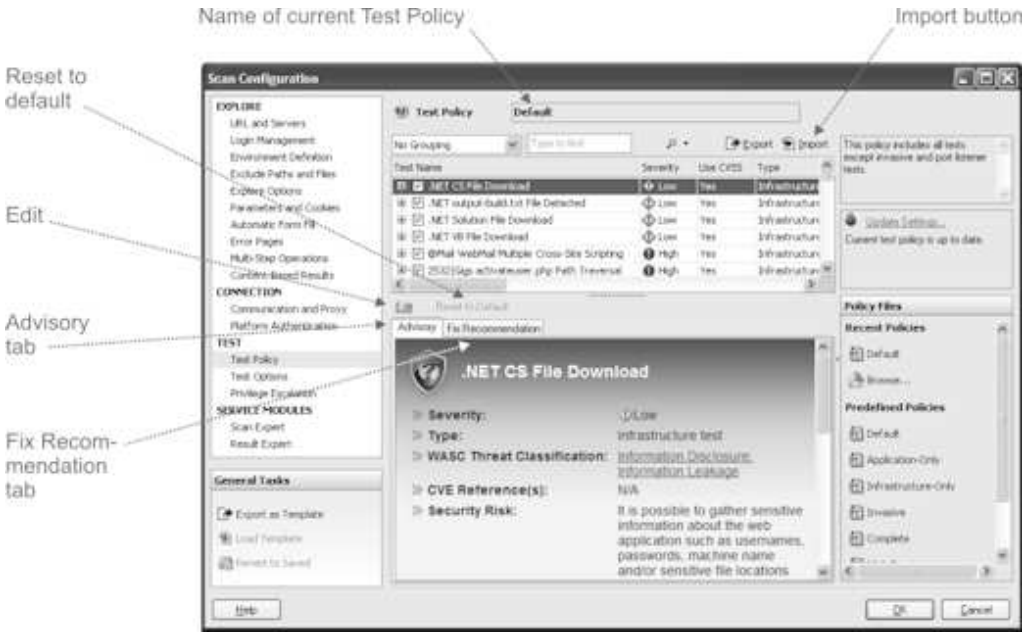
Remarque : Si votre examen est envoyé à un autre ordinateur, le conseil d'origine *par défaut* pour le problème, et non votre conseil édité, sera affiché (sauf si vous envoyez le fichier .xml à l'autre ordinateur, et que l'utilisateur l'enregistre dans le dossier des conseils personnalisés *de cet ordinateur*, voir «Onglet Préférences», à la page 261).

Remarque : Si IBM publie une version mise à jour d'un conseil ou d'une recommandation de correction que vous avez édité, la version mise à jour n'apparaîtra pas dans votre interface AppScan (sauf si vous annulez les modifications effectuées en cliquant sur le bouton *Rétablir les valeurs par défaut*).

Procédure

1. Sélectionnez le test requis.

   Les conseils et recommandations de correction pour le test sélectionné apparaissent dans le panneau inférieur.



2. Cliquez sur l'icône **Editer** au-dessus de l'onglet Conseils. (Quel que soit le test, les conseils et recommandations de correction sont stockés dans le même fichier. Peu importe donc lequel des deux onglets se trouve dans la partie supérieure lorsque vous cliquez sur **Editer**.)

   Le fichier de conseil est ouvert dans l'éditeur XML intégré.

3. Editez le texte comme nécessaire, puis cliquez sur **OK**.

   Remarque : Si vous utilisez une syntaxe XML non valide, ou des balises qui ne font pas partie du schéma du fichier de conseil, un avertissement s'affiche et les modifications ne sont pas sauvegardées.

   L'éditeur XML se ferme et les modifications apparaissent dans le conseil en cours.

Restaurer des conseils par défaut :
Pourquoi et quand exécuter cette tâche

Si les conseils d'un test particulier ont été modifiés par l'utilisateur, le bouton Restaurer la valeur par défaut est actif lorsque ce test est sélectionné.

Procédure

Sélectionnez les tests appropriés dans le Gestionnaire de stratégies de test et cliquez sur **Restaurer la valeur par défaut**.

Vue Optimisation du test

L'option Optimisation du test utilise le filtrage intelligent des tests de AppScan pour exécuter des examens plus rapidement.

Généralement, un examen AppScan Standard complet standard envoie des milliers de tests et son exécution peut prendre plusieurs heures, voire plusieurs jours. Au cours des premières étapes de développement, ou pour avoir une évaluation globale rapide du contexte de sécurité actuel de votre produit, vous pouvez utiliser Optimisation du test pour obtenir les résultats requis dans un délai plus court.

Nos filtres de test intelligents s'appuient sur l'analyse statistique et filtrent certains tests (ou même des variantes de test spécifiques) pour générer un examen plus court qui identifie uniquement les vulnérabilités les plus fréquentes, graves et importantes. Les groupes de correctif et les correctifs iFixes AppScan permettent de vous maintenir à jour grâce aux filtres d'optimisation les plus récents. Grâce à l'option Optimisation du test, vous pouvez réduire considérablement la durée de l'examen, lorsque vous accordez davantage d'importance à la vitesse qu'à la profondeur de l'examen.

Option	Description
Normal (par défaut)	Effectue un examen en profondeur, pour envoyer tous les tests appropriés au site, selon la configuration. Ce paramètre est recommandé lorsqu'un examen plus long ne va pas interrompre votre flux de développement.
Optimisé	Accélère l'examen en envoyant uniquement des tests pour les vulnérabilités les plus fréquentes, graves et importantes.

Voir aussi : «Compréhension de l'option Optimisation du test», à la page 325

Vue Options de test

Vue Options de test de la boîte de dialogue Configuration.

Cette vue permet de configurer divers paramètres affectant la longueur et la précision de l'examen. Les paramètres par défaut sont cependant suffisants dans la plupart des cas.

Paramètre	Détails
Options de test :	
Utiliser des tests adaptatifs	AppScan peut envoyer plusieurs milliers de tests à un site. Cependant, pour réduire le temps d'examen, il peut envoyer des tests préliminaires qui déterminent, de façon intelligente, quels sont les tests appropriés à envoyer et quels sont ceux qui ne le sont pas. Ce sont les "tests adaptatifs". Ils peuvent considérablement réduire le temps d'examen, sans pour autant faire baisser l'efficacité. Décochez cette case si vous souhaitez qu'AppScan envoie *tous* ses tests au site.
Autoriser l'examen en plusieurs phases	AppScan analyse les réponses aux tests qu'il envoie à votre application. A partir de cette analyse, AppScan découvre fréquemment du contenu supplémentaire, tel que des liens invisibles lors de la première "phase" de l'examen. L'examen en plusieurs phases permet à AppScan de répéter les étapes d'exploration et de test sur ce contenu nouvellement détecté. (La phase supplémentaire est généralement plus courte puisqu'elle n'implique que les nouveaux liens.) L'examen en plusieurs phases est configuré par défaut pour permettre un maximum de 4 phases d'examen. Notez que l'examen en plusieurs phases s'applique uniquement lorsque vous exécutez un examen intégral. Si vous utilisez les fonctions Exploration uniquement et Test uniquement, le résultat sera un examen à une seule phase.
Envoyer les tests sur les pages de connexion et de déconnexion	Nous vous recommandons d'autoriser AppScan à effectuer des tests des pages de connexion et de déconnexion, sauf si votre application interdit l'accès aux utilisateurs qui fournissent une entrée interdite ; le flux de l'application serait altéré si AppScan testait ces pages.

Paramètre	Détails
Ne pas envoyer d'identificateurs de session lors des tests des pages de connexion.	(Actif uniquement si la case précédente est cochée.) Il est recommandé de laisser cette case cochée, car les identificateurs de session peuvent limiter la réussite des tests des pages de connexion. Désactivez cette option uniquement si vous êtes certain que des jetons de session valides sont nécessaires pour tester vos pages de connexion. Notez que même lorsque cette case n'est pas sélectionnée, *certains* tests sont tout de même envoyés avec des identificateurs de session, pour empêcher les résultats faux positifs.
Analyser les résultats pour rechercher les problèmes déclenchés par inadvertance	Lorsque cette option est sélectionnée, AppScan analyse chaque réponse du test pour détecter d'autres problèmes de sécurité en plus de celui qu'il a testé. Désélectionnez cette option si l'application est très grande ou si les examens génèrent un grand nombre de résultats faux positifs.
Inclure toutes les variantes de chaque problème	(Actif uniquement si la case précédente est cochée.) Lorsque cette option est sélectionnée, AppScan analyse toutes les variantes de chaque problème déclenché par inadvertance. Lorsqu'elle est désélectionnée, une seule variante par problème est analysée. Il n'est généralement pas nécessaire de cocher cette case, car cela augmente considérablement la durée de l'analyse.
Tester les problèmes de sécurité des cookies dans les demandes de soumission de formulaire uniquement	Lorsque ce paramètre est sélectionné (par défaut), AppScan applique les tests associés à des cookies uniquement aux cookies utilisés dans les demandes de soumission de formulaire. Pour une précision plus élevée (impliquant également une durée d'examen plus longue), décochez cette case afin qu'AppScan soumette des tests de cookie pour toutes les requêtes HTTP pertinentes.
Sauvegarder les informations sur les variantes de test non vulnérables	Lors d'un examen, AppScan envoie plusieurs milliers de variantes du test au site testé. La plupart des réponses indiquent qu'il n'y a aucune menace concernant la sécurité, et AppScan annule par défaut tous ces résultats "non vulnérables", réduisant ainsi considérablement le volume des données de résultats. Si vous cochez cette case, AppScan enregistre toutes les variantes non vulnérables. Un avertissement s'affiche, cette option risquant de réduire la performance d'AppScan et d'augmenter considérablement l'espace disque requis. Pour plus de détails, voir «Variantes non vulnérables», à la page 226.
Activer l'analyse de la sécurité JavaScript	Active une analyse statique de JavaScript capable de détecter divers problèmes côté client, principalement le scriptage intersite basé sur DOM, dans le code JavaScript côté client. Pour plus de détails, voir «Analyse JavaScript».
Gestion des problèmes :	
Appliquer les classifications de bruit précédentes à cet examen	Si, lors d'un examen précédent, vous avez classé un ou plusieurs problèmes comme "Bruit" (ne s'appliquant pas à votre application), les mêmes paramètres sont automatiquement appliqués aux examens à venir, sauf si vous décochez cette case. Pour plus de détails, voir «Etat du problème : Ouvert ou Bruit», à la page 209.

Remarque : Si vous apportez des modifications aux Options de test *après* un examen, il est possible qu'une invite vous demande de procéder à un nouvel examen, car toutes les modifications peuvent s'appliquer aux résultats existants.

Analyse JavaScript

Cette section décrit les grandes lignes du fonctionnement de l'analyse statique de JavaScript et la façon dont les résultats sont présentés.

Résultats de l'analyse JavaScript

AppScan effectue une analyse statique du code source JavaScript, par conséquent les problèmes identifiés incluent les informations de trace au niveau de la source, en présentant le code source vulnérable. Vous pouvez visualiser les informations de trace dans l'onglet Informations sur les problèmes de la sous-fenêtre Détail.

Les lignes du code numérotées et mises en évidence indiquent, étape par étape, comment des données non fiables sont propagées depuis la source jusqu'au collecteur, jusqu'à leur utilisation non sécurisée.

AppScan utilise la technologie avancée d'analyse des chaînes pour éliminer les résultats faussement positifs et classifier les problèmes de manière plus précise.

Principe de l'analyse de chaîne

AppScan met en œuvre deux étapes d'analyse pour chaque page : une analyse des données ou des flux de données corrompus, et une analyse de chaîne. Dans la première analyse, AppScan recherche la trace d'un flux complet ne passant pas par une étape de nettoyage. Si une telle trace est trouvée, AppScan la valide à l'aide de dans une deuxième phase, à l'aide de la technique d'analyse du préfixe de chaîne, SPA (string prefix analysis), qui est une variante de l'analyse de chaîne (string analysis).

Dans certains cas, si la source est une URL, ou une portion d'URL, la trace n'est exploitable que si un agresseur informatique peut prendre le contrôle des portions d'URL contenant l'hôte et le chemin au niveau de la terminaison du flux. SPA valide ces cas en suivant les opérations de la chaîne manipulant l'URL source. SPA considère que l'hôte et le chemin de l'URL ne sont pas contrôlés par le cyber-attaquant tant que la portion de la requête et/ou de l'ancre sont :

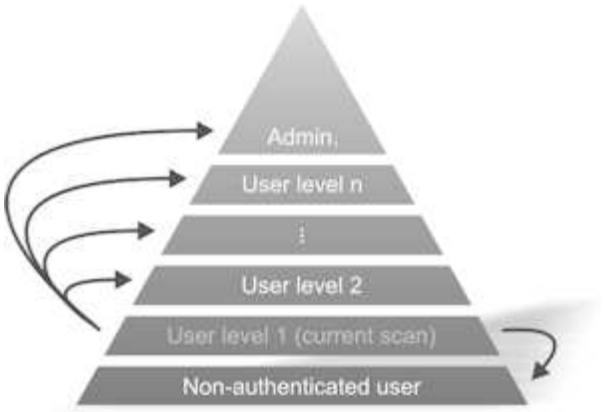
Au niveau de la terminaison du flux, SPA vérifie si un cyber-attaquant peut prendre le contrôle des portions d'URL contenant l'hôte et le chemin. S'il détermine que les portions contenant l'hôte et le chemin sont fixes et ne sont pas contrôlées par un agresseur, le problème est éliminé.

Si la cible du réacheminement commence par le préfixe `javascript:` ou `mailto:`, le problème est classifié comme “attaque XSS par injection DOM” ou “usurpation d'adresse courriel” respectivement.

Vue Escalade des droits d'accès

La vue Escalade des droits d'accès de la boîte de dialogue Configuration permet de comparer les résultats pour différents niveaux d'utilisateur.

Pourquoi et quand exécuter cette tâche



AppScan peut faire référence à des examens exécutés à l'aide de divers droits utilisateur afin de déterminer quelles ressources privilégiées sont accessibles aux utilisateurs dont les droits d'accès sont insuffisants. Vous pouvez le faire de deux manières :

- **Par comparaison avec un utilisateur privilégié supérieur :** vous faites pointer AppScan vers des résultats d'examen produits à l'aide d'un niveau supérieur de droits d'accès que l'examen en cours. Lors de l'examen, AppScan tente d'accéder aux liens supplémentaires disponibles à l'utilisateur de niveau supérieur à l'aide des droits d'accès en cours (niveau inférieur). Les résultats de l'examen indiquent quelles tentatives ont abouti.
- **Par comparaison avec un utilisateur non authentifié :** Vous pointez AppScan pour numériser les résultats qui ont été produits *sans* authentification utilisateur. AppScan exécute ensuite une analyse à l'aide de l'authentification en cours et note les nouveaux liens auxquels il accède. Il se déconnecte ensuite et tente d'accéder à ces nouveaux liens *sans* authentification. Les résultats de l'examen indiquent quelles tentatives ont abouti.

Important : Les examens comparés doivent avoir la même configuration pour les examens et des données d'exploration équivalentes. Par exemple, si le site a été exploré manuellement avant le test dans l'un des examens, la *même* exploration manuelle doit être effectuée avant l'étape de test dans les examens comparés avec lui.

Procédure

1. **(Pour la comparaison avec un utilisateur disposant de droits plus élevés :)** Dans la zone supérieure ("Tests pour utilisateur disposant de droits plus élevés"), cliquez sur  et accédez à un examen exécuté avec des droits d'accès supérieurs à ceux de l'examen en cours.
2. Cliquez sur **Ouvrir**.
3. Entrez un nom qui représente le niveau d'authentification utilisé dans l'examen (par exemple Invité, Administrateur), puis cliquez sur **OK**.

   L'examen sélectionné est ajouté à la liste, et son rôle (par ex. Administrateur, Opérateur, Visiteur) apparaît dans la colonne de gauche.
4. Répétez ces étapes pour ajouter des examens avec différents niveaux d'authentification si nécessaire.

Remarque : Vous pouvez ajouter plusieurs examens pour des tests pour utilisateur disposant de droits plus élevés, un pour chaque rôle. Par exemple, si l'examen en cours est configuré avec le nom d'utilisateur et le mot de passe d'un utilisateur normal, vous pouvez ajouter deux examens à cette liste : un exécuté avec des droits d'administrateur, l'autre exécuté avec des droits de superviseur. Les résultats indiqueront quelles ressources d'utilisateur trouvées sont accessibles à l'utilisateur normal.

5. **(Pour la comparaison avec un utilisateur non authentifié :)** Vous pouvez également, facultativement, charger les résultats d'un examen exécuté *sans* authentification. Pour ce faire, dans la zone inférieure, cliquez sur  , et accédez aux résultats de l'examen.

Vue Logiciels malveillants

La vue Logiciels malveillants de la boîte de dialogue Configuration permet de configurer des tests d'identification des logiciels malveillants.

Un test d'identification des logiciels malveillants se compose de deux modules offrant diverses options de configuration. Ils sont configurés à partir de cette vue. La configuration du test n'affecte pas les examens standard.

Paramètre	Détails
Tests de recherche de logiciels malveillants	**Rechercher les liens vers des sites Web externes malveillants** Lorsque cette case est cochée, AppScan recherche dans l'application les éventuels liens externes non souhaités durant l'examen. Une connexion Internet est requise.
Portée	Vous pouvez également créer une liste d'expressions régulières définissant les URL à *exclure* des examens d'identification des logiciels malveillants. Utilisez  pour ajouter une expression régulière et, dans la boîte de dialogue qui s'affiche, cliquez sur  pour ouvrir Expression Test PowerTool qui vous aidera à vérifier la syntaxe de vos expressions régulières. Si vous avez besoin d'aide supplémentaire pour écrire des expressions régulières, suivez les liens : http://www.regular-expressions.info/quickstart.html
Résultats supplémentaires	Les cases à cocher de cette section permettent d'élargir la portée de l'analyse des logiciels malveillants. Lorsqu'AppScan analyse les résultats pour les liens classés comme "Malveillants", il peut également signaler ceux classés comme **Indésirables** et **Inoffensifs**, ainsi que ceux **Non classés** par ISS, qui peuvent néanmoins être problématiques. Sélectionnez les types d'incidents à inclure dans les résultats. **Remarque :** Certains liens correspondant au type de problème "Non classé" peuvent en réalité être malveillants. **Remarque :** L'inclusion des liens inoffensifs peut augmenter considérablement le nombre de résultats.

Vue Scan Expert

Vue Scan Expert de la boîte de dialogue Configuration des examens.

Scan Expert exécute une brève exploration avant que l'examen principal ne commence. Il analyse les résultats de cette exploration pour évaluer l'efficacité des paramètres que vous avez configurés et suggère des modifications le cas échéant. Les modifications suggérées peuvent alors être implémentées avant de démarrer l'examen principal afin d'en optimiser l'efficacité. (Pour plus de détails, voir «Scan Expert», à la page 164.)

Les paramètres de cette vue permettent de décider la précision de l'exploration de Scan Expert, si les modifications de configuration sont implémentées automatiquement ou manuellement et quels "modules" de la configuration sont inclus à l'évaluation.

Remarque : Par défaut, Scan Expert s'exécute automatiquement avant chaque examen complet. Vous pouvez vérifier ou modifier ce paramètre en sélectionnant **Outils > Options... > Préférences**.

Paramètre	Détails
Comportement de Scan Expert	**Limite de l'évaluation :** Définissez à quelle vitesse (ou profondeur) vous souhaitez que Scan Expert explore votre application. Une exploration plus profonde peut permettre une évaluation plus complète. Vous pouvez définir un nombre maximal d'URL à explorer lors de l'évaluation, une durée, ou les deux. Si vous limitez l'évaluation par *les deux*, l'évaluation s'arrêtera lorsque la *première* des deux limites sera atteinte. (Remarque : L'examen peut ne pas toujours s'arrêter exactement à la limite, mais peu de temps après.) **Après l'évaluation :** Définissez si les recommandations de Scan Expert doivent être implémentées et si l'examen doit être démarré automatiquement, ou si le système doit attendre que vous révisiez les recommandations et implémentiez manuellement celles que vous approuvez. (Notez que certains modules ne peuvent pas être implémentés automatiquement ; ainsi, si vous sélectionnez des paramètres "activés automatiquement" pour ces modules, ces derniers ne seront pas évalués.)
Modules	Le panneau Modules répertorie tous les modules pouvant être évalués par Scan Expert. Cochez/décochez les cases pour que les modules sélectionnés soient ceux que vous souhaitez inclure à l'évaluation. Utilisez les flèches de déplacement vers le haut et vers le bas pour réorganiser l'ordre des modules (pour des raisons pratiques uniquement ; cela n'affecte pas la manière dont ils sont traités). Pour plus de détails, voir «Modules Scan Expert».

Voir aussi : «Scan Expert», à la page 164

Modules Scan Expert

Tableau des modules Scan Expert et de leur description.

La liste est organisée dans l'ordre dans lequel les modules s'exécutent. S'il existe un conflit entre les recommandations de plusieurs modules, celui situé le plus *bas* dans la liste prévaut.

Si vous ajoutez votre propre module, celui-ci est ajouté au bas de la liste, de sorte que votre nouveau module prévaut en cas de conflit avec les modules existants.

Si nécessaire, utilisez les flèches vers le haut et vers le bas pour faire monter ou descendre des modules dans la liste.

Module	Description
Détection de navigation basée sur des paramètres	Vérifie si l'application utilise la navigation basée sur des paramètres et facilite la configuration correcte de l'examen pour cette utilisation.
Authentification de serveur	Recherche les détails manquants sur l'authentification NTLM et HTTP, ainsi que les échecs.
Serveur proxy	Vérifie qu'aucune erreur de connexion proxy ou d'authentification ne s'est produite.
Certificat côté client	Détecte si un certificat client est requis.
Connexion enregistrée manquante	Si l'examen est configuré pour détecter les pages de connexion automatiquement, alerte l'utilisateur lorsqu'aucune page n'est détectée.
Détection des infrastructures AJAX	Recherche les marqueurs des infrastructures AJAX courantes qui requièrent l'exécution de JavaScript.

Module	Description
Détection des ID session	Vérifie si des ID session ont été détectés pour la séquence de connexion automatique ou enregistrée.
Formulaires non remplis	Détecte les formulaires non remplis.
Détection des serveurs non testés	Détecte les URL vers des serveurs autres que le serveur de l'URL de départ, dans le même domaine que cette URL. Si ces liens sont détectés, le module recommande de les ajouter à la liste des serveurs et domaines supplémentaires (Configuration > URL et serveurs).
Délai de communication	Evalue la précision de la configuration du délai d'attente des communications.
Nombre d'unités d'exécution	Evalue la capacité de l'application à supporter plusieurs unités d'exécution d'examen.
Détection des pages d'erreur	Détecte les pages d'erreur personnalisées dans l'application.
Chemin d'accès sensible à la casse	Vérifie la sensibilité à la casse dans le serveur d'applications Web.
URL suspectes	Détecte les URL suspectes qui devraient être exclues de l'examen.
Lien de déconnexion manquant	Détecte les pages de déconnexion.
Limite de profondeur	Vérifie si les liens sont inaccessibles, à cause d'une limite de profondeur. Si c'est le cas, le module peut suggérer l'accroissement ou la désactivation de la limite de profondeur.
Détection des objets Flash	Détecte l'utilisation de Flash dans l'application Web.
Services Web	Détecte l'existence de services Web dans l'application.
Vérification des paramètres environnementaux	Lorsque l'onglet Paramètres environnementaux contient des questions générales, avertit l'utilisateur si aucune réponse n'a été fournie à ces questions.
Détection de WebSphere Portal	Vérifie si l'application testée est basée sur WebSphere Portal.
Evaluation Scan Expert	Vérifie si l'évaluation Scan Expert a été effectuée correctement.
Détection Hacme Bank	Vérifie si l'application testée est McAfee Foundstone Hacme Bank.
Détection WebGoat	Vérifie si l'application testée est WebGoat de l'OWASP

«Vue Scan Expert», à la page 118

Vue Configuration avancée

L'onglet **Avancé** de la boîte de dialogue **Configuration des examens** permet de modifier des paramètres avancés du registre qui affectent des examens spécifiques (Examen > Configuration des examens > onglet Avancé) et devrait être utilisé uniquement par des utilisateurs AppScan expérimentés ou conformément aux instructions de l'équipe de support en vue de traiter un problème.

Conseil : Les paramètres avancés du registre affectant AppScan *généralement* (et non pas un examen spécifique) sont situés sous l'onglet **Avancé** de la boîte de dialogue **Options** (Outils > Options > onglet Avancé).

Remarque : Chaque paramètre est associé à un ID que vous pouvez utiliser dans vos communications avec l'équipe de support. Les éléments de la grille peuvent être triés par nom ou par ID en cliquant sur l'en-tête de la colonne pertinente.

Remarque : Lorsqu'un paramètre par défaut constitué par une expression régulière est supprimé, il est considéré comme non défini (et non comme une expression régulière englobant tout).

Nom	Description	Scénarios d'utilisation possibles
Basés sur les actions :		
Navigateur de lecture de connexion	Lorsque vous enregistrez la séquence de connexion, le navigateur AppScan intégré est toujours utilisé pour effectuer l'enregistrement basé sur les actions. Toutefois, vous pouvez configurer le navigateur utilisé par AppScan lors de la *lecture* de l'enregistrement pendant l'examen. Les options sont les suivantes : • 0 = Internet Explorer (version intégrée) • 1 = Chromium • 2 = Chrome • 3 = Firefox Valeur par défaut : 0	
Navigateur de lecture d'opérations en plusieurs étapes	Lorsque vous enregistrez une séquence en plusieurs étapes, le navigateur AppScan intégré est toujours utilisé pour effectuer l'enregistrement basé sur les actions. Toutefois, vous pouvez configurer le navigateur utilisé par AppScan lors de la *lecture* de l'enregistrement pendant l'examen. Les options sont les suivantes : • 1 = Chromium • 2 = Chrome • 3 = Firefox Valeur par défaut : 1	
Délai d'attente de non-interaction pour la lecture d'opérations en plusieurs étapes	Délai d'attente sans interaction (en secondes) avant l'arrêt de la lecture d'une opération en plusieurs étapes. Valeur par défaut : 10	
Délai d'attente pour la tentative de connexion	Durée (en secondes) pendant laquelle AppScan attend que le navigateur tente à nouveau d'effectuer une connexion basée sur les actions, avant de provoquer la fermeture du navigateur. Valeur par défaut : 120	
Communication :		

Nom	Description	Scénarios d'utilisation possibles
Valeur d'en-tête de requête langage Accept	Chaîne envoyée pour l'en-tête du langage ACCEPT dans toutes les requêtes HTTP. Si la valeur n'est pas définie par l'utilisateur, AppScan utilise la valeur envoyée par le navigateur lorsque l'utilisateur ouvre celui-ci pour la première fois au cours de l'examen, pour enregistrer la procédure de connexion ou une opération en plusieurs étapes, ou pour afficher une page. Remarque : Si vous modifiez le navigateur par défaut, consultez les conditions décrites à la rubrique «Modification du navigateur par défaut», à la page 334. Valeur par défaut : en-US	Lors de l'étape d'exploration, AppScan peut recevoir une réponse inattendue en raison de la valeur de l'en-tête Internet Explorer. Dans ce cas, vérifiez quelle valeur doit être utilisée dans l'en-tête de langage ACCEPT lors de l'interaction avec le site, et définissez-la dans ce paramètre (ou dans Internet Explorer).

En-têtes personnalisés	Permet de définir des en-têtes personnalisés à ajouter à toutes les requêtes envoyées par AppScan au site.
	
	Valeur par défaut : vide
		Si votre site attend un contenu d'en-tête spécifique (par exemple, si l'accès au site s'effectue via un plug-in client ou de navigateur spécifique), définissez le ou les en-têtes ici. Chaque en-tête doit être précédé par un délimiteur. L'en-tête et sa valeur doivent être séparés par un deux-points suivi d'un espace.
		
		Format : délimiteur|en-tête|deux-points et espace|valeur
		
		Exemple 1 :
		`;Header: Value`
		
		(Dans cet exemple, le délimiteur est **;**)
		
		Exemple 2 :
		`,Header1: Value1,Header2: Value2`
		
		(Dans cet exemple, le délimiteur est **,**)

Forcer une demande HTTP sans paramètre dans chaque action de formulaire	Dans certains cas, la logique côté serveur peut se comporter différemment lorsqu'une soumission de formulaire *sans* paramètre est reçue. Si l'option a pour valeur True, AppScan envoie une demande supplémentaire, sans paramètre, à chaque formulaire. En conséquence, des pages d'erreur personnalisées comportant des liens vers d'autres pages Web et d'autres fonctions peuvent être renvoyées. Valeur par défaut : Vrai	Si vous remarquez, lorsque vous affichez le trafic au cours de l'examen, que des soumissions de formulaire sans paramètre entraînent des dépassements de délai d'attente ou des pannes de l'application, vous pouvez choisir d'associer cette option à la valeur False.
Port SSL GSC	Ce paramètre définit le numéro de port utilisé dans GSC pour la communication SSL. Valeur par défaut : 443	Si les liens sont fournis via une Exploration GSC, AppScan identifie HTTPS en fonction de ce numéro de port. Si votre application utilise un port différent pour la communication SSL, définissez-le ici. Si vous n'avez pas défini le port SSL correct, AppScan enverra tous les tests en HTTP.

Nom	Description	Scénarios d'utilisation possibles
Inclure les en-têtes de débogage AppScan dans toutes les demandes	Si cette option a pour valeur True, un en-tête HTTP est ajouté à toutes les demandes envoyées par AppScan au site. Le nom de l'en-tête est "X-AppScan-Debug" et sa valeur inclut des informations sur la raison pour laquelle AppScan envoie cette demande particulière (exploration, test, lecture de la connexion, recherche des serveurs arrêtés, etc.). Valeur par défaut : Faux	La configuration de l'examen en vue de l'envoi d'en-têtes "X-AppScan-Debug" peut être utile pour le suivi du trafic AppScan dans des outils externes tels que des débogueurs Web, des proxys, des analyseurs et des renifleurs. Remarque : Il se peut que certains sites rejettent les demandes incluant ce type d'en-tête.
Longueur de réponse maximale	AppScan tronque les réponses longues pour éviter des problèmes de consommation de la mémoire. Ce paramètre définit la longueur de réponse maximale autorisée, en Mo. Les réponses plus longues sont traitées comme des erreurs. Valeur par défaut : 8	Si des liens semblent être absents dans AppScan, ou que la session est interrompue, et que l'application a l'habitude de renvoyer des réponses longues, l'augmentation de la longueur de réponse maximale peut être la solution à ce problème.
Supprimer l'en-tête de codage ACCEPT	AppScan supprime tous les codages qu'il ne prend pas en charge. Si ce paramètre est activé, AppScan supprimera l'intégralité de l'en-tête et non pas seulement les codages qu'il ne prend pas en charge. Valeur par défaut : Vrai	Si le serveur rejette les demandes d'AppScan, renvoie des réponses inattendues ou si AppScan ne parvient pas à maintenir ouverte la session, consultez le journal du trafic et comparez les demandes envoyées par AppScan à celles de votre navigateur habituel. Si l'en-tête de codage ACCEPT est différent ou manquant dans votre navigateur, vous devez activer ce paramètre.
Réutiliser les connexions serveur	Par défaut, AppScan ferme les connexions TCP après leur utilisation, car les connexions ouvertes, ainsi que les données sauvegardées, peuvent avoir un impact sur les résultats de l'examen. Si cette option a pour valeur True, AppScan laisse les connexions ouvertes après leur utilisation et tente de les réutiliser dès que possible. Valeur par défaut : Faux	Si des erreurs indiquant que les ressources du réseau sont épuisées surviennent sur le serveur Web, vous pouvez tenter de résoudre le problème en associant ce paramètre à la valeur True.
Ordre des packages de sécurité	AppScan prend en charge l'authentification Basic, Digest, NTLM, Negotiate, et Kerberos HTTP. Editez cette valeur pour forcer AppScan à utiliser ou non une méthode spécifique ou pour appliquer un ordre de préférence pour la sélection des méthodes lorsque le site ou le proxy en admet plusieurs. Par exemple, pour autoriser NTLM et Basic seulement et utiliser NTLM de préférence si disponible, remplacez la chaîne par : `ntlm, basic` Valeur par défaut : basic, digest, ntlm, negotiate, kerberos	Si votre site utilise une méthode d'authentification spécifique et que l'accès est refusé à AppScan, vous pouvez définir la méthode requise comme méthode unique pour tenter de résoudre le problème. Pour tester votre site avec des méthodes spécifiques, par exemple Basic et NTLM, vous pouvez configurer un examen avec la méthode Basic seulement et un deuxième examen avec la méthode NTLM seulement.
Norm. des barres obliques	Normalisez les URL en remplaçant deux barres obliques consécutives (ou plus) par une seule. Valeur par défaut : Vrai	Si les URL de votre site utilisent des barres obliques consécutives, désactivez ce paramètre.

Nom	Description	Scénarios d'utilisation possibles
Traiter la réponse en cas d'erreur comme valide	AppScan traite les pages d'erreur différemment des pages ordinaires (par exemple, leurs liens ne sont pas analysés). Ce paramètre vous permet d'indiquer à AppScan de traiter les pages d'erreur comme s'il s'agissait de pages ordinaires pour l'URL de départ uniquement ou dans tous les cas. Lorsque la valeur définie est 0, AppScan traite toutes les réponses en cas d'erreur comme non valides. Lorsque la valeur définie est 1, AppScan traite toutes les réponses en cas d'erreur pour l'adresse URL de départ (4xx et 5xx) comme étant valides. Lorsque la valeur définie est 2, AppScan considère que toutes les réponses en cas d'erreur sont valides pour les pages standard et l'adresse URL de départ. Valeur par défaut : 0	Si la réponse à votre adresse URL de départ est une page d'erreur, associez la valeur 1 au paramètre. Pour que l'examen procède à l'extraction de données à partir de pages d'erreur et les teste, associez la valeur 2 au paramètre. La modification du paramètre par défaut peut avoir un impact sur les performances.
Flash :		
Couverture	Définit le "niveau de couverture" de l'examen. 1=examen plus rapide ; 2=couverture plus complète. Valeur par défaut : 1	Pour une couverture plus complète (mais plus lente) du contenu Flash, attribuez la valeur 2 à ce paramètre.
Exclure des instances	Indiquez les instances d'interface graphique problématiques à exclure de l'examen Flash. N'utilisez cette option que si le service de support vous le demande.	Si l'examen échoue ou ne se termine jamais en raison de la répétition d'opérations. Séparez les instances par une virgule.
Chaîne de télécharg. vers l'aval de fichier	Pour pouvoir examiner les films Flash de façon efficace, il est important qu'AppScan puisse identifier les commandes ayant pour résultat la réception d'un fichier par téléchargement. Utilisez cette zone pour les définir. Si vous cliquez sur une commande contenant les chaînes définies, AppScan s'interrompt pendant la durée du "Délai d'attente entre les opérations longues", même si les chaînes ne sont pas incluses dans le paramètre "Chaîne d'opération longue". Valeur par défaut : Télécharger	Si le film implique des téléchargements de fichiers vers l'aval, ils doivent être définis ici. S'il en existe plusieurs, séparez-les par un point-virgule. Exemple : Download;Save;CopyDownload;Save;Copy
Chemin de télécharg. vers l'amont de fichier	Chemin d'un fichier qu'AppScan peut télécharger vers l'application à la demande du film. Valeur par défaut : vide	Si le film Flash réclame le téléchargement amont d'un fichier, définissez son chemin, sans oublier son nom, et vérifiez son existence. Vous devez également définir la "Chaîne de téléchargement vers l'amont de fichier".

Nom	Description	Scénarios d'utilisation possibles
Chaîne de télécharg. vers l'amont de fichier	Pour pouvoir examiner les films Flash de façon efficace, il est important qu'AppScan puisse identifier les commandes permettant à l'utilisateur d'envoyer un fichier par téléchargement. Utilisez cette zone pour les définir. Si vous cliquez sur une commande contenant les chaînes définies, AppScan s'interrompt pendant la durée du "Délai d'attente entre les opérations longues", même si les chaînes ne sont pas incluses dans le paramètre "Chaîne d'opération longue". Valeur par défaut : Upload;Browse	Si le film permet à l'utilisateur de télécharger des fichiers vers l'amont, le texte des liens ou des commandes autorisant ces opérations doit être défini dans cette zone. S'il en existe plusieurs, séparez-les par un point-virgule. Exemple : Upload;Browse;Add Le "Chemin de téléchargement vers l'amont de fichier" doit aussi être défini.
Une dépendances de films Flash existe	Indique que le site comporte un film Flash contenant un autre film Flash dont dépend le premier film. Valeur par défaut : Faux	Si le site contient un film Flash qui charge un autre film Flash et que le premier film dépend du deuxième film, définissez la valeur sur True.
Facteur de fréquence des images	Lors des lectures Flash, la fréquence des images est augmentée en fonction de ce facteur (1,2,3,4). Valeur par défaut : 4	Par défaut, AppScan accélère la fréquence des images d'après un facteur de 4 lors de la lecture de films au cours d'un examen. Si ceci est trop rapide pour imiter une utilisation réelle, vous pouvez sélectionner un facteur plus faible.
Délai d'attente de chargement du film	Durée (en millisecondes) pendant laquelle AppScan attend qu'un film soit chargé avant de commencer à l'explorer. Valeur par défaut : 1600	Si AppScan commence à explorer un fichier avant la fin de son chargement, les résultats seront inexacts. Dans le cas où le chargement du film est plus long que la valeur par défaut, vous devez augmenter celle-ci.
Chaîne d'opération longue	Après la plupart des opérations, le navigateur Flash attend pendant la durée déterminée dans "Durée d'attente standard" avant de continuer, pour permettre au film d'atteindre son nouvel état. Lorsque la durée de certaines opérations risque d'être plus longue, et que l'examen pourrait donc se poursuivre avant que le film n'ait changé d'état, vous devez définir des "Opérations longues" (téléchargement de fichiers ou connexion, par exemple) pour lesquelles le navigateur s'interrompt plus longtemps. Valeur par défaut : vide	Les liens "Upload" ou "Login" correspondent à des opérations susceptibles d'être définies comme "longues". Dans le cas de l'envoi d'un fichier par téléchargement, le lien à définir est celui qui déclenche réellement le téléchargement du fichier, et non celui qui permet à l'utilisateur de *sélectionner* un fichier à télécharger. Si vous entrez plusieurs chaînes, séparez-les par un espace.
Délai d'attente entre les opérations longues	Durée (en millisecondes) pendant laquelle le navigateur Flash attend la fin et le changement d'état des opérations définies au paramètre "Chaîne d'opération longue". Valeur par défaut : 5000	Si une "opération longue" a été définie, son "délai d'attente" doit l'être aussi, dans cette zone.
Intervalle entre deux échantillons	Intervalle minimal (ms) entre des "opérations utilisateur" (telles que des clics de souris), pour permettre au film d'atteindre son nouvel état. Valeur par défaut : 160	Si le film comporte un grand nombre d'animations, l'attente requise pour un clic de l'utilisateur ou le renseignement d'un formulaire peut être plus longue que la valeur par défaut. Vous pouvez augmenter ce délai ici.
Général :		

Nom	Description	Scénarios d'utilisation possibles
Suppression des fenêtres contextuelles d'erreur de script dans le navigateur AppScan	Supprime les fenêtres contextuelles d'erreur de script dans le navigateur intégré AppScan pendant l'enregistrement et la lecture de la connexion basée sur les actions, l'exploration manuelle, l'enregistrement en plusieurs étapes et l'affichage dans le navigateur. Valeur par défaut : Faux	Si des messages d'erreur contextuels inappropriés interfèrent avec l'enregistrement et la lecture de la connexion basée sur les actions, vous pouvez les supprimer en définissant cette valeur sur True. Notez que d'autres fenêtres contextuelles, comme des erreurs "Authentification HTTP" et des invites "Installer le contrôle ActiveX" seront également supprimées.
Fusionner les tests redondants	Lorsqu'il est défini sur True, AppScan envoie un seul ensemble de tests sur deux demandes (ou plus) qui sont identiques, à l'exception des cookies supplémentaires. S'il est défini sur False, toutes ces demandes seront testées séparément. Valeur par défaut : Vrai	La définition de ce paramètre sur False peut affecter les performances. Ne faites cette modification que si le Support vous le conseille.
Filtre d'extensions de fichier proxy	Expression régulière définissant les extensions de fichier qui seront supprimées de la liste des URL sauvegardées lorsque vous enregistrez une connexion, une exploration manuelle ou une opération en plusieurs étapes. Si vous supprimez une extension de l'expression régulière, les adresses URL se terminant par cette extension ne sont pas filtrées dans les enregistrements. Valeur par défaut : "\.(zip | Z | tar | t?gz | sit | cab | pdf | ps | doc | ppt | xls | rtf | dot | mp(p | t | d | e | a | 3 | 4 | ga) | m4p | mdb | csv | pp(s | a) | xl(w | a) | dbf | slk | prn | dif | avi | mpe?g | mov(ie)? | qt | moov | rmi? | as(f | x) | m1v | wm(v | f | a) | wav | ra | au | aiff | midi? | m3u | gif | jpe?g | bmp | png | tif?f | ico | pcx | css | xml)$"	Parfois, lorsqu'un type de fichier particulier est nécessaire, par exemple un fichier image CAPTCHA inclus dans votre enregistrement de connexion pour référence, vous pouvez supprimer son extension de fichier (en l'occurrence `jp?g`) de l'expression régulière.
Nettoyer les journaux	Supprime les informations sensibles des journaux. Valeur par défaut : Faux	Si vous devez supprimer des informations sensibles des journaux, activez cette option et définissez le schéma à supprimer dans l'option "Schéma d'information sensible". Notez que la modification de ce paramètre est sans effet sur les journaux déjà générés.
Nettoyer les rapports	Supprime les informations sensibles des rapports. Valeur par défaut : Vrai	Si vous devez supprimer des informations sensibles des rapports, activez cette option et définissez le schéma à supprimer dans l'option "Schéma d'information sensible". Le mot de passe défini dans Configuration > Remplissage automatique de formulaires est exclu de tous les rapports, même si aucun modèle n'est défini. Notez que la modification de ce paramètre est sans effet sur les rapports déjà générés.

Nom	Description	Scénarios d'utilisation possibles
Envoyer tous les tests via GSC	AppScan peut utiliser GSC pour envoyer des tests sur l'ensemble ou une partie des liens trouvés par GSC. 0 = Envoi des messages SOAP uniquement à l'aide de GSC 1 = Utilisation de GSC pour l'envoi de tous les tests sur les liens trouvés par GSC 2 = Pas d'envoi de tests à l'aide de GSC Valeur par défaut : 0	Si vous n'avez pas défini de paramètres de sécurité spéciaux lors de l'exploration de votre site dans GSC, le fait de laisser AppScan (et non GSC) envoyer des tests pendant l'étape Test réduit la durée de l'examen de manière significative. Toutefois, si plusieurs tests n'ont pas reçu de réponse ou ont reçu des réponses d'erreur inattendues, alors le problème est certainement dû à la différence entre la manière dont GSC et AppScan envoient des demandes. L'envoi de ces tests à l'aide de GSC peut permettre de résoudre le problème.
Schéma d'information sensible	Expression régulière qui définit un ou plusieurs groupes à exclure des journaux et des rapports si l'option Nettoyer les journaux ou Nettoyer les rapports est activée. Valeur par défaut : vide	Si vous devez supprimer des informations sensibles des rapports ou des journaux, activez l'option appropriée ("Nettoyer les journaux " ou "Nettoyer les rapports") et définissez ici un ou plusieurs groupes dans une expression régulière. Le texte sensible est remplacé par : **CONFIDENTIAL 1**, **CONFIDENTIAL 2**, etc. Le mot de passe défini dans Configuration > Remplissage automatique de formulaires est exclu de tous les rapports, même si aucun modèle n'est défini.
JavaScript :		
Exécution JavaScript automatique dans une exploration manuelle	Vous pouvez configurer AppScan afin d'extraire *tous* les liens générés par JavaScript sur des pages explorées manuellement, même ceux non déclenchés lors de l'exploration manuelle. Valeur par défaut : Faux	Ceci peut permettre d'augmenter la portée de l'exploration manuelle.
Vider le cache	Si la valeur de ce paramètre est True, l'exécution de JavaScript (si elle est activée) ne met pas en cache les demandes envoyées au cours de la connexion. Cela peut augmenter la durée de l'examen et la taille de fichier. Valeur par défaut : Faux	
Extraire les liens externes	Lorsque l'exécution de JavaScript est activée, cela permet à AppScan d'extraire les liens externes même si leur serveur n'est pas configuré dans AppScan en tant que serveur supplémentaire. Valeur par défaut : Faux	Les pages HTML comportent fréquemment des liens vers des fichiers source JavaScript externes, tels que des fichiers source Dojo et jQuery. Si vous désirez que l'exécution de JavaScript puisse accéder à tous les liens pertinents identifiés lors de la phase d'exploration, sans avoir à ajouter les serveurs à la liste Serveurs et domaines supplémentaires testés par AppScan, activez ce paramètre. Notez qu'AppScan extraira le lien, mais sans le tester, ni l'analyser pour de nouveaux liens.

Nom	Description	Scénarios d'utilisation possibles
Filtre JavaScript et Flash	Cette expression régulière définit les pages sur lesquelles JavaScript ne sera pas exécuté et sur lesquelles Flash ne sera pas analysé lors de la phase d'exploration de l'examen. (Elle ne limite pas *l'analyse* de JavaScript.) Valeur par défaut : vide	Si AppScan s'arrête ou se fige régulièrement sur une page spécifique avec un contenu JavaScript ou Flash (ceci peut être confirmé en consultant le journal du trafic), la définition de cette page ici résoudra le problème.
Schéma de lien JavaScript	AppScan utilise divers schémas pour identifier les liens dans le code JavaScript. Si votre site utilise des schémas inhabituels, vous devez les définir dans cette expression régulière. Valeur par défaut : vide	Si AppScan semble ignorer des liens de votre code JavaScript et que votre site utilise des schémas de lien JavaScript inhabituels, définissez ici un ou plusieurs schémas pour indiquer à AppScan ce qu'il doit rechercher.
Localisation :		
Codage HTML	Remplace le codage défini dans les réponses HTML de votre site. Valeur par défaut : vide	Si le contenu des réponses dans les résultats d'examen présente une déformation, cela peut être dû au fait que : 1) La méthode de codage n'a pas été correctement identifiée par AppScan, ou 2) La méthode de codage n'est pas correctement définie dans le code HTML de votre site. Pour résoudre le problème 1 : sélectionnez la méthode correcte dans la liste déroulante Options d'exploration. Pour résoudre le problème 2 : entrez la méthode de codage correcte ici.
Paramètres et cookies :		
Exclure des tests les paramètres JSON redondants	Le corps de type de contenu JSON peut contenir plusieurs valeurs d'un paramètre unique qui doivent être testées individuellement. Si vous définissez cette option à la valeur True, AppScan tente d'identifier les valeurs redondantes et de limiter les tests à un sous-ensemble de paramètres, ce qui réduit la durée de l'examen. Valeur par défaut : Vrai	Si vous constatez qu'un paramètre important n'a pas été testé, définissez cette option à la valeur False.
Exclure des tests les paramètres XML redondants	Le corps de type de contenu XML peut contenir plusieurs valeurs d'un paramètre unique qui doivent être testées individuellement. Si vous définissez cette option à la valeur True, AppScan tente d'identifier les valeurs redondantes et de limiter les tests à un sous-ensemble de paramètres, ce qui réduit la durée de l'examen. Valeur par défaut : Vrai	Si vous constatez qu'un paramètre important n'a pas été testé, définissez cette option à la valeur False.

Nom	Description	Scénarios d'utilisation possibles
Suivre les paramètres personnalisés dans les en-têtes	Ce paramètre s'applique uniquement aux examens sauvegardés à l'aide d'AppScan version 8.7.0.1 ou antérieures. Dans les versions ultérieures, le comportement par défaut est devenu True et il est possible de contrôler les valeurs de chaque paramètre et cookie dans : **Configuration > Paramètres et cookies > Définition de paramètre > Options de suivi > Correspondance : En-tête et corps** (par défaut) ou **Corps uniquement** (voir «Définition de paramètre», à la page 78). Par défaut, AppScan (versions 8.7.0.1 et antérieures) recherche des paramètres personnalisés uniquement dans le corps des réponses, et non dans leurs en-têtes. Si vous attribuez la valeur True à ce paramètre, AppScan effectue alors également une recherche dans les en-têtes. Valeur par défaut : Faux **Remarque :**	Si AppScan ferme la session suite à des modifications d'un paramètre dans un en-tête de réponse, la modification de ce paramètre peut résoudre le problème. Ceci peut augmenter la durée de l'examen.
Suivre les paramètres dynamiques à l'étape de test uniquement s'il existe du contenu en ligne	Le suivi des paramètres dynamiques au cours de l'étape de test peut entraîner des problèmes de performance. Par conséquent, par défaut, le suivi des paramètres dynamiques n'est effectué au cours de l'étape de test que dans les réponses comportant du contenu en ligne. Valeur par défaut : Vrai	N'associez la valeur False à ce paramètre que si ce type de suivi est essentiel.
Détection de serveur arrêté :		
Rechercher "serveur arrêté" dans Exploration	Permet d'envoyer des demandes de signal de présence pour vérifier la condition "Serveur arrêté" pendant l'étape d'exploration. Valeur par défaut : Vrai	Si AppScan reçoit des erreurs de type serveur arrêté pendant l'étape d'exploration bien que le serveur soit en opération, ceci peut être dû au fait que le serveur bloque les demandes de signal de présence fréquentes. Si AppScan connaît des arrêts de session fréquents pendant l'examen, ceci peut être dû au fait que l'adresse URL de départ est envoyée au serveur comme signal de présence, sans cookies. La désactivation de ce paramètre peut résoudre le problème mais AppScan ne sera alors pas en mesure de vérifier l'état du serveur.

Nom	Description	Scénarios d'utilisation possibles
Rechercher "serveur arrêté" dans Test	Permet d'envoyer des demandes de signal de présence pour vérifier la condition "Serveur arrêté" pendant l'étape de test. Valeur par défaut : Vrai	Si AppScan reçoit des erreurs de type serveur arrêté pendant l'étape de test bien que le serveur soit en opération, ceci peut être dû au fait que le serveur bloque les demandes de signal de présence fréquentes. Si AppScan connaît des arrêts de session fréquents pendant l'examen, ceci peut être dû au fait que l'adresse URL de départ est envoyée au serveur comme signal de présence, sans cookies. La désactivation de ce paramètre peut résoudre le problème mais AppScan ne sera alors pas en mesure de vérifier l'état du serveur.
Etape d'exploration - tentatives de reconnexion	Lorsqu'AppScan est sur le point de terminer l'étape d'exploration mais que plusieurs tests ont échoué pour cause de "serveur arrêté", et que le serveur est toujours arrêté, AppScan effectuera plusieurs tentatives de connexion au serveur. Valeur par défaut : 5	Si vous savez que votre serveur est sensible ou constatez que l'examen s'est arrêté en raison d'une erreur de communication et qu'une série de tests a échoué pour les mêmes raisons, vous devez augmenter cette valeur.
Intervalle entre deux tentatives de demande	Intervalle en secondes avant un nouvel envoi des demandes ayant échoué (y compris des demandes de signal de présence). Valeur par défaut : 1	Si vous êtes conscient que votre connexion est médiocre ou votre serveur instable (ce qui peut conduire à des résultats "faux négatifs" ou réduire la couverture de l'application), vous pouvez augmenter cet intervalle pour réduire l'impact.
Nombre limite de tentatives de demande	Nombre de nouvelles tentatives de relance des demandes ayant échoué. Valeur par défaut : 2	L'augmentation de la valeur de ce paramètre peut augmenter l'efficacité de l'examen si votre serveur est instable ou que la communication est médiocre.
Délai d'attente d'arrêt du serveur	Lorsqu'AppScan ne parvient pas à se connecter au serveur ou que la session se ferme, ce paramètre définit la durée (en secondes) pendant laquelle AppScan tentera de se reconnecter ou de rouvrir la session avant d'arrêter l'examen. Valeur par défaut : 185	Si votre connexion est lente, ou si votre serveur met du temps à se recharger après un arrêt, vous pouvez choisir d'augmenter ce paramètre.
intervalle des pulsations serveur arrêté	Intervalle en secondes entre signaux de présence de "serveur arrêté". Valeur par défaut : 3 s Max : 60 s	Si AppScan reçoit des erreurs de type serveur arrêté pendant l'examen, ceci peut être dû à une connexion médiocre ou à un serveur instable. L'augmentation de cet intervalle peut permettre de résoudre le problème.
Etape de test - tentatives de reconnexion	Lorsqu'AppScan est sur le point de terminer l'étape de test mais que plusieurs tests ont échoué pour cause de "serveur arrêté", et que le serveur est toujours arrêté, AppScan effectuera plusieurs tentatives de connexion au serveur. Valeur par défaut : 5	Si vous savez que votre serveur est sensible ou constatez que l'examen s'est arrêté en raison d'une erreur de communication et qu'une série de tests a échoué pour les mêmes raisons, vous devez augmenter cette valeur.
Gestion des sessions :		

Nom	Description	Scénarios d'utilisation possibles
Domaines des publicités	Expression régulière décrivant les domaines courants des publicités sur le Web. Les demandes envoyées à ces domaines lors de l'enregistrement de la séquence de connexion seront ignorées. Valeur par défaut : ad\d.googlesyndication|doubleclick\.net|coremetrics\.|webtrends\.|112\.2o7\.net|view.atdmt.com|ad.yieldmanager.com|ads.adbrite.com|oasn04.247realmedia.com| segment-pixel.invitemedia.com"	La séquence de connexion étant réexécutée continuellement au cours de l'examen, vous pouvez améliorer l'efficacité de l'examen en éliminant par filtrage les demandes non nécessaires. Si vous supprimez toute l'expression régulière, aucun domaine ne sera éliminé.
Analyser l'enregistrement de connexion	Lorsque vous enregistrez une séquence de connexion, (Configuration des examens > Gestion de connexion), AppScan l'analyse et met à jour les paramètres de la détection En session (schéma En session, demande En session et ID session reçus lors de la connexion). Valeur par défaut : Vrai	Si l'analyse prend trop de temps, vous pouvez remplacer ce paramètre par False. Cependant, si vous le faites, vous devez configurer la détection En session manuellement.
Effacer les cookies avant de lire la connexion	Détermine si les cookies sont supprimés avant la relecture de la séquence de connexion. Valeur par défaut : Vrai	
Valeurs de paramètre statique commun	Valeurs de paramètres statiques courantes. Utilisées pour la détection de valeurs de paramètres non aléatoires qui ne doivent pas faire l'objet d'un suivi lors de la connexion. Valeurs par défaut : |true|false|\bon\b|\boff\b|\bout\b|checked|enabled|log\s?in|log\s?out|exit|submit|sign|ever|disabled|agree	
Désactiver la mise en mémoire tampon en session pendant l'étape d'exploration	Pendant l'étape d'exploration : Si la réponse à une demande indique que l'utilisateur était hors session lors de son envoi, AppScan met en file d'attente la demande afin de la renvoyer. Cela garantit l'examen d'une partie aussi grande que possible du site. Valeur par défaut : Faux	Si votre site met souvent l'utilisateur hors session, la mise en mémoire tampon en session risque de provoquer une exécution indéfinie de l'étape d'exploration. Si vous affectez la valeur True à cette option, l'étape d'exploration est plus rapide, mais la couverture d'examen du site risque d'être réduite.
En session avant opérations en plusieurs étapes	Par défaut, AppScan vérifie le statut en session avant de réexécuter les opérations en plusieurs étapes. Valeur par défaut : Vrai	Si vous voulez tester des opérations en plusieurs étapes avec un utilisateur non authentifié, ou si vos séquences en plusieurs étapes incluent des étapes de connexion, affectez à ce paramètre la valeur False. **Important :** Si l'option **Configuration > Gestion de connexion > Détails > Activer la détection en session** est *désélectionnée* et que ce paramètre avancé a la valeur True (par défaut), toute la séquence de connexion sera réexécutée avant chaque opération en plusieurs étapes.
Intervalle des pulsations En session	Intervalle en secondes entre les signaux de présence En session. Valeur par défaut : 5	Si une fin de session intervient sur AppScan durant l'examen, ceci peut être dû à une connexion médiocre ou à un serveur instable. L'augmentation de cet intervalle peut permettre de résoudre le problème.

Nom	Description	Scénarios d'utilisation possibles
Filtre du type de contenu de connexion	Expression régulière qui définit des types de contenu qui doivent être exclus des séquences de connexion et d'opération en plusieurs étapes. Lorsqu'une séquence de connexion ou d'opération en plusieurs étapes est enregistrée, les demandes dont les réponses comprennent des en-têtes avec ces types de contenu seront supprimées de la séquence. Ainsi, lorsqu'AppScan réexécute la séquence pendant l'examen, les demandes dont les réponses comprennent des en-têtes avec ces types de contenu ne seront pas envoyées dans la séquence. Par défaut : text/javascript|application/javascript| application/x-javascript|image|text/css	Si la procédure de connexion de votre site, ou l'une des opérations en plusieurs étapes que vous avez enregistrées, nécessite de cliquer sur un lien contenant un en-tête dont le contenu figure dans cette liste, vous devez le supprimer de l'expression régulière.
Intervalle entre les nouvelles tentatives de connexion	Intervalle en secondes avant un nouvel envoi des demandes de connexion ayant échoué. Valeur par défaut : 3	Si une fin de session intervient dans AppScan et que les tentatives de relance de la connexion échouent, ceci peut être dû au fait que le serveur est sensible aux tentatives de connexion répétées. L'augmentation de cet intervalle peut permettre de résoudre le problème.
Filtre de type de contenu à plusieurs parties	Pour réduire la consommation de mémoire superflue, certains types de contenu sont automatiquement exclus par filtrage des demandes à plusieurs parties (demandes contenant plusieurs types de contenu). Seuls les types de contenu définis dans cette expression régulière sont inclus dans les demandes à plusieurs parties. Les autres types de contenu sont filtrés et exclus. Le contenu qui *ne possède pas* d'en-tête de type de contenu est inclus par défaut et défini par la valeur suivante : `content_without_content_type_header` Valeur par défaut : text/|text/plain|application/javascript| application/json|application/rtf|application/xml| text/xml|content_without_content_type_header	Si un type de contenu important est exclu des demandes, ajoutez-le à cette expression régulière. Il est également possible de réduire la consommation de mémoire en supprimant les types de contenu inutiles afin qu'ils ne soient pas envoyés.
Hôtes de paramètres de navigation	Expression régulière décrivant les hôtes. Utilisée pour la détection des paramètres de navigation (par valeur) ne devant pas faire l'objet d'un suivi pendant la séquence de connexion. Valeur par défaut : https?://	Si votre site utilise des hôtes inhabituels dans les paramètres de navigation, qui ne sont pas exclus par l'expression régulière par défaut, ajoutez-les pour améliorer l'efficacité de l'examen. Si vous supprimez cet élément, les paramètres de navigation peuvent ne pas être identifiés correctement.

Nom	Description	Scénarios d'utilisation possibles
Scripts de paramètres de navigation	Expression régulière décrivant des scripts côté serveur utilisés lors de la détection des paramètres de navigation (par valeur de paramètre) qui ne doivent pas faire l'objet d'un suivi pendant la séquence de connexion. Valeur par défaut : /[^/\.]+\ .(htm | jsp | jsf | ws | dll | asp | php | do)	Si votre site utilise des scripts côté serveur inhabituels dans les paramètres de navigation, qui ne sont pas exclus par l'expression régulière par défaut, ajoutez-les pour améliorer l'efficacité de l'examen. Si vous supprimez cet élément, les paramètres de navigation peuvent ne pas être identifiés correctement.
Paramètres de navigation	Expression régulière décrivant des paramètres de navigation qui ne doivent pas faire l'objet d'un suivi lors de la séquence de connexion. Par défaut : \bnav | url | page | step | redirect | request | location | target | argument | item | article | goto | node | action | ctrl | control | source | menu | frame | command	Si votre site utilise des paramètres de navigation inhabituels qui ne sont pas exclus par l'expression régulière par défaut, ajoutez-les pour améliorer l'efficacité de l'examen. La modification de l'expression régulière peut générer une couverture insuffisante de l'examen ou un suivi de session inadéquat.
Analyser la page En session	S'il est défini sur False, AppScan n'analysera pas la page en session et ne mettra pas à jour les paramètres ou les cookies suivis dont les valeurs ont été modifiées dans la page en session. Valeur par défaut : Vrai	Si votre page En session ne contient pas de cookies ou de paramètres suivis, vous pouvez améliorer les performances en modifiant la valeur de ce paramètre sur False. Si la valeur est False, AppScan ne mettra pas à jour les valeurs des paramètres ou des cookies suivis sur la page En session, ce qui peut entraîner un passage hors session.
Demandes entre pulsations	A la suite d'une demande de détection de session, AppScan enverra au moins le nombre de demandes définies ici avant d'envoyer une autre demande de détection de session. Valeur par défaut : 1	Si en raison de la lenteur de la réponse du serveur l'examen est constitué principalement de demandes de détection en session (voir le journal du trafic), l'augmentation de cette valeur peut réduire la durée de l'examen.
Délai d'attente pour la tentative de connexion basée sur les actions	Durée en secondes pendant laquelle AppScan attend que le navigateur tente à nouveau d'effectuer une connexion basée sur les actions, avant de provoquer la fermeture du navigateur. Valeur par défaut : 120 secondes	
Schémas spéciaux :		
Exclure du remplissage automatique de formulaires	Les noms de paramètres répertoriés ici sont exclus du remplissage automatique de formulaires. Valeur par défaut : ^CFID __EVENTVALIDATION __VIEWSTATE ^CFTOKEN __EVENTARGUMENT __EVENTTARGET ^BV_	Les paramètres dont la valeur est très longue peuvent ralentir l'examen et accroître la taille des fichiers. Si votre application utilise des paramètres dont les valeurs sont longues et qui ne sont pas requis pour remplir les formulaires, ajoutez-les à cette liste.
Tests :		

Nom	Description	Scénarios d'utilisation possibles
CSRF : Schéma de demande significative	Par défaut, AppScan teste les requêtes POST et celles avec réponse "Transaction Successful" pour identifier des attaques CSRF (Cross-Site Request Forgery). Ce paramètre vous permet de définir des demandes supplémentaires comme étant "significatives" d'une vulnérabilité à une attaque CSRF, outre les requêtes POST. Cette définition est utilisée en conjonction avec "CSRF : Schéma de réponse significative. Valeur par défaut : ^POST	Si vous désirez tester également la vulnérabilité à des attaques CSRF de requêtes GET, modifiez cette expression régulière.
CSRF : Schéma de réponse significative	Par défaut, AppScan teste les requêtes POST et celles avec réponse "Transaction Successful" pour identifier des attaques CSRF (Cross-Site Request Forgery). Ce paramètre vous permet de définir des *réponses* supplémentaires comme étant "significatives" d'une vulnérabilité à une attaque CSRF, outre les réponses "Transaction Successful". Cette définition est utilisée en conjonction avec "CSRF : Schéma de demande significative. Valeur par défaut : Transaction Successful	Si vous désirez tester la vulnérabilité à des attaques CSRF de demandes recevant d'autres types de réponse, définissez-les dans cette expression régulière.
Seuil de différence	AppScan doit souvent comparer deux réponses et déterminer si elles sont "similaires" ou "différentes", afin de définir si un test a abouti ou non. Il utilise alors des algorithmes pour attribuer un pourcentage de similarité (où 100 % indique que les deux réponses sont identiques). Dans certains cas, il détermine les résultats du test en fonction du "Seuil de similarité" et dans d'autres, en *fonction* du "Seuil de différence". Il est possible de configurer ces deux seuils. Pour la plupart des tests, le seuil de similarité par défaut est de 95 % et le seuil de différence par défaut est de 75 %. Cela implique les points suivants : • Pour les résultats de test dépendant de la *similarité*, un pourcentage de similarité de 95 % *ou plus* indique que les deux pages sont similaires. • Pour les résultats de test dépendant de la *différence*, un pourcentage de similarité de 75 % *ou moins* indique que les deux pages sont différentes. Toute valeur saisie pour ce paramètre située entre 1 et 100 (pourcentage) se substitue au seuil de différence par défaut pour tous les tests. Vous pouvez également, si vous le souhaitez, régler le seuil de similarité. Valeur par défaut : 0 (Utiliser les seuils AppScan)	Si votre site ne contient pas de texte "dynamique" pouvant générer de petites différences dans des réponses similaires, le fait d'indiquer une valeur inférieure à 75 risque de réduire les résultats faussement positifs. **Conseil :** Vous pouvez également, si vous le souhaitez, régler le seuil de similarité (voir ci-dessous).
Désactiver le test des cookies	Ce paramètre permet de désactiver le test des cookies. Valeur par défaut : Faux	Si le test des cookies pour votre application allonge considérablement la durée de l'examen, vous pouvez le désactiver. Cependant, ceci peut entraîner l'omission de problèmes de sécurité ("faux négatifs").

Nom	Description	Scénarios d'utilisation possibles
Désactiver le test des cookies pour le contenu statique	Désactive le test des cookies dans les demandes pour des pages portant cette extension. Valeur par défaut : ;htm;html;ahtm;ahtml; chtm;chtml;fhtm;fhtml;mht; mhtm;mhtml;css;css1;js;	Afin de réduire la durée de l'examen et la consommation de la mémoire, vous pouvez envisager d'exclure des types supplémentaires d'extensions de page. Dans ce cas, ajoutez-les à la liste des extensions à exclure, en les séparant par un point-virgule.
Ne pas tester le répertoire ou la page	Cette option permet de définir une expression régulière afin de protéger des répertoires ou des pages spécifiques des attaques pendant l'étape de test. Seuls seront exclus les répertoires ou pages définis et non les sous-répertoires ou fichiers. Valeur par défaut : /wps/[^/]*/!ut/	Si vous savez que certains répertoires ou pages ne sont pas vulnérables ou craignez que leur test ne nuise à la stabilité du site, vous pouvez les exclure de l'examen en les définissant dans cette expression régulière. Pour exclure un dossier *et tous ses sous-dossiers*, reportez-vous à la rubrique «Vue Exclusion de chemins et de fichiers», à la page 65
Extraire les liens de toutes les réponses	Par défaut, lors de la phase de test, AppScan ne recherche de nouveaux liens que dans les réponses vulnérables. Valeur par défaut : Faux	Si vous pensez qu'AppScan risque d'ignorer des liens ou que sa couverture est insuffisante, vous pouvez activer ce paramètre, bien que ceci augmente la durée de l'examen et la taille de fichier.
Suivre tous les liens automatiques	Par défaut, AppScan ne suit que des liens* automatiques susceptibles de comporter des vulnérabilités. Il s'agit d'iFrame, Frame et Redirect. Vous pouvez le configurer afin de suivre *tous* les types de lien automatique. Notez que les requêtes correspondant à l'expression régulière définies dans "Liens automatiques à ignorer" ne seront *jamais* envoyées, quelle que soit la valeur de ce paramètre. Valeur par défaut : Faux	Si vous pensez que votre site peut comporter une vulnérabilité dans d'autres types de liens automatiques, comme des scripts, activez ce paramètre. Ceci augmentera la durée d'examen et la taille de fichier.
Connexion après test	Envoyer les tests dans une même unité d'exécution et vérifier en session, ou envoyer la séquence de connexion après chaque test. 0 = False 1 = Envoyer les tests dans une même unité d'exécution et vérifier en session après chaque test. Si une fin de session est détectée, envoie la séquence de connexion. 2 = Envoyer les tests dans une même unité d'exécution et envoyer la séquence de connexion après chaque test. Valeur par défaut : 0	Les paramètres 1 et 2 peuvent s'avérer nécessaires pour les applications comportant une session sensible ou nécessitant des déconnexions fréquentes pour éviter les problèmes de session ou de mémoire. La sélection de ces paramètres peut augmenter la durée d'examen de façon significative.
Opération en plusieurs étapes : limite de validation	Nombre maximal de demandes consécutives provenant d'une opération en plusieurs étapes qui seront validées via des tests de script intersite. Valeur par défaut : 0	

Nom	Description	Scénarios d'utilisation possibles
Schéma à ignorer dans la réponse	Cette expression régulière définit les sections de la réponse à ignorer par AppScan lors de l'analyse des réponses du test. Lors de la comparaison des réponses en vue de décider si un test a réussi, AppScan calcule le pourcentage de modification dans la réponse complète. Si la réponse est très longue et la modification minime, AppScan peut ignorer cette différence et ne pas identifier la vulnérabilité. Valeur par défaut : <input[^>]+(__VIEWSTATE|__ EVENTTARGET| __EVENTARGUMENT| __EVENTVALIDATION) [^>]+>	Si votre site envoie des réponses incluant des sections longues qui ne sont pas importantes, la définition des sections ici peut améliorer la précision et les performances de l'examen.
Régénérer l'intervalle de réponse d'origine	Intervalle, en secondes, de régénération de la réponse d'origine (en renvoyant la demande) lors de la phase de test. L'une des méthodes utilisées par AppScan pour décider si une réponse de test révèle une vulnérabilité consiste à la comparer avec la réponse d'exploration. Lorsqu'une réponse d'exploration est antérieure à la valeur définie ici, la demande d'exploration est envoyée de nouveau, avant d'envoyer les tests, de sorte qu'une réponse d'exploration mise à jour puisse être utilisée pour la comparaison. Cette règle est essentielle lorsque la réponse d'exploration est susceptible de varier dans le temps et que la comparaison de la réponse de test avec la réponse d'exploration obsolète risque de produire un résultat faussement positif. Valeur par défaut : 30 (secondes)	Si vous êtes certain que les réponses de l'application ne deviendront jamais obsolètes, vous pouvez remplacer la valeur de ce paramètre par zéro afin de réduire la durée d'examen. Les demandes de l'étape d'exploration ne seront jamais envoyées une nouvelle fois.
Envoyer des tests de programme d'écoute des ports	Par défaut, AppScan n'envoie pas de tests d'écoute des ports en raison des risques d'échec et du temps de validation. Valeur par défaut : Faux	Si le site externe fait partie de votre réseau et connaît par conséquent les adresses IP locales, vous pouvez souhaiter activer ce type de test d'injection SQL en aveugle.

Nom	Description	Scénarios d'utilisation possibles
Seuil de similarité	AppScan doit souvent comparer deux réponses et déterminer si elles sont "similaires" ou "différentes", afin de définir si un test a abouti ou non. Il utilise alors des algorithmes pour attribuer un pourcentage de similarité (où 100 % indique que les deux réponses sont identiques). Dans certains cas, il détermine les résultats du test en fonction du "Seuil de similarité" et dans d'autres, en *fonction* du "Seuil de différence". Il est possible de configurer ces deux seuils. Pour la plupart des tests, le seuil de similarité par défaut est de 95 % et le seuil de différence par défaut est de 75 %. Cela implique les points suivants : • Pour les résultats de test dépendant de la *similarité*, un pourcentage de similarité de 95 % *ou plus* indique que les deux pages sont similaires. • Pour les résultats de test dépendant de la *différence*, un pourcentage de similarité de 75 % *ou moins* indique que les deux pages sont différentes. Toute valeur saisie pour ce paramètre située entre 1 et 100 (pourcentage) se substitue au seuil de similarité pour tous les tests. Valeur par défaut : 0 (Utiliser les seuils AppScan)	Si votre site ne contient pas de texte "dynamique" pouvant générer de petites différences dans des réponses similaires, vous pouvez augmenter ce pourcentage pour réduire le nombre de messages faussement positifs. **Conseil :** Vous pouvez également, si vous le souhaitez, régler le seuil de différence (voir ci-dessus).
XSS : Tester toutes les sondes reflétées	Généralement, plusieurs occurrences du texte de charge trouvées dans une réponse du site ont le même niveau de vulnérabilité. Par conséquent, AppScan n'en teste qu'une seule. Valeur par défaut : Faux	Paramétrez cette valeur sur True si vous voulez tester *toutes* les occurrences du texte de charge dans une même réponse.

* **Connexion automatique :** lien sur la page Web que le navigateur envoie automatiquement, sans aucune interaction de l'utilisateur.

Structure des fichiers d'examen

Explique la structure de base d'un fichier SCAN standard AppScan.

Lorsque vous sauvegardez un examen standard AppScan, les données sont sauvegardées dans un fichier dont l'extension est SCAN. Il s'agit d'une archive ZIP contenant plusieurs composants, notamment :

`RESULTSDB.FDB`
Résultats de l'examen, tels qu'affichés dans la vue Données.

`templateConfig.xml`
Modèle d'examen (configuration). Le contenu est identique au fichier SCANT standard AppScan pour la même configuration.

Fichiers `Manual_Explore_#.exd`
Un ou plusieurs fichiers numérotés pour les séquences d'exploration manuelle. Ils peuvent être importés dans d'autres examens.

Modèles d'examen

Un modèle d'examen est simplement une *configuration* d'examen sauvegardée de sorte à pouvoir la réutiliser.

- Le modèle standard peut être utilisé pour exécuter un examen sans modifier aucune configuration (vous devez, toutefois, au moins définir l'URL de départ de l'examen).
- Vous pouvez utiliser un des «Modèles prédéfinis» fournis et conçus pour tester AppScan sur un site de test spécifique ou sur un type de site particulier.
- Vous pouvez créer des «Modèles d'examen définis par l'utilisateur», à la page 139 personnalisés configurés pour répondre à vos exigences spécifiques.

Lorsque vous sauvegardez un *modèle d'examen* vous enregistrez les définitions de configuration de l'examen (pour une utilisation future). Lorsque vous sauvegardez un *examen* vous sauvegardez la configuration *et* les résultats d'examen.

Modèles prédéfinis

Pourquoi et quand exécuter cette tâche

AppScan est livré avec certains modèles d'examen prédéfinis qui ont été configurés pour générer un résultat optimal lors d'un test AppScan sur un site test. Ces modèles vous évitent d'avoir à ajuster les diverses options de configuration pour optimiser votre examen. (Les mises à jour de ces modèles peuvent être incluses dans les mises à jour AppScan de façon régulière.)

- Examen standard
- Examen rapide et léger (configuré pour générer rapidement des résultats pertinents)
- Navigation basée sur paramètres
- WebSphere Commerce
- WebSphere Portail
- demo.testfire.net (pour examen du site Web "Altoro Mutual Bank", créé à des fins de démonstration)
- Site de production (configuré pour une utilisation avec des sites de production opérationnels), voir «Examen des environnements de production opérationnels», à la page 323 pour plus de détails)
- Banque Hacme
- WebGoat v5
- Worklight (pour un examen dans un environnement de serveur IBM Worklight)

Le tableau ci-dessous présente des détails de configuration de base de certains modèles prédéfinis.

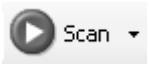
Tester l'application	Exclusion du chemin d'accès	Limite de chemin d'accès	Méthode d'exploration*	Sensible à la casse	Connexion
WebGoat	.*attack\?Num=.*	Désactivé	Profondeur en premier	Oui	Nom d'utilisateur : guest Mot de passe : guest
demo.testfire.net	aucun	5	Largeur en premier	Non	Nom d'utilisateur : jsmith Mot de passe : demo1234

* Pour plus de détails sur la *Méthode d'exploration* , voir «Vue Options d'exploration», à la page 71

Pour procéder à un examen avec un modèle prédéfini :

Procédure

1. Sélectionnez un modèle :
   - Dans l'*écran d'accueil*, sélectionnez l'une des zones *Modèles prédéfinis* ou
   - Dans l'écran principal, cliquez sur  (ou sur **Fichier** > **Nouveau**), puis dans la zone *Modèles prédéfinis* sélectionnez le modèle requis.

2. Cliquez sur **Sauvegarder sous**, entrez le nom de l'examen et enregistrez l'examen.
3. Définissez l'URL de départ pour l'examen (voir «Vue URL et serveurs», à la page 47).
4. Le cas échéant, enregistrez la procédure de connexion ou entrez le nom d'utilisateur et le mot de passe (voir «Onglet Connexion», à la page 52).
5. Cliquez sur 

.

Modèle de navigation basée sur des paramètres

Explique la configuration de ce modèle prédéfini.

Le modèle de navigation à base de paramètres inclut les paramètres ci-dessous qui permettent de répondre aux exigences d'examen de ce type de site.

Elément	Localisation	Paramètre	Commentaires
Limite pour les chemins d'accès redondants	Options d'exploration	500	La valeur peut être augmentée si nécessaire.
Limite de profondeur	Options d'exploration	10	Permet de gérer les liens de publication ASP.NET 2.0.
Valeurs par défaut du réglage de la redondance	Paramètres et cookies	1ère et 3ème cases à cocher sélectionnées	
Paramètre supplémentaire	Paramètres et cookies	Toutes les cases à cocher Réglage de la redondance sont désélectionnées ("Ne pas assurer le suivi")	Le paramètre se présente sous la forme d'une expression régulière : `.*(?i)(page|redirect|content|target|EVENTTARGET|EVENTARGUMENT|goto|node|action|ctrl|source.*` Il pourrait être nécessaire de modifier cette expression régulière si votre site utilise un paramètre de navigation absent de la liste

Voir aussi :

«Sites utilisant une navigation basée paramètres», à la page 322

«Exigences pour les sites dont la navigation est basée sur des paramètres», à la page 323

Modèles d'examen définis par l'utilisateur

Lorsque vous configurez un examen, vous pouvez sauvegarder la configuration en tant que modèle pour l'utiliser dans les examens ultérieurs.

Pourquoi et quand exécuter cette tâche

Vous pouvez sauvegarder le modèle avant l'exécution de l'examen, ou bien sauvegarder un examen terminé en tant que modèle pour d'autres examens. Vous pouvez aussi, si vous disposez d'un examen avec des résultats intéressants, et que vous souhaitez réexécuter cet examen via le processus de développement et d'assurance qualité, l'enregistrer en tant que modèle d'examen.

Procédure

1. Procédez de l'une des façons suivantes :
   - Configurez un examen à l'aide de l'**Assistant de configuration des examens**.
   - Configurez un examen à l'aide de la boîte de dialogue **Configuration des examens**.

- Chargez un examen enregistré pour lequel vous souhaitez sauvegarder la configuration comme modèle.

2. Dans le menu **Fichier**, cliquez sur **Sauvegarder sous**.
3. Choisissez le type de fichier **.scant** dans la boîte de dialogue **Sauvegarder sous**.
4. Entrez un nom facilement reconnaissable pour le modèle.
5. Cliquez sur **Sauvegarder**.

Ouverture de modèles d'examen

Pourquoi et quand exécuter cette tâche

Après avoir sauvegardé un modèle, vous pouvez le charger pour exécuter un examen basé sur la configuration d'examen prédéfinie du modèle ou pour modifier ce modèle.

Procédure

1. Procédez de l'une des façons suivantes :
   - Glissez-déplacez le fichier SCAN ou SCANT de son dossier vers l'interface d'AppScan.

     Limitation : Cette fonction ne fonctionne pas sur les systèmes Microsoft Windows 8 sur lesquels l'utilisateur dispose d'autorisations d'administrateur.
   - Cliquez sur **Fichier > Nouveau**, sélectionnez le modèle que vous souhaitez utiliser, décochez la case **Lancer l'assistant de configuration des examens**, puis cliquez sur **OK**.

   Les configurations prédéfinies du modèle d'examen sélectionné sont chargées.
2. Pour démarrer l'examen :
   - Cliquez sur menu **Examen > Démarrer l'examen > [Examen intégral / Explorer / Test]**.
   - Si Démarrer l'examen n'est pas disponible, cliquez sur **Nouvel examen > [Examen intégral / Explorer / Test]**.

Editer des modèles d'examen

Pourquoi et quand exécuter cette tâche

Vous pouvez éditer un modèle d'examen avec une modification permanente pour tous les examens qui se baseront sur ce modèle.

Vous ne pouvez pas éditer de façon permanente le modèle d'examen par défaut. Si vous modifiez la configuration Par défaut, les modifications sont utilisées dans l'examen suivant mais ne sont pas conservées dans le modèle d'examen par défaut.

Procédure

1. Ouvrez un modèle d'examen (voir «Ouverture de modèles d'examen»).
2. Modifiez les paramètres de configuration.
3. Procédez de l'une des façons suivantes :
   - **Assistant de configuration des examens** : sur la dernière page de l'assistant, sélectionnez **Je démarrerai l'examen ultérieurement**. Puis, dans le menu **Fichier**, cliquez sur **Sauvegarder** ou **Sauvegarder sous** et choisissez le type de fichier **scant**.
   - Boîte de dialogue **Configuration des examens :** cliquez sur **Sauvegarder comme modèle.**

Modification de la configuration pendant un examen

Si vous lancez un examen, puis modifiez la configuration, vous devrez le relancer, ou au moins relancer l'étape de test, pour voir l'effet des modifications. En règle générale :

- Si vous avez modifié les configurations d'exploration, vous devez relancer l'examen intégral de l'application en exécutant les étapes d'exploration et de test (**Examen > Nouvel examen > Nouvel examen (intégral)**).
- Si vous avez modifié les configurations de test, vous ne devez pas réexécuter l'étape d'exploration (si elle est terminée), il suffit d'effectuer un nouveau test de l'application (**Examen > Nouvel examen > Nouveau test**).

Chapitre 5. Exploration manuelle

Cette section traite des différentes manières d'explorer manuellement une application ou des services avant de procéder à l'étape de test ou à un examen automatique (qui inclut à la fois les étapes d'exploration automatique et de test).

L'exploration manuelle d'un site consiste à collecter les données pouvant être utilisées par AppScan pour s'assurer que, lors du test du site, les parties de l'application ou les services n'ayant pas été pris en compte lors de l'étape d'exploration automatique seront couverts. Cela peut être nécessaire si une entrée utilisateur spécifique est requise, ou si le site répond uniquement à un type d'outil ou de périphérique différent. Vous pouvez procéder à une exploration manuelle via AppScan, l'utiliser en tant que proxy d'enregistrement ou via le service GSC (Generic Service Client).

En règle générale :

AppScan
: est utilisé pour l'exploration manuelle lorsque le site n'inclut pas de services. Vos actions et vos entrées sont enregistrées et utilisées par AppScan pour créer les tests de l'examen.

AppScan comme proxy d'enregistrement
: est utilisé lorsque vous voulez procéder à une exploration manuelle via votre propre périphérique distant (par exemple, un téléphone portable) ou une application externe (par exemple, un simulateur ou un émulateur portable) avec AppScan configuré en tant que proxy d'enregistrement. Exemples de scénario d'utilisation : services Web SOAP, services non SOAP n'incluant pas d'enveloppe de sécurité, applications nécessitant un navigateur différent. Les demandes sont envoyées au site à partir d'une application ou d'un périphérique externe, avec AppScan configuré en tant que proxy d'enregistrement. Cela permet à AppScan d'enregistrer et d'utiliser les réponses pour créer les tests de l'examen.

GSC (Generic Service Client)
: est utilisé pour explorer les services Web disposant d'un fichier WSDL. GSC crée une interface simple pour envoyer les demandes au service ; les réponses sont importées dans AppScan et utilisées pour créer les tests de l'examen.

Utilisation d'AppScan

L'exploration manuelle vous permet d'explorer des parties spécifiques de l'application en remplissant en même temps les zones et les formulaires. Cela permet de vous assurer que des zones spécifiques du site sont couvertes et qu'AppScan dispose des informations requises pour remplir correctement les formulaires.

Le navigateur AppScan s'ouvre, et vous enregistrez vos actions, les liens et les données saisies tout en parcourant l'application. Lorsque vous arrêtez l'enregistrement, AppScan affiche la liste des liens explorés, ainsi que les données du remplissage automatique de formulaires qu'il peut désormais utiliser lors qu'il explore ou teste le site de façon automatique.

L'exploration manuelle peut être faite avant l'étape d'exploration automatique de l'examen, à sa place, ou après elle.

Remarque : Les URL reconnues lors d'une exploration manuelle sont testées individuellement, comme celles reconnues pendant une exploration automatique. Si AppScan doit tester des URL qui ne sont accessibles qu'en cliquant sur plusieurs liens dans *un ordre spécifique*, vous devez enregistrer une opération en plusieurs étapes (voir «Vue Opérations en plusieurs étapes», à la page 95).

Avant une exploration automatique

Plusieurs raisons peuvent vous conduire à choisir d'exécuter une exploration manuelle avant une exploration automatique :

- Vous voulez utiliser l'exploration manuelle pour fournir à AppScan des données pour le remplissage des formulaires et avoir la possibilité de les explorer manuellement au fur et à mesure que vous les insérez dans les formulaires.
- Vous voulez vous assurer qu'AppScan teste une partie spécifique et importante du site.
- Vous souhaitez procéder à l'examen d'un processus utilisateur spécifique (URL, fichiers et paramètres auxquels accède un utilisateur selon un certain scénario) et vous pouvez créer une exploration manuelle uniquement pour ce processus. Cette exploration manuelle peut se faire avant de commencer un examen.
- Votre application utilise des scripts ou des applets Java qui ne révèlent certaines parties de l'application que lorsque des états (survol ou déplacement de la souris, par exemple) se suivent dans un ordre particulier. Notez qu'il ne s'agit pas d'une opération en plusieurs étapes. Pour une opération en plusieurs étapes, AppScan doit visiter les liens dans un ordre spécifique. Dans ce cas, il suffit que AppScan ait le lien pour pouvoir le tester en une seule étape, comme n'importe quel autre lien.

Après avoir effectué une exploration manuelle, vous pouvez continuer par une étape d'exploration automatique (**Exploration uniquement** ou **Examen intégral**), pour que l'examen couvre la totalité de l'application.

A la place d'une exploration automatique

Vous pouvez parfois choisir d'exécuter une exploration manuelle *à la place* d'une exploration automatique :

- Vous ne voulez examiner qu'une petite partie du site et vous préférez utiliser une exploration pour définir les parties à tester.

  Après l'exploration manuelle, vous pouvez terminer l'examen en cliquant sur **Test uniquement**.

Après une exploration automatique

Deux principales raisons peuvent vous conduire à choisir d'exécuter une exploration manuelle *après* une exploration automatique :

- L'examen a eu pour effet de catégoriser certaines URL comme interactives (voir «Interaction utilisateur nécessaire», à la page 204), ce qui signifie qu'AppScan n'a pas pu insérer automatiquement les données requises. Vous pouvez explorer manuellement ces URL pour saisir ces données.

  Remarque : Si vous le faites, les URL sont retirées de la liste des URL interactives.
- Votre site inclut des fichiers SWF (Adobe Flash). AppScan les teste, s'il est configuré pour cela (voir «Vue Options d'exploration», à la page 71), mais si vous vous rendez compte que certains fichiers ont été omis, vous pouvez les identifier auprès d'AppScan à l'aide de l'exploration manuelle. Il n'est pas nécessaire d'explorer le film lui-même. Il suffit de cliquer sur le fichier SWF, de fermer l'exploration manuelle, puis de relancer l'exploration automatique.

Enregistrer une exploration manuelle

Procédure

1. Cliquez sur **Examen > Exploration manuelle > Utilisation du navigateur**.

   Le navigateur intégré d'AppScan s'ouvre, avec le bouton **Enregistrer** sélectionné (grisé).

   Remarque : Le navigateur par défaut est utilisé. Vous pouvez sélectionner le navigateur par défaut comme étant soit l'un des deux navigateurs intégrés (IE ou Chromium), soit un navigateur externe pris en charge, dans Outils > Options > Onglet Préférences

2. Parcourez le site manuellement en renseignant les données et en cliquant sur les liens au fur et à mesure.
3. Lorsque vous avez fini l'exploration, cliquez sur **Pause** ou fermez simplement le navigateur.

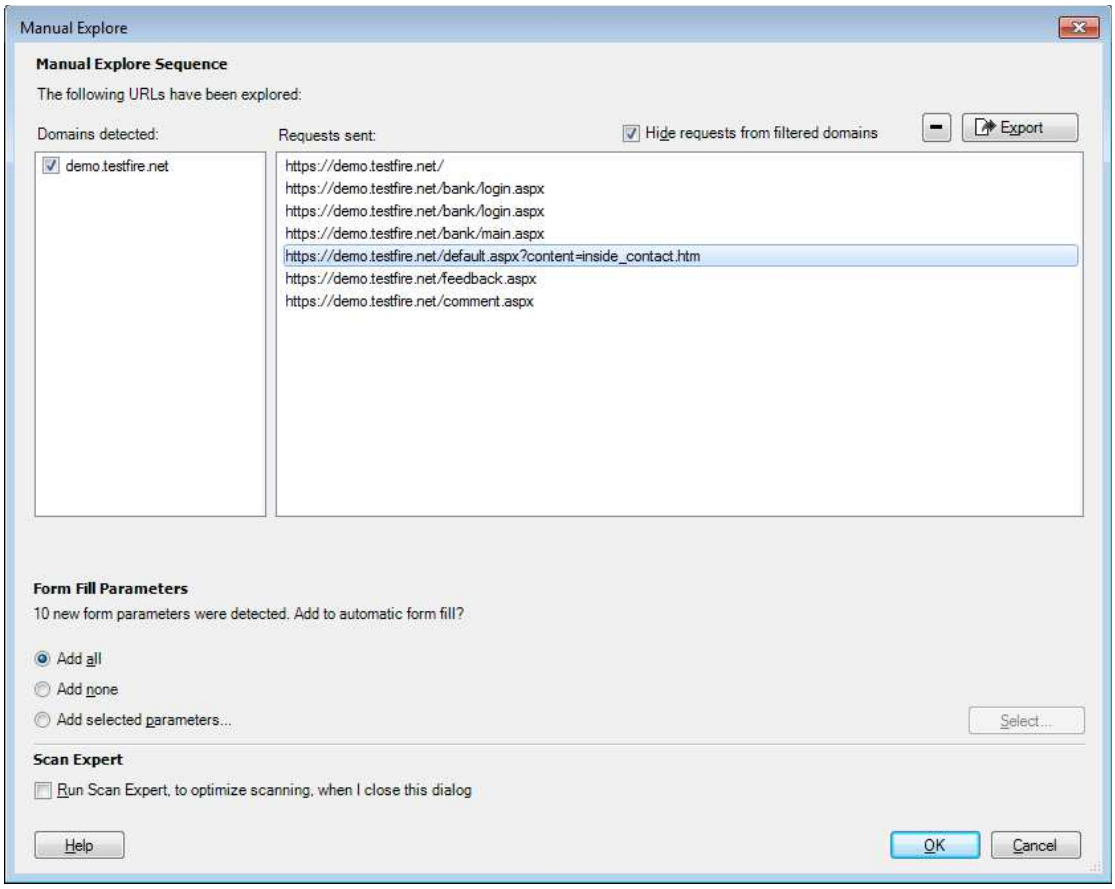
   Remarque : Vous pouvez créer un enregistrement d'exploration manuelle couvrant plusieurs parties distinctes de l'application : Cliquez sur **Pause**, accédez à un autre emplacement, puis cliquez sur **Enregistrer** pour reprendre l'enregistrement.
   La boîte de dialogue **URL explorées** apparaît, affichant les URL visitées lors de votre connexion.

   Conseil : Vous pouvez supprimer toute étape indésirable (liens) de la séquence en sélectionnant le lien et en cliquant sur .

Utilisation de la séquence d'exploration manuelle

Cette section décrit la vérification, l'édition et l'exportation de la séquence.

Pourquoi et quand exécuter cette tâche



Procédure

1. Vous pouvez supprimer toute étape indésirable (liens) de la séquence en sélectionnant le lien et en cliquant sur .
2. Vérifiez la liste.

   Si l'exploration manuelle réalisée est une procédure standard du site, vous pouvez souhaiter la sauvegarder pour une utilisation lors d'examens ultérieurs. Pour plus d'informations, voir «Exporter des données d'exploration manuelle», à la page 147.

Si vous avez rempli des formulaires HTML lors de l'exploration manuelle, AppScan détermine quelles informations peuvent être ajoutées aux paramètres de remplissage automatique des formulaires. Si une entrée applicable est trouvée, un message s'affiche dans la moitié basse de la boîte de dialogue et les boutons radio sont activés :

`[n] new form parameters were detected. Add to Automatic Form Fill?`

- Si vous voulez que *toutes* les entrées enregistrées soient ajoutées au Remplissage automatique de formulaires, cliquez sur **Ajouter tout**. Vos entrées sont automatiquement ajoutées aux informations de Remplissage automatique de formulaires.
- Si vous ne voulez pas que vos entrées enregistrées soient sauvegardées, cliquez sur **Ne rien ajouter**. Même si elles ne sont pas sauvegardées de façon permanente, vos entrées manuelles ont déjà été appliquées.
- Si vous voulez ajouter uniquement des paramètres et des valeurs sélectionnés, cliquez sur **Ajouter les paramètres sélectionnés**, puis cliquez sur **Sélectionner**. La boîte de dialogue **Ajouter les paramètres de formulaire détectés automatiquement** s'affiche (voir «Ajouter les paramètres de formulaire détectés automatiquement»).

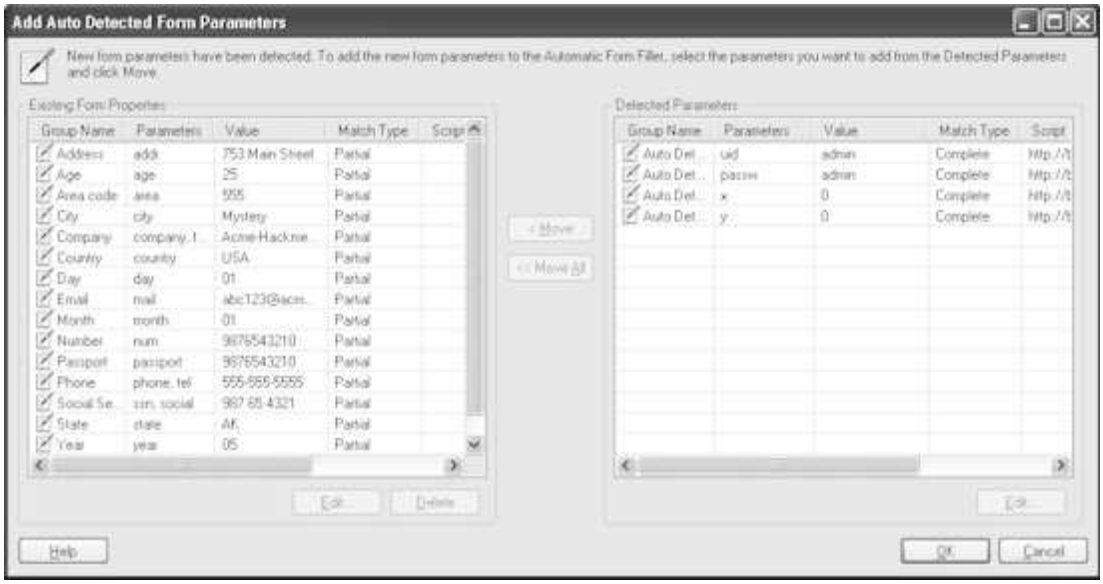
3. A l'aide des liens que vous avez ajoutés, une évaluation Scan Expert peut révéler des faiblesses dans la configuration. Pour exécuter Scan Expert lorsque cette boîte de dialogue se ferme, cochez la case **Scan Expert**. (Pour plus d'informations, voir «Scan Expert», à la page 164.)
4. Cliquez sur **OK**.

   AppScan crée les demandes de test de votre exploration manuelle. Cette opération peut prendre un certain temps.

Ajouter les paramètres de formulaire détectés automatiquement

Pourquoi et quand exécuter cette tâche

La boîte de dialogue **Ajouter les paramètres de formulaire détectés automatiquement** permet de sélectionner les nouveaux paramètres de formulaire détectés que vous souhaitez ajouter aux Propriétés des formulaires à utiliser automatiquement dans les futurs examens.



Procédure

1. Dans la liste **Paramètres détectés** (panneau de droite), sélectionnez les lignes que vous souhaitez ajouter à l'outil de remplissage automatique des formulaires (panneau de gauche), puis cliquez sur **Déplacer** ; ou sélectionnez n'importe quel paramètre dans la liste et cliquez sur **Déplacer tout**.

Les paramètres que vous déplacez dans **Paramètres de formulaire existants** seront disponibles pour les futurs examens de ces URL.

2. Cliquez sur **OK**.

   AppScan analyse les URL que vous avez explorées et crée des tests basés sur cette analyse.

Exporter des données d'exploration manuelle

Les procédures standard peuvent être "enregistrées" sous la forme d'une exploration manuelle puis importées dans les analyses futures.

Pourquoi et quand exécuter cette tâche

Si l'exploration manuelle réalisée est une procédure standard du site, vous pouvez enregistrer les données (demandes envoyées et réponses reçues) pour une utilisation lors d'examens ultérieurs. Les données sont enregistrées en tant que fichier de données d'exploration (.EXD) au format XML et peuvent être chargées si nécessaire, ce qui évite d'avoir à enregistrer la même procédure à chaque fois.

Procédure

1. Enregistrez l'exploration manuelle comme dans les premières étapes de la procédure précédente.
2. Lorsque la boîte de dialogue **URL explorées** s'affiche, cliquez sur **Exporter**.

   Une boîte de dialogue **Sauvegarder sous** s'affiche.
3. Entrez un nom pour le fichier, puis cliquez sur **OK**.

   Remarque : Pour visualiser ou modifier l'emplacement par défaut dans lequel le fichier est sauvegardé, voir **Options > Préférences** (voir «Onglet Préférences», à la page 261).

Que faire ensuite

Tâches associées :

«Enregistrer une exploration manuelle», à la page 144

«Importer des données d'exploration manuelle»

Redirige vers :

«Utilisation d'AppScan», à la page 143

Importer des données d'exploration manuelle

Si vous avez sauvegardé des procédures standard sous la forme d'une exploration manuelle, vous pouvez les importer dans un autre examen pour les tester à nouveau, même sur un autre serveur.

Pourquoi et quand exécuter cette tâche

Vous pouvez importer une procédure d'exploration manuelle précédemment enregistrée pour l'utiliser comme partie d'un nouvel examen. Ceci s'avère utile lorsque des procédures standard doivent être examinées à nouveau. Ceci peut être effectué même pour l'examen de la même application sur un autre serveur (voir l'étape 3 ci-dessous).

Les formats de fichier d'exploration manuelle pris en charge sont : EXD, HAR, DAST.CONFIG et CONFIG.

Procédure

1. Cliquez sur **Fichier > Importer > Données d'exploration**.

2. Accédez fichier d'exploration manuelle sauvegardé (EXD, HAR, DAST.CONFIG ou CONFIG), et cliquez sur **Ouvrir**.

   La boîte de dialogue Importer apparaît.
3. Par défaut, la case **Importer avec les réponses** est cochée et AppScan analyse ces réponses lorsqu'il prépare le test du site. Si le site est modifié de sorte que cela affecte les réponses, vous pouvez décocher cette case de sorte qu'AppScan renvoie les demandes et collecte des réponses à jour. Toutefois, dans ce cas, il peut être plus efficace de procéder à une nouvelle exploration manuelle.

   Remarque : Si le fichier a été sauvegardé dans une version d'AppScan ne prenant pas en compte les données de réponse, la case n'est pas cochée et apparaît en grisé. Vous pouvez sélectionner **Continuer quand même ?** pour importer les demandes, les envoyer au site et collecter de *nouvelles* réponses à analyser pour le test. Toutefois, dans ce cas, il peut être plus efficace de procéder à une nouvelle exploration manuelle.
4. Pour lancer l'examen, cliquez sur **Continuer** ou **Continuer quand même**.
   a. AppScan analyse les données de l'étape d'exploration afin de rechercher d'éventuels conflits hôte.

      Si le fichier couvre des hôtes qui ne sont pas compris dans la configuration en cours, la boîte de dialogue Conflits dans le fichier des données d'exploration apparaît. Résolvez les conflits en sélectionnant une **action** appropriée pour chaque hôte :
      - **Ignorer** : Ne pas explorer cet hôte.
      - **Ajouter aux hôtes testés** : Ajouter l'hôte listé aux serveurs de l'examen.
      - **Remplacer par <nom d'hôte>** : Pour chaque hôte défini dans l'examen, une option permet de remplacer l'hôte du conflit par un hôte déjà présent dans la configuration de l'examen.

        Remarque : Cette fonction permet réellement d'enregistrer une exploration manuelle sur un hôte et de réexécuter le processus sur un autre serveur hébergeant la même application. Elle peut être utilisée par exemple pour enregistrer un processus sur un serveur de transfert et le réexécuter sur un serveur de production.
   b. L'examen commence :
      - Si les données importées incluent des réponses, les données mises en cache sont analysées en prévision de l'étape de test.
      - Si les données importées n'incluent *pas* de réponses, une étape d'exploration complète est lancée, suivie d'une analyse des réponses afin de formuler des tests pour l'étape de test.
   c. Lorsque l'exploration et l'analyse sont terminées, l'examen s'interrompt.
5. A ce stade, vous pouvez choisir de procéder à une exploration manuelle ou automatique.
6. Pour procéder à l'étape de test de l'examen, cliquez sur **Examiner > Continuer > Test**.

Que faire ensuite

Tâches associées :

«Enregistrer une exploration manuelle», à la page 144

«Exporter des données d'exploration manuelle», à la page 147

Redirige vers :

«Utilisation d'AppScan», à la page 143

Utiliser AppScan comme serveur proxy

Vous pouvez définir AppScan pour qu'il agisse en tant que serveur proxy, puis explorer manuellement votre application à l'aide d'un utilitaire de navigation tiers (navigateur, client de services Web, script

d'exploration automatique, téléphone mobile, etc.) via AppScan. Dans ce mode d'opération, AppScan enregistre le trafic HTTP/HTTPS qui passe par lui, l'analyse et crée les tests appropriés.

Pourquoi et quand exécuter cette tâche

Remarque : L'exploration avec AppScan comme serveur proxy peut être utilisée pour explorer des services Web SOAP et non SOAP ou lorsque le client d'application n'est pas compatible avec Internet Explorer. En configurant votre client de services Web pour utiliser AppScan comme proxy, AppScan collecte les demandes aux services Web telles qu'envoyées par le client. GSC (Generic Service Client), fourni avec AppScan, est utilisé à cette fin pour les services Web SOAP. Voir «Exploration à l'aide de l'enregistreur du trafic externe», à la page 150.

Remarque : Dans l'éventualité où le navigateur AppScan produirait des messages d'erreur et non votre navigateur externe, vous pouvez utiliser cette fonction pour les parcourir manuellement à l'aide d'un navigateur externe, avec AppScan comme proxy. (Si cela se produit, contactez l'équipe de support d'AppScan pour que le problème puisse être résolu.)

Procédure

1. Vérifiez que AppScan n'est pas configuré pour utiliser les paramètres de proxy Internet Explorer. Dans **Configuration des examens > Vue Connexion**, procédez comme suit :
   - Sélectionnez **Ne pas utiliser de proxy**
   - Sélectionnez **Utiliser les paramètres personnalisés du proxy**, tapez l'adresse et le port du proxy et des informations d'authentification.

   Remarque : Si vous n'effectuez pas cette opération, le paramètre est automatiquement remplacé par **Ne pas utiliser de proxy** lorsque vous commencez l'exploration.
2. Recherchez le port d'écoute AppScan. Ouvrez **Outils > Options > onglet Enregistrement du proxy** (voir «Onglet Enregistrement du proxy», à la page 261).

   La zone **Port proxy** affiche le port qu'AppScan utilise pour écouter le trafic arrivant à l'application Web. Il peut s'agir d'un port qu'AppScan s'affecte à lui-même (le numéro de port que vous recherchez sera grisé) ou d'un port que vous avez sélectionné manuellement.
3. Configurez votre navigateur Web pour qu'il utilise AppScan comme son proxy :

   Dans votre navigateur, recherchez la section relative à la configuration d'un serveur proxy. Modifiez le nom d'hôte ou l'adresse par l'adresse IP (l'hôte local est généralement une entrée acceptée) utilisée par la machine exécutant AppScan et modifiez le port par le port d'écoute AppScan.
4. Exécutez une exploration manuelle de votre application (pour plus de détails, voir «Utilisation d'AppScan», à la page 143) :
   a. Cliquez sur **Examen > Exploration manuelle**, pour ouvrir le navigateur interne AppScan.
   b. Sans fermer le navigateur interne, ouvrez votre navigateur externe.
   c. Explorez manuellement l'application, si nécessaire.
   d. Fermez le navigateur externe.
   e. Fermez le navigateur interne AppScan.

Configurer votre navigateur pour qu'il utilise AppScan en tant que proxy

Exemple montrant comment configurer le navigateur pour qu'il utilise AppScan en tant que proxy.

Procédure

1. Dans AppScan, cliquez sur **Outils > Options > onglet Options d'examen**.

   Supposons que le port est défini sur **Automatique** et a le numéro **4744**.
2. Ouvrez **Microsoft Internet Explorer > Outils > Options Internet > onglet Connexions > Paramètres réseau** et cochez la case dans la section **Serveur proxy**.

   Les zones de saisie **Adresse** et **Port** sont activées.

3. Dans Internet Explorer, entrez la configuration trouvée dans AppScan :
   Adresse : `localhost` et **Port** : `4744`

Utilisation d'AppScan comme proxy d'enregistrement

Vous pouvez utiliser l'enregistreur de trafic externe d'AppScan comme un proxy d'enregistrement, et explorer manuellement des services RESTful ou d'autres services Web non-SOAP - ou des services SOAP ne nécessitant pas d'enveloppes de sécurité - avec un téléphone mobile, un simulateur ou un émulateur. AppScan affiche les domaines et les demandes dans son enregistreur de trafic externe et crée les tests appropriés en fonction de l'entrée.

Remarque : Pour les services Web qui comportent un fichier WSDL et utilisent des enveloppes de sécurité SOAP, utilisez plutôt GSC pour explorer le service (pour plus de détails, voir «Utilisation de GSC», à la page 153).

Remarque : Si votre application utilise la protection "man-in-the-middle", elle ne peut pas être examinée en utilisant AppScan comme proxy.

Exploration à l'aide de l'enregistreur du trafic externe

Il s'agit d'un exemple de flux de travaux simple pour un examen des services Web non SOAP.

Pourquoi et quand exécuter cette tâche

Cet exemple de flux de travaux affiche chaque étape conceptuelle séparément.

Remarque : Vous pouvez configurer et envoyer des demandes à partir de plusieurs périphériques mobiles via la même instance de l'enregistreur du trafic externe. Tous les domaines et demandes seront listés simultanément.

Procédure

1. **Sélectionnez un modèle**
   Cliquez sur **Fichier > Nouveau** et sélectionnez un modèle :
   - IBM Worklight Developer :
     a. Sélectionnez le modèle Worklight.
     b. Si le code de votre application Worklight utilise l'authentification d'application (authenticité) : Dans le serveur Worklight, ouvrez la console Worklight et assurez-vous que l'authentification d'application (authenticité) est désactivée, ou désactivez-la dans le code de l'application.
   - Autres environnements : Utilisez le modèle Examen standard.

   Remarque : Si Internet Explorer est configuré sur votre machine pour utiliser AppScan comme proxy, vous devez vérifier qu'AppScan n'est pas configuré pour utiliser vos paramètres de proxy Internet Explorer, car cela provoquerait une boucle. Pour résoudre ce conflit, sélectionnez l'une des deux options suivantes dans l'onglet Configuration > Communication et proxy :
   - **Ne pas utiliser de proxy**
   - **Utiliser les paramètres personnalisés du proxy**

   Si vous enregistrez une exploration manuelle à l'aide de l'enregistreur du trafic externe sans procéder à cette opération, ce paramètre est automatiquement remplacé par **Ne pas utiliser de proxy**. Le réglage de redondance au cours de l'étape de test est utilisé, que cette case soit cochée ou non.
2. Dans la boîte de dialogue de bienvenue de l'assistant, sélectionnez Périphérique externe/client (avec AppScan comme proxy d'enregistrement) et cliquez sur **Suivant**.
3. Suivez les étapes de l'assistant :
   a. «Enregistrement du proxy», à la page 39

b. (Facultatif :) «Paramètres de connexion», à la page 39
c. «Certificat SSL», à la page 40
d. «Gestion de connexion», à la page 40
e. (Facultatif :) «Gestion de connexion - Détails», à la page 41
f. «Stratégie de test», à la page 41
g. «Complet», à la page 42

4. Lorsque l'enregistreur du trafic externe s'affiche à l'état "En attente des connexions entrantes", explorez manuellement le service Web à partir de votre périphérique/application :
   a. A l'aide de votre périphérique ou application, explorez le service Web.

      Au cours de l'exploration, les domaines détectés s'affichent dans la sous-fenêtre de gauche de l'enregistreur et les adresses URL dans la sous-fenêtre de droite.
   b. Ensuite, dans AppScan, cliquez sur **Arrêter l'enregistrement**.
5. Révisez et éditez les données d'exploration manuelle :

   Domaines détectés

   Tous les domaines auxquels des demandes ont été envoyées sont listés et sélectionnés par défaut pour être ajoutés à la liste des serveurs et domaines supplémentaires (Configuration > URL et serveurs > Serveurs et domaines supplémentaires) afin qu'il soient inclus dans l'examen. Désélectionnez ceux que vous ne voulez pas inclure dans l'examen.

   Conseil : Désélectionnez les domaines qui appartiennent à d'autres sociétés.

   Demandes envoyées

   Toutes les demandes envoyées par le périphérique à des domaines *sélectionnés* (dans la sous-fenêtre de gauche), sont listées. Si vous sélectionnez/désélectionnez des domaines dans la sous-fenêtre de gauche, la liste des demandes est mise à jour. Vous pouvez supprimer des demandes spécifiques si elles ne sont pas requises.

   Conseil : Si le nombre total de demandes filtrées dépasse 200, l'examen sera plus efficace si vous en supprimez certaines.

   Remarque : A ce stade, vous pouvez cliquer sur **Exporter** pour enregistrer les données d'exploration à utiliser sur une autre machine.
6. Cliquez sur OK pour fermer l'enregistreur.

   AppScan met un certain temps à traiter et à afficher les données.
7. Pour démarrer l'étape de test, cliquez sur **Examen > Test uniquement**.

   L'étape de test commence et les résultats de l'examen s'affichent une fois celle-ci terminée.

   Rubriques connexes :

   •
   • «Onglet Enregistrement du proxy», à la page 261
   • Chapitre 8, «Résultats : Problèmes de sécurité», à la page 207

Enregistreur de connexion externe

Lors d'une exploration manuelle avec AppScan comme proxy d'enregistrement, cet enregistreur affiche le trafic reçu au cours de la connexion et vous permet de l'éditer et d'approuver son utilisation lors d'une connexion à l'application pendant l'examen.

L'enregistreur de connexion externe s'ouvre lorsque vous cliquez sur **Configuration > Gestion de connexion > Enregistrer > Utiliser le périphérique externe** et permet d'enregistrer la séquence de connexion. Il affiche les demandes envoyées.

Elément	Description
Etat de connexion du proxy	Indique si les connexions entrantes sont enregistrées, et d'autres messages d'état.
Ecoute sur le port	Indique le port affecté à l'enregistreur.
Enregistrement de la configuration du proxy	Ouvrez l'onglet Outils > Options > Enregistrement du proxy pour modifier le port ou toute autre configuration de proxy d'enregistrement (pour plus de détails, voir «Onglet Enregistrement du proxy», à la page 261).
Demandes de connexion envoyées	Affiche toutes les demandes envoyées au cours de l'exploration manuelle. Les demandes provenant des domaines sélectionnés dans la sous-fenêtre de gauche apparaissent en noir, les autres en gris.
Arrêter l'enregistrement	Arrête l'enregistrement des demandes entrantes, mais garde ouverte la boîte de dialogue pour la révision et l'édition de la séquence d'enregistrement. Pour supprimer de la liste les demandes individuelles non pertinentes pour l'examen, sélectionnez une demande et cliquez sur [-] .
OK	Ferme l'enregistreur.

Pour plus d'informations sur l'ensemble du workflow, voir «Exploration à l'aide de l'enregistreur du trafic externe», à la page 150.

Voir aussi :

- «Onglet Enregistrement du proxy», à la page 261
- «Réglage de la redondance», à la page 83

...

Enregistreur du trafic externe

Lors d'une exploration manuelle avec AppScan comme proxy d'enregistrement, cet enregistreur affiche les domaines détectés et le trafic reçu et vous permet de contrôler lesquels seront testés. Une version limitée de l'enregistreur est utilisée pour enregistrer la séquence de connexion.

L'enregistreur du trafic externe s'affiche lorsque vous cliquez sur **Exploration manuelle > Utilisation du périphérique externe**.

Elément	Description
Etat de connexion du proxy	Indique si les connexions entrantes sont enregistrées, et d'autres messages d'état.
Ecoute sur le port	Indique le port affecté à l'enregistreur. Pour modifier le port, ou toute autre configuration d'enregistrement du proxy, cliquez sur **Enregistrement de la configuration du proxy** (pour plus de détails, voir «Onglet Enregistrement du proxy», à la page 261).
Trafic enregistré	
Domaines détectés (sous-fenêtre de gauche)	Liste de tous les domaines détectés dans le trafic enregistré. Sélectionnez les domaines à inclure dans l'examen. Lorsque vous fermez l'enregistreur, tous les domaines sélectionnés sont ajoutés à la liste Serveurs et domaines supplémentaires (Configuration > URL et serveurs > Serveurs et domaines supplémentaires) et ils seront inclus dans l'examen.

Elément	Description
Demandes envoyées (sous-fenêtre de droite)	Affiche toutes les demandes envoyées au cours de l'exploration manuelle. Les demandes provenant des domaines sélectionnés dans la sous-fenêtre de gauche apparaissent en noir, les autres en gris. • Pour afficher *uniquement* les demandes provenant des domaines sélectionnés, cochez la case **Masquer les demandes dans les domaines filtrés** • Pour supprimer de la liste les demandes individuelles non pertinentes pour l'examen, sélectionnez une demande et cliquez sur [-] .
Exporter	Cliquez sur ce bouton pour exporter l'enregistrement à utiliser sur une autre machine. Ce bouton est actif uniquement une fois l'enregistrement arrêté.
Appliquer le réglage de la redondance de l'étape d'exploration	(Sélectionné par défaut) Lorsque cette option est sélectionnée, le réglage de la redondance de l'étape d'exploration (onglet Configuration > Paramètres et cookies > Valeurs par défaut du réglage de la redondance > Explorer) est appliqué à l'enregistrement en cours lorsque vous fermez la boîte de dialogue afin d'éviter les demandes en double. Désélectionnez cette case à cocher uniquement si des cookies générés lors de l'exploration manuelle risqueraient d'être perdus si elle était sélectionnée.
Arrêter l'enregistrement	Arrête l'enregistrement en laissant la boîte de dialogue ouverte dans le but d'afficher et de modifier les listes. **Remarque :** Une fois l'enregistrement arrêté, celui-ci ne peut pas reprendre sans perte des données en cours.
OK	Ferme la boîte de dialogue et ajoute tous les domaines sélectionnés à la liste des serveurs et domaines supplémentaires inclus dans l'examen (Configuration > URL et serveurs > Serveurs et domaines supplémentaires).

Pour le flux de travaux, voir «Exploration à l'aide de l'enregistreur du trafic externe», à la page 150.

Voir aussi :

- «Onglet Enregistrement du proxy», à la page 261
- «Réglage de la redondance», à la page 83

...

Utilisation de GSC

GSC (Generic Service Client) utilise le fichier WSD de votre service Web pour fournir une interface simple qui affiche les services disponibles et permet d'entrer des paramètres et de visualiser les résultats. Utilisez l'interface GSC pour explorer votre service Web manuellement afin qu' AppScan puisse utiliser vos entrées pour créer les tests appropriés.

Remarque : GSC est utilisé pour explorer les services Web qui sont définis avec un fichier WSDL. Si toutefois votre service ne comporte pas de fichier WSDL ou n'utilise pas d'enveloppes de sécurité SOAP, ou que vous disposez de votre propre application pour effectuer l'étape d'exploration, vous pouvez à la place utiliser un périphérique mobile, un émulateur ou un simulateur avec l'enregistreur de trafic externe d'AppScan intégré que vous avez configuré en tant que proxy d'enregistrement (pour plus de détails, voir «Utilisation d'AppScan comme proxy d'enregistrement», à la page 150).

Après avoir envoyé divers paramètres au service, reçu des réponses et fermé GSC, cliquez sur **Exécuter uniquement des tests** afin de lancer un examen automatique en fonction des entrées. (Cet examen est en fait une étape de test uniquement, car l'étape d'exploration s'est terminée lors de l'exploration manuelle à l'aide de GSC.)

Si SSL est utilisé sans certificat côté client, aucune configuration particulière de GSC n'est requise (si vous utilisez la version GSC livrée avec AppScan 8.0). Pour la configuration CCS, reportez-vous au centre de documentation GSC, accessible depuis la barre d'outils GSC principale.

Remarque : AppScan reste ouvert tant que GSC l'est également mais fonctionne uniquement lorsque GSC est fermé.

Remarque : Certaines des fonctionnalités décrites dans le fichier d'aide de GSC peuvent ne pas s'appliquer lorsqu'elles sont utilisées via AppScan.

Exploration à l'aide de GSC

Il s'agit d'un exemple de flux de travaux simple pour un examen des services Web SOAP.

Avant de commencer

Pour permettre l'envoi des tests aux services Web, GSC doit être installé sur votre système. Lors de l'installation d'AppScan, le système vous a demandé si vous souhaitiez l'installer. Si vous ne l'avez pas installé, vous pouvez le faire à tout moment en cliquant sur le fichier GSC_Setup.exe situé dans votre dossier principal AppScan.

Procédure

1. Ouvrez la vue URL et serveurs de la boîte de dialogue Configuration des examens, et dans la zone URL de démarrage, ajoutez l'un des éléments suivants :
   - URL du fichier WSDL
   - Chemin d'accès au fichier WSDL sur votre réseau local, indiqué au format suivant :
     `file////c:/mywsdlfile.wsdl`

   Restriction : Lorsque le fichier WSDL est fourni localement, GSC ne peut pas extraire le nom de domaine du fichier. Par conséquent, si vous choisissez la seconde option, vous devez indiquer à GSC le nom de domaine dans la zone **Serveurs et domaines supplémentaires**. Exemple :
   `demo.testfire.net`
2. Si nécessaire, cochez la case Sensible à la casse.
3. Cliquez sur **OK** pour fermer la boîte de dialogue Configuration des examens.
4. Cliquez sur **Examiner > Exploration des services Web**.
   GSC s'ouvre et une arborescence des services Web apparaît dans le panneau de gauche. (Cliquez sur les icônes  pour développer l'arborescence et visualiser les services Web individuels.)
5. Explorez les services :
   a. Cliquez sur un service dans l'arborescence pour le sélectionner. Une interface apparaît dans le panneau de droite pour l'envoi des demandes au service.
   b. Dans l'onglet Message du panneau de droite, entrez la valeur à envoyer.
   c. Cliquez sur **Invoke** (Appeler) pour envoyer la demande.
      Les résultats s'affichent dans le panneau principal, et la demande est ajoutée à la sous-fenêtre Call History (Historique des appels) située dans la partie inférieure gauche de l'écran.
   d. Répétez cette opération pour ajouter d'autres services, le cas échéant.
6. Lorsque vous avez envoyé suffisamment de demandes, fermez GSC.
   GSC se ferme et des tests sont créés en fonction des données.
7. Pour démarrer l'examen, cliquez sur **Examiner > Test uniquement**.

Résultats

Une fois l'examen terminé, les résultats s'affichent.

Exemple

Voir Chapitre 8, «Résultats : Problèmes de sécurité», à la page 207

Examen d'un site incluant un service Web SOAP *faisant partie* du site

Utilisez cette procédure si votre site inclut un service Web et d'autres pages qui nécessitent un examen.

Pourquoi et quand exécuter cette tâche

Si votre site contient des services Web et d'autres pages à scanner, vous devez explorer les services Web manuellement à l'aide de GSC mais laisser AppScan explorer le reste du site automatiquement, puis tester *intégralement* le site. Dans ce cas, vous devez indiquer à AppScan à la fois l'URL du fichier WSDL du service Web *et* une URL de départ pour l'exploration du site.

Procédure

1. Cliquez sur **Examiner > Configuration des examens > URL et serveurs** et dans la zone **URL de départ**, entrez l'URL du fichier WSDL pour le service Web.
2. Dans la zone **Serveurs et domaines supplémentaires**, cliquez sur  et entrez l'URL de départ pour examiner l'application.
3. Cliquez sur **Explorer les services web**.
   GSC s'ouvre.
4. Envoyez des demandes au service, puis fermez GSC.
5. Cliquez sur **Examiner > Examen intégral**.
   AppScan explore l'application puis teste tout le site et présente les résultats.
   Voir aussi :
   Chapitre 8, «Résultats : Problèmes de sécurité», à la page 207

Chapitre 6. Examen en cours

La présente section décrit comment démarrer un examen, ce qui se produit lors de l'examen, comment manipuler manuellement l'étape d'exploration et comment exporter les résultats d'un examen.

Démarrer des examens

Remarque : S'il est configuré, Scan Expert s'exécute avant l'examen principal lorsque vous démarrez l'examen. Il évalue votre configuration et suggère des modifications pour optimiser l'examen principal. Pour plus d'informations, voir «Scan Expert», à la page 164.

Démarrer des examens à partir de l'assistant de configuration des examens

Pourquoi et quand exécuter cette tâche

Si vous utilisez l'**Assistant de configuration des examens** (voir «Assistant de configuration des examens», à la page 31) pour créer votre examen, l'étape finale de l'assistant propose des options pour démarrer ce dernier.

Procédure

Sélectionnez une option (voir tableau ci-dessous), et cliquez sur **Terminer**.

Option	Cliquez pour :
Démarrer un examen automatique intégral	Démarrer un examen avec la configuration créée à l'instant dans l'assistant, démarrer avec l'exploration automatique et procéder automatiquement à l'étape de test.
Ne commencer qu'avec l'exploration automatique	Démarrer avec l'étape d'exploration automatique d'un examen, mais ne pas procéder automatiquement à l'étape de test.
Commencer avec l'exploration manuelle	Ouvrir le navigateur pour permettre une exploration manuelle de l'application (voir «Utilisation d'AppScan», à la page 143).
Je démarrerai l'examen ultérieurement	Fermer l'assistant sans procéder à l'examen (par exemple, si vous souhaitez éditer la configuration de l'examen avant de le démarrer, ou si vous souhaitez démarrer l'examen ultérieurement).
Démarrer Scan Expert lorsque l'assistant de configuration des examens a été exécuté	Scan Expert analyse votre configuration et suggère des modifications de configuration pour que l'examen soit plus efficace. (Pour plus de détails, voir «Scan Expert», à la page 164.) Sélectionnez cette option pour exécuter Scan Expert dès la fermeture de l'assistant.

Démarrer des examens à partir du menu Examen ou de la barre d'outils

Pourquoi et quand exécuter cette tâche

Lorsqu'AppScan est ouvert, vous pouvez démarrer un examen avec la configuration en cours à partir du menu Examen ou de la barre d'outils.

Procédure

Dans le menu **Examen**, ou à partir du bouton dans la barre d'outils, sélectionnez l'une des options suivantes :

Si la configuration *ne comprend pas* de données d'exploration manuelle ou automatique :

Icône	Option	Description
	Examen intégral	Exécute un examen intégral. Explorez l'application tant qu'il existe encore des URL non visitées, puis continuez automatiquement avec l'étape de test. (Si un examen en plusieurs phases est configuré, terminez les phases le cas échéant.)
	Exploration uniquement	Explore le site mais ne le teste pas. Cela vous permet d'examiner les résultats de l'exploration et, si nécessaire, d'explorer le site manuellement avant de procéder à l'étape de test.
	Test uniquement	(Cette option est désactivée lorsqu'il n'existe pas de données d'exploration de test).

Si la configuration comprend des données d'exploration manuelle ou automatique :

Icône	Option	Description
	Continuer l'examen intégral	Explore et teste le site à l'aide de cette configuration, y compris les données d'exploration manuelle et automatique.
	Continuer Exploration uniquement	Explore le site automatiquement et ajoute les données aux données d'exploration manuelle et automatique. Cela vous permet d'examiner les résultats de l'exploration et, si nécessaire, d'explorer le site manuellement avant de procéder à l'étape de test.
	Continuer Test uniquement	Teste le site à l'aide des données d'exploration manuelle et automatique uniquement.

Remarque : Si vous avez configuré une ou plusieurs opérations en plusieurs étapes et qu'elles constituent un sous-ensemble significatif de votre site pour lequel vous souhaitez procéder à un examen, vous pouvez exécuter un examen sur ces séquences uniquement (voir «Examiner uniquement les opérations en plusieurs étapes», à la page 192).

Démarrer des examens à partir de la boîte de dialogue Bienvenue

Lorsque vous démarrez AppScan, la boîte de dialogue **Bienvenue** s'affiche.

Remarque : Si la boîte de dialogue **Bienvenue** ne s'affiche pas au démarrage, voir «Onglet Général», à la page 264 pour la faire apparaître à nouveau.

Vous pouvez :

- «Créer un nouvel examen» ou
- «Charger un examen existant», à la page 159

Créer un nouvel examen

Procédure

1. Sélectionnez **Créer un examen**.
2. Procédez de l'une des façons suivantes :
   - Si vous souhaitez exécuter l'examen en utilisant l'une des configurations prédéfinies, cochez la case **Lancer l'assistant de configuration des examens**. (Voir «Examen automatique», à la page 163.)

- Si vous souhaitez apporter des modifications à la configuration avant de lancer l'examen, *désélectionnez* la case à cocher **Lancer l'assistant de configuration des examens**. (Voir «Assistant de configuration des examens», à la page 31.)

3. Cliquez sur un modèle d'examen. Si vous n'avez pas besoin d'un modèle spécifique, sélectionnez Examen standard.

Charger un examen existant

Procédure

1. Sélectionnez **Open an Existing Scan** (Ouvrir un examen existant).
2. Sélectionnez un examen enregistré dans la liste, ou cliquez sur **Parcourir** pour ouvrir un examen enregistré non répertorié.
3. Cliquez sur **OK**.

Démarrer des examens à partir de la boîte de dialogue Nouvel examen

Vous pouvez ouvrir la boîte de dialogue **Nouvel examen** à tout moment (**Fichier > Nouveau**). Cette boîte permet d'ouvrir l'assistant de configuration des examens ou de choisir un modèle d'examen sur lequel vous pouvez immédiatement exécuter un examen complet.

Lancement de l'assistant de configuration des examens :

1. Vérifiez que la case **Lancer l'assistant de configuration des examens** est cochée ou non cochée selon les besoins.
2. Dans la liste Modèles prédéfinis, cliquez sur le modèle requis. Si vous n'avez pas besoin d'un modèle *spécifique*, cliquez sur **Examen standard**.

   Remarque : Pour utiliser un modèle enregistré, cliquez sur **Parcourir**, sélectionnez le fichier SCANT requis et cliquez ensuite sur **Ouvrir**.

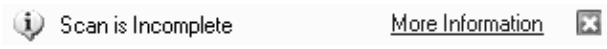
Progression de l'examen

Lorsqu'un examen commence, le **panneau de progression** apparaît au-dessous de la liste des résultats.

Il contient :

- Current l'URL en cours d'exploration ou de test ;
- le pourcentage définitif de l'étape de test ou d'exploration ;
- s'il s'agit d'une étape d'examen suivante, le numéro de l'étape courante (voir «Examen en plusieurs phases automatique», à la page 163) ;
- le temps (mm:ss ou hh:mm:ss ou jj:hh:mm:ss) écoulé depuis le début de l'examen.

Si l'examen est interrompu à cause des problèmes de communication ou sur votre demande, le panneau de notification s'affiche à la place du panneau de progression.



Le **panneau de notification** indique :

- les problèmes de communication et le délai d'attente avant la reprise automatique ;
- la notification indiquant que l'examen est incomplet ;

- le lien « Informations complémentaires » qui ouvre une boîte de dialogue expliquant ce qui a été effectué jusqu'à présent et comment poursuivre.

Interrompre et continuer des examens

Vous pouvez suspendre un examen à tout moment et le reprendre par la suite. Si un examen a été suspendu pour des problèmes de connexion, vous pouvez continuer l'examen une fois l'incident résolu.

Remarque : Lorsque vous mettez un examen en pause, l'arrêt n'est pas tout à fait immédiat.

1. Pour mettre un examen en pause, cliquez sur le bouton **Pause** dans la barre d'outils (ou cliquez sur **Examen > Pause**).

   Le **panneau de notification** apparaît et affiche : `L'examen est incomplet`.

2. Pour continuer un examen mis en pause, cliquez sur le bouton **Examen** dans la barre d'outils et sélectionnez une des options suivantes :
   - **Examen intégral :** Reprenez l'analyse intégrale. (Poursuivez l'étape d'exploration tant qu'il existe encore des URL non visitées, puis continuez automatiquement avec l'étape de test. Si un examen en plusieurs phases est configuré, terminez les phases le cas échéant.)
   - **Exploration uniquement :** Reprenez et terminez l'étape d'exploration, mais ne continuez pas l'étape de test.
   - **Test uniquement :** Reprenez l'étape de test en ignorant toute URL non visitée n'ayant pas été explorée lorsque l'examen était interrompu.

Examens interrompus en raison de problèmes de connectivité

Un examen peut être arrêté en raison de problèmes de connectivité entre AppScan et le serveur qu'il examine ou entre AppScan et le serveur proxy Web local.

Lorsqu'un problème de connexion est détecté, un décompte de 90 secondes commence pendant lequel AppScan attend que ce problème soit résolu. Si le problème est corrigé pendant le décompte, le panneau de notification disparaît et l'examen reprend.

S'il existe un problème de communication, le **panneau de notification** affiche le message :

`Trying to connect to: <IP> Explore/Test stops in <n>`

- L'adresse IP indiquée est celle du serveur examiné, l'adresse IP du serveur proxy (si le problème de connexion concerne le proxy Web) ou une liste d'adresses IP (si l'examen se connecte à plusieurs serveurs et que plusieurs d'entre eux sont arrêtés).
- Le nombre `<n>` est le décompte de 90 secondes.
- Si le problème n'est pas corrigé lorsque le décompte atteint zéro, l'examen s'arrête.
- Une fois le problème résolu, vous pouvez poursuivre l'examen là où il avait été arrêté (**Examiner > Continuer**) ou exécuter à nouveau l'examen (**Examiner > Nouvel examen**).

Examens arrêtés en raison de problèmes d'application

Pourquoi et quand exécuter cette tâche

Il arrive qu'un examen s'arrête et que le **panneau de notification** affiche un lien pour des **Informations complémentaires**.

Procédure

1. Cliquez sur **Informations complémentaires**.

   Une boîte de message s'affiche, expliquant que faire ensuite. Les instructions expliquent comment trouver la liste des URL interactives ou la liste des liens rompus par manque d'authentification

NTLM. Si un examen trouve l'une de ces deux listes et ne parvient pas à la résoudre automatiquement, la boîte de message **Informations complémentaires** récapitule le problème.

2. Utilisez les procédures suivantes selon les besoins :
   - «Traitement des URL interactives»
   - «Traitement des demandes ayant échoué»

Traitement des URL interactives

Comment inclure des URL d'examen nécessitant une interaction d'utilisateur.

Pourquoi et quand exécuter cette tâche

Si l'examen est arrêté car il n'est pas parvenu à remplir automatiquement tous les formulaires d'entrée, vous pouvez terminer l'exploration manuellement.

Procédure

1. Sélectionnez la vue **Données d'application**.
2. Sélectionnez l'écran **Interaction utilisateur nécessaire**.
3. Créez une exploration manuelle de ces URL (voir «Explorer manuellement des URL interactives», à la page 204) et insérez les valeurs de l'outil de remplissage des formulaires.
4. Poursuivez l'examen, de préférence en incluant une étape d'exploration automatique.

Traitement des demandes ayant échoué

Comment traiter les demandes qui ont échoué par manque d'authentification NTLM.

Pourquoi et quand exécuter cette tâche

Si l'examen rencontre des liens rompus du fait d'une authentification NTLM manquante, il s'arrête.

Procédure

1. Sélectionnez la vue **Données d'application**.
2. Sélectionnez l'écran **Demandes ayant échoué**.
3. Dans la boîte de dialogue **Configuration des examens** > **Connexion/Déconnexion**, entrez vos détails d'authentification de plateforme.
4. Poursuivez l'examen avec une nouvelle exécution de l'étape d'exploration.

Sauvegarder et charger des examens

Lorsque vous sauvegardez un examen, la configuration et toutes les données collectées par AppScan jusqu'à présent (lors des étapes d'exploration et de test) sont sauvegardées dans un fichier .SCAN.

Après avoir sauvegardé un examen, vous pouvez charger le fichier .SCAN pour reprendre ou réexécuter l'examen.

Sauvegarder des examens

Pourquoi et quand exécuter cette tâche

Vous pouvez enregistrer un examen qui est terminé, mis en pause ou qui a été interrompu pour des raisons externes.

Procédure

Cliquez sur **Fichier > Sauvegarder** (ou appuyez sur **[Ctrl] + S**).

Remarque : Pour afficher ou modifier le dossier par défaut dans lequel les examens sont sauvegardés, cliquez sur **Outils > Options > Préférences**. Pour plus de détails, voir «Onglet Préférences», à la page 261.

Sauvegarde automatique de l'examen

Pourquoi et quand exécuter cette tâche

Vous pouvez définir AppScan pour qu'il enregistre automatiquement les données dans un fichier .SCAN lors de l'examen. Lorsque cette option est sélectionnée, AppScan procède à une sauvegarde à la fois périodiquement (à un intervalle que vous définissez) et à des moments précis de l'examen.

Procédure

Cliquez sur **Outils > Options > onglet Options d'examen**, puis cochez la case **Sauvegarde automatique lors de l'examen**. Vous pouvez également ajuster l'intervalle entre les sauvegardes.
L'examen en cours sera enregistré à l'intervalle que vous avez sélectionné. Il sera également enregistré :

- lorsque vous démarrez ou poursuivez toute partie de l'examen ;
- lorsque l'étape d'exploration se termine ;
- lorsque l'étape de test se termine.

Lorsqu'un nouvel examen démarre et qu'une sauvegarde automatique est activée, un message apparaît expliquant que l'examen doit être enregistré, car la sauvegarde automatique est activée.

- Cliquez sur **Oui** pour ouvrir une boîte de dialogue **Sauvegarder sous** et enregistrer les examens.
- Cliquez sur **Non** pour désactiver la fonction "Sauvegarde automatique lors de l'examen" pour l'examen en cours uniquement.
- Cliquez sur **Désactiver** pour désactiver la fonction "Sauvegarde automatique lors de l'examen" pour cet examen et tous les examens futurs.

Charger des examens enregistrés

Procédure

Cliquez sur **Fichier > Ouvrir** et sélectionnez un examen.
La barre de progression **Chargement** apparaît pendant un moment, puis l'**Arborescence de l'application** de l'examen, tel qu'exploré ou testé lors de la dernière sauvegarde, apparaît dans la fenêtre principale.

Importation d'un modèle d'examen existant

Cette section décrit comment importer le modèle d'examen à partir d'un examen enregistré dans une version d'AppScan antérieure à la version 8.6.

Dans AppScan version 8.6, le format du fichier d'examen a été revu et les examens enregistrés dans des versions antérieures ne peuvent pas être ouverts dans la version actuelle. Si nécessaire, vous pouvez importer le modèle en vue d'une utilisation dans un nouvel examen.

Pour importer le modèle d'examen, procédez comme suit :

1. Modifiez l'extension du fichier d'examen de SCAN en ZIP.
2. Ouvrez le fichier ZIP, puis localisez `templateconfig.xml` et procédez à son extraction.
3. Changez son extension de XML en SCANT.
4. Ouvrez-le avec AppScan.

Examen automatique

Un examen automatique complet consiste en un ou plusieurs cycles d'une étape d'exploration suivis d'une étape de test.

«Examen en plusieurs phases automatique»

Etape d'exploration

Lorsque vous démarrez un examen automatique complet, l'étape d'exploration commence la première. Lors de cette étape, AppScan procède comme suit :

- Explore l'application comme un utilisateur le ferait, depuis l'URL de départ fournie dans la configuration de l'examen (voir «Vue URL et serveurs», à la page 47) vers chaque URL de l'application n'ayant pas été exclue.

  Remarque : La configuration des examens vous permet de filtrer sur l'étape d'exploration (voir «Vue Exclusion de chemins et de fichiers», à la page 65). Si vous excluez des chemins spécifiques de cette étape ou si vous définissez des limites d'exploration spécifiques, ces filtres s'appliquent à l'étape d'exploration.
- Construit l'**Arborescence de l'application**, un modèle hiérarchique des adresses URL de l'application.
- Analyse les adresses URL explorées et génère des tests.

Etape de test

Lors de l'étape de test, AppScan procède comme suit :

- Se connecte à l'application.
- Exécute des tests préliminaires sur les adresses URL, qui aident à interpréter les résultats.
- Teste les adresses URL en envoyant des requêtes destinées à révéler les vulnérabilités.
- Enregistre la réponse à chaque requête.
- Fournit les résultats du test.

Lors de l'étape de test, la vue **Problèmes** de sécurité de la **liste des résultats** contient les résultats de l'examen.

Examen en plusieurs phases automatique

Pourquoi et quand exécuter cette tâche

Certains tests peuvent révéler de nouvelles zones de l'application Web non accessibles par le biais d'une navigation normale dans le site Web (par exemple, listages de répertoires ou contenu du fichier robots.txt). Si l'examen en plusieurs phases est activé, AppScan ajoute des URL reconnues lors de l'étape de test à la liste des URL à explorer. Lorsque l'étape de test est terminée, AppScan explore alors automatiquement les URL nouvellement reconnues, crée de nouveaux tests pour elles et les teste.

Par défaut, les examens peuvent contenir jusqu'à quatre phases, le cas échéant. Vous pouvez configurer AppScan pour exécuter entre 1 et 10 phases.

Remarque : Le paramètre d'examen en plusieurs phases s'applique uniquement si vous exécutez un examen intégral. Si vous activez les fonctions **Exploration uniquement** et **Test uniquement**, le résultat sera un examen à une seule phase.

Procédure

1. Ouvrez la vue **Configuration des examens** | **Options de test**.
2. Cochez la case **Autoriser l'examen en plusieurs phases**.

3. Dans la zone de saisie **Nombre max. de phases**, entrez le nombre maximal de phases que vous souhaitez autoriser (nombre entre **1** et **10** ; par défaut **4**).

   Pendant que AppScan teste le site, il analyse les réponses du test à la recherche d'éventuelles URL supplémentaires auxquelles il n'aurait pas pu accéder lors de l'étape d'exploration initiale. Il peut alors exécuter des étapes supplémentaires d'exploration et de test sur ces nouveaux liens. Le nombre entré ici détermine le nombre de fois que AppScan exécutera ces étapes supplémentaires. (Par défaut, l'examen en plusieurs phases est activé avec quatre phases.)

   Remarque : Le panneau de progression (voir «Progression de l'examen», à la page 159) indique quelle phase de l'examen est actuellement en cours.

   Remarque : Si vous procédez à un nouvel examen de votre application (**Examen > Nouvel examen**), le numéro de phase recommence à 1.

   Remarque : Si vous enregistrez un examen, le numéro de l'étape en cours est enregistré. Si vous chargez cet examen pour l'exécuter de nouveau, il commence à partir du numéro de phase enregistré.

Scan Expert

Scan Expert est une fonction permettant d'explorer le comportement de votre application et de votre réseau afin d'évaluer l'efficacité de votre configuration d'examen. En fonction des résultats, il peut recommander d'apporter des modifications à la configuration afin d'assurer un examen plus rigoureux.

Scan Expert se connecte à votre application et y exécute une courte étape d'exploration. Dans le même temps, le panneau d'examen indique la progression et l'arborescence de l'application affiche les parties de l'application ayant été explorées comme lors d'un examen régulier. Le panneau Scan Expert s'ouvre également (indiquant qu'il ne s'agit pas d'un examen régulier).

Différentes utilisations de Scan Expert :

- Scan Expert peut être configuré pour s'exécuter automatiquement avant un examen complet. Selon sa configuration, il peut :
  - Proposer des recommandations que vous pouvez accepter ou rejeter manuellement, ou
  - Appliquer des recommandations activées automatiquement (toutes les recommandations ne sont pas activées automatiquement) et continuer l'examen.

  (Pour plus d'informations, voir «Vue Scan Expert», à la page 118. Pour activer/désactiver l'exécution automatique de Scan Expert au début des examens, accédez à **Outils > Options... > Préférences**.)
- Scan Expert peut être exécuté indépendamment à tout moment, en vue de l'évaluation de la configuration :
  - Pour que Scan Expert exécute une brève étape d'exploration sur l'application, puis analyse les réponses pour évaluer la configuration, cliquez sur **Examen > Exécuter une évaluation Scan Expert**.
  - Si vous avez déjà exploré l'application, vous gagnerez du temps en laissant Scan Expert analyser les données *existantes* sans exécuter sa propre étape d'exploration. Cliquez sur **Examen > Exécuter uniquement l'analyse Scan Expert**.
- Si vous essayez de démarrer un examen et qu'AppScan détecte un problème grave lié à la configuration, ce dernier peut tout de même exécuter Scan Expert, même s'il n'est pas configuré en vue de son exécution automatique, afin de tenter de résoudre le problème.

Recommandations Scan Expert

Une fois l'étape d'exploration terminée, Scan Expert analyse les réponses reçues et recommande des modifications à apporter à la configuration. En fonction de la manière dont Scan Expert a été configuré (voir «Vue Scan Expert», à la page 118), les suggestions peuvent s'appliquer automatiquement ou s'afficher sous la forme d'une liste interactive.

Le tableau ci-dessous récapitule les options disponibles dans la liste de Recommandations Scan Expert.

Option	Description
Recommandation	Les recommandations qu'AppScan peut mettre en œuvre sans entrées utilisateur supplémentaires sont automatiquement sélectionnées. Sélectionnez/désélectionnez les cases à cocher selon les besoins. Les recommandations dont la mise en œuvre requiert une entrée utilisateur apparaissent avec un lien bleu. Cliquez sur le lien pour ouvrir la boîte de dialogue Configuration dans l'onglet approprié et entrez les données requises (en enregistrant par exemple une procédure de connexion).
Informations complémentaires	Cliquez pour ouvrir la fenêtre Informations complémentaires pour la recommandation sélectionnée. Cette fenêtre contient le raisonnement à l'origine de la recommandation et des instructions d'application manuelle de cette recommandation.
Edition manuelle	Permet d'appliquer manuellement la recommandation sélectionnée en ouvrant la boîte de dialogue Configuration des examens dans la vue appropriée.
Appliquer les recommandations	Met à jour la configuration de l'examen afin de suivre toutes les recommandations de la case cochée et ferme le panneau Scan Expert.
Ignorer tout	Annule toutes les recommandations et ferme le panneau Scan Expert.

Examen glass box

Présentation

Cette section décrit les principes de l'examen glass box et sa configuration.

Tandis qu'un examen standard regarde l'application comme une "boîte noire", et analyse sa *sortie* sans "regarder à l'intérieur". L'examen glass box utilise un agent installé sur le serveur d'applications pour inspecter le code lui-même pendant l'examen. D'où le terme "glass box" (boîte de verre). Pour l'effectuer, l'agent glass box AppScan doit être installé sur le même serveur que l'application que vous souhaitez tester, et non sur la machine locale sur laquelle AppScan est installé.

L'examen glass box présente les avantages suivants :

- Pendant l'étape d'exploration, l'examen glass box révèle les paramètres HTTP qui affectent le côté serveur, mais qui ne figurent pas dans les réponses, et qui ne seraient donc pas détectés par un test de type "boîte noire" uniquement.
- Pendant l'étape de test, l'examen glass box peut vérifier la réussite ou l'échec de certains tests, par exemple les tests d'injection SQL en aveugle, avec plus de précision, ce qui génère moins de résultats "faussement positifs". Il peut aussi révéler l'existence de certains problèmes de sécurité qui ne sont pas détectables par les techniques de test de type boîte noire.
- L'examen glass box permet à AppScan de vous présenter la vulnérabilité dans le code source réel, en simplifiant à la fois le reporting et la résolution du problème.

L'examen glass box ajoute une dimension supplémentaire à l'examen en termes de type et de nombre de problèmes détectés, et d'informations sur la résolution des problèmes.

Pour configurer et utiliser l'examen glass box :

Tâche	Description
1. Installer l'agent	Installez l'agent glass box AppScan sur votre serveur d'applications. ***Cette opération n'est à faire qu'une fois sur un seul serveur.*** **Remarque :** Des agents peuvent être installés sur plusieurs serveurs, mais un seul serveur peut être inclus dans un examen glass box.
2. Définir l'agent	Définissez les agents installés dans AppScan, pour qu'il puisse communiquer avec eux. ***Cette opération n'est à faire qu'une fois pour chaque machine AppScan.*** **Remarque :** Plusieurs instances d'AppScan (sur des machines différentes) peuvent utiliser le même agent glass box de serveur Web, mais pas simultanément.
3. Configurer l'examen	Configurez l'*examen* pour utiliser l'agent glass box nécessaire. Par défaut, il est configuré automatiquement, mais il peut être réglé dans **Configuration des examens > Glass Box**. ***Cette opération doit être répétée pour chaque examen.***
4. Exécuter l'examen	Examinez votre application avec la fonction Examen glass box activée.
5. Mettre à jour les règles d'agent	**Mettez à jour** les règles de l'agent lorsque vous y êtes invité par le processus de mise à jour automatique, de sorte que la version des règles sur le serveur Web reste synchronisée avec les règles de la version locale d'AppScan. **Remarque :** Après avoir exécuté le processus de mise à jour, vous devez redémarrer le serveur d'applications Web.

Pour plateformes Java

Installation et utilisation de l'agent glass box sur un serveur Java.

Installation de l'agent glass box

Cette section décrit la manière de configurer l'agent glass box côté serveur, pour permettre les examens glass box.

L'agent glass box d'AppScan doit être installé sur un ou plusieurs serveurs d'applications, en copiant certains fichiers du répertoire d'installation d'AppScan sur le serveur.

Remarque : L'agent glass box installe et utilise un agent Java dédié (`gbAgent.jar`). Si d'autres agents Java sont définis sur le serveur Web, vous pouvez ajouter un agent glass box sur la ligne de commande du serveur d'applications (le chemin exact dépend de votre installation) :

```
java ... -javaagent:c:\otherAgent\otherAgent.jar
  -javaagent:c:\glassbox\gbAgent.jar ...
```

Configurations requises

Les plateformes et technologies suivantes sont prises en charge.

Logiciel	Détails
JRE	Les versions 6 et 7 de JRE sont prises en charge. La version 8 *ne l'est pas*.

Logiciel	Détails
Système d'exploitation	Systèmes Microsoft Windows pris en charge (version 32–bits et 64–bits) : • Microsoft Windows Server 2012 • Microsoft Windows Server 2012 R2 • Microsoft Windows Server 2008 R2 Systèmes Linux pris en charge : • Linux RHEL 5, 6, 6.1, 6.2, 6.3, 6.4 Systèmes UNIX pris en charge : • UNIX AIX 6.1, 7.1 • UNIX Solaris (SPARC) 10, 11
Conteneur Java EE	JBoss AS 6, 7; JBoss EAP 6.1; Tomcat 6.0, 7.0; WebLogic 10, 11, 12; WebSphere 7.0, 8.0, 8.5, 8.5.5

Avant de commencer

Vous gagnerez du temps à préparer les informations ci-après avant de commencer l'installation. Il se peut que vous deviez consulter l'administrateur du serveur d'applications Web pour obtenir ces informations.

- Système d'exploitation de votre serveur (Windows, Linux ou Unix)
- Votre serveur d'applications Java EE (WebSphere, WebLogic, Tomcat ou JBoss) et le mode dans lequel il est installé (service standard ou comme service de système d'exploitation)
- Emplacement de déploiement des applications Web du serveur d'applications Java EE (par exemple : `D:\apache-tomcat-6.0.32\webapps`)
- Emplacement de l'environnement Java Runtime utilisé par votre serveur d'applications Java EE (par exemple : `C:\Program Files (x86)\Java\jre6`)
- Données d'identification permettant d'administrer le serveur d'applications Java EE (aux fins du déploiement d'une nouvelle application Web)

Remarque : Si le serveur doit fonctionner en mode sécurisé, vous devez ajouter des droits spécifiques. Voir «Droits nécessaires pour fonctionner en mode sécurisé», à la page 176.

Journaux

Les journaux glass box sont sauvegardés à l'emplacement suivant :
`[Installation folder]\instrumentation.log`

Installation automatique avec le programme d'installation de l'agent glass box :

Cette section explique comment installer l'agent glass box automatiquement via l'interface utilisateur.

Pourquoi et quand exécuter cette tâche

Lorsque AppScan est installé, les fichiers nécessaires à l'installation de l'agent du serveur sont sauvegardés dans un dossier dédié sur votre machine. Pour effectuer cette tâche, vous devez accéder à ce dossier et à votre serveur d'applications.

Procédure

1. Ouvert `...\Program Files\IBM\AppScan Standard\Glass box`
   Le chemin exact dépend de l'emplacement dans lequel vous avez installé AppScan.
2. Copiez le fichier de configuration approprié sur le serveur Web :
   - **Serveur Linux :** Copiez le fichier `GB_Java_Setup.bin`

- **Serveur Windows :** Copiez le fichier `GB_Java_Setup.exe`

3. Lancez l'application GB_Java_Setup, puis suivez les instructions en ligne. Au cours de ce processus, le système demande de :
   - Sélectionner le serveur d'applications Web. Si ce serveur n'est pas répertorié (par exemple, JBoss Service, Tomcat Service ou WebLogic Service), sélectionnez **Autre**.
   - Définir un nom d'utilisateur et un mot de passe pour l'agent. Ultérieurement, lorsque l'agent sera défini dans AppScan, ces données d'identification seront nécessaires pour activer les communications entre le produit et l'agent. Seuls des caractères anglais ASCII peuvent être utilisés.

   Remarque : Si vous avez sélectionné **Autre**, continuez comme une installation *manuelle*, à partir de l'étape 5.

   Remarque : Vous pouvez également être invité à fournir le chemin du dossier JAVA_HOME (JDK) ou JRE_HOME (JDK ou JRE) correspondant à votre infrastructure.

   Conseil : Les options de langue de l'interface du programme d'installation n'incluent que les langues prises en charge par votre système d'exploitation. Pour exécuter le programme d'installation dans une autre langue, vous pouvez ouvrir le programme d'installation via la ligne de commande en ajoutant l'indicateur correspondant à la langue de votre choix. Par exemple, pour exécuter le programme d'installation en japonais sur un système d'exploitation anglais, exécutez la commande `GB_Java_Setup.bin -l ja`
   - Un script de démarrage est créé dans le dossier d'installation de l'agent glass box
   - Si vous disposez d'un bureau, un raccourci pour le démarrage du serveur et l'activation de l'agent glass box est créé.

   Important : Pour réaliser l'examen glass box, le serveur d'applications doit être démarré selon l'une de ces deux méthodes qui activent en même temps l'agent glass box.

Installation automatique via la ligne de commande :

Cette section décrit comment installer l'agent glass box via la ligne de commande.

Pourquoi et quand exécuter cette tâche

Lorsque AppScan est installé, les fichiers nécessaires à l'installation de l'agent du serveur sont sauvegardés dans un dossier dédié sur votre machine. Pour effectuer cette tâche, vous devez accéder à ce dossier et à votre serveur d'applications.

Procédure

1. Ouvert `...\Program Files\IBM\AppScan Standard\Glass box`
   Le chemin exact dépend de l'emplacement dans lequel vous avez installé AppScan.
2. Copiez le fichier de configuration approprié sur le serveur Web :
   - Pour un serveur Linux, copiez le fichier `GB_Java_Setup.bin`
   - Pour un serveur Windows, copiez le fichier `GB_Java_Setup.exe`
3. Exécutez une ligne de commande contenant *tous* les arguments suivants *qui s'appliquent à votre serveur*, séparés par un espace.

Commande	Description
`GB_Java_Setup.bin` (Linux) ou `GB_Java_Setup.exe` (Windows)	Fichier de configuration.
`-i console`	

Commande	Description
-l en	Définit la langue de l'installation. Utilisez le code correspondant à votre langue ("en" correspond à l'anglais).
-DCHOSEN_INSTALL_SET=JBoss / WebSphe / Tomcat / WebLogic / Other	Entrez le type de serveur sur lequel vous installez l'agent. **Remarque :** Si votre serveur n'est pas répertorié (par exemple, s'il s'agit de JBoss Service, Tomcat Service ou WebLogic Service), sélectionnez **Autre**.
-DUSER_INSTALL_DIR=value	Définit le chemin d'installation de l'agent.
-DGLASS_USERNAME=value	Définit un nom d'utilisateur pour accéder à l'agent. Seuls des caractères anglais et des nombres peuvent être utilisés.
-DGLASS_PASSWORD=value	Définit un mot de passe pour accéder à l'agent. Seuls des caractères anglais et des nombres peuvent être utilisés.
-DWEBLOGIC_PATH / -DJBOSS_PATH / -DTOMCAT_PATH / -DWEBSPHERE_PATH=value	Définit le chemin du répertoire d'installation du serveur Web. **Exemples** (l'emplacement réel dépend de votre système) : WebLogic : C:\weblogic\user_projects\domains\base_domain\ JBoss : C:\jboss-6.0.0\ Tomcat : C:\apache-tomcat-6.0.32\ WebSphere : C:\Program Files\IBM\WebSphere\AppServer\profiles\AppSrv01\
-DJBOSS_SERVER_NAME=value / -DWEBSPHERE_SERVER_NAME=value	Nom du serveur.
-DWEBLOGIC_USERNAME / -DWEBSPHERE_USERNAME=value -DWEBLOGIC_PASSWORD / -DWEBSPHERE_PASSWORD=value	Nom d'utilisateur et mot de passe pour accéder au serveur d'applications
-DWEBLOGIC_LIB=value	Chemin d'accès au dossier LIB, par exemple : C:\weblogic\wlserver_10.3\server\lib\
-DWEBLOGIC_TARGET=value	Nom du serveur/de la cible.
-DWEBLOGIC_PORT=value	Port d'administration.
-DSELECTED_JBOSS_TYPE=value	Utilisez l'une des valeurs suivantes : JBoss AS JBoss EAP Standalone JBoss EAP Managed Domain

Exemple pour WebSphere :

```
GB_Java_Setup.bin –i console –l en -DCHOSEN_INSTALL_SET=WebSphe
-DUSER_INSTALL_DIR=/opt/glass_box -DGLASS_USERNAME=jsmith
-DGLASS_PASSWORD=1234
-DWEBSPHERE_PATH=/opt/IBM/WebSphere/AppServer/profiles/AppSrv01
-DWEBSPHERE_SERVER_NAME=server1
-DWEBSPHERE_USERNAME=admin -DWEBSPHERE_PASSWORD=admin_pw
```

4. Vérifiez que votre serveur Web s'est arrêté à la fin de la procédure. Si ce n'est pas le cas, arrêtez-le manuellement.
5. Redémarrez le serveur Web en utilisant le raccourci clavier sur le bureau, ou le script de démarrage situé dans le dossier d'installation de l'agent glass box, pour activer l'agent glass box.

Installation manuelle sur un serveur JBoss ou un serveur JBoss Service :

La présente section décrit comment installer manuellement l'agent glass box sur un serveur JBoss ou JBoss Service.

Pourquoi et quand exécuter cette tâche

Lorsque AppScan est installé, les fichiers nécessaires à l'installation de l'agent du serveur sont sauvegardés dans un dossier dédié sur votre machine. Pour effectuer cette tâche, vous devez accéder à ce dossier et à votre serveur d'applications.

Procédure

1. Ouvrez `...\Program Files\IBM\AppScan Standard\Glass box`
   Le chemin absolu dépend de l'emplacement dans lequel vous avez installé AppScan.
2. Localisez le fichier `GB_Java_Manual_Setup.zip` et copiez-le sur votre serveur Web.
3. Extrayez le contenu de ce dossier dans votre emplacement préféré sur le serveur.
4. Définissez un nom d'utilisateur et un mot de passe pour l'agent (seuls des caractères anglais ASCII peuvent être utilisés) :
   - **Serveur Linux :** Exécutez `AgentCredentials.sh <username> <password>`

     Remarque : `AgentCredentials.sh` doit avoir des permissions d'exécution.
   - **Serveur Windows :** Exécutez `AgentCredentials.bat <username> <password>`
5. Déployez l'application Web GBootStrap :
   a. Connectez-vous à la console d'administration JBoss. L'emplacement par défaut est `http://<server_name>:<port_number>/admin-console/`
   b. Cliquez sur **Applications > Fichiers WAR de l'application Web**, puis sur **Ajouter une nouvelle ressource**.
   c. Entrez le chemin du fichier `GBootStrap.war` (qui se situe dans le dossier glass box que vous avez extrait), puis cliquez sur **Continuer**.

   Un message confirme que la création de la ressource a abouti.
6. Arrêtez le serveur/service JBoss.
7. Fournissez l'agent Java gbAgent.jar (qui se trouve dans le dossier que vous avez extrait) en tant qu'argument JVM en exécutant l'*une* des opérations suivantes :
   - **Via la variable d'environnement** : Configurez la machine virtuelle Java de JBoss à l'aide de la variable d'environnement JAVA_OPTS (si celle-ci n'existe pas, créez-la) avec la valeur :

     ```
     -javaagent:"<path_to_gbAgent.jar>/gbAgent.jar"
     -Djava.net.preferIPv4Stack=true
     -Djboss.modules.system.pkgs=com.ibm.glassbox.asm.agent,
       com.ibm.glassbox.agent,com.ibm.glassbox.logger,
       com.ibm.glassbox.jsp,org.jboss.byteman
     ```
   - **Via des scripts batch/sh :** Transmettez les arguments à la machine JVM exécutant JBoss en éditant les fichiers de configuration fournis avec le serveur :

     Serveur Linux :

     a. Dans le dossier JBoss, recherchez et ouvrez le fichier approprié dans un éditeur (situé généralement dans `/bin`) :
        – **JBoss AS :** `run.sh`
        – **JBoss EAP Standalone :** `standalone.sh`
        – **JBoss EAP Managed Domain :** `domain.sh`
     b. Recherchez la ligne commençant par `JAVA_OPTS` et ajoutez-lui le code suivant :

```
export JAVA_OPTS=$JAVA_OPTS "-javaagent:<path_to_gbAgent.jar>/gbAgent.jar"
-Djava.net.preferIPv4Stack=true
-Djboss.modules.system.pkgs=com.ibm.glassbox.asm.agent,
  com.ibm.glassbox.agent,
  com.ibm.glassbox.logger,
  com.ibm.glassbox.jsp,org.jboss.byteman
```

c. Enregistrez et fermez le fichier.

Serveur Windows :

a. Dans le dossier JBoss, recherchez et ouvrez le fichier approprié dans un éditeur (situé généralement dans `/bin`) :
   - **JBoss AS :** `run.conf`
   - **JBoss EAP Standalone :** `standalone.conf`
   - **JBoss EAP Managed Domain :** `domain.conf`

b. Recherchez la ligne commençant par `set JAVA_OPTS=` et ajoutez-lui la ligne suivante :

```
set JAVA_OPTS=$JAVA_OPTS "-javaagent:<path_to_gbAgent.jar>\gbAgent.jar"
-Djava.net.preferIPv4Stack=true
-Djboss.modules.system.pkgs=com.ibm.glassbox.asm.agent,
  com.ibm.glassbox.agent,com.ibm.glassbox.logger,
  com.ibm.glassbox.jsp,org.jboss.byteman"
```

c. Enregistrez et fermez le fichier.

Important : Vérifiez que JAVA_OPTS est initialisé une seule fois, et avant les lignes ci-dessus, afin que les autres attributions JAVA_OPTS n'écrasent pas `-javaagent`.

Remarque : Pour ajouter des arguments à JAVA_OPTS, utilisez la convention %JAVA_OPTS% / $ JAVA_OPTS.

8. Redémarrez le serveur/service JBoss.

Installation manuelle sur un serveur Tomcat :

Cette section décrit comment installer manuellement l'agent glass box sur un serveur Tomcat.

Pourquoi et quand exécuter cette tâche

Lorsque AppScan est installé, les fichiers nécessaires à l'installation de l'agent du serveur sont sauvegardés dans un dossier dédié sur votre machine. Pour effectuer cette tâche, vous devez accéder à ce dossier et à votre serveur d'applications.

Procédure

1. Ouvrez `...\Program Files\IBM\AppScan Standard\Glass box`
   Le chemin absolu dépend de l'emplacement dans lequel vous avez installé AppScan.
2. Localisez le fichier `GB_Java_Manual_Setup.zip` et copiez-le sur votre serveur Web.
3. Extrayez le contenu de ce dossier dans votre emplacement préféré sur le serveur.
4. Définissez un nom d'utilisateur et un mot de passe pour l'agent (seuls des caractères anglais ASCII peuvent être utilisés) :
   - **Serveur Linux :** Exécutez `AgentCredentials.sh <username> <password>`

     Remarque : `AgentCredentials.sh` doit avoir des permissions d'exécution.
   - **Serveur Windows :** Exécutez `AgentCredentials.bat <username> <password>`
5. Déployez l'application Web GBootStrap.
   - Méthode préférée :
     a. Connectez-vous à Tomcat Manager. L'emplacement par défaut est `http://<server_name>:<port_number>/manager/html`

b. Dans **Deploy table > War file to deploy**, cliquez sur **Choose file**
c. Recherchez GBootStrap.war (qui se situe dans le dossier glass box que vous avez extrait) puis cliquez sur **Open**
d. Cliquez sur **Deploy** et vérifiez que GBootStrap a été ajouté à la liste des applications.

- Autre méthode :
  a. Copiez le fichier GBootStrap.war à partir du dossier glass box que vous avez extrait
  b. Collez-le dans le dossier `\webapps`, à l'emplacement par défaut :
     `C:\apache-tomcat-[version]\webapps`

6. Fermez Tomcat.
7. Configurez l'utilisation permanente de l'agent glass box par Tomcat de l'*une* des manières suivantes :
   - **Via la variable d'environnement :** Configurez la machine virtuelle Java de JBoss à l'aide de la variable d'environnement JAVA_OPTS (si celle-ci n'existe pas, créez-la) avec la valeur `-javaagent:<path_to_gbAgent.jar>/gbAgent.jar`.
   - **Via des scripts batch/sh :** Transmettez les arguments à la machine JVM exécutant Tomcat en éditant les scripts de configuration fournis :

     Serveur Linux :
     a. Dans le dossier Tomcat (qui se trouve généralement dans `<path_to_Tomcat_folder>/bin`), ouvrez `startup.sh`
     b. Recherchez la ligne commençant par `CATALINA_OPTS` et ajoutez-lui la ligne suivante :
        `export CATALINA_OPTS = $CATALINA_OPTS -javaagent:<path_to_gbAgent.jar>/gbAgent.jar`
     c. Enregistrez et fermez le fichier.

     Serveur Windows :
     a. Dans le dossier Tomcat (qui se trouve généralement dans `<path_to_Tomcat_folder>\bin`), ouvrez `startup.bat`
     b. Recherchez la ligne commençant par `set CATALINA_OPTS=` et ajoutez la ligne suivante en dessous :
        `set CATALINA_OPTS = %CATALINA_OPTS% -javaagent:<path_to_gbAgent.jar>/gbAgent.jar`
     c. Enregistrez et fermez le fichier.

   Important : Vérifiez que CATALINA_OPTS est initialisé une seule fois, et avant les lignes ci-dessus, afin que les autres attributions CATALINA_OPTS n'écrasent pas `-javaagent`.

   Remarque : Pour ajouter des arguments à CATALINA_OPTS, utilisez la convention %CATALINA_OPTS% / $ CATALINA_OPTS.
8. Redémarrez Tomcat.

Installation manuelle sur un serveur Tomcat Service :

La présente section décrit comment installer manuellement l'agent glass box sur un serveur Tomcat Service/Daemon.

Pourquoi et quand exécuter cette tâche

Lorsque AppScan est installé, les fichiers nécessaires à l'installation de l'agent du serveur sont sauvegardés dans un dossier dédié sur votre machine. Pour effectuer cette tâche, vous devez accéder à ce dossier et à votre serveur d'applications.

Procédure

1. Ouvrez `...\Program Files\IBM\AppScan Standard\Glass box`
   Le chemin absolu dépend de l'emplacement dans lequel vous avez installé AppScan.

2. Localisez le fichier `GB_Java_Manual_Setup.zip` et copiez-le sur votre serveur Web.
3. Extrayez le contenu de ce dossier dans votre emplacement préféré sur le serveur.
4. Définissez un nom d'utilisateur et un mot de passe pour l'agent (seuls des caractères anglais ASCII peuvent être utilisés) :
   - **Serveur Linux :** Exécutez `AgentCredentials.sh <username> <password>`

     Remarque : `AgentCredentials.sh` doit avoir des permissions d'exécution.
   - **Serveur Windows :** Exécutez `AgentCredentials.bat <username> <password>`
5. Déployez l'application Web GBootStrap :
   - Connectez-vous à Tomcat Manager. L'emplacement par défaut est `http://<server_name>:<port_number>/manager/html`
   - Dans **Deploy table > War file to deploy**, cliquez sur **Choose file**.
   - Recherchez GBootStrap.war (qui se situe dans le dossier glass box que vous avez extrait) puis cliquez sur **Open**.
   - Cliquez sur **Deploy** et vérifiez que GBootStrap a été ajouté à la liste des applications.
6. Fermez Tomcat.
7. Configurez l'utilisation de l'agent glass box par Tomcat :
   a. Localisez Tomcat JVM dans `...\Tomcat 7.0\bin\tomcat7w.exe`
   b. Cliquez deux fois dessus et sélectionnez l'onglet **Properties > Java**.
   c. Dans la zone Options Java, ajoutez ce qui suit en tant que nouvelle ligne : `-javaagent:<path_to_gbAgent.jar>/gbAgent.jar`

      Remarque : Si d'autres agents Java sont définis sur le serveur Web, vous pouvez *ajouter* un agent glass box dans la zone des options Java (le chemin exact dépend de votre installation) :

      `... -javaagent:c:\...\otherAgent.jar` **`-javaagent:c:\glassbox\gbAgent.jar ...`**
   d. Cliquez sur **OK**.
8. Redémarrez Tomcat.

Installation manuelle sur un serveur WebLogic :

Cette section décrit comment installer manuellement l'agent glass box sur un serveur WebLogic.

Pourquoi et quand exécuter cette tâche

Lorsque AppScan est installé, les fichiers nécessaires à l'installation de l'agent du serveur sont sauvegardés dans un dossier dédié sur votre machine. Pour effectuer cette tâche, vous devez accéder à ce dossier et à votre serveur d'applications.

Procédure

1. Ouvrez `...\Program Files\IBM\AppScan Standard\Glass box`

   Le chemin absolu dépend de l'emplacement dans lequel vous avez installé AppScan.
2. Localisez le fichier `GB_Java_Manual_Setup.zip` et copiez-le sur votre serveur Web.
3. Extrayez le contenu de ce dossier dans votre emplacement préféré sur le serveur.
4. Définissez un nom d'utilisateur et un mot de passe pour l'agent (seuls des caractères anglais ASCII peuvent être utilisés) :
   - **Serveur Linux :** Exécutez `AgentCredentials.sh <username> <password>`

     Remarque : `AgentCredentials.sh` doit avoir des permissions d'exécution.
   - **Serveur Windows :** Exécutez `AgentCredentials.bat <username> <password>`
5. Déployez l'application Web GBootStrap :

a. Connectez-vous à la console d'administration WebLogic. L'emplacement par défaut est `http://<server_name>:<port_number>/console/`
b. Dans la sous-fenêtre **Domain Structure**, cliquez sur **Deployments**, puis sur **Install**.
c. Dans la zone **Path**, entrez le chemin du fichier GBootStrap.war, puis cliquez sur **Next**.
d. Sélectionnez le bouton d'option **Install this deployment as an application**, puis cliquez sur **Next**.
e. Vérifiez que la zone **Name** contient **GBootStrap**.
f. Cliquez sur **Finish**, puis sur **Save**.
g. Dans la sous-fenêtre **Domain Structure**, cliquez sur **Deployments**, et vérifiez que **GBootStrap** a été ajouté, et que la colonne **Health** contient une coche verte.

6. Fermez le serveur WebLogic.
7. Fournissez l'agent Java gbAgent.jar (qui se trouve dans le dossier que vous avez extrait) en tant qu'argument JVM en exécutant l'*une* des opérations suivantes :
   - **Via la variable d'environnement** : Configurez la machine virtuelle JVM de WebLogic à l'aide de la variable d'environnement JAVA_OPTS (si celle-ci n'existe pas, créez-la) avec la valeur :
     - **Serveur Linux :** `-javaagent:<path_to_gbAgent.jar>/gbAgent.jar`
     - **Serveur Windows :** `-javaagent:<path_to_gbAgent.jar>\gbAgent.jar`
   - **Via des scripts batch/sh :** Transmettez les arguments à la machine JVM exécutant WebLogic en éditant les scripts de configuration fournis avec le serveur :

     Serveur Linux :

     a. Dans le dossier WebLogic (qui se trouve généralement dans `<path_to_Weblogic_folder>\bin`), ouvrez le fichier de démarrage dans un éditeur :
        - **Serveur Admin :** Ouvert `DOMAIN_NAME/bin/startWebLogic.sh`
        - **Serveur géré :** Ouvrez `DOMAIN_NAME/bin/startManagedWebLogic.sh`

     b. Recherchez la ligne commençant par `JAVA_OPTIONS` et ajoutez-lui la ligne suivante :
     ```
     export JAVA_OPTIONS = $JAVA_OPTIONS -javaagent:"<path_to_gbAgent.jar>/gbAgent.jar"
     ```
     c. Enregistrez et fermez le fichier.

     Serveur Windows :

     a. Dans le dossier WebLogic (qui se trouve généralement dans `<path_to_WebLogic_folder>\bin`), ouvrez `startWebLogic.bat`
     b. Recherchez la ligne commençant par `set JAVA_OPTIONS` et ajoutez la ligne suivante en dessous :
     ```
     set JAVA_OPTIONS = %JAVA_OPTIONS% -javaagent:<path_to_gbAgent.jar>/gbAgent.jar
     ```
     c. Enregistrez et fermez le fichier.

   Important : Vérifiez que JAVA_OPTIONS est initialisé une seule fois, et avant les lignes ci-dessus, afin que les autres attributions JAVA_OPTIONS n'écrasent pas `-javaagent`.

   Remarque : Pour ajouter des arguments à JAVA_OPTIONS, utilisez la convention %JAVA_OPTIONS% / $ JAVA_OPTIONS.
8. Redémarrez le serveur WebLogic.

Installation manuelle sur un serveur WebLogic Service :

La présente section décrit comment installer manuellement l'agent glass box sur un serveur WebLogic Service/Daemon.

Pourquoi et quand exécuter cette tâche

Lorsque AppScan est installé, les fichiers nécessaires à l'installation de l'agent du serveur sont sauvegardés dans un dossier dédié sur votre machine. Pour effectuer cette tâche, vous devez accéder à ce dossier et à votre serveur d'applications.

Procédure

1. Ouvrez `...\Program Files\IBM\AppScan Standard\Glass box`
   Le chemin absolu dépend de l'emplacement dans lequel vous avez installé AppScan.
2. Localisez le fichier `GB_Java_Manual_Setup.zip` et copiez-le sur votre serveur Web.
3. Extrayez le contenu de ce dossier dans votre emplacement préféré sur le serveur.
4. Définissez un nom d'utilisateur et un mot de passe pour l'agent (seuls des caractères anglais et des nombres peuvent être utilisés) :
   - **Serveur Linux :** Exécutez `AgentCredentials.sh <username> <password>`

     Remarque : `AgentCredentials.sh` doit avoir des permissions d'exécution.
   - **Serveur Windows :** Exécutez `AgentCredentials.bat <username> <password>`
5. Déployez l'application Web GBootStrap :
   a. Connectez-vous à la console d'administration WebLogic. L'emplacement par défaut est `http://<server_name>:<port_number>/console/`
   b. Dans la sous-fenêtre **Domain Structure**, cliquez sur **Deployments**, puis sur **Install**.
   c. Dans la zone **Path**, entrez le chemin du fichier GBootStrap.war, puis cliquez sur **Next**.
   d. Sélectionnez le bouton d'option **Install this deployment as an application**, puis cliquez sur **Next**.

      Remarque : Si l'option d'installation est désactivée (grisée), il peut s'avérer nécessaire de modifier le réglage du mode de verrouillage et d'édition pour activer celle-ci.
   e. Vérifiez que la zone **Name** contient **GBootStrap**.
   f. Cliquez sur **Finish**, puis sur **Save**.
   g. Dans la sous-fenêtre **Domain Structure**, cliquez sur **Deployments**, et vérifiez que **GBootStrap** a été ajouté, et que la colonne **Health** contient une coche verte.
6. Arrêtez le service WebLogic.
7. Configurez WebLogic pour utiliser l'agent glass box en localisant la clé de registre `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\<WEBLOGIC_SERVICE>` et en modifiant la valeur de `CmdLine` pour inclure `-javaagent:<path_to_gbAgent.jar>/gbAgent.jar`
8. Redémarrez le service.

Installation manuelle sur un serveur WebSphere :

Cette section explique comment installer manuellement l'agent glass box sur un serveur WebSphere.

Pourquoi et quand exécuter cette tâche

Lorsque AppScan est installé, les fichiers nécessaires à l'installation de l'agent du serveur sont sauvegardés dans un dossier dédié sur votre machine. Pour effectuer cette tâche, vous devez accéder à ce dossier et à votre serveur d'applications.

Procédure

1. Ouvrez `...\Program Files\IBM\AppScan Standard\Glass box`
   Le chemin absolu dépend de l'emplacement dans lequel vous avez installé AppScan.
2. Localisez le fichier `GB_Java_Manual_Setup.zip` et copiez-le sur votre serveur Web.
3. Extrayez le contenu de ce dossier dans votre emplacement préféré sur le serveur.
4. Définissez un nom d'utilisateur et un mot de passe pour l'agent (seuls des caractères anglais ASCII peuvent être utilisés) :
   - **Serveur Linux :** Exécutez `AgentCredentials.sh <username> <password>`

     Remarque : `AgentCredentials.sh` doit avoir des permissions d'exécution.

- **Serveur Windows :** Exécutez `AgentCredentials.bat <username> <password>`

5. Déployez l'application Web GBootStrap :
   a. Connectez-vous à la console Integrated Solutions de WebSphere. L'emplacement par défaut est `http://<server_name>:<port_number>/ibm/console/`

      Remarque : Si plusieurs profils sont définis, connectez-vous à la console du profil approprié.
   b. Sélectionnez **Nouvelles applications > Nouvelle application d'entreprise**.
   c. Dans la zone **Chemin de la nouvelle application**, ajoutez le chemin du fichier GBootStrap.war.
   d. Dans la zone **Racine de contexte**, entrez `GBootStrap`, puis cliquez sur **Suivant**.

      L'assistant Installation d'une nouvelle application s'ouvre.
   e. A moins que vous ne vouliez modifier les options par défaut, cliquez simplement sur le bouton **Suivant** jusqu'au bout de l'assistant. Si vous êtes invité à enregistrer la configuration, faites-le. Lorsque vous avez été jusqu'au bout de l'assistant, `GBootstrap.war` s'affiche dans la liste des applications. Une croix rouge ou une flèche verte dans la colonne Etat de l'application indique s'il est activé. S'il n'est *pas* activé (croix rouge), sélectionnez-le et cliquez sur **Démarrer**. Une flèche verte indique que GBootstrap.war est activé.
6. Maintenant, sélectionnez **Serveurs > Serveurs d'applications**.
7. Dans la sous-fenêtre de droite, cliquez sur le nom du serveur.
8. Cliquez sur l'onglet **Configuration** pour le positionner en avant-plan.
9. Sous Infrastructure du serveur, cliquez sur **Gestion des processus et Java > Définition des processus**.
10. Sous Propriétés supplémentaires, cliquez sur **Machine virtuelle Java**.
11. Ajoutez l'argument suivant aux arguments JVM génériques :

    `-javaagent:c:/path/to/gbAgent.jar` (l'exemple correspond à un système d'exploitation Windows ; pour d'autres systèmes, le chemin doit être modifié).

    Remarque : Le chemin ne doit pas contenir d'espace.

    Remarque : Si d'autres agents Java sont définis sur le serveur Web, vous pouvez *ajouter* un agent glass box dans la zone des arguments JVM génériques (le chemin exact dépend de votre installation) :

    `... -javaagent:c:\otherAgent\otherAgent.jar` **`-javaagent:c:\glassbox\gbAgent.jar ...`**
12. Cliquez sur **Appliquer**, et enregistrez la configuration si vous y êtes invité.
13. Redémarrez le serveur WebSphere.

Droits nécessaires pour fonctionner en mode sécurisé

La présente section décrit les droits spécifiques que vous devez ajouter si le serveur d'applications Web doit fonctionner en mode sécurisé lors de l'examen.

Si le serveur doit fonctionner en mode sécurisé (c'est le cas lorsque Java Security Manager est activé), vous devez ajouter les droits spécifiques ci-après à l'application Web GBootStrap :

- Droit d'accéder à "getClassLoader" (java.lang.RuntimePermission)
- Droit d'utiliser "accessClassInPackage.sun.net.www.protocol.*" (java.lang.RuntimePermission)
- Droit de lecture de la propriété "java.io.tmpdir" (java.util.PropertyPermission)
- Droit de lecture/écriture/suppression sur "<<ALL FILES>>" (tous les fichiers)

Si nécessaire, consultez le manuel de votre serveur Web pour savoir comment et où ajouter ces droits de sécurité Java. Les sections suivantes fournissent des sources et des exemples qui peuvent vous aider. Notez que ce ne sont que des exemples et que vous devrez probablement les adapter à vos besoins.

IBM WebSphere

Guide :

http://publib.boulder.ibm.com/infocenter/wasinfo/v7r0/topic/com.ibm.websphere.express.doc/info/exp/ae/tsec_waspolicyfile.html

Lignes à ajouter :

```
grant codeBase "file:${application}" {
 permission java.lang.RuntimePermission "getClassLoader";
 permission java.lang.RuntimePermission
"accessClassInPackage.sun.net.www.protocol.*";
 permission java.io.FilePermission "<>", "read, write, delete";
 permission java.util.PropertyPermission "java.io.tmpdir", "read";
};
```

Emplacement :

```
<profile_root>/config/cells/<cell_name>/applications/<ear_file_name>
/deployments/<application_name>/META-INF/was.policy
```

Exemples de lignes à ajouter :

```
"C:\Program Files (x86)\IBM\WebSphere\AppServer\profiles\AppSrv01
\config\cells\ROIS-PSNode01Cell\applications\GBootStrap_war.ear
\deployments\GBootStrap_war\META-INF\was.policy")
```

Apache Tomcat

Guide :

http://tomcat.apache.org/tomcat-6.0-doc/security-manager-howto.html#Configuring_Tomcat_With_A_SecurityManager

Lignes à ajouter :

```
grant codeBase "file:${catalina.base}/webapps/GBootStrap/-"{
 permission java.lang.RuntimePermission "getClassLoader";
 permission java.lang.RuntimePermission
"accessClassInPackage.sun.net.www.protocol.*";
 permission java.io.FilePermission "<<ALL FILES>>">>", "read, write, delete";
 permission java.util.PropertyPermission "java.io.tmpdir", "read";
};
```

Emplacement :

```
<CATALINA_HOME>/conf/catalina.policy
```

Exemples de lignes à ajouter :

```
"C:\Software\Tomcat\apache-tomcat-6.0.33\conf\catalina.policy"
```

Weblogic

Guide :

http://download.oracle.com/docs/cd/E13222_01/wls/docs81/security/server_prot.html

Reportez-vous à la section "Définition de règles de sécurité d'application".

Lignes à ajouter :

```
<security-permission>
 <description>
  Allow getting the J2EEJ2SETest4 property
 </description>
```

```
 <security-permission-spec>
  grant {
    permission java.util.PropertyPermission
"welcome.J2EEJ2SETest4","read";
  };
 </security-permission-spec>
</security-permission>
```

Ligne à ajouter :

```
weblogic.xml
```

JBoss

Guide :

http://docs.jboss.org/jbossweb/latest/security-manager-howto.html

Lignes à ajouter :

```
grant codeBase "file:${catalina.base}/webapps/GBootStrap/-"{
 permission java.lang.RuntimePermission "getClassLoader";
 permission java.lang.RuntimePermission
"accessClassInPackage.sun.net.www.protocol.*";
 permission java.io.FilePermission "ALL FILES", "read, write, delete";
 permission java.util.PropertyPermission "java.io.tmpdir", "read";
};
```

Ligne à ajouter :

```
CATALINA_HOME/conf/catalina.policy
```

Définition de l'agent glass box dans AppScan

Cette section décrit la façon de configurer AppScan pour accéder à l'agent glass box sur le serveur.

Pourquoi et quand exécuter cette tâche

Une fois l'agent glass box installé sur le serveur d'applications, vous devez le définir auprès d'AppScan pour que celui-ci puisse accéder à l'agent. Lorsque cela est fait, AppScan utilise automatiquement l'agent pour les examens de type glass box lorsque cela s'impose (à moins que vous ne l'ayez désélectionné dans la configuration des examens).

Restriction : Vous pouvez définir le même agent serveur sur plusieurs machines AppScan, mais un agent ne peut effectuer qu'un seul examen à la fois.

Restriction : Vous pouvez définir plusieurs agents, mais un seul agent peut être sélectionné dans une configuration d'examen.

Procédure

1. Dans **Configuration > onglet URL et serveurs**, définissez l'**URL de départ**. Notez que dans cet exemple, l'URL inclut le port 8080.

   ```
   https://altoro.testfire.net:8080/
   ```

2. Cliquez sur **OK** pour fermer la boîte de dialogue de configuration.
3. Cliquez sur **Outils > Gestion de l'agent Glass Box**.

   La boîte de dialogue Agents glass box s'affiche, contenant les agents déjà définis.

4. Pour ajouter un nouvel agent à la liste, cliquez sur  .

   La boîte de dialogue Définition des agents glass box s'affiche. L'URL de l'agent glass box est automatiquement remplie en fonction de l'URL de départ que vous avez entrée précédemment.

Important : L'URL de l'agent glass box contient automatiquement une valeur de port extraite de l'URL de départ (dans ce cas, 8080). Si vous avez installé votre agent sur un port différent, remplacez la valeur du port par la valeur correcte. Dans cet exemple, la valeur du port a été remplacée par 8888.

```
http://altoro.testfire.net:8888/GBootStrap/
```

5. Remplissez les zones et options suivantes en fonction des besoins.

Option	Description
Nom d'utilisateur et mot de passe	Saisissez le nom d'utilisateur et le mot de passe définis lorsque l'agent avait été installé sur le serveur.
Paramètres du journal d'agent	(Facultatif :) Cliquez pour ouvrir ces paramètres. **Remarque :** Les paramètres du journal d'agent sont enregistrés dans l'agent côté serveur.
Nombre max de lignes du journal :	(Facultatif :) Utilisez la règle pour limiter la taille du journal.
Contenu du journal	(Facultatif :) Sélectionnez le niveau d'information à inclure dans le journal : **Erreurs :** Inclure les messages d'erreur uniquement ; **Avertissements :** Inclure les messages d'erreur et d'avertissement ;**Informations :** Inclure les messages d'erreurs, d'avertissements et d'information ; **Débogage :** Inclure tous les messages. Les journaux glass box sont sauvegardés à l'emplacement suivant : `[Installation folder]\instrumentation.log`

AppScan tente de se connecter au serveur d'agent. Si la connexion aboutit, une icône verte "Connecté" apparaît. En cas de problème, une icône rouge apparaît avec un message du type "Impossible de se connecter à l'agent" ou "Données d'identification requises".

Remarque : Si votre site fournit à la fois HTTP et HTTPS, vérifiez si l'URL de départ est HTTPS (sinon, remplacez-la par HTTPS).

Remarque : Si un message d'erreur s'affiche, voir

http://www.ibm.com/support/docview.wss?uid=swg21567723

6. Cliquez sur **OK** pour fermer la boîte de dialogue de définition.
   L'agent est ajouté à la liste.
7. Cliquez sur **OK** pour fermer la liste.
   L'agent est maintenant défini sur cette machine.

Modification des données d'identification de l'utilisateur :

Cette section décrit la façon de modifier le nom d'utilisateur et le mot de passe utilisés pour accéder à l'agent glass box.

Pourquoi et quand exécuter cette tâche

Lorsque l'agent glass box est installé, vous êtes invité à définir un nom d'utilisateur et un mot de passe pour accéder à l'agent. Ces données d'identification permettent de garantir que l'agent n'est accessible qu'à AppScan. Si vous devez changer les données d'identification après l'installation, suivez les instructions ci-dessous.

Procédure

1. Sur le serveur d'applications, ouvrez une ligne de commande dans le répertoire d'installation.
2. Définissez les nouvelles données d'identification :
   - Pour un serveur Linux : Exécuter `AgentCredentials.sh <newusername> <newpassword>`
   - Pour un serveur Windows : Exécutez `AgentCredentials.bat <newusername> <newpassword>`
3. Annulez le déploiement de GBootStrap sur le serveur.
4. Déployez le nouveau fichier GBootStrap.war modifié depuis le dossier d'installation glass box sur le serveur.

Configuration d'un examen glass box

Bien que l'examen soit configuré automatiquement, cette section décrit les options que vous pouvez modifier si vous le souhaitez.

Procédure

1. Configurez l'examen de façon habituelle.
2. Dans **Configuration > onglet Glass Box**, sélectionnez l'un des agents glass box définis dans la liste déroulante et, éventuellement, ajustez les paramètres :

Paramètre	Détails
Utiliser cet agent glass box	Si l'agent glass box a été installé sur votre serveur d'applications, et s'il est défini dans AppScan, vous pouvez le sélectionner et l'utiliser dans l'examen. Si vous avez entré une URL de départ, AppScan tente de sélectionner l'agent adéquat automatiquement. Lorsqu'un agent est sélectionné, AppScan tente de s'y connecter, et indique s'il y a réussi. **Remarque :** Si vous sélectionnez un agent et que vous recevez le message "Données d'identification requises", vérifiez que les données d'identification fournies dans Outils > Gestion de Glass Box sont correctes. Si le serveur requis ne s'affiche pas dans la liste déroulante, vous pouvez le définir en cliquant sur le lien **Gestion de l'agent glass box**. **Restriction :** Un seul agent glass box peut être sélectionné pour être utilisé dans un examen. Si l'application à examiner utilise plusieurs serveurs, vous devez réaliser l'examen pour chaque serveur séparément à l'aide des agents respectifs.

Utiliser Glass Box dans l'étape d'exploration	(Sélectionné par défaut.)
	
	Cette fonction peut élargir la couverture du site en examinant le code source côté serveur pour rechercher les paramètres qui affectent le comportement du serveur, mais qui n'apparaissent pas dans la réponse.
	
	Exemple de code sur le serveur :
	`String debugOn = request.getParameter("debug");`
	`if (debugOn == "true"){`
	`response.getWriter().println(SECRET_SERVER_DATA);`
	`}`
	
	Dans cet exemple, le développeur a laissé le paramètre `"debug"` dans le code. Il n'apparaît dans aucun lien sur le site, mais si un cyber-attaquant envoyait une requête le contenant, il pourrait obtenir `SECRET_SERVER_DATA`.

Paramètre	Détails
Utiliser Glass Box dans l'étape de test	(Sélectionné par défaut.) Cochez cette case pour envoyer des tests glass box pendant l'étape de test de l'examen. Cette fonction peut vérifier la réussite ou l'échec de certains tests, par exemple les tests d'injection SQL en aveugle, avec plus de précision, et révéler l'existence de certains problèmes de sécurité qui ne sont pas détectables par les techniques de test de type boîte noire.
Ignorer les tests de boîte noire équivalents	(Désélectionné par défaut.) Cela signifie que les tests glass box et les tests de boîte noire de la même vulnérabilité (Classification des menaces par le consortium WASC) sont envoyés. En effet, même si les tests glass box sont généralement plus précis et fournissent des résultats plus détaillés, il arrive qu'un test glass box échoue et que le test de boîte noire équivalent aboutisse. Si les résultats pour votre application sont inchangés lorsque des tests de boîte noire sont ignorés, vous pouvez réduire le temps d'examen en cochant cette case.

La barre d'état indique que l'examen glass box est activé et que vous pouvez commencer l'examen.

Examen à l'aide de glass box

La présente section décrit l'examen glass box.

Pourquoi et quand exécuter cette tâche

Une fois que l'agent glass box a été défini dans AppScan, les examens glass box sont activés par défaut. Vous pouvez utiliser la boîte de dialogue Configuration des examens pour vérifier que le bon agent serveur a été sélectionné, et que l'examen glass box a été configuré pour s'exécuter dans le cadre de l'examen.

L'examen glass box peut découvrir des URL masquées à l'étape d'exploration, ainsi que des problèmes et des informations complémentaires au cours de l'étape de test.

Procédure

1. Cliquez sur la vue **Configuration > Glass box**.
2. Sélectionnez l'agent à utiliser dans la liste déroulante.

   Remarque : Si votre agent n'apparaît pas dans la liste, cliquez sur le lien **Gestion de l'agent glass box**, et définissez-le.
3. Vérifiez qu'au moins l'une des deux options d'examen glass box est sélectionnée :
   - Utiliser Glass Box dans l'étape d'exploration
   - Utiliser Glass Box dans l'étape de test

   Remarque : La case à cocher **Ignorer les tests de boîte noire équivalents** est désélectionnée par défaut. Cela signifie que les tests glass box et les tests de boîte noire de la même vulnérabilité (Classification des menaces par le consortium WASC) sont envoyés. En effet, même si les tests glass box sont généralement plus précis et fournissent des résultats plus détaillés, il arrive qu'un test glass box échoue et que le test de boîte noire équivalent aboutisse. Si les résultats pour votre application sont inchangés lorsque des tests de boîte noire sont ignorés, vous pouvez réduire le temps d'examen en cochant cette case.
4. Cliquez sur **Examiner > Examen intégral** pour démarrer l'examen.

   L'examen démarre et les messages de la barre d'état indiquent que l'examen glass box est actif.

   Les résultats de l'examen incluront des données glass box dans l'onglet Informations sur les problèmes, le cas échéant.

Désinstallation de l'agent glass box

Cette section explique comment désinstaller l'agent glass box sur le serveur.

Désinstallation automatique :

Cette section explique comment désinstaller l'agent glass box automatiquement via l'interface utilisateur.

Pourquoi et quand exécuter cette tâche

L'agent glass box peut être désinstallé automatiquement *uniquement* s'il a été installé automatiquement à l'aide du programme d'installation de l'agent glass box. S'il a été installé manuellement, il doit aussi être désinstallé manuellement, en suivant les instructions dans les sections suivantes de ce guide.

Pour effectuer cette tâche, vous devez accéder à votre serveur d'applications.

Procédure

1. Ouvrez le répertoire glass box sur votre serveur.
2. Lancez le programme de désinstallation :
   - **Serveur Linux :** Double cliquez sur `Uninstall.bin`
   - **Serveur Windows :** Double cliquez sur `Uninstall.exe`
3. Suivez les instructions en ligne pour désinstaller complètement l'agent glass box.

Désinstallation manuelle sur un serveur JBoss :

Cette section décrit comment désinstaller manuellement l'agent glass box sur un serveur JBoss.

Pourquoi et quand exécuter cette tâche

Lorsque la glass box est installée sur le serveur d'applications, l'installation comprend un agent Java et une application Web GBootStrap. Pour désinstaller la glass box, vous devez supprimer les deux. Pour effectuer cette tâche, vous devez accéder à votre serveur d'applications.

Procédure

1. Annulez le déploiement de l'application Web GBootStrap :
   a. Connectez-vous à la console d'administration JBoss. L'emplacement par défaut est `http://<server_name>:<port_number>/admin-console/`
   b. Cliquez sur **Applications > Fichiers WAR de l'application Web**, puis dans l'entrée GBootStrap.war, cliquez sur **Supprimer**.
   c. Lorsque le programme vous demande de confirmer, cliquez sur **OK**.
2. Fermez le serveur JBoss.
3. Supprimez l'agent Java de JAVA_OPTS. Pendant l'installation manuelle, JAVA_OPTS est modifié afin d'inclure gbAgent.jar. Consultez les instructions d'installation pour savoir comment supprimer gbAgent.jar de JAVA_OPTS, et restaurer JAVA_OPTS à son état d'origine.

4. Supprimez le répertoire glass box du serveur JBoss, sauf s'il doit être encore utilisé par d'autres serveurs d'application Web.
5. Redémarrez le serveur JBoss.

Désinstallation manuelle sur un serveur JBoss Service :

Cette section décrit comment désinstaller manuellement l'agent glass box sur un serveur JBoss Service.

Pourquoi et quand exécuter cette tâche

Lorsque la glass box est installée sur le serveur d'applications, l'installation comprend un agent Java et une application Web GBootStrap. Pour désinstaller la glass box, vous devez supprimer les deux. Pour effectuer cette tâche, vous devez accéder à votre serveur d'applications.

Procédure

1. Annulez le déploiement de l'application Web GBootStrap :
   a. Connectez-vous à la console d'administration JBoss. L'emplacement par défaut est `http://<server_name>:<port_number>/admin-console/`
   b. Cliquez sur **Applications > Fichiers WAR de l'application Web**, puis dans l'entrée GBootStrap.war, cliquez sur **Supprimer**.
   c. Lorsque le programme vous demande de confirmer, cliquez sur **OK**.
2. Arrêtez le service JBoss.
3. Supprimez l'agent Java de JAVA_OPTS. Pendant l'installation manuelle, JAVA_OPTS est modifié afin d'inclure gbAgent.jar. Consultez les instructions d'installation pour savoir comment supprimer gbAgent.jar de JAVA_OPTS, et restaurer JAVA_OPTS à son état d'origine.
4. Supprimez le répertoire glass box du serveur JBoss, sauf s'il doit être encore utilisé par d'autres serveurs d'application Web.
5. Redémarrez le service.

Désinstallation manuelle sur un serveur Tomcat :

Cette section décrit comment désinstaller manuellement l'agent glass box sur un serveur Tomcat.

Pourquoi et quand exécuter cette tâche

Lorsque la glass box est installée sur le serveur d'applications, l'installation comprend un agent Java et une application Web GBootStrap. Pour désinstaller la glass box, vous devez supprimer les deux. Pour effectuer cette tâche, vous devez accéder à votre serveur d'applications.

Procédure

1. Annulez le déploiement de l'application Web GBootStrap :
   a. Connectez-vous à Tomcat Manager. L'emplacement par défaut est `http://<server_name>:<port_number>/manager/html`
   b. Dans la liste des applications, sélectionnez **GBootStrap.war**, puis cliquez sur **Commands > Undeploy**.
   c. Lorsque le programme vous demande de confirmer, cliquez sur **OK**.
2. Arrêtez le serveur Tomcat.
3. Supprimez l'agent Java de CATALINA_OPTS. Pendant l'installation manuelle, CATALINA_OPTS est modifié afin d'inclure gbAgent.jar. Consultez les instructions d'installation pour savoir comment supprimer gbAgent.jar de CATALINA_OPTS, et restaurer CATALINA_OPTS, à son état d'origine.
4. Supprimez le répertoire glass box sur le serveur Tomcat, sauf s'il doit être encore utilisé par d'autres serveurs d'application Web.

5. Redémarrez le serveur Tomcat.

Désinstallation manuelle sur un serveur Tomcat Service :

Cette section décrit comment désinstaller manuellement l'agent glass box sur un serveur Tomcat Service.

Pourquoi et quand exécuter cette tâche

Lorsque la glass box est installée sur le serveur d'applications, l'installation comprend un agent Java et une application Web GBootStrap. Pour désinstaller la glass box, vous devez supprimer les deux. Pour effectuer cette tâche, vous devez accéder à votre serveur d'applications.

Procédure

1. Annulez le déploiement de l'application Web GBootStrap :
   a. Connectez-vous à Tomcat Manager. L'emplacement par défaut est `http://<server_name>:<port_number>/manager/html`
   b. Dans la liste des applications, sélectionnez **GBootStrap.war**, puis cliquez sur **Commands > Undeploy**.
   c. Lorsque le programme vous demande de confirmer, cliquez sur **OK**.
2. Arrêtez Tomcat Service.
3. Supprimez l'agent Java des arguments JVM :
   a. Localisez Tomcat JVM dans `...\Tomcat 7.0\bin\tomcat7w.exe`
   b. Cliquez deux fois dessus et sélectionnez l'onglet **Properties > Java**.
   c. Dans la zone Java Options, supprimez la ligne suivante (si elle existe) : `-javaagent:c:/path/to/gbAgent.jar`
   d. Cliquez sur **OK**.
4. Redémarrez Tomcat Service.

Désinstallation manuelle sur un serveur WebLogic :

Cette section décrit comment désinstaller manuellement l'agent glass box sur un serveur WebLogic.

Pourquoi et quand exécuter cette tâche

Lorsque la glass box est installée sur le serveur d'applications, l'installation comprend un agent Java et une application Web GBootStrap. Pour désinstaller la glass box, vous devez supprimer les deux. Pour effectuer cette tâche, vous devez accéder à votre serveur d'applications.

Procédure

1. Annulez le déploiement de l'application Web GBootStrap :
   a. Connectez-vous à la console d'administration WebLogic. L'emplacement par défaut est `http://<server_name>:<port_number>/console/`
   b. Dans la sous-fenêtre Domain Structure, cliquez sur **Deployments**, puis cochez la case **GBootStrap** et cliquez sur **Delete**.
   c. Dans la sous-fenêtre Domain Structure, cliquez sur **Deployments** et vérifiez que GBootStrap a été supprimé.
2. Arrêtez le serveur WebLogic.
3. Supprimez l'agent Java de JAVA_OPTIONS : Pendant l'installation manuelle, JAVA_OPTIONS est modifié afin d'inclure gbAgent.jar. Consultez les instructions d'installation pour savoir comment supprimer gbAgent.jar de JAVA_OPTIONS, et restaurer JAVA_OPTIONS à son état original.
4. Supprimez le répertoire glass box sur le serveur WebLogic, sauf s'il doit être encore utilisé par d'autres serveurs d'application Web.

5. Redémarrez le serveur WebLogic.

Désinstallation manuelle sur un serveur WebLogic Service :

Cette section décrit comment désinstaller manuellement l'agent glass box sur un serveur WebLogic Service.

Pourquoi et quand exécuter cette tâche

Lorsque la glass box est installée sur le serveur d'applications, l'installation comprend un agent Java et une application Web GBootStrap. Pour désinstaller la glass box, vous devez supprimer les deux. Pour effectuer cette tâche, vous devez accéder à votre serveur d'applications.

Procédure

1. Annulez le déploiement de l'application Web GBootStrap :
   a. Connectez-vous à la console d'administration WebLogic. L'emplacement par défaut est `http://<server_name>:<port_number>/console/`
   b. Dans la sous-fenêtre Domain Structure, cliquez sur **Deployments**, puis cochez la case **GBootStrap** et cliquez sur **Delete**.
   c. Dans la sous-fenêtre Domain Structure, cliquez sur **Deployments** et vérifiez que GBootStrap a été supprimé.
2. Arrêtez WebLogic Service.
3. Supprimez l'agent Java de JAVA_OPTIONS : Pendant l'installation manuelle, JAVA_OPTIONS est modifié afin d'inclure gbAgent.jar. Consultez les instructions d'installation pour savoir comment supprimer gbAgent.jar de JAVA_OPTIONS, et restaurer JAVA_OPTIONS à son état original.
4. Redémarrez le service.

Désinstallation manuelle sur un serveur WebSphere :

Cette section décrit comment désinstaller manuellement l'agent glass box sur un serveur WebSphere Service.

Pourquoi et quand exécuter cette tâche

Lorsque la glass box est installée sur le serveur d'applications, l'installation comprend un agent Java et une application Web GBootStrap. Pour désinstaller la glass box, vous devez supprimer les deux. Pour effectuer cette tâche, vous devez accéder à votre serveur d'applications.

Procédure

1. Annulez le déploiement de l'application Web GBootStrap :
   a. Connectez-vous à la console d'administration Integrated Solutions de WebSphere. L'emplacement par défaut est `http://<server_name>:9043/console/`

      Remarque : Si plusieurs profils sont définis, connectez-vous à la console du profil approprié.
   b. Sélectionnez **Applications > Application Types > WebSphere Enterprise Application**.
   c. Dans la zone Enterprise Applications, cochez la case **GBootStrap** puis cliquez sur **Uninstall**.
   d. Suivez les instructions de l'assistant pour supprimer l'application GBootStrap.
      GBootStrap est supprimé de la liste des applications.
   e. Sélectionnez **Serveurs > Serveurs d'applications**.
   f. Dans la sous-fenêtre de droite, cliquez sur le nom du serveur.
   g. Cliquez sur l'onglet **Configuration** pour le positionner en avant-plan.

h. Dans Infrastructure du serveur, cliquez sur **Gestion des processus et Java > Définition des processus**.
i. Dans Propriétés supplémentaires, cliquez sur **Machine virtuelle Java**.

2. Dans les arguments JVM génériques, supprimez l'agent glass box en effaçant `-javaagent:c:/path/to/gbAgent.jar`

   Remarque : Cet exemple concerne les systèmes d'exploitation Windows. Pour les autres systèmes d'exploitation, modifiez le chemin.
3. Cliquez sur **Appliquer**, et enregistrez la configuration si vous y êtes invité.
4. Redémarrez WebSphere.

Pour plateformes .NET

Installation et utilisation de l'agent glass box sur un serveur .NET.

Installation de l'agent glass box

La présente section décrit l'installation de l'agent glass box sur un serveur .NET.

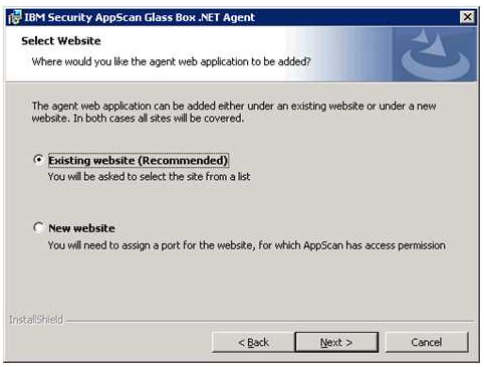
Avant de commencer

L'agent glass box d'AppScan doit être installé sur un ou plusieurs serveurs d'applications, en copiant certains fichiers du répertoire d'installation d'AppScan sur le serveur. Pour effectuer cette tâche, vous devez accéder à votre serveur d'applications. Les technologies et systèmes suivants sont pris en charge :

Elément	Détails
Système d'exploitation	Systèmes d'exploitation pris en charge (versions 32–bits et 64–bits) : • Microsoft Windows Server 2012 • Microsoft Windows Server 2012 R2 • Microsoft Windows Server 2008 R2
Autre	Microsoft IIS 7.0 ou ultérieure Microsoft .NET Framework 4.0 ou 4.5 doit être installé, et IIS doit être configuré au niveau racine pour pouvoir fonctionner avec cette version d'ASP.net.

Procédure

1. Ouvrez `...\Program Files\IBM\AppScan Standard\Glass box`
   Le chemin absolu dépend de l'emplacement dans lequel vous avez installé AppScan.
2. Localisez le fichier `GB_DotNET_Setup.exe` et copiez-le sur votre serveur Web.
3. Cliquez deux fois dessus pour lancer l'assistant.
4. Suivez les étapes de l'assistant.



5. Lorsque vous devez choisir d'effectuer l'installation sur un nouveau site Web ou sur un site Web existant, sélectionnez l'option recommandée (sauf si vous êtes sûr que l'autre option est plus adaptée).

   Remarque : La recommandation d'une option par rapport à une autre dépend du système. Lorsque cela est possible, il est recommandé d'utiliser un "site Web existant", mais dans certains cas, l'utilisation d'un "nouveau site Web" est conseillée. En général un "site Web existant" est préférable, car il ne nécessite pas de nouveau port, lequel devrait être configuré dans AppScan et exigerait une configuration de pare-feu supplémentaire pour être accessible à AppScan.
6. Cette étape dépend du choix que vous avez fait à l'étape précédente :
   a. **Site existant :** Si vous choisissez "Site existant", vous devez maintenant sélectionner un site dans une liste de sites existants.

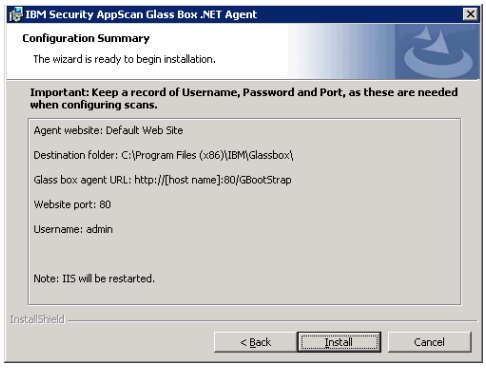
      Remarque : En présence de plusieurs sites, l'assistant liste ces derniers par ordre de préférence. Si l'assistant identifie certains sites comme potentiellement problématiques, ces derniers seront affichés dans le bas de la liste et porteront le libellé "non recommandé". Toutefois, l'ordre, et même le libellé "non recommandé" ne sont que des suggestions et, dans certains cas, vous pouvez décider de sélectionner un site intitulé "non recommandé".

      Conseil : Quelle que soit votre sélection, tous les sites pourront être surveillés mais, lorsque cela est possible, essayez de sélectionner le site que vous envisagez de configurer comme URL de départ de votre *premier* examen.
   b. **Nouveau site :** Si vous choisissez "Nouveau site", vous devez maintenant affecter un port. Vous devez définir un port qui permettra d'accéder à AppScan lors d'un examen à partir d'une machine distante.

      Important : Vous devrez fournir le numéro de port lors de la configuration d'AppScan.

      Remarque : Vous pouvez utiliser le bouton **Test** pour vérifier que le port sélectionné est actuellement disponible. Toutefois, cette action est effectuée automatiquement lorsque vous cliquez sur **Suivant**.
7. Définissez le nom d'utilisateur de l'agent et le mot de passe pour l'agent d'application Web glass box.

   Important : Vous devrez fournir ces données d'identification lors de la configuration d'un examen avec glass box.
8. L'écran récapitulatif apparaît avant l'installation réelle.



   Important : Avant de cliquer sur **Installer**, assurez-vous d'avoir noté le nom d'utilisateur, le mot de passe et le port car vous en aurez besoin pour configurer AppScan.
9. Cliquez sur **Installer**.

   Remarque : L'installation comprend le redémarrage d'IIS.
   Lorsque le processus est terminé, un message final vous indique s'il a abouti ou échoué.

Remarque : Si l'installation échoue pour une raison quelconque, la boîte de dialogue finale fournit un lien vers le journal d'installation qui pourra être utilisé en cas de dépannage. Il peut être intéressant de tenter une installation sur un site nouveau ou différent sur le serveur, voire sur un site "non recommandé". Dans tous les cas, vous devez effectuer la désinstallation avant de tenter l'installation à nouveau. Les deux journaux d'installation se trouvent dans le dossier %temp%. Les noms des deux journaux d'installation sont les suivants :

```
glassbox_setup_api.txt
glassbox_setup_msi.txt
```

Notez que le processus de désinstallation comporte le redémarrage de votre IIS.

Remarque : Les journaux glass box sont sauvegardés à l'emplacement suivant :

```
C:\Program Files (x86)\IBM\Glassbox\GBootStrap\GlassBoxLog.log
```

Définition de l'agent glass box dans AppScan

Cette section décrit la façon de configurer AppScan pour accéder à l'agent glass box sur le serveur.

Pourquoi et quand exécuter cette tâche

Une fois l'agent glass box installé sur le serveur d'applications, vous devez le définir auprès d'AppScan pour que celui-ci puisse accéder à l'agent. Lorsque cela est fait, AppScan utilise automatiquement l'agent pour les examens de type glass box lorsque cela s'impose (à moins que vous ne l'ayez désélectionné dans la configuration des examens).

Restriction : Vous pouvez définir le même agent serveur sur plusieurs machines AppScan, mais un agent ne peut effectuer qu'un seul examen à la fois.

Restriction : Vous pouvez définir plusieurs agents, mais un seul agent peut être sélectionné dans une configuration d'examen.

Procédure

1. Dans **Configuration > onglet URL et serveurs**, définissez l'**URL de départ**. Notez que dans cet exemple, l'URL inclut le port 8080.

   ```
   https://altoro.testfire.net:8080/
   ```

2. Cliquez sur **OK** pour fermer la boîte de dialogue de configuration.
3. Cliquez sur **Outils > Gestion de l'agent Glass Box**.

   La boîte de dialogue Agents glass box s'affiche, contenant les agents déjà définis.

4. Pour ajouter un nouvel agent à la liste, cliquez sur  .

   La boîte de dialogue Définition des agents glass box s'affiche. L'URL de l'agent glass box est automatiquement remplie en fonction de l'URL de départ que vous avez entrée précédemment.

   Important : L'URL de l'agent glass box contient automatiquement une valeur de port extraite de l'URL de départ (dans ce cas, 8080). Si vous avez installé votre agent sur un port différent, remplacez la valeur du port par la valeur correcte. Dans cet exemple, la valeur du port a été remplacée par 8888.

   ```
   http://altoro.testfire.net:8888/GBootStrap/
   ```

5. Remplissez les zones et options suivantes en fonction des besoins.

Option	Description
Nom d'utilisateur et mot de passe	Saisissez le nom d'utilisateur et le mot de passe définis lorsque l'agent avait été installé sur le serveur.
Paramètres du journal d'agent	(Facultatif :) Cliquez pour ouvrir ces paramètres. **Remarque :** Les paramètres du journal d'agent sont enregistrés dans l'agent côté serveur.

Option	Description
Nombre max de lignes du journal :	(Facultatif :) Utilisez la règle pour limiter la taille du journal.
Contenu du journal	(Facultatif :) Sélectionnez le niveau d'information à inclure dans le journal : **Erreurs :** Inclure les messages d'erreur uniquement ; **Avertissements :** Inclure les messages d'erreur et d'avertissement ;**Informations :** Inclure les messages d'erreurs, d'avertissements et d'information ; **Débogage :** Inclure tous les messages. Les journaux glass box sont sauvegardés à l'emplacement suivant : `[Installation folder]\instrumentation.log`

AppScan tente de se connecter au serveur d'agent. Si la connexion aboutit, une icône verte "Connecté" apparaît. En cas de problème, une icône rouge apparaît avec un message du type "Impossible de se connecter à l'agent" ou "Données d'identification requises".

Remarque : Si votre site fournit à la fois HTTP et HTTPS, vérifiez si l'URL de départ est HTTPS (sinon, remplacez-la par HTTPS).

Remarque : Si un message d'erreur s'affiche, voir

http://www.ibm.com/support/docview.wss?uid=swg21567723

6. Cliquez sur **OK** pour fermer la boîte de dialogue de définition.
   L'agent est ajouté à la liste.
7. Cliquez sur **OK** pour fermer la liste.
   L'agent est maintenant défini sur cette machine.

Configuration d'un examen glass box

Bien que l'examen soit configuré automatiquement, cette section décrit les options que vous pouvez modifier si vous le souhaitez.

Procédure

1. Configurez l'examen de façon habituelle.
2. Dans **Configuration > onglet Glass Box**, sélectionnez l'un des agents glass box définis dans la liste déroulante et, éventuellement, ajustez les paramètres :

Paramètre	Détails
Utiliser cet agent glass box	Si l'agent glass box a été installé sur votre serveur d'applications, et s'il est défini dans AppScan, vous pouvez le sélectionner et l'utiliser dans l'examen. Si vous avez entré une URL de départ, AppScan tente de sélectionner l'agent adéquat automatiquement. Lorsqu'un agent est sélectionné, AppScan tente de s'y connecter, et indique s'il y a réussi. **Remarque :** Si vous sélectionnez un agent et que vous recevez le message "Données d'identification requises", vérifiez que les données d'identification fournies dans Outils > Gestion de Glass Box sont correctes. Si le serveur requis ne s'affiche pas dans la liste déroulante, vous pouvez le définir en cliquant sur le lien **Gestion de l'agent glass box**. **Restriction :** Un seul agent glass box peut être sélectionné pour être utilisé dans un examen. Si l'application à examiner utilise plusieurs serveurs, vous devez réaliser l'examen pour chaque serveur séparément à l'aide des agents respectifs.

Utiliser Glass Box dans l'étape d'exploration	(Sélectionné par défaut.)
	
	Cette fonction peut élargir la couverture du site en examinant le code source côté serveur pour rechercher les paramètres qui affectent le comportement du serveur, mais qui n'apparaissent pas dans la réponse.
	
	Exemple de code sur le serveur :
	`String debugOn = request.getParameter("debug");`
	`if (debugOn == "true"){`
	`response.getWriter().println(SECRET_SERVER_DATA);`
	`}`
	
	Dans cet exemple, le développeur a laissé le paramètre `"debug"` dans le code. Il n'apparaît dans aucun lien sur le site, mais si un cyber-attaquant envoyait une requête le contenant, il pourrait obtenir `SECRET_SERVER_DATA`.

Utiliser Glass Box dans l'étape de test	(Sélectionné par défaut.) Cochez cette case pour envoyer des tests glass box pendant l'étape de test de l'examen. Cette fonction peut vérifier la réussite ou l'échec de certains tests, par exemple les tests d'injection SQL en aveugle, avec plus de précision, et révéler l'existence de certains problèmes de sécurité qui ne sont pas détectables par les techniques de test de type boîte noire.
Ignorer les tests de boîte noire équivalents	(Désélectionné par défaut.) Cela signifie que les tests glass box et les tests de boîte noire de la même vulnérabilité (Classification des menaces par le consortium WASC) sont envoyés. En effet, même si les tests glass box sont généralement plus précis et fournissent des résultats plus détaillés, il arrive qu'un test glass box échoue et que le test de boîte noire équivalent aboutisse. Si les résultats pour votre application sont inchangés lorsque des tests de boîte noire sont ignorés, vous pouvez réduire le temps d'examen en cochant cette case.

La barre d'état indique que l'examen glass box est activé et que vous pouvez commencer l'examen.

Examen à l'aide de glass box

La présente section décrit l'examen glass box.

Pourquoi et quand exécuter cette tâche

Une fois que l'agent glass box a été défini dans AppScan, les examens glass box sont activés par défaut. Vous pouvez utiliser la boîte de dialogue Configuration des examens pour vérifier que le bon agent serveur a été sélectionné, et que l'examen glass box a été configuré pour s'exécuter dans le cadre de l'examen.

L'examen glass box peut découvrir des URL masquées à l'étape d'exploration, ainsi que des problèmes et des informations complémentaires au cours de l'étape de test.

Procédure

1. Cliquez sur la vue **Configuration > Glass box**.
2. Sélectionnez l'agent à utiliser dans la liste déroulante.

   Remarque : Si votre agent n'apparaît pas dans la liste, cliquez sur le lien **Gestion de l'agent glass box**, et définissez-le.
3. Vérifiez qu'au moins l'une des deux options d'examen glass box est sélectionnée :
   - Utiliser Glass Box dans l'étape d'exploration
   - Utiliser Glass Box dans l'étape de test

   Remarque : La case à cocher **Ignorer les tests de boîte noire équivalents** est désélectionnée par défaut. Cela signifie que les tests glass box et les tests de boîte noire de la même vulnérabilité (Classification des menaces par le consortium WASC) sont envoyés. En effet, même si les tests glass box sont généralement plus précis et fournissent des résultats plus détaillés, il arrive qu'un test glass box échoue et que le test de boîte noire équivalent aboutisse. Si les résultats pour votre application sont inchangés lorsque des tests de boîte noire sont ignorés, vous pouvez réduire le temps d'examen en cochant cette case.
4. Cliquez sur **Examiner > Examen intégral** pour démarrer l'examen.

   L'examen démarre et les messages de la barre d'état indiquent que l'examen glass box est actif.

   Les résultats de l'examen incluront des données glass box dans l'onglet Informations sur les problèmes, le cas échéant.

Désinstallation de l'agent glass box

La présente section décrit la désinstallation de l'agent glass box d'un serveur .NET.

Pourquoi et quand exécuter cette tâche

Pour effectuer cette tâche, vous devez accéder à votre serveur d'applications.

Procédure

Procédez de l'une des façons suivantes :

- Utilisez la fonction Ajout/Suppression de programmes de Microsoft Windows.
- Exécutez GB_.NET_Setup.exe une nouvelle fois et sélectionnez l'option Désinstallation dans l'assistant.

Examens partiels

Plusieurs options du menu Examen vous permettent d'effectuer une partie de l'examen ou d'examiner une partie de votre site.

Tâche	Description
Exploration uniquement	Vous pouvez laisser AppScan explorer votre site et créer le modèle de site, mais sans procéder à l'étape de test de l'examen. De cette manière, vous pouvez examiner le modèle de site et les données d'application regroupés pour vérifier qu'ils répondent à vos exigences, et effectuer une exploration manuelle, si nécessaire, avant de procéder à un examen intégral.

Tâche	Description
Test uniquement	Si vous avez précédemment exécuté la tâche Exploration uniquement ou si vous avez arrêté un examen complet avant son achèvement, vous pouvez laisser AppScan tester votre site à l'aide des résultats d'exploration existants. Cela peut réduire la durée de l'examen si, par exemple, la structure du site n'a pas changé, mais que vous souhaitez voir les effets des modifications de sécurité qui lui ont été apportées. **Remarque :** Dans un examen intégral, il y a souvent des parties du site qui sont révélées au cours de l'étape de test. Lorsque cela se produit, AppScan exécute une phase supplémentaire d'étapes de test et d'exploration. Il peut exister plusieurs de ces phases dans un examen. Si vous utilisez les fonctions Exploration uniquement et Test uniquement, le résultat sera un examen à une seule phase, qui peut ne pas inclure toutes les parties du site.
Nouvel examen (intégral)	Supprime les résultats d'examen actuels et exécute un examen intégral à l'aide de la configuration en cours.
Nouvelle exploration	Supprime les résultats d'examen actuels et exécute une étape d'exploration uniquement à l'aide de la configuration en cours.
Nouveau test	Supprime les résultats de test actuels et exécute une nouvelle étape de test à l'aide de la configuration en cours et des résultats de l'exploration. **Limitation :** Si la réponse obtenue lors du nouveau test est identique à la réponse d'origine, le résultat n'est pas mis à jour et il indique l'horodatage de la réponse d'origine.

Examiner uniquement les opérations en plusieurs étapes

Vous pouvez définir une opération en plusieurs étapes et l'utiliser pour tester une partie seulement du site.

Pourquoi et quand exécuter cette tâche

Une opération en plusieurs étapes est une séquence de demandes qui doivent être envoyées dans un ordre précis pour atteindre certaines parties de l'application. (Pour plus de détails, voir «Vue Opérations en plusieurs étapes», à la page 95.) Dans certains cas, ces opérations peuvent ne représenter que la seule partie de l'application que vous souhaitez examiner.

Procédure

1. Configurez l'examen, avec au moins une opération en plusieurs étapes. (Voir «Vue Opérations en plusieurs étapes», à la page 95.)
2. (Recommandé :) Exécutez Scan Expert pour évaluer la configuration. (Voir «Scan Expert», à la page 164.)
3. Dans le menu Examen cliquez sur **N'examiner que les opérations en plusieurs étapes**.

   AppScan examine les opérations configurées et affiche les résultats.

   Remarque : Notez que seuls les tests directement associés à la séquence sont envoyés. (Les tests d'infrastructure du site, par exemple, ne sont pas envoyés.) Cela signifie que lorsque l'examen est passé, la barre d'état (partie inférieure gauche) peut indiquer que d'autres tests sont à envoyer. Si vous utilisez la fonction d'examen des opérations en plusieurs étapes uniquement pour exécuter un examen *complet* sur une *partie* du site, vous devez poursuivre avec l'étape Test uniquement (étape suivante) pour envoyer ces tests.
4. (Facultatif) Cliquez sur **Examen > Test uniquement** pour effectuer un examen complet de la partie du site testée.

   L'infrastructure et d'autres tests restants sont envoyés au site, et les résultats sont ajoutés aux résultats de l'examen.

Modification de la configuration pendant un examen

Si vous lancez un examen, puis modifiez la configuration, vous devrez le relancer, ou au moins relancer l'étape de test, pour voir l'effet des modifications. En règle générale :

- Si vous avez modifié les configurations d'exploration, vous devez relancer l'examen intégral de l'application en exécutant les étapes d'exploration et de test (**Examen > Nouvel examen > Nouvel examen (intégral)**).
- Si vous avez modifié les configurations de test, vous ne devez pas réexécuter l'étape d'exploration (si elle est terminée), il suffit d'effectuer un nouveau test de l'application (**Examen > Nouvel examen > Nouveau test**).

Exporter les résultats de l'examen

Lorsqu'un examen est terminé, les résultats s'affichent dans la fenêtre principale. Les différentes vues (Problèmes, Résolutions, Données d'application) offrent les résultats de l'examen filtrés par utilisation.

Vous pouvez exporter les résultats de l'examen à partir d'AppScan de différentes manières :

- Configurez et générez un rapport AppScan, exportez-le au format PDF ou dans tout autre format lisible. Voir Chapitre 10, «Rapports», à la page 233.
- Sélectionnez les variantes de test à partir de la vue Problèmes et autorisez AppScan à joindre un fichier .zip des informations de la variante à un nouveau message électronique. Voir Chapitre 8, «Résultats : Problèmes de sécurité», à la page 207.
- Générez une base de données ou un fichier XML à partir des résultats complets de l'examen. Voir «Générer des fichiers XML et des bases de données de résultats d'examen» ci-dessous.

Générer des fichiers XML et des bases de données de résultats d'examen

Avant de commencer

Vous pouvez exporter tous les résultats de l'examen sous la forme d'un fichier XML ou sous la forme d'une base de données relationnelle. (L'option de la base de données exporte les résultats dans une structure de base de données Firebird. Il s'agit d'une source ouverte, et suit les normes ODBC et JDBC.)

Le schéma d'une sortie XML est appelé **ScanExport.xsd** et se trouve dans le dossier AppScan **\Docs**, par exemple :

```
[AppScan Standard installation folder]\Docs\ScanExport.xsd
```

Procédure

1. Cliquez sur **Fichier > Exporter** et sélectionnez **XML** ou **DB**.
2. Naviguez jusqu'à l'emplacement de votre choix, et entrez un nom pour le fichier.
3. Cliquez sur **Sauvegarder**.

Que faire ensuite

«Accès aux informations contenues dans un fichier base de données exporté»

Accès aux informations contenues dans un fichier base de données exporté

Procédure

1. Téléchargez le moteur de base de données Firebird : http://firebird.sourceforge.net/index.php?op=files&id=engine
2. Téléchargez un pilote Firebird (choisissez-en un) :
   - **Pilote Firebird ODBC :** http://firebird.sourceforge.net/index.php?op=files&id=odbc

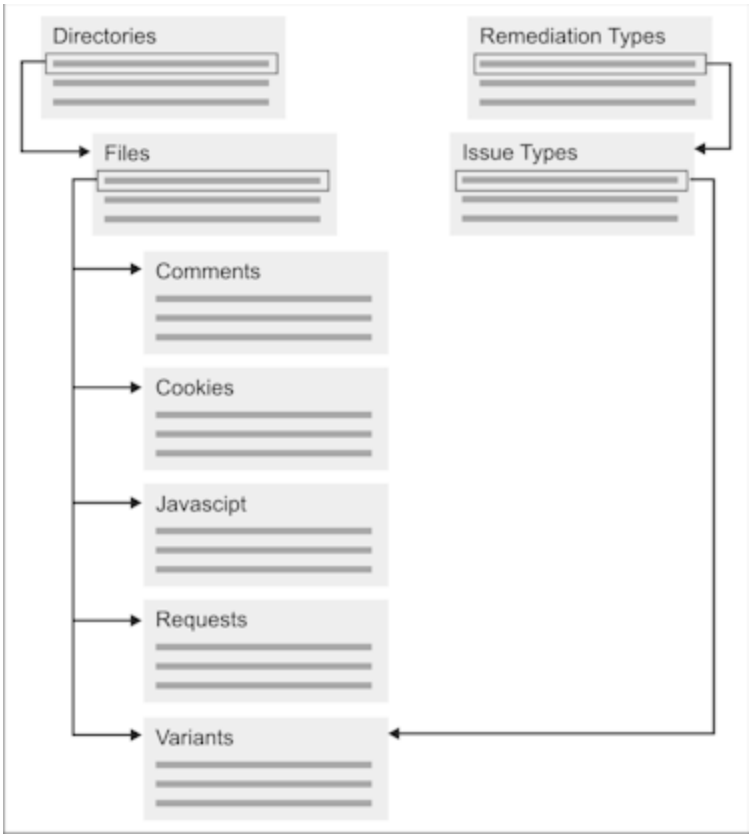
- **Pilote Firebird JDBC :** http://firebird.sourceforge.net/index.php?op=files&id=jaybird

3. Ouvrez Firebird avec le nom d'utilisateur `SYSDBA` et le mot de passe `masterkey`, à l'aide de n'importe quel client ODBC ou JDBC conforme.

Structure de base de données Firebird

Lorsque des résultats d'examen sont exportés dans une structure de base de données Firebird, ils peuvent être visualisés à l'aide de l'un des nombreux afficheurs ODBC et JDBC. La structure des composants de base de données appropriés est illustrée dans la figure ci-dessous et décrite dans les sous-sections suivantes.

Remarque : Certaines zones de la base de données sont des zones AppScan internes qui ne sont pas utiles à l'utilisateur. Ces zones sont marquées "AppScan Internal" dans les tableaux suivants.



Annuaire

La section Répertoire de la base de données contient une ligne pour chaque répertoire ou sous-répertoire de l'examen.

Nom de zone	Explication/Commentaires
ID	ID AppScan pour le répertoire
PRENOM	Nom du répertoire
PARENTID	Répertoire dans lequel ce répertoire est contenu (s'il s'agit d'un sous-répertoire)
PATH	Chemin du répertoire
DIRTYPE	Type de répertoire : Hôte/Application

Fichiers

La section Fichiers de la base de données contient une ligne pour chaque fichier.

Nom de zone	Explication/Commentaires
ID	ID AppScan pour le fichier
FILENAME	Nom du fichier
PARENTID	ID du répertoire contenant ce fichier

Commentaires

La section Commentaires contient une ligne pour chaque commentaire HTML trouvé dans la page du site.

Nom de zone	Explication/Commentaires
ENGINEID	ID AppScan pour le commentaire
FILEID	ID du fichier dans lequel le commentaire a été trouvé
SHORTTEXT	Texte du commentaire (peut être tronqué)

Cookies

La section Cookies contient une ligne pour chaque cookie trouvé.

Nom de zone	Explication/Commentaire
ID	ID AppScan pour le cookie
REQCOOKIEID	AppScan Interne
RESPCOOKIEID	AppScan Interne
PRENOM	Nom du fichier du cookie
COOKIEVALUE	Valeur du cookie
SETINURL	URL source du cookie
FILEID	ID AppScan du fichier où est sauvegardé le cookie
PATH	Attribut du chemin du cookie
COOKIEDOMAIN	Attribut du domaine du cookie
EXPIRES	Date d'expiration du cookie
SECURE	Attribut sécurisé du cookie

Types de problème

La section Types de problème contient une ligne pour chaque problème trouvé.

Nom de zone	Explication/Commentaire
ENGINEID	ID AppScan pour ce problème
PRENOM	Nom du problème tel qu'il apparaît dans l'interface graphique
INVASIVE	Problème invasif : Y/N

Nom de zone	Explication/Commentaire
SEVERITY	Code de gravité de ce problème tel qu'indiqué dans l'interface graphique AppScan : 4 = Tous 3 = Elevé 2 = Moyen 1 = Faible 0 = Informations
THREATCLASS	Classification des menaces telle qu'elle apparaît dans l'interface graphique
THREATCLASSREFERENCE	URL vers la référence Internet sur cette classification (si appropriée)
REMEDIATIONTYPEID	ID AppScan pour le type de résolution
ADVISORYID	AppScan Interne
ENTITYTYPE	AppScan Interne
INFRASTRUCTURE	AppScan Interne

JavaScript

La section Javascript contient une ligne pour chaque Javascript trouvé dans les pages du site.

Nom de zone	Explication/Commentaires
ENGINEID	ID AppScan pour le Javascript
FILEID	ID du fichier dans lequel Javascript a été trouvé
SHORTTEXT	Texte de Javascript (peut être tronqué)

Types de résolution

La section Résolution contient une ligne pour chaque Résolution.

Nom de zone	Explication/Commentaires
ENGINEID	ID pour le type de résolution
PRENOM	Nom du type de résolution tel qu'il apparaît dans l'interface graphique
REMEDIATIONPRIORIY	Code de priorité de résolution (1=le plus élevé)

Demandes

La section Demandes contient une ligne pour chaque demande de test envoyée.

Nom de zone	Explication/Commentaires
ENGINEID	ID AppScan pour la demande de test
FILEID	ID AppScan du fichier auquel a été envoyée la demande
URL	URL de la demande
QUERY	Paramètres envoyés dans la demande
STATUS	AppScan Interne
REASONID	AppScan Interne

Nom de zone	Explication/Commentaires
XMLTYPE	AppScan Interne
LOGINTYPE	AppScan Interne

Paramètres de script

Cette section contient une ligne pour chaque paramètre envoyé dans une demande de test.

Nom de zone	Explication/Commentaires
ENGINEID	ID AppScan pour le paramètre
FILEID	ID du fichier dans lequel le paramètre a été envoyé
PRENOM	Paramètre effectif envoyé
PARAMETERTYPE	Type de paramètre : Get/Post

Variantes

La section Variantes contient une ligne pour chaque variante.

Nom de zone	Explication/Commentaires
ENGINEID	ID AppScan pour la variante.
ENTITYNAME	Nom du cookie auquel la variante est envoyée (si applicable)
FILEID	ID du fichier dans lequel la variante a été envoyée
ISSUETYPE	Nom du type de problème tel qu'il apparaît dans l'interface graphique
REMEDIATIONTYPE	AppScan Interne
SEQUENCEINDEX	AppScan Interne

Chapitre 7. Résultats : Données d'application

AppScan offre trois manières de visualiser et d'utiliser les résultats de l'examen : Données d'application, Problèmes de sécurité et Tâches de résolution. La présente section décrit la vue Données d'application.

Cette vue permet de vérifier si toutes les parties du site qui doivent être couvertes par l'examen sont effectivement explorées, avant de lancer l'étape de test. Elle présente des résultats provenant uniquement de l'étape d'exploration, sans référence à l'étape de test.

Dans la vue **Afficher le sélecteur**, cliquez sur :

Données d'application : Arborescence de l'application

L'**Arborescence de l'application** affiche les dossiers, les adresses URL et les fichiers explorés.

Après l'étape d'exploration, vous pouvez réviser l'**Arborescence de l'application** pour facilement visualiser votre application et vous assurer que tout a été exploré.

Le nœud que vous sélectionnez dans l'**Arborescence de l'application** agit comme un filtre pour les données répertoriées dans la **Liste des résultats**. S'il n'existe aucun résultat pour un type de données spécifique, sélectionnez un nœud d'un niveau supérieur dans l'arborescence. Si vous sélectionnez **Mon application**, toutes les données d'un type spécifique sont affichées dans la liste.

Données d'application : Liste de résultats

La liste des résultats affiche des listes d'URL, de paramètres et de scripts qui ont été reconnus lors de l'étape d'exploration, *pour le nœud sélectionné dans l'arborescence de l'application*. Le tableau ci-dessous répertorie les catégories de données.

Type de données	Description
«Demandes», à la page 200	URL accédées par AppScan.
«Paramètres», à la page 200	Scripts et leurs paramètres associés reconnus par AppScan.
«Cookies», à la page 201	Cookies reconnus par AppScan.
Pages	Toutes les pages explorées par AppScan.
«Demandes ayant échoué», à la page 202	Liens ne répondant pas à des demandes.
«URL filtrées», à la page 203	URL n'ayant pas été explorées, soit à cause de paramètres AppScan par défaut, soit à cause de vos filtres d'exploration définis (voir «Vue Exclusion de chemins et de fichiers», à la page 65).
«Interaction utilisateur nécessaire», à la page 204	URL requérant une entrée utilisateur ne pouvant pas être fournie automatiquement par AppScan. Pour savoir comment définir une entrée de paramètre de formulaire, voir «Onglet Connexion», à la page 52.
«Commentaires», à la page 205	Commentaires sur vos pages Web accessibles aux utilisateurs.

Type de données	Description
«JavaScript», à la page 205	JavaScripts reconnu par AppScan.

Dans la liste de résultats :

- Déplacez la souris sur chaque catégorie de données (Demandes, Paramètres, etc.) pour voir le nombre d'éléments dans cette catégorie (pour le nœud sélectionné dans l'arborescence de l'application).
- Cliquez sur une catégorie pour afficher les éléments qu'elle comporte (dans la liste de résultats).
- Cliquez sur un élément de la liste de résultats pour afficher ses caractéristiques dans la sous-fenêtre Détails.

La liste de résultats et la sous-fenêtre Détails pour chaque type de données sont décrites dans les sections suivantes.

Demandes

Cette vue liste les demandes pour lesquelles AppScan a reçu une réponse valide. En fonction de ces réponses, AppScan génère des tests afin de révéler les faiblesses du site, qui seront envoyées lors de l'étape de test.

Si le corps de la demande ou de la réponse contient XML (y compris XHTML ou SOAP), l'icône URL visitées est remplacée par l'icône XML : 

Demandes dans la liste de résultats

La **Liste des résultats** affiche l'URL de chaque page visitée par AppScan, ainsi que la méthode et les paramètres.

- Vous pouvez visualiser une URL visitée en cliquant avec le bouton droit de la souris sur une demande, puis en cliquant sur **Afficher dans le navigateur** ou en sélectionnant l'URL et en cliquant sur le lien **Afficher dans le navigateur** dans le **Panneau des détails**.
- Vous pouvez créer un test manuel pour l'URL en cliquant avec le bouton droit de la souris sur l'élément **URL visitée**, puis en cliquant sur **Test manuel** ou en sélectionnant l'URL et en cliquant sur le lien **Test manuel** dans le **Panneau des détails**. (Pour en savoir plus, voir «Tests manuels», à la page 223.)

Demandes dans le Panneau des détails

Le **Panneau des détails** inclut des liens vers **Afficher dans le navigateur** et **Test manuel**, qui opèrent de la même manière que les commandes de clic droit dans la **Liste des résultats**.

L'onglet **Demande/Réponse** s'affiche et présente la demande et la réponse immédiate de l'URL sélectionnée dans la **Liste des résultats**.

Paramètres

Il s'agit de demandes comprenant un ou plusieurs paramètres.

La liste **Liste des résultats** affiche tous les paramètres trouvés lors de l'étape d'exploration. Les URL de cette liste sont celles qui sont considérées comme les plus vulnérables à des attaques malveillantes. Cette liste peut s'avérer cruciale pour évaluer si l'examen a généré un ensemble de demandes de test utile.

Pour chaque paramètre de la liste Paramètres de script, AppScan affiche un nom, un type, une valeur, une URL (sous-fenêtre Résultats) et une valeur (sous-fenêtre Détail), et indique si le paramètre fait l'objet d'un suivi. Un nom de paramètre peut être répertorié plusieurs fois s'il a une URL différente ou s'il a des valeurs différentes sur la même URL.

Le tableau ci-dessous présente les options disponibles lorsque vous cliquez avec le bouton droit de la souris sur un élément de la liste.

Tableau 8. Options accessibles par clic droit

Option	Fonction
Copier l'URL	Copie de l'URL sélectionnée dans le presse-papiers.
Ajouter à la liste de l'onglet Paramètres et cookies	Ajout du nom du paramètre sélectionné (toutes valeurs) dans la liste de la boîte de dialogue Configuration, par clic droit et sélection de la liste d'**ajout aux paramètres et aux cookies**. La boîte de dialogue Définition de paramètre s'ouvre. Vous pouvez alors configurer le traitement par AppScan de ce paramètre.
Exclure cette combinaison chemin-paramètre-valeur de l'examen	Exclusion d'une valeur de paramètre spécifique de l'examen en cas de présence dans une adresse URL. Lorsque vous sélectionnez cette option, la boîte de dialogue Editer l'exclusion ou l'exception s'ouvre ; elle contient les données correspondantes. **Exemple** Prenons l'exemple d'un site dont l'adresse URL est la suivante : `http://site/command` et un paramètre « action ». Chaque valeur déclenche une réponse différente du serveur : • `action=login`, redirige vers la page de connexion • `action=logout`, la session est arrivée à expiration • `action=clean`, supprime les données utilisateur du serveur Pour qu'AppScan puisse examiner ce site, il doit exclure `http://site/command` lorsque `action=logout` ou `clean`, mais pas `action=login` ou toute autre valeur. Pour ce faire, vous pouvez utiliser cette fonction pour exclure `http://site/command` avec le nom de paramètre `action` et la valeur `logout` ou `clean`. Pour plus de détails, voir «Ajouter de nouvelles exclusions ou exceptions», à la page 66
Ne pas tester le ou les paramètres sélectionnés	Exclusion d'un ou plusieurs noms de paramètre (toutes valeurs) de l'étape de test de l'examen. Ce paramètre s'applique à toutes les valeurs du paramètre spécifié. Il ne concerne pas l'étape d'exploration. Le nom de paramètre est ajouté à la liste dans la vue Paramètres et cookies de la boîte de dialogue Configuration, avec la valeur **Exclusion de test** définie à "Yes". Pour plus de détails, voir «Vue Paramètres et cookies», à la page 76

Cookies

Cookies répertorie tous les cookies trouvés par AppScan lors de l'examen, définis par des réponses, générés par des scripts Java ou déjà présents sur l'hôte avant l'examen.

- La Liste des résultats affiche tous les cookies trouvés lors de l'étape d'exploration. Pour chaque cookie, la liste affiche un nom, une URL avec cookie défini, des valeurs, un chemin, un domaine, une date d'expiration, un contexte, et indique si le cookie fait l'objet d'un suivi, s'il est exclus des tests et s'il est sécurisé.

  Remarque : L'URL répertoriée est celle menant à la réponse définissant le cookie (même s'il en existe d'autres comprenant la commande Set Cookie). Si le cookie n'a pas été défini par une réponse (par exemple s'il a été généré par un script Java ou s'il était déjà présent sur l'hôte), N/A s'affiche dans la zone URL de la réponse.

- Vous pouvez ajouter tout cookie à la liste dans la boîte de dialogue Configuration en cliquant avec le bouton droit de la souris et en sélectionnant **Ajouter ce cookie à l'onglet Paramètres et cookies**. La boîte de dialogue Définition de paramètre s'ouvre pour permettre la configuration du traitement de ce cookie par AppScan.
- Lorsqu'un cookie est sélectionné, la sous-fenêtre de détail affiche les informations suivantes :

Elément	Description
Chemin d'accès	Le dossier ou sous-dossier spécifique de votre application auquel ce cookie est envoyé. L'attribut du chemin est utilisé pour spécifier le sous-ensemble des URL d'un domaine pour lequel le cookie est valide. Si un cookie a déjà communiqué un domaine correspondant (élément suivant), alors le composant du nom de chemin de l'URL est comparé à l'attribut du chemin, et s'il existe une correspondance, le cookie est considéré comme valide et est envoyé avec la requête d'URL.
Domaine	Domaine ou sous-domaine dans lequel ce cookie sera envoyé. (Si le domaine n'est pas défini, le cookie est envoyé dans le domaine émis par la commande Set Cookie et dans tous ses sous-domaines.)
Arrive à expiration	La date et l'heure auxquelles le cookie expirera et sera supprimé de l'ordinateur de l'utilisateur.
Sécurisé	`Yes` (sécurisé) ou `No`. Si un cookie est marqué comme **Sécurisé**, il sera uniquement transmis si le canal de communication avec l'hôte est sécurisé (actuellement uniquement aux serveurs HTTPS). Si **Sécurisé** n'est pas spécifié, le cookie est considéré comme sûr et est envoyé à tous les canaux.
URL de la demande	Première demande envoyée par AppScan avec le cookie.

Demandes ayant échoué

Il s'agit de demandes envoyées qui n'ont pas retourné de réponse valide. Cela se produit généralement lorsque le site est hors service, lorsque qu'il y a d'autres incidents de communication ou lorsqu'une demande renvoie un état de message d'erreur à la place de la page demandée.

Remarque : Si une adresse URL figurant dans l'arborescence d'application contient *uniquement* des réponses d'erreur, elle est barrée.

- Où une page d'erreur est la réponse attendue
- Vous pouvez renvoyer la demande à un lien rompu plutôt que de répéter l'examen dans sa totalité. Si l'application a été modifiée ou corrigée depuis l'exécution de l'étape d'exploration, réexécutez la procédure suivante pour explorer de nouveau les liens rompus.

  Remarque : Si votre application requiert une connexion, nous vous recommandons de vous connecter manuellement à AppScan (voir «Onglet Connexion», à la page 52) avant de suivre la procédure suivante afin d'éviter que les liens rompus ne soient explorés en dehors des schémas d'utilisation standard.
- Vous pouvez visualiser tous les liens rompus en sélectionnant **Demandes ayant échoué** dans la sous-fenêtre Résultat.
- Lorsque vous cliquez sur **Réessayer toutes les demandes ayant échoué**, ces liens sont supprimés de la liste des liens rompus et ajoutés dans la liste des liens non visités. AppScan poursuit alors l'étape d'exploration en visitant les liens de la liste des liens non visités lorsque c'est possible. Cette étape d'exploration se termine lorsque tous les liens non visités ont été explorés.

  Remarque : Si des incidents de communication existent entre AppScan et votre serveur lors d'un examen, certains liens peuvent être marqués comme liens rompus. Lorsque des incidents de communication surviennent, AppScan tente de renvoyer ses demandes pendant 90 secondes. Si la connexion n'est pas établie pendant ce laps de temps, l'examen s'arrête. Le panneau de notification de la fenêtre principale vous signale le problème et indique que le délai a expiré. Si cette notification s'affiche, vous devez corriger la connexion entre AppScan et votre application avant de tenter de réparer les liens.

- La sous-fenêtre Détail affiche la page de réponse d'un lien rompu spécifique en cliquant sur le bouton **Afficher dans le navigateur**.

URL filtrées

Il s'agit d'URL qui n'ont pas été visitées par AppScan, car elles n'ont pas été filtrées hors de l'exploration : soit par des filtres standard, soit par des filtres définis lorsque vous avez configuré l'examen (voir «Vue Exclusion de chemins et de fichiers», à la page 65).

URL filtrées dans la Liste des résultats

La **Liste des résultats** affiche les URL qui n'ont pas été explorées et indique le type de filtre (raison pour laquelle cette page a été filtrée).

Vous pouvez visualiser une URL filtrée en cliquant dessus avec le bouton droit de la souris, puis en cliquant sur **Afficher dans le navigateur**.

Le tableau suivant répertorie les principaux filtres pouvant être configurés.

Nom du filtre	Signification et mode de configuration
Limite de profondeur	L'URL a été filtrée en raison de la limite configurée dans **Configuration > Options d'exploration > Limites d'examen > Limite de profondeur**.
Filtre d'extension de fichier	Les différentes extensions sont répertoriées dans **Configuration > Exclusion de chemins et de fichiers > Types de fichier à exclure**.
DOM probablement identique	Page exclue de l'examen, car AppScan estime que la réponse présentera une structure (DOM) identique à celle d'une page déjà explorée et qu'elle ne contiendra probablement aucun nouvel élément à tester. Cet élément est contrôlé par **Configuration > Options d'exploration > Principal > Filtrer les pages susceptibles d'être identiques en fonction de leur structure (DOM)**.
Filtre des chemins d'accès	Les différents chemins sont répertoriés dans **Configuration > Exclusion de chemins et de fichiers > Exclusion de chemins d'accès**.
Limite de chemin d'accès	L'URL a été filtrée en raison de la limite configurée dans **Configuration > Options d'exploration > Limites d'examen > Limite de chemin d'accès redondant**.
Corps similaire	Demande (provenant d'une page qui n'a pas été filtrée en raison d'un élément DOM identique) exclue de l'examen, car le contenu du corps de la réponse est identique à celui d'une demande précédemment explorée. Cet élément est contrôlé par **Configuration > Options d'exploration > Principal > Filtrer les pages identiques en fonction de leur structure (DOM)**.
DOM identique	Page ayant été exclue de l'examen, car sa structure (DOM) est identique à celle d'une page déjà explorée et parce qu'elle ne contient probablement aucun nouvel élément à tester. Cet élément est contrôlé par **Configuration > Options d'exploration > Principal > Filtrer les pages identiques en fonction de leur structure (DOM)**.
Limite du nombre total de liens visités	L'URL a été filtrée en raison de la limite configurée dans **Configuration > Options d'exploration > Limites d'examen > Limite de page totale**.
Serveur Web non testé	Le domaine est différent de celui de l'URL de départ et n'est pas un des domaines supplémentaires configurés dans **Configuration > URL et serveurs > Serveurs et domaines supplémentaires**.

URL filtrées dans le Panneau des détails

La **sous-fenêtre Détail** contient un lien permettant d'afficher l'URL dans un navigateur : **Afficher dans le navigateur**. **Ce qui correspond à un clic droit sur Afficher dans le navigateur** dans la **Liste des Résultats**.

L'onglet **Demande/Réponse** affiche la demande qui aurait été envoyée à l'URL si elle n'avait pas été filtrée.

Référence associée:

«Vue Exclusion de chemins et de fichiers», à la page 65
Vue Exclusion de chemins et de fichiers de la boîte de dialogue Configuration.

«Vue Options d'exploration», à la page 71
Vue Options d'exploration de la boîte de dialogue Configuration.

Interaction utilisateur nécessaire

Il s'agit de requêtes qui n'ont pas été envoyées, car elles nécessitent une entrée de l'utilisateur que AppScan n'a pas pu fournir. Vous pouvez configurer AppScan pour fournir une entrée (voir «Vue Remplissage automatique de formulaires», à la page 90). Si certains paramètres de votre application sont manquants, ou si vous choisissez de ne pas utiliser l'outil de remplissage automatique des formulaires, AppScan vous fournit une liste des URL interactives à revoir.

- Vous pouvez examiner la liste des URL interactives. Si vous souhaitez que ces pages soient examinées, indiquez les informations utilisateur requises dans une exploration manuelle.
- Nous vous recommandons d'examiner attentivement la liste des URL interactives, de remplir les données requises et d'envoyer ces demandes. AppScan inclut alors ces URL lors de l'étape de test.
- En permettant à AppScan d'envoyer ces demandes, les nouvelles parties du site qui étaient précédemment inaccessibles deviennent accessibles. Par conséquent, après avoir visité des URL interactives, vous devez explorer de nouveau votre application (**Examen > Nouvel examen > Explorer**).

Voir «Explorer manuellement des URL interactives»).

Explorer manuellement des URL interactives

Pourquoi et quand exécuter cette tâche

Les URL interactives sont des requêtes qui n'ont pas été envoyées, car elles nécessitent une entrée de l'utilisateur que AppScan n'a pas pu fournir. Si certains paramètres de votre application sont manquants, ou si vous choisissez de ne pas utiliser l'outil de remplissage automatique des formulaires, AppScan vous fournit une liste des URL interactives à la fin de l'examen.

Procédure

1. Dans **Vue Données > Liste des résultats**, cliquez sur **Interaction utilisateur nécessaire**.

   La liste des URL avec une entrée interactive s'affiche.

   Remarque : Une seule URL peut apparaître plusieurs fois, chaque instance provenant d'un formulaire différent.
2. Cliquez avec le bouton droit de la souris sur une URL de la liste, puis cliquez sur **Explorer manuellement cette URL**.

   Le navigateur, avec les boutons **Exploration manuelle**, apparaît ouvert sur cette URL. Terminez l'exploration manuelle. Voir «Enregistrer une exploration manuelle», à la page 144.

   Une fois l'exploration manuelle terminée, AppScan analyse la nouvelle Exploration.

   Si de nouvelles URL ont été trouvées, un message s'affiche, recommandant de poursuivre l'exploration (**Examen > Continuer l'examen > Explorer**).
   - Si aucune URL nouvelle n'a été trouvée, mais que de nouveaux tests ont été créés, un message s'affiche, recommandant de passer à l'étape de test (**Examen > Continuer l'examen > Test**).
   - Si de nouvelles URL ont été trouvées et de nouveaux tests ont été créés, un message s'affiche, recommandant de continuer les étapes d'exploration et de test (**Examen > Continuer l'examen > Examen intégral**).

Commentaires

Les *commentaires* sont des commentaires HTML trouvés par AppScan lors de l'étape d'exploration. Les commentaires cachés d'une page HTML peuvent contenir des informations utiles aux pirates. Il arrive parfois que des développeurs laissent sur la page finale, volontairement ou involontairement, des commentaires qui leur sont destinés ou qui sont destinés à d'autres développeurs. Un pirate peut rassembler des informations internes utiles à partir de ces commentaires, telles que des mots de passe de débogage.

Commentaires dans la liste des résultats

La liste des commentaires affiche la première ligne du commentaire ainsi que la première URL où il se trouve. Si AppScan trouve le même commentaire plusieurs fois, seule la première instance est répertoriée.

Commentaires dans le Panneau des détails

La **sous-fenêtre Détail** affiche la totalité du commentaire de l'élément sélectionné dans la **liste des résultats**. Révisez les commentaires ici afin de déterminer lequel est à supprimer de l'application finale.

JavaScript

JavaScript recense le code JavaScript détecté par AppScan lors de l'étape d'exploration.

JavaScript dans la liste des résultats

La liste affiche la première ligne de JavaScriptet la première URL où elle a été trouvée. Si le même script est trouvé sur plusieurs URL, seule la première instance est répertoriée.

JavaScript dans la sous-fenêtre Détail

La **sous-fenêtre Détail** affiche la totalité du script de l'élément sélectionné dans la **liste des résultats**. Révisez le code ici pour les commentaires devant être supprimés de l'application finale.

Données d'application : Panneau des détails

Dans la vue Données d'application, la sous-fenêtre Détails affiche une grande variété d'options de données et de barre d'outils, en fonction du type de données sélectionné.

Type de données	Options de la barre d'outils
Demandes	Afficher dans le navigateur, Définir comme page d'erreur, Test manuel, Rechercher (mot/phrase).
Paramètres	Demandes (basculer), Afficher dans le navigateur, Définir comme page d'erreur, Test manuel, Rechercher (mot/phrase).
Cookies	Aucun.
Pages	Onglet Informations de page. Onglet Demande/Réponse Demandes (basculer), Afficher dans le navigateur, Définir comme page d'erreur, Test manuel, Rechercher (mot/phrase).
Demandes ayant échoué	Afficher dans le navigateur, Définir comme page d'erreur, Rechercher (mot/phrase).
Filtré	Afficher dans le navigateur, Définir comme page d'erreur, Rechercher (mot/phrase).
Interaction utilisateur nécessaire	Explorer manuellement cette URL, Rechercher (mot/phrase).
Commentaires	Aucun.
JavaScripts	Rechercher (mot/phrase).

Chapitre 8. Résultats : Problèmes de sécurité

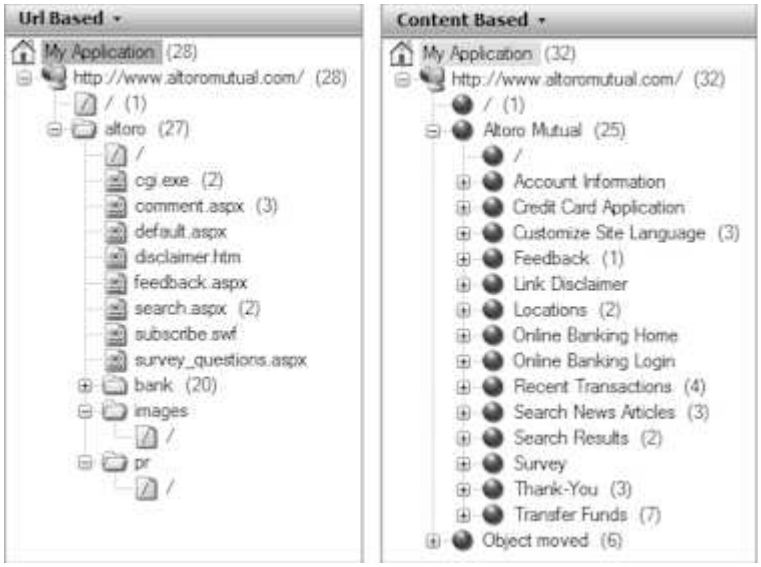
AppScan offre trois manières de visualiser et d'utiliser les résultats de l'examen : Problèmes de sécurité, Tâches de résolution et Données d'application. La présente section décrit la vue Problèmes de sécurité.

La vue Problèmes de sécurité permet d'accéder aux résultats d'un examen. Vous pouvez visualiser des résultats à un niveau élevé ou sélectionner des tests ou des objets spécifiques et accéder à plus de détails. Ces détails comprennent des conseils, des recommandations de correction, des demandes/réponses ainsi que les différences entre les variantes de test ayant provoqué des problèmes. Vous pouvez modifier la gravité des problèmes, renvoyer des tests (avec ou sans modifications) et créer des rapports basés sur les problèmes.

Dans la vue **Afficher le sélecteur**, cliquez sur :

Problèmes de sécurité : Arborescence de l'application

L'**Arborescence de l'application** affiche les dossiers et les fichiers de l'application examinée. Chaque nœud de l'arborescence dispose d'un compte qui présente le nombre de problèmes contenus dans le nœud.



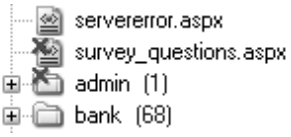
Dans l'Arborescence de l'application, vous pouvez :

- Sélectionner un nœud pour filtrer les problèmes affichés dans la **Liste des résultats**.
- Utiliser le menu du clic droit pour afficher dans le navigateur, procéder à une exploration manuelle, procéder à un test manuel, copier l'URL dans le presse-papiers et exclure l'URL de l'examen. (Voir «Menu "clic droit" de l'arborescence de l'application», à la page 23.)
- Si vous avez défini des règles basées sur le contenu, vous pouvez basculer de la vue basée sur l'URL à la vue basée sur le contenu en cliquant sur la zone de liste déroulante en haut du panneau. (Voir «Vue Résultats basés sur le contenu», à la page 103.)

Exclure une URL de l'examen

Toute URL ou tout nœud de l'arborescence de l'application peut être exclu des examens à venir en cliquant dessus avec le bouton droit de la souris et en sélectionnant **Exclure de l'examen**. (Pour réintégrer l'URL ou le nœud, cliquez de nouveau avec le bouton droit de la souris et sélectionnez **Inclure dans l'examen**).

Lorsqu'une URL ou un nœud est exclu de l'examen, un **X** rouge apparaît dans l'icône correspondante dans l'arborescence de l'application.



Lorsque vous excluez des URL de cette manière, des éléments "Exclure" sont ajoutés à la liste **Exclure ou inclure des chemins d'accès** (voir «Vue Exclusion de chemins et de fichiers», à la page 65).

Problèmes de sécurité : Liste de résultats

La Liste des résultats affiche les problèmes appropriés au nœud sélectionné dans l'arborescence de l'application. Si vous avez sélectionné le nœud Mon application, la Liste des résultats présente tous les problèmes trouvés dans votre application Web.

Les problèmes sont regroupés par Type. Toutes les URL sont répertoriées sous chaque type. Tous les problèmes sont répertoriés sous chaque URL. (Les variantes individuelles des problèmes ne sont pas affichées dans la Liste des résultats mais peuvent être visualisées à partir du Panneau des détails.)

Chaque nœud de l'arborescence dispose d'une icône de gravité qui indique la gravité du problème, et d'un compte qui indique le nombre de problèmes de ce type qui ont été trouvés. S'il s'agit de type et d'URL, l'icône de gravité indique la gravité du problème le plus sévère inclus sous le nœud.

Vous pouvez modifier le tri des problèmes ainsi que leurs valeurs de gravité (voir «Niveaux de sécurité», à la page 209).

Vous pouvez désigner des problèmes que vous ne souhaitez pas traiter pour le moment comme Bruit, soit en les supprimant de l'affichage des résultats, soit en les faisant apparaître barrés (voir «Etat du problème : Ouvert ou Bruit», à la page 209).

Le nombre total de problèmes de sécurité (en haut de la liste) est une mesure des emplacements vulnérables du site et dépend en partie de sa structure. Si vous définissez une structure basée sur le contenu (voir «Vue Résultats basés sur le contenu», à la page 103), le nombre total des problèmes dans l'arborescence de l'application peut ne pas être identique à celui de l'arborescence de l'application basée sur l'URL (pour les mêmes résultats). Lorsque la structure du site est basée sur le contenu (plutôt que sur l'URL), et que la vue basée sur le contenu est correctement configurée, le nombre de problèmes de la vue basée sur le contenu représente plus précisément le nombre d'« emplacements vulnérables » existant

dans le site. Le nombre total de *variantes* (en haut de la liste entre parenthèses) est indépendant de la structure du site et ne change pas entre la vue basée sur le contenu et la vue basée sur l'URL.

Niveaux de sécurité

Dans le cas de problèmes, l'icône de gravité indique le niveau de gravité du problème. Dans le cas de Types de problèmes et d'URL, elle indique la gravité la plus sévère de tous les problèmes situés sous ce nœud.

Icône	Indique	Description	Exemples
	Gravité élevée	Danger direct pour votre application, votre serveur Web ou vos informations	Exécution de commandes sur le serveur, vol d'informations client, déni de service
	Gravité moyenne	Menace via un accès non autorisé aux zones confidentielles, bien que la base de données et le système d'exploitation ne courent pas de risque	Divulgation de la source des scripts, navigation forcée
	Gravité faible	Autorise une reconnaissance non autorisée	Divulgation du chemin du serveur, divulgation des adresses IP internes
	Message d'information	Problèmes dont vous devez avoir connaissance, pas nécessairement des problèmes de sécurité	Activation de méthodes non sécurisées

Tâches associées:

«Changer de niveau de gravité»

Changer de niveau de gravité

Procédure

Vous pouvez changer la gravité affectée à un noeud en cliquant sur celui-ci avec le bouton droit de la souris et en sélectionnant **Gravité >**, suivie de la nouvelle valeur.

Remarque : Si vous changez le niveau de gravité d'un type ou d'un noeud d'URL, le nouveau niveau est attribué à tous les problèmes situés sous ce noeud.

Etat du problème : Ouvert ou Bruit

Les problèmes qui ne sont pas appropriés pour votre application peuvent être désignés comme "Bruit" et être supprimés des résultats.

Pourquoi et quand exécuter cette tâche

Si un problème spécifique découvert par AppScan n'est pas approprié pour votre application (signifiant qu'il s'agit effectivement d'un résultat "faux positif" pour votre application), par exemple un problème existant uniquement dans l'environnement de développement mais pas dans l'environnement de déploiement, vous pouvez décider de le classer comme "Bruit".

Il existe deux options d'affichage pour les problèmes marqués comme Bruit : Inclus à la liste des résultats comme texte grisé barré et Non inclus à la liste des résultats.

Procédure

Pour basculer d'une option d'affichage à une autre, cliquez sur **Affichage > Afficher les problèmes marqués comme Bruit**.

Résultats

Lorsqu'une marque de contrôle apparaît en regard de l'élément de menu, des problèmes marqués comme Bruit sont inclus dans la liste des résultats, mais avec du texte grisé barré.

Exemple

Les définitions de Bruit s'appliquent de la manière suivante :

- Sur le poste de travail sur lequel l'examen est configuré, les désignations de Bruit sont sauvegardées et s'appliquent automatiquement aux examens futurs, *lorsque l'examen est sauvegardé*. (L'emplacement du fichier de classification des bruits est défini dans Outils > Options > onglet Général.)
- Lorsque vous ouvrez un examen sauvegardé, *y compris sur un poste de travail différent*, ces problèmes sont désignés comme Bruit *pour cet examen*, même si le poste de travail a des définitions différentes. (Toutefois, notez que si vous *sauvegardez* l'examen sur le second poste de travail, ses définitions seront enregistrées sur ce poste de travail, y écrasant tout fichier de classification des bruits.)

Que faire ensuite

Voir aussi :

«Changer l'état d'un problème»

«Vue Options de test», à la page 114

Changer l'état d'un problème

Vous pouvez changer l'état attribué à un nœud.

Procédure

Cliquez avec le bouton droit de la souris sur un noeud et sélectionnez **Etat >**, suivi de la nouvelle valeur ("Ouvert" pour les problèmes appropriés, "Bruit" pour les problèmes non appropriés à votre application).

Remarque : Si vous changez l'état d'un type ou d'un noeud d'URL, le nouvel état est attribué à tous les problèmes situés sous ce noeud.

Exporter et importer des états de problème

Si vous avez désigné certains problèmes comme "Bruit" (non appropriés à votre application), vous pouvez exporter ces désignations pour les utiliser sur d'autres postes de travail.

Pourquoi et quand exécuter cette tâche

Pour exporter des désignations Bruit afin de les utiliser sur d'autres postes de travail :

Procédure

Cliquez sur **Fichier > Exporter > Données d'examen croisés**, et enregistrez les données en tant que fichier XML.

Que faire ensuite

Pour importer les états d'un autre poste de travail, cliquez sur **Fichier > Importer > Données d'examen croisés**.

Renvoyer des tests

Pourquoi et quand exécuter cette tâche

Vous pouvez renvoyer un test sans exécuter une étape complète d'examen intégral ou de test. Par exemple, si les résultats d'un test semblent incohérents par rapport aux résultats d'un examen précédent, vous pouvez renvoyer ce test.

Procédure

1. Dans la **Liste de résultats**, cliquez avec le bouton droit de la souris sur un noeud.
2. Dans le menu qui s'affiche, cliquez sur **Nouveau test**.

   AppScan envoie toutes les demandes de test comprises dans le nœud sélectionné, et les nouveaux résultats sont ajoutés dans la **liste des résultats**.

Menu "clic droit"

Le menu clic droit de la Liste des résultats des problèmes de sécurité comprend les options suivantes :

Elément	Explication
Gravité	Modifie la valeur de la Gravité pour l'élément sélectionné (sélectionner Elevée, Moyenne, Faible, Information).
Etat	Par défaut, l'état du problème est toujours Ouvert. Si vous n'avez pas besoin de vous rapporter à certains problèmes, vous pouvez définir ces derniers comme Bruit. (Options : Ouvert/Bruit)
Nouveau test	Renvoie le test sélectionné et ajoute le résultat à ceux de l'examen.
Test manuel	Crée un test manuel (voir «Tests manuels», à la page 223).
Supprimer	Supprime l'élément sélectionné des résultats du test (la réintégration est impossible).
Définir comme non vulnérable	Définit le résultat comme non vulnérable, de sorte qu'il n'apparaît pas dans les résultats du test (mais peut être visualisé et réintégré à partir de la liste des variantes non vulnérables, voir «Liste de variantes non vulnérables», à la page 226)
Rapport Faux positif	Zippe et envoie les informations relatives au test par courrier électronique au service d'assistance AppScan ou aux membres de votre organisation (voir «Rapport Faux positif des résultats de test», à la page 222)
Générer les informations sur les problèmes	Remplit l'onglet Informations sur les problèmes pour le résultat sélectionné uniquement. **Conseil :** Pour mettre à jour les informations sur les problèmes de *tous* les résultats, sélectionnez **Outils > Générer les informations sur tous les problèmes** au lieu de cette option.

Filtrage des problèmes de sécurité dans la Liste des résultats

Vous pouvez filtrer la **Liste des résultats** à la recherche de types de problèmes ou d'un problème spécifique.

Procédure

1. Dans le menu **Edition**, cliquez sur **Rechercher** (ou appuyez sur **Ctrl + F**).

   La barre **Rechercher** apparaît dans la fenêtre principale, sous la **Liste des résultats**.
2. Dans l'**Arborescence de l'application**, sélectionnez un nœud.
   - Si vous sélectionnez le nœud **Mon application**, la recherche se fait parmi tous les résultats.
   - Si vous sélectionnez un nœud dans l'arborescence, la recherche se fait dans le nœud sélectionné et ses sous-nœuds.
3. Dans la zone de saisie **Rechercher** de la barre **Rechercher**, entrez une chaîne ou une partie de chaîne.

4. Dans la zone de liste déroulante **Rechercher dans**, sélectionnez où rechercher la chaîne dans les résultats. Les options sont les suivantes : Numéro d'ID de test, Problème de sécurité, URL, ID CVE, ID CWE, XFID (ID X-Force), Données de demande/réponse, Description de la variante, Paramètre/Cookie ou Tous.
5. Cliquez sur **Rechercher maintenant** ou appuyez sur **Entrée**.

   Les résultats apparaissent dans la **liste des résultats**, écrasant la liste précédemment affichée.

   Si vous entrez une autre chaîne **Rechercher** et cliquez à nouveau sur **Rechercher maintenant**, la nouvelle recherche est réalisée sur le nœud sélectionné dans l'**Arborescence de l'application**, et non sur les résultats affichés de la précédente recherche.

Pour rechercher :	**Rechercher :**	**Rechercher dans :**
La variante portant l'ID : `"5016"` (voir le sous-onglet **Propriétés** du **Panneau des détails**)	`"5016"`	ID
Problèmes de script intersite	`"cross"`	Nom du test
Pages de connexion avec des problèmes	`"login"`	Adresse URL de test
Problèmes associés à la manipulation des mots de passe	`"passwd"`	Demande/réponse

Trier la Liste des résultats

Pourquoi et quand exécuter cette tâche

Vous pouvez réorganiser les problèmes dans la Liste des résultats. Par défaut, les problèmes sont triés par gravité.

Procédure

1. Cliquez sur l'en-tête de colonne **Classés par.**
2. Cliquez sur une commande dans le menu pour trier les problèmes :
   - **Gravité** - Les noms de test sont répertoriés par ordre de gravité, de la gravité Elevée à la gravité Information.
   - **Nombre** - Nombre de problèmes dans chaque test. Les tests trouvant la plupart des problèmes sont répertoriés les premiers.
   - **Nom** - Ordre alphabétique par nom de test.

   Les problèmes sont à nouveau triés dans la **Liste des résultats**.

   Pour inverser l'ordre de tri (ascendant ou descendant), cliquez sur la deuxième colonne de la **Liste des résultats**. Cliquez de nouveau sur la deuxième colonne pour réinitialiser l'ordre.

Problèmes de sécurité : Panneau des détails

Le panneau des détails affiche des informations utiles relatives à un test sélectionné ainsi que toutes ses variantes, sélectionnées dans la **Liste des résultats**.

Le panneau des détails contient quatre onglets (un clic sur un onglet permet d'afficher son contenu) : «Onglet Informations sur les problèmes», «Onglet Conseils», à la page 217, «Onglet Recommandation de correction», à la page 219, «Onglet Demande/Réponse», à la page 220.

Onglet Informations sur les problèmes

Le premier onglet de la sous-fenêtre Détail récapitule les informations disponibles.

Pendant l'examen, lorsque des problèmes sont détectés et ajoutés à l'arborescence, l'onglet Informations sur les problèmes fournit un récapitulatif des informations disponibles dans les autres onglets de la

sous-fenêtre Détail, ainsi que des informations supplémentaires précieuses, comme l'évaluation des mesures CVSS pour le problème, et les captures d'écran associées qu'il est possible d'enregistrer avec les résultats et d'inclure dans vos rapports.

Zone/Icône	Description
En-tête	En-tête du problème comprenant l'URL, l'Entité et le Risque pour la sécurité (Elevé, Moyen, Faible ou Message d'information).
Evaluation des mesures CVSS	Evaluation moyenne basée sur les trois groupes de mesures CVSS : De base, Temporelle et Environnementale. Cliquez sur le lien pour l'édition (voir «Paramètres CVSS», à la page 214).
	Vous permet d'inclure des captures d'écran, d'autres images associées de votre choix, ainsi que vos propres commentaires dans les résultats d'examen, et de les inclure dans des rapports (voir «Modification des informations sur les problèmes», à la page 214).
Conseil (case jaune)	Ces informations se rapportent à la zone Contenu (ci-dessous) et expliquent ce qui est à regarder dans la ou les image(s) ou code HTML apparaissant ici.
Contenu (captures d'écran ou code HTML)	Selon le problème, cette zone peut inclure une capture d'écran, deux captures d'écran pour comparaison, une capture d'écran avec fenêtre en incrustation simulée ou un code HTML. Dans le cas d'un code HTML, vous pouvez activer ou désactiver le retour à la ligne en cliquant sur située dans l'angle supérieur droit de la zone de contenu.
Raisonnement (case bleue)	Explique ce qu'a exécuté AppScan, et pourquoi il considère que c'est un problème.
Récapitulatif technique (case grise)	Détails techniques des actions menées par AppScan pour tester ce problème et manière dont la réponse a été validée.

Barre d'outils Informations sur les problèmes

La barre d'outils au-dessus de la sous-fenêtre Détail présente la gravité actuelle du problème sélectionné, ainsi que son état, et permet de basculer d'un problème à un autre.

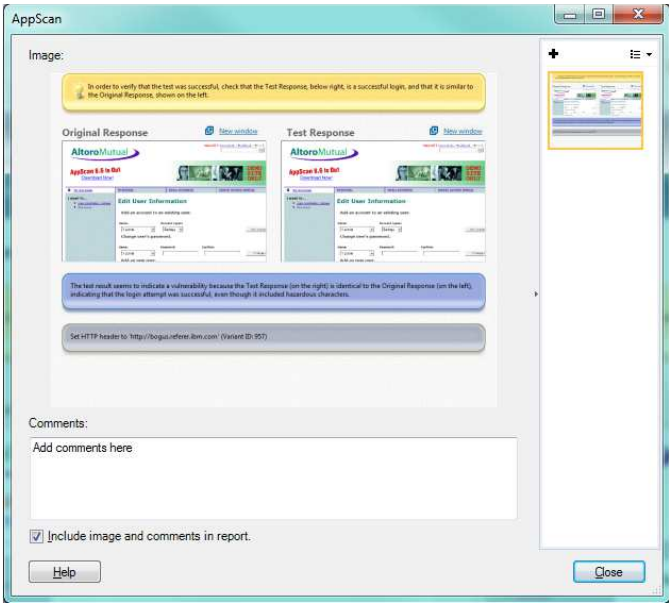
- **Gravité :** Sélectionnez l'un des quatre paramètres de gravité standards ou ajustez manuellement les paramètres CVSS pour ce problème.
- **Etat :** Les options sont "Ouvert" ou "Bruit". La valeur par défaut est Ouvert. Sélectionnez Bruit pour les problèmes qui ne sont pas importants. Par défaut, les résultats marqués comme Bruit apparaissent dans la Liste des résultats séparés par une ligne. Pour les supprimer tous en même temps de l'affichage, désélectionnez **Outils > Afficher les problèmes marqués comme bruit**.

Modification des informations sur les problèmes

Ajoutez des images et des commentaires aux informations sur les problèmes pour les inclure dans des rapports.

Il est possible d'enregistrer des captures d'écran de l'onglet Informations sur les problèmes, ainsi que les images associées de votre choix et vos propres commentaires, avec les résultats d'examen, et de les inclure dans des rapports.

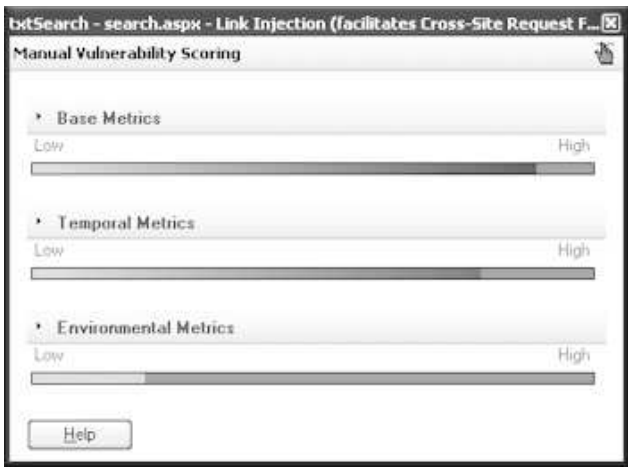
- Cliquez sur  située en haut à droite de l'onglet Informations sur les problèmes pour éditer les informations sur les problèmes.



Zone/Icône	Description
Image	Affiche l'image disponible actuellement sélectionnée dans les miniatures contenues dans le panneau de droite.
	Cliquez sur cette icône pour ajouter une image à ce problème dans les résultats d'examen.
	Cliquez sur cette icône pour sauvegarder l'image en cours sur votre ordinateur.
	Cliquez sur cette icône pour supprimer l'image en cours des résultats d'examen.
Commentaires	Entrez des commentaires sur l'image actuellement affichée, qui seront enregistrés avec l'examen.
Inclure l'image et les commentaires dans le rapport	Sélectionnez cette option pour inclure *l'image actuellement affichée et les commentaires* dans les rapports. Vous pouvez configurer chaque image séparément. Tous les images sont incluses par défaut.

Paramètres CVSS

Vous pouvez affiner manuellement le paramètre de gravité d'un problème spécifique à l'aide de mesures CVSS. Pour ce faire, à partir de la barre d'outils Informations sur les problèmes, cliquez sur **Gravité > Paramètres CVSS**.



A partir de la fenêtre CVSS, si vous cliquez sur le nom de l'une des trois sections, cette section s'ouvre pour la configuration. Vous pouvez restaurer les paramètres par défaut en cliquant sur , qui devient active une fois les modifications effectuées.

Mesures de base

Il s'agit des mesures de vulnérabilité qui sont constantes dans le temps et entre les environnements utilisateur.

Mesure	Explication	Options
Vecteur d'accès	Indique si la vulnérabilité est exploitable en local uniquement, mais aussi à partir de réseaux adjacents ou d'une connexion réseau ("exploitable à distance").	Local, Réseau adjacent, Réseau
Complexité de l'accès	Difficulté impliquée dans l'exploitation de cette vulnérabilité.	Elevée, Moyenne, Faible
Authentification	Nombre de fois qu'un pirate doit s'authentifier pour exploiter la vulnérabilité.	Aucune, Une, Plusieurs
Impact sur la confidentialité	Impact sur la confidentialité si cette vulnérabilité est correctement exploitée.	Aucun, Partiel, Complet
Impact sur l'intégrité	Etendue des risques pour l'intégrité du système (précision des informations fournies par l'application) si cette vulnérabilité est correctement exploitée.	Aucun, Partiel, Complet
Impact sur la disponibilité	Impact sur la disponibilité des ressources d'information si cette vulnérabilité est correctement exploitée.	Aucun, Partiel, Complet

Mesures temporelles

Il s'agit des mesures de vulnérabilité qui peuvent changer dans le temps.

Mesure	Explication	Options
Possibilité d'exploitation	Etat actuel des techniques d'exploitation qui utilisent cette vulnérabilité.	Non prouvé, Preuve de concept, Fonctionnel, Elevé, Non défini
Niveau de résolution	Niveau de résolution disponible pour se protéger de la vulnérabilité.	Correctif officiel, Correctif temporaire, Solution palliative, Non disponible, Non défini
Niveau de fiabilité du rapport	Degré de fiabilité dans l'existence et les détails techniques de la vulnérabilité.	Non confirmé, Non corroboré, Confirmé, Non défini

Mesures environnementales

Ces mesures reflètent l'environnement de l'application et doivent être définies de manière globale à l'aide de la boîte de dialogue Configuration et de l'onglet Mesures environnementales. Ne les modifiez ici que si cette vulnérabilité est spécifique à un composant de l'environnement d'application qui possède des caractéristiques différentes.

Mesure	Explication	Options
Dommage collatéral potentiel	Dommage ou vol potentiel si l'application est vulnérable.	Aucun, Faible, Moyennement faible, Moyen, Moyennement élevé, Elevé, Non défini
Distribution cible	Proposition des systèmes dans l'environnement qui sont des cibles potentielles.	Aucune, Faible, Moyenne, Elevée, Non définie
Exigence de disponibilité	Importance relative de la disponibilité (des informations).	Aucune, Faible, Moyenne, Elevée, Non définie
Exigence de confidentialité	Importance relative de la confidentialité (des informations utilisateur).	Aucune, Faible, Moyenne, Elevée, Non définie

Mesure	Explication	Options
Exigence d'intégrité	Importance relative de l'intégrité (précision) des informations.	Aucune, Faible, Moyenne, Elevée, Non définie

Restaurer les paramètres de gravité par défaut

Procédure

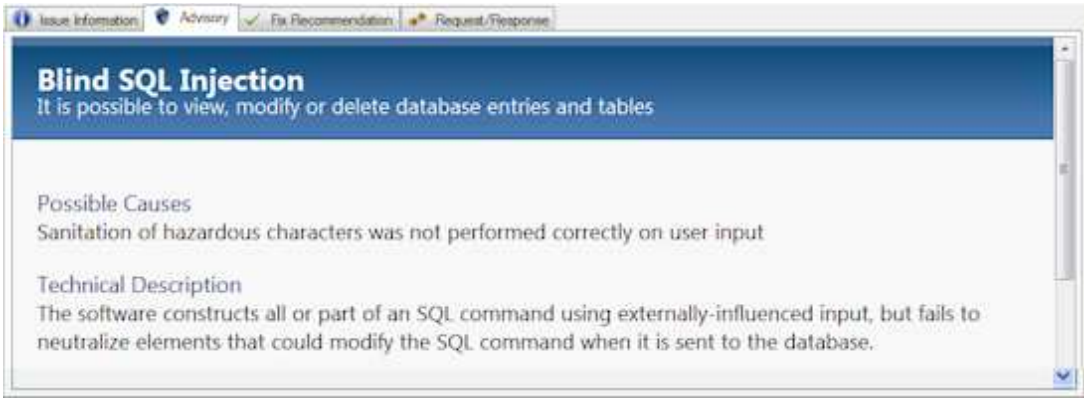
Si vous avez modifié manuellement le paramètre de gravité pour un problème particulier (en sélectionnant une autre gravité ou en ajustant les paramètres CVSS), vous pouvez restaurer le paramètre précédent.

- Pour remplacer votre paramètre manuel (Elevé/Moyen/Faible/Information) par un paramètre basé sur les paramètres CVSS en cours pour ce problème : dans la barre d'outils Informations sur les problèmes, cliquez sur **Gravité > Utiliser CVSS pour déterminer la gravité**.
- Pour restaurer les paramètres CVSS *par défaut* : Dans la barre d'outils Informations sur les problèmes, cliquez sur **Gravité > Paramètres CVSS**, et dans la fenêtre des paramètres CVSS qui s'ouvre, cliquez sur  .

Onglet Conseils

L'onglet Conseil est le deuxième de la sous-fenêtre.

Les informations présentes dans l'onglet Conseil fournissent des détails techniques sur le problème sélectionné et des liens de référence pour plus de détails. Ces informations sont essentielles lorsque vous devez expliquer ce qui est à corriger, et pourquoi.



L'onglet **Conseil** peut inclure toutes ou partie des sections suivantes :

Nom du test
Nom du test tel qu'il apparaît dans la liste des résultats.

Gravité
Niveau de gravité attribué à cette vulnérabilité.

Type Indique si cette vulnérabilité est au niveau application ou au niveau infrastructure.

Classification des menaces par le consortium WASC
Lien Internet à la page WASC (Web Application Security Consortium) décrivant cette classe de menace.

ID CVE
Références des normes de l'industrie pour ce type de vulnérabilité (voir «Support CVE», à la page 218.)

ID CWE
Références des normes de l'industrie pour ce problème (voir «Prise en charge de CWE».)

XFID ID X-Force de ce problème (voir «Support X-Force», à la page 219.)

Risque pour la sécurité
Explication sur le risque que ce problème fait courir à la sécurité de votre application.

Module de formation
Présentation Adobe Flash expliquant le problème.

Causes possibles
Suggère comment le problème a pu survenir dans votre application.

Description technique
Description technique détaillée du problème

Produits concernés
Produits tiers qui ont pu être affectés par le problème.

Références et liens appropriés
Liens vers des informations supplémentaires.

Support CVE

CVE (Common Vulnerabilities and Exposures) est une liste de normes de l'industrie fournissant des noms usuels à des expositions et vulnérabilités de sécurité publiquement connues, facilitant ainsi le partage de données entre des bases de données et des outils distincts. (Pour plus d'informations, voir le site Web CVE à l'adresse : http://cve.mitre.org/)

AppScan Les conseils fournis par sur les vulnérabilités auxquelles un ID CVE a été affecté, incluent la référence et un lien vers la description sur le site Web CVE. (Les ID CVE commencent par les lettres CVE pour les vulnérabilités acceptées ou CAN pour les vulnérabilités candidates.)

Vous pouvez :

- Afficher l'ID CVE d'un résultat de test dans les conseils relatifs au test (voir «Onglet Conseils», à la page 217)
- Cliquer sur l'ID CVE pour le lier à ses descriptions sur le site Web CVE
- Inclure des ID CVE (au sein des conseils) dans les rapports
- Afficher l'ID CVE testé par tout test particulier, dans la vue Stratégie de test (Configuration des examens > Stratégie de test ; voir «Vue Stratégie de test», à la page 109)
- Afficher la liste de tous les tests ayant des ID CVE en recherchant les chaînes CVE et CAN dans la vue Stratégie de test
- Rechercher un CVE particulier par la localisation de son ID dans la vue Stratégie de test

Prise en charge de CWE

CWE (Common Weakness Enumeration) est une liste de normes de l'industrie fournissant des noms usuels pour les faiblesses logicielles publiquement connues. facilitant ainsi le partage de données entre des bases de données et des outils distincts. (Pour plus d'informations, voir le site Web CWE à l'adresse : http://cwe.mitre.org/)

AppScan Les conseils d' relatifs aux vulnérabilités auxquels un ID CVE a été affecté incluent le numéro de référence et un lien vers la description sur le site Web CWE. Des vulnérabilités spécifiques ont leur propre ID CWE (en plus de l'ID *incident*) comme le montre la sous-fenêtre Détails de la variante.

Vous pouvez :

- Afficher l'ID CWE pour un incident dans les conseils (voir «Onglet Conseils», à la page 217)
- Afficher l'ID CWE pour une variante et un incident parent, dans l'onglet Détails de la variante (voir «Détails de la variante», à la page 221)

- Cliquez sur l'ID CWE pour le lier à sa description sur le site Web CWE
- Inclure les ID CWE ID (au sein de ces conseils) dans les rapports
- Rechercher un CWE particulier en localisant son numéro de référence dans la vue Stratégie de test

Pour connaître la version de la base de données CWE utilisée dans la version actuelle d'AppScan, reportez-vous aux Notes sur l'édition situées sous [répertoire_installationAppScan Standard]\Docs. Si une mise à jour journalière modifie la base de données utilisée, la modification sera enregistrée dans le journal des mises à jour (**Menu Aide > Journal des mises à jour**).

Support X-Force

X-Force est l'une des bases de données les plus complètes répertoriant les menaces et les vulnérabilités qui existent. Tous les conseils AppScan concernant les vulnérabilités incluent leur propre XFID, ainsi qu'un lien vers le site X-Force qui vous fournira des informations supplémentaires sur un problème de sécurité en particulier.

Vous pouvez effectuer les actions suivantes :

- Afficher l'XFID d'un problème dans le conseil concernant ce problème (voir «Onglet Conseils», à la page 217)
- Afficher l'XFID d'une variante, et le problème parent, dans l'onglet Détails de la variante (voir «Détails de la variante», à la page 221)
- Cliquer sur l'XFID pour le relier à sa description sur le site Web X-Force
- Inclure des XFID (faisant partie du conseil) dans des rapports
- Rechercher un XFID à l'aide de son numéro de référence dans la vue Stratégie de test

Onglet Recommandation de correction

Le troisième onglet de la sous-fenêtre des détails montre les correctifs recommandés.

Les informations contenues dans l'onglet Recommandation de correction sont les tâches exactes devant être exécutées pour sécuriser votre application Web face à un problème sélectionné spécifique.

L'onglet **Recommandation de correction** affiche les recommandations connues pour la correction du problème sélectionné. Ces solutions peuvent nécessiter des instructions pas à pas.

Les recommandations de correction sont triées de la façon suivante :

- **Général** - toujours sélectionné
- **.Net** - Microsoft .NET
- **Java EE** - Sun Java Platform, Enterprise Edition

Remarque : Vous pouvez définir AppScan de sorte que l'onglet Recommandation de correction, que vous ne trouvez pas approprié, soit masqué. Pour plus de détails, voir «Onglet Préférences», à la page 261.

Onglet Demande/Réponse

L'onglet Demande/Réponse est le quatrième de la Sous-fenêtre Détail.

L'onglet **Demande/Réponse** fournit des informations concernant les tests et leurs variantes spécifiques qui ont été transmis à votre application Web afin d'en découvrir les failles. Un test peut faire l'objet de différentes variantes. Une *variante* est une légère modification de la demande de test originale qu' AppScan envoie à votre serveur d'application Web. (AppScan envoie tout d'abord une demande censée être légale et suivre la logique métier de votre application. Ensuite, il envoie une demande similaire, modifiée afin de découvrir comment votre application gère les demandes illégales ou comportant des erreurs. Chaque demande de test peut se voir associer un certain nombre de variantes, autant que nécessaire pour couvrir toutes les règles de sécurité à tous les niveaux de la base de données AppScan.)

Prenons l'exemple d'un test qui est lancé pour vérifier que vous avez bien fait respecter les règles d'entrée utilisateur pour un paramètre spécifique. Une variante peut vérifier que les apostrophes ne constituent pas des entrées valides, cependant qu'une autre peut vérifier que les guillemets ne sont pas admis.

La variante elle-même est affichée avec un texte en rouge, et la validation (partie de la réponse indiquant l'existence d'un problème de sécurité) est mise en évidence en jaune.

En plus des nombreuses informations explicatives, l'onglet **Demande/Réponse** fournit des fonctions avancées pour la compréhension et l'utilisation des résultats d'un examen.

L'onglet **Demande/Réponse** comporte deux sous-fenêtres et une barre d'outils figure dans sa partie supérieure. La barre d'outils et les onglets sont présentés ci-dessous ; le tableau suivant contient un récapitulatif.

Outil	Fonction
Variante < >	Indique le nombre de variantes du test en cours. Cliquez sur les icônes **<** et **>** pour basculer respectivement de la variante précédente à la variante suivante.
Test/Original	Bascule entre les informations du test et les informations d'origine.
Mise en évidence suivante	(Disponible lorsque le texte de validation est mis en évidence). Déplace le curseur jusqu'au texte mis en évidence suivant.
Afficher dans le navigateur	Ouvre le navigateur intégré pour afficher la page en cours, ainsi que l'option permettant d'effectuer une capture d'écran à partir du navigateur. Lorsque le navigateur s'ouvre, vous pouvez prendre une capture d'écran de la page en cliquant sur l'icône de la caméra  dans la barre d'outils du navigateur. La capture d'écran est ajoutée à l'onglet Informations sur les problèmes.
Options > Rapport Faux positif	Permet d'envoyer la variante en cours par courrier électronique au service d'assistance AppScan ou dans votre entreprise. (Voir «Rapport Faux positif des résultats de test», à la page 222.)
Options > Test manuel	Modifie le test et l'enregistre en tant que test manuel. (Voir «Tests manuels», à la page 223.)
Options > Supprimer la variante	Supprime définitivement la variante sélectionnée des résultats du test (irréversible). Cette action peut également être effectuée en cliquant avec le bouton droit de la souris sur la variante dans la sous-fenêtre Résultat.

Outil	Fonction
Options > Définir comme non vulnérable	Modifie la définition de la variante sélectionnée par non vulnérable. Les réponses positives définies par l'utilisateur comme non vulnérables sont supprimées des résultats de l'examen et n'apparaissent plus dans les rapports, mais peuvent être visualisées (et réinstallées) via la liste des variantes non vulnérables. (Voir «Liste de variantes non vulnérables», à la page 226.)
Options > Définir comme page d'erreur	Ajoute la page en cours à la liste des pages d'erreur (boîte de dialogue Configuration de l'examen > Pages d'erreur) et met à jour les résultats pour refléter le fait que cette réponse est une page d'erreur.
Options > Ajouter aux informations sur le problème	Exécute Result Review sur le problème en cours et ajoute toute nouvelle information disponible à l'onglet Informations sur les problèmes.
Rechercher	Entrez le texte pour rechercher une chaîne spécifique. (Voir «Filtrage des problèmes de sécurité dans la Liste des résultats», à la page 211.)
Détails de la variante	La sous-fenêtre de droite affiche des informations détaillées sur la variante en cours : ID, Description, Différence (différence entre cette variante et la demande d'origine), Raisonnement et ID CWE.

Afficher des variantes

Pourquoi et quand exécuter cette tâche

Chaque test peut avoir plusieurs variantes appropriées, chacune d'elle modifiant légèrement une demande pour vérifier la sécurité de votre application face aux nombreuses techniques d'attaque.

Procédure

1. Cliquez sur **Tester**.
2. Cliquez sur les boutons flèche de droite ou de gauche pour visualiser les demandes de variante.

   Pour chaque test de variante envoyée, la partie modifiée de la demande est mise en évidence en rouge. Pour obtenir une explication plus détaillée de la variante, voir l'onglet **Détails de la variante**.

Détails de la variante

Détails de la variante dans un onglet latéral de l'onglet de réponse à la demande du panneau des détails.

L'onglet **Détails de la variante**, situé dans l'onglet **Demande/Réponse** du **panneau de détails**, décrit la variante et explique son objectif.

Section	Description
ID	Un numéro d'ID est attribué à chaque variante afin d'en faciliter la recherche et la gestion.
Description	Description brève du test
Différence	Affiche les modifications apportées à la demande initiale pour ce test. Les modifications sont mises en évidence en rouge. (Ces modifications peuvent être : modification de la valeur d'un paramètre, d'un cookie ou d'une méthode ; modification d'un chemin ; suppression d'un paramètre, suppression ou ajout d'un en-tête HTTP ; suppression ou ajout d'un paramètre au corps.)
Raisonnement	Explique pourquoi le résultat du test indique une vulnérabilité.
ID CVE	ID CVE de la vulnérabilité (voir «Support CVE», à la page 218).
ID CWE	ID CWE de la variante et du problème parent. (Voir «Prise en charge de CWE», à la page 218).

Prise de captures d'écran

Vous pouvez prendre des captures d'écran de votre application qui montrent la vulnérabilité, pour les inclure dans des rapports.

Procédure

1. Sélectionnez un élément dans la **liste des résultats** et accédez à la variante requise.
2. Dans l'onglet **Sous-fenêtre Détail > Demande/Réponse**, cliquez sur **Afficher dans le navigateur**.
3. Dans le navigateur, cliquez sur l'**icône Caméra**  .

   Une capture d'écran de la page en cours est ajoutée aux données dans l'onglet Informations sur les problèmes et sera incluse dans les rapports.

Rapport Faux positif des résultats de test

Vous pouvez envoyer les informations de test par courrier électronique au support AppScan pour :

- rapporter un résultat classé par AppScan comme positif (indiquant une vulnérabilité) mais que vous pensez négatif (*n'indiquant pas* une vulnérabilité.
- demander au support AppScan pour quelle raison un résultat a été classé comme positif.

Vous pouvez également utiliser la fonction permettant de zipper le résultat et de l'envoyer par courrier électronique aux développeurs et auditeurs de votre propre organisation.

Remarque : Par défaut, AppScan enregistre les données dans un format chiffré accessible uniquement au service d'assistance. Si vous envoyez le fichier au sein de votre propre organisation, vous devez configurer AppScan pour qu'il enregistre les informations sous la forme d'un fichier .zip. Dans **Outils | Options | onglet Général**, décochez la case **Encrypt Attachments**.

Rapporter une seule variante fausse positive

Procédure

1. Sélectionnez un élément dans la **Liste de résultats**.
2. Dans la **sous-fenêtre Détail > onglet Demande/Réponse**, accédez aux variantes du problème sélectionné.
3. Lorsque la variante que vous souhaitez envoyer s'affiche, cliquez sur **Rapport Faux positif** dans la barre d'outils du Panneau des détails.

   La boîte de dialogue Rapport Faux positif s'ouvre.
4. Cliquez sur Sauvegarder le fichier et enregistrez le fichier sur le disque.

   Selon votre paramètre de chiffrement (voir ci-dessous), le fichier est sauvegardé codé ou au format .zip.
5. Pour envoyer le fichier au service d'assistance d'AppScan, cliquez sur le lien **Browse to your support provider** (Accéder au site de votre fournisseur de support), connectez-vous et téléchargez le fichier.

Rapporter un ensemble de variantes faux positif

Pourquoi et quand exécuter cette tâche

Vous pouvez rapporter toutes les informations de variante de n'importe quel problème, URL ou élément enfant dans une seule pièce jointe à l'aide du menu clic droit de la liste des résultats.

Procédure

1. Dans la **liste des résultats**, cliquez avec le bouton droit de la souris sur un problème, une URL ou un paramètre, et sélectionnez **Rapport Faux positif**.

   La boîte de dialogue Rapport Faux positif s'ouvre.
2. Cliquez sur Sauvegarder le fichier et enregistrez le fichier sur le disque.

   Selon votre paramètre de chiffrement (voir ci-dessous), le fichier est sauvegardé codé ou au format .zip.

   Remarque : Par défaut le fichier est chiffré. Pour modifier ce paramètre accédez à **Outils > Options > Générales > Rapport Faux positif**, et désélectionnez la case **Encrypt attachments** (Crypter les pièces jointes).
3. Pour envoyer le fichier au service d'assistance d'AppScan, cliquez sur le lien **Browse to your support provider** (Accéder au site de votre fournisseur de support), connectez-vous et téléchargez le fichier.

Chiffrement de rapports faux positifs

Pourquoi et quand exécuter cette tâche

Par défaut, la fonction Rapport Faux positif enregistre les données dans un format chiffré que seul le personnel du support AppScan peut ouvrir.

Si vous comptez envoyer la pièce jointe au sein votre organisation, le destinataire ne pourra pas la décoder ; vous devez donc désactiver la fonctionnalité de chiffrement.

Procédure

1. Cliquez sur **Outils > Options > Général > Rapport Faux positif**.
2. Cochez/décochez la case de chiffrement des pièces jointes (**Encrypt attachments**) comme nécessaire.

Tests manuels

Pourquoi et quand exécuter cette tâche

La fonction **Test manuel** permet d'envoyer vos propres tests et de les sauvegarder en tant que problèmes de sécurité à inclure à vos rapports.

Vous ne pouvez créer un test manuel que lorsque vous avez obtenu les résultats d'exploration. Les tests manuels sont uniquement sauvegardés pour l'examen en cours. Notez que si vous effectuez un nouvel examen, le test sera perdu.

Vous pouvez baser votre test manuel sur un test existant ou en créer un nouveau de toute pièce.

Procédure

1. Pour baser le test manuel sur une variante existante :
   - dans la **Liste des résultats**, cliquez sur une variante de test ou
   - dans la **liste des résultats**, cliquez sur un test, puis dans la **sous-fenêtre Détail**, utilisez la barre d'outils pour accéder à la variante requise.

   Sinon, pour créer une nouvelle variante de toute pièce, ouvrez simplement la boîte de dialogue **Test manuel** (étape suivante) sans sélectionner de variante existante.
2. Ouvrez la boîte de dialogue **Test manuel** :
   - Dans le menu **Outils**, cliquez sur **Test manuel** ou
   - Cliquez avec le bouton droit de la souris sur un nœud dans l'**Arborescence de l'application** ou dans la **liste des résultats**, puis sélectionnez **Test manuel** dans le menu contextuel, ou

- Cliquez sur le bouton **Test manuel** dans **Données d'application > sous-fenêtre Détail** pour la variante sélectionnée.

La boîte de dialogue **Test manuel** apparaît, affichant les propriétés de la variante de test sélectionnée.

3. Dans la zone **Nom d'hôte/Adresse IP**, entrez le serveur auquel le test sera envoyé.
4. Dans la zone **Port**, entrez le port à utiliser par AppScan pour atteindre le serveur.

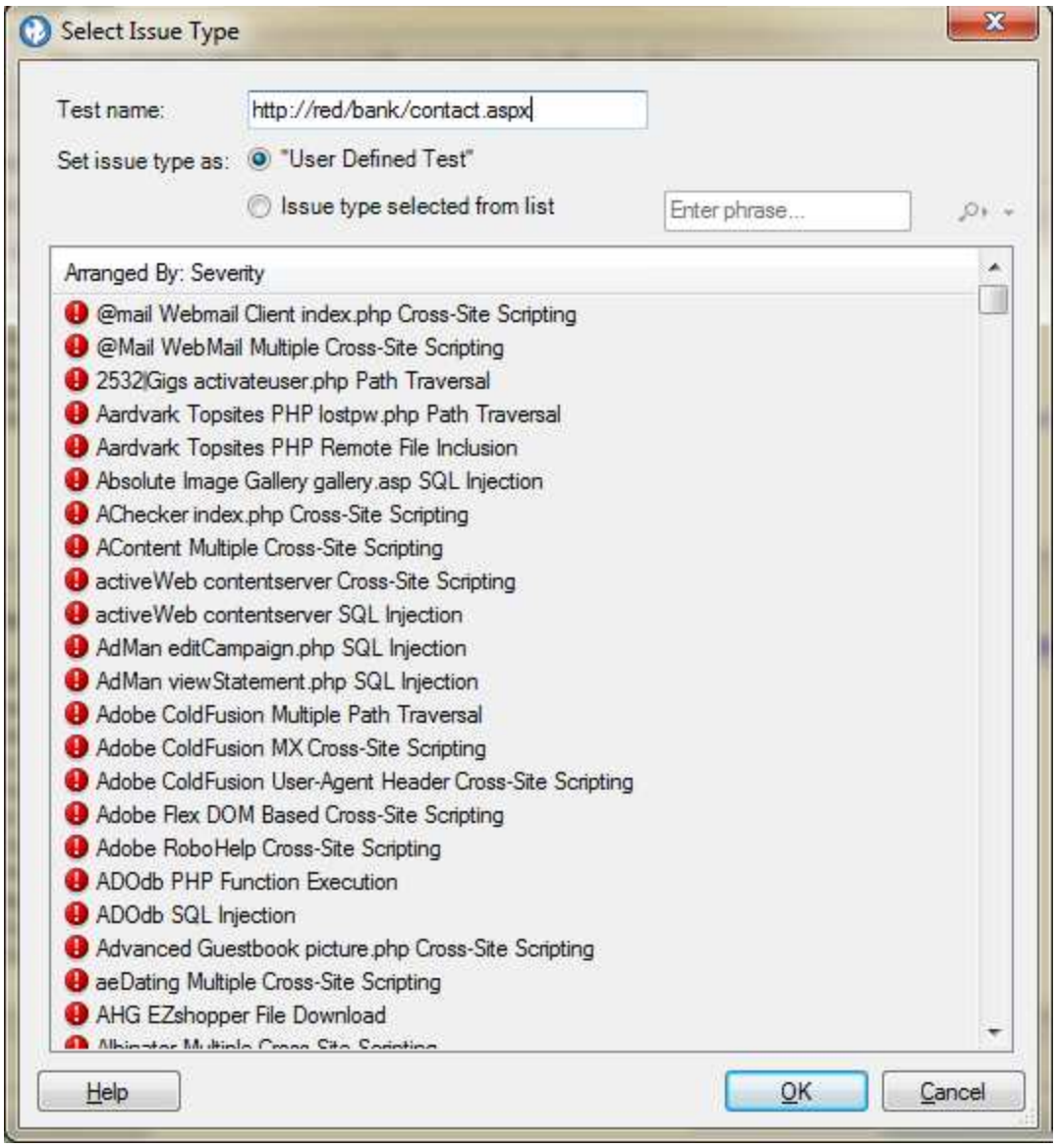
   Le port par défaut est **80** ; à moins que SSL soit sélectionné, auquel cas le port par défaut est **443**.
5. Si nécessaire, vous pouvez éditer la **Demande**.
6. Dans la liste **Options**, sélectionnez ou désélectionnez les options suivantes :

Option	Cliquer sur
SSL	Envoyer la demande via SSL.
Se connecter avant d'envoyer la demande	Envoyer une demande de connexion à l'application avant d'envoyer le test manuel.
Longueur automatique du contenu	Mettre automatiquement à jour l'en-tête **Content-Length HTTP** dans la demande selon la valeur égale au contenu de la demande lorsque vous l'éditez. Si cette option est sélectionnée, l'utilisateur ne peut pas éditer la valeur de la longueur du contenu. Si l'en-tête de la demande ne comprend pas le paramètre **Content-Length**, cette option n'a aucun effet.

7. Cliquez sur **Envoyer**.

   La demande est envoyée et la réponse s'affiche dans la zone de saisie **Réponse** (panneau inférieur).
8. Pour visualiser la réponse dans le navigateur intégré, cliquez sur **Afficher dans le navigateur**.
9. Pour ajouter ce test manuel à l'examen en cours, cliquez sur **Sauvegarder**.

   La boîte de dialogue **Sélectionner le type de problème** apparaît, avec le bouton radio **Test défini par l'utilisateur** sélectionné par défaut.



10. Dans la zone **Nom du test**, vous pouvez laisser le nom par défaut (l'URL) ou définir un nouveau nom.
11. Pour enregistrer le test sous un type de test existant (plutôt que sous le type de test défini par l'utilisateur par défaut), sélectionnez le deuxième bouton radio puis cliquez sur un type de test dans la liste.

    Remarque : Pour localiser un problème dans la liste avec la fonction Rechercher, tapez une partie du nom du problème dans la zone Rechercher. Cliquez sur l'icône de loupe pour passer d'un résultat de recherche à un autre.
12. Cliquez sur **OK**.

    La boîte de dialogue se ferme. Le nouveau test est ajouté aux résultats et sera inclus lorsque vous continuerez l'examen en cours (**Examen > Continuer > Examen/Test**).

    Remarque : Si vous procédez à un nouvel examen, le test n'est pas inclus.

Variantes non vulnérables

Lors d'un examen, AppScan envoie plusieurs milliers de variantes de test au site qu'il teste. La plupart des réponses indiquent qu'il n'y a aucune menace concernant la sécurité, et AppScan annule par défaut tous ces résultats "non vulnérables".

- Si nécessaire, vous pouvez configurer AppScan pour enregistrer toutes les variantes non vulnérables.
- Vous pouvez également modifier l'état de résultats individuels en "non vulnérables".

«Sauvegarder toutes les variantes non vulnérables»

«Définir des variantes comme non vulnérables»

«Liste de variantes non vulnérables»

«Supprimer des variantes», à la page 227

Sauvegarder toutes les variantes non vulnérables

Pourquoi et quand exécuter cette tâche

Vous pouvez configurer AppScan pour qu'il enregistre toutes les variantes de test non vulnérables, si vous souhaitez les vérifier.

ATTENTION :
La sauvegarde des informations de variante de test non vulnérable peut ralentir la performance d'AppScan et augmenter de façon significative l'espace disque requis.

Procédure

Dans **Configuration des examens > Options de test**, cochez la case **Sauvegarder les informations sur les variantes de test non vulnérables**.

Définir des variantes comme non vulnérables

Pourquoi et quand exécuter cette tâche

Lorsque vous définissez une variante de test comme *non vulnérable*, elle ne s'affiche pas dans les résultats de l'examen ou n'est pas incluse dans les rapports. Vous conservez cependant la possibilité de visualiser ses détails (via la «Liste de variantes non vulnérables») et de la réintégrer plus tard si nécessaire.

Procédure

Procédez de l'une des façons suivantes :

- Dans la Liste des résultats, cliquez avec le bouton droit de la souris et sélectionnez **Définir comme non vulnérable**.
- Sélectionnez la variable dans la Liste des résultats et dans la barre d'outils Demande/Répons et cliquez sur **Définir comme non vulnérable**.

La variante est supprimée de l'affichage des résultats d'examen et ne sera pas incluse dans les rapports.

Liste de variantes non vulnérables

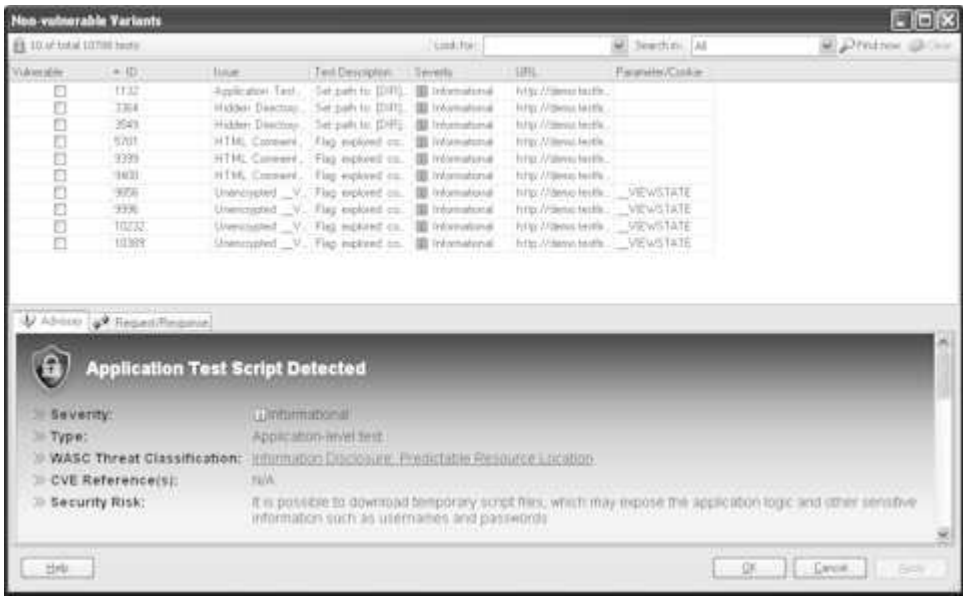
La liste de variantes non vulnérables permet de visualiser des détails de variantes non vulnérables ayant été enregistrés avec les résultats de l'examen et de les réintégrer si nécessaire.

Les variantes peuvent être ajoutées à cette liste de deux manières :

- AppScan a été configuré pour sauvegarder les informations de variantes de test non vulnérables (voir «Vue Options de test», à la page 114).
- Vous avez modifié manuellement un résultat catégorisé par AppScan comme "vulnérable" en "non vulnérable" (voir description dans la précédente section).

Afficher des variantes non vulnérables
Procédure

Dans le menu **Affichage**, cliquez sur **Variantes non vulnérables**.



Réintégrer des variables non vulnérables comme vulnérables
Procédure

1. Cochez la case pour une ou plusieurs variantes de la liste des variantes non vulnérables que vous souhaitez réintégrer comme vulnérables.
2. En bas de la boîte de dialogue, cliquez sur **Appliquer**.
3. Cliquez sur **OK** pour confirmer.

Supprimer des variantes
Pourquoi et quand exécuter cette tâche

Lorsque vous supprimez des variantes (au lieu de les définir comme non vulnérables), elles sont toutes supprimées des résultats de l'examen et ne peuvent pas être réintégrées par la suite. (Pour y accéder de nouveau, vous devrez exécuter un nouvel examen.)

Procédure

Procédez de l'une des façons suivantes :

- Dans la Liste des résultats, cliquez avec le bouton droit de la souris et sélectionnez **Supprimer**.
- Sélectionnez la variante dans la Liste des résultats, et cliquez sur **Supprimer la variante** dans la barre d'outils Demande/Réponse.

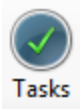
La variante est supprimée des résultats de l'examen et ne sera pas incluse dans les rapports.

Chapitre 9. Résultats : Tâches de résolution

AppScan offre trois manières de visualiser et d'utiliser les résultats de l'examen : Problèmes de sécurité, Tâches de résolution et Données d'application. La présente section décrit la vue Tâches de résolution.

La vue Tâches de résolution fournit des solutions conçues pour aborder les problèmes identifiés lors d'un examen. Une tâche de résolution aborde généralement un certain nombre de problèmes de sécurité.

Dans la vue **Afficher le sélecteur**, cliquez sur :



.

Tâches de résolution : Arborescence de l'application

L'**Arborescence de l'application** affiche les dossiers et les fichiers de l'application examinée. Chaque nœud de l'arborescence dispose d'un compte qui présente le nombre de tâches de résolution contenues dans le nœud. Le compte de chaque nœud est identique ou inférieur au compte de la vue **Problèmes**, car de nombreux problèmes peuvent être adressés par une seule tâche de résolution.

L'**Arborescence de l'application** affiche des tâches de résolution dans les niveaux suivants :

- **Nom de tâche**
- **URL**
- **Paramètre** ou **Cookie**

Une seule tâche conçue pour un problème trouvé sur plusieurs URL est répertoriée une seule fois avec les URL indiquées en dessous.

Sélectionnez un nœud dans l'**Arborescence de l'application** pour filtrer la **liste des résultats** qui affichera uniquement les résultats du nœud sélectionné.

Tâches de résolution : Liste de résultats

La **liste des résultats** affiche les tâches de résolution appropriées pour le nœud sélectionné dans l'**Arborescence de l'application**. Si vous avez sélectionné le nœud **Mon application**, la **liste des résultats** présente toutes les tâches de résolution appropriées pour votre application.

Les tâches de résolution sont regroupées par type de résolutions pouvant être effectuées pour remédier aux problèmes. A chaque élément de résolution correspond une icône qui indique la priorité de la tâche à effectuer et un compte qui indique le nombre de fichiers, de paramètres ou de cookies qui seront affectés par cette résolution.

Chaque tâche peut contenir des URL, qui peuvent contenir des fichiers, des paramètres et des cookies. Vous pouvez modifier le tri des résolutions ainsi que les ordres de priorité.

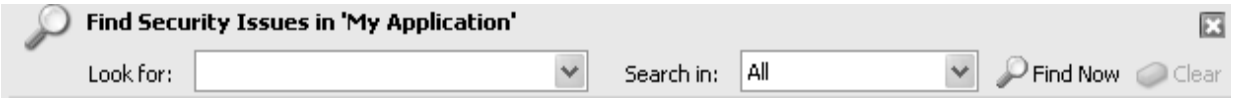
Rechercher des tâches de résolution dans la Liste des résultats

Pourquoi et quand exécuter cette tâche

Vous pouvez filtrer la **liste des résultats** à la recherche de types de tâches de résolution ou d'une résolution spécifique.

Procédure

1. Dans le menu **Edition**, cliquez sur **Rechercher** (ou appuyez sur **Ctrl + F**).
   La barre **Rechercher** apparaît dans la fenêtre principale, au-dessus de la **liste des résultats**.



2. Dans l'**Arborescence de l'application**, sélectionnez un nœud.
   - Si vous sélectionnez le nœud **Mon application**, la recherche se fait parmi tous les résultats.
   - Si vous sélectionnez un nœud dans l'arborescence, la recherche se fait dans le nœud sélectionné et ses sous-nœuds.
3. Dans la zone de saisie **Rechercher** de la barre **Rechercher**, entrez une chaîne ou une partie de chaîne.
4. Dans la liste **Rechercher dans**, sélectionnez la partie de la résolution dans laquelle vous souhaitez rechercher :

Rechercher dans	Pour trouver une chaîne dans
Résolution	nom de la résolution tel qu'il apparaît dans la liste des résultats
URL	nom de chemin des URL pour lesquelles les résultats de résolution sont appropriés
Détails	détails de la tâche de résolution
Tous	toutes les options ci-dessus

5. Cliquez sur **Rechercher maintenant** ou appuyez sur **Entrée**.
   Les résultats apparaissent dans la **liste des résultats**, écrasant la liste précédemment affichée. Si vous entrez une autre chaîne **Rechercher** et cliquez à nouveau sur **Rechercher maintenant**, la nouvelle recherche est réalisée sur le nœud sélectionné dans l'**Arborescence de l'application**, et non sur les résultats affichés de la précédente recherche.

Exemple

Pour rechercher	Rechercher	Rechercher dans
Tâches de résolution concernant les répertoires virtuels :	`"virtual direc"`	Résolution

Pour rechercher	Rechercher	Rechercher dans
Tâches de résolution concernant les pages de connexion :	"login"	URL

Trier les tâches de résolution

Pourquoi et quand exécuter cette tâche

Vous pouvez réorganiser les tâches de résolution dans la **Liste de résultats**. Par défaut, les tâches sont triées par priorité.

Procédure

1. Cliquez sur l'en-tête de colonne **Classés par.**
   Un menu apparaît.
2. Cliquez sur une commande du menu pour trier les résolutions :
   - **Priorité** - Les noms de tâche sont répertoriés par ordre de priorité, de la priorité Elevée à la priorité Faible.
   - **Nombre** - Nombre d'URL, de paramètres et de cookies affectés. Les tâches résolvant la majorité des problèmes sont répertoriées les premières.
   - **Nom** - Ordre alphabétique par nom de tâche.

   Les tâches de résolution sont à nouveau triées dans la **Liste des résultats**.

   Pour inverser l'ordre de tri (ascendant ou descendant), cliquez sur la deuxième colonne de la **Liste des résultats**. Cliquez de nouveau sur la deuxième colonne pour revenir à l'ordre précédent.

Manipuler les niveaux de priorité

Pourquoi et quand exécuter cette tâche

Les icônes des tâches de résolution indiquent leurs niveaux de priorité. Le tableau suivant explique ces icônes.

Icône	Indique
	Tâche de priorité élevée
	Tâche de priorité moyenne
	Tâche de priorité faible

Une priorité est affectée aux tâches de résolution en fonction de la gravité du problème. Si la gravité est Elevée, la priorité est élevée ; si elle est Moyenne, la priorité est moyenne ; et si elle est Faible ou Information, la priorité est faible.

Vous pouvez afficher les paramètres de priorité par défaut comme point de départ. Vous pouvez modifier la priorité affectée aux tâches de résolution. Le nouveau paramètre de priorité affecte toutes les résolutions ayant le même nom de tâche.

Procédure

Dans la **liste des résultats**, cliquez avec le bouton droit de la souris sur une tâche de résolution et sélectionnez **Priorité > Elevée/Moyenne/Faible**.
L'icône de la tâche de résolution change pour correspondre à la nouvelle priorité.

Supprimer des tâches de résolution de la Liste des résultats

Pourquoi et quand exécuter cette tâche

Vous pouvez supprimer une tâche de la **Liste de résultat**, qui supprimera le nœud sélectionné et tous les objets contenus dans ce nœud.

Procédure

1. Dans la **Liste de résultats**, cliquez avec le bouton droit de la souris sur un noeud.
2. Dans le menu qui s'affiche, cliquez sur **Supprimer**.

   Un message s'affiche, vous demandant de confirmer la suppression et vous rappelant que les données des tests seront définitivement supprimées.
3. Cliquez sur **Oui**.

   La tâche de résolution est supprimée ; ce qui n'affecte pas les problèmes. Ces derniers seront toujours disponibles à partir de la vue Problèmes.

Tâches de résolution : Panneau des détails

Le **Panneau des détails** de la vue Résolutions contient un onglet. Il affiche la tâche de résolution actuellement sélectionnée dans la **Liste des résultats**.

Les informations dans le **Panneau des détails** incluent : Nom de tâche, Problèmes (liste des résultats d'examen adressée par cette tâche) et Détails (une ou plusieurs solutions possibles).

Chapitre 10. Rapports

La présente section explique comment générer des rapports à partir des résultats de l'examen.

Concepts associés:

«Exporter les résultats de l'examen», à la page 193

Présentation des rapports

Une fois que AppScan a évalué la vulnérabilité de votre site, vous pouvez générer des rapports personnalisés configurés pour le personnel de votre organisation (développeurs, auditeurs internes, testeurs d'effraction, responsables, cadres).

Les cinq types de rapports de base disponibles sont décrits ci-dessous. Le rapport de sécurité comprend de nombreuses options pouvant être incluses ou exclues selon la personne à laquelle il est destiné.

Vous pouvez ouvrir et visualiser les rapports depuis AppScan, et vous pouvez sauvegarder un rapport sous la forme d'un fichier s'ouvrant à l'aide d'une application tiers telle qu'Acrobat Reader.

Icône	Nom	Brève description
	«Rapports de sécurité», à la page 235	Rapport des problèmes de sécurité trouvés lors de l'examen. Les informations de sécurité peuvent être très importantes et peuvent être filtrées selon vos besoins. Six modèles standard sont inclus, mais chacun d'eux peut facilement être ajusté de manière à inclure ou exclure des catégories d'informations, selon les besoins.
	«Rapports sur les normes de l'industrie», à la page 238	Rapport de la conformité (ou non-conformité) de votre application avec un comité d'industries, ou votre propre liste de contrôle standard personnalisée.
	«Rapports sur la conformité à la réglementation» , à la page 240	Rapport de la conformité (or non-conformité) de votre application avec un large choix de règles ou de normes juridiques, ou avec votre propre modèle de conformité légale personnalisé.
	«Rapport de l'analyse des écarts», à la page 251	Le rapport de l'analyse des écarts compare deux ensembles de résultats d'examens et affiche la différence dans les URL et/ou problèmes de sécurité détectés.
	«Rapports basés sur un modèle» , à la page 253	Rapport personnalisé contenant des données définies par l'utilisateur et un formatage des documents également défini par l'utilisateur, aux formats DOC et DOCX de Microsoft Word.

Configurer la présentation d'un rapport

L'onglet Présentation de la boîte de dialogue Créer un rapport permet de personnaliser l'affichage de vos rapports. (Cette fonction est facultative, vous pouvez simplement générer des rapports à l'aide des présentations par défaut.)

Procédure

1. Dans la boîte de dialogue **Créer un rapport**, cliquez sur l'onglet **Présentation**.
2. Sélectionnez les options de présentation que vous souhaitez et entrez les valeurs appropriées :

Options de présentation	Description
Inclure la page de garde	Ajoute une page de garde à votre rapport. Si cette option est sélectionnée, les options de la page de garde sont activées.
Logo de la société	Inclut le logo de votre société en haut à gauche de la page de garde. (Cliquez sur dans la zone Logo de la société et accédez au fichier de logo de votre ordinateur.) Le logo AppScan est le logo par défaut.
Logo supplémentaire	Inclut un logo supplémentaire en haut à droite de la page de garde. (Cliquez sur dans la zone Logo de la société et accédez au fichier de logo de votre ordinateur.)
Type de rapport	Inclut le type de rapport (texte non éditable) dans la partie inférieure de la page de garde.
Titre du rapport	Inclut le titre par défaut, ou un titre que vous entrez, comme titre principal au centre de la page de garde.
Description	Inclut la description par défaut, ou une description que vous entrez, comme description sur la page de garde.
Date du rapport	Inclut la date dans le pied de page de chaque page intérieure du rapport.
En-tête/Pied de page	Ajoute un en-tête et/ou un pied de page à chaque page intérieure. Entrez le texte que vous souhaitez voir apparaître.
Table des matières	Inclut une table des matières dans le rapport.
Sauvegarder comme présentation par défaut	Sauvegarde les paramètres de présentation et le texte en vue d'un usage ultérieur.

Visualiser et sauvegarder des rapports

Les rapports peuvent être générés et affichés dans l'Afficheur de rapports d'AppScan et sauvegardés sous différents formats.

Procédure

1. Configurez le type de rapport, le modèle et les filtres, si nécessaire.
2. Pour afficher un aperçu de l'afficheur de rapports, cliquez sur **Prévisualisation**.
3. Pour enregistrer le rapport, cliquez sur **Enregistrer le rapport**, nommez le rapport puis sélectionnez un format : PDF (Adobe Acrobat Reader), HTML (navigateur Web), RTF (Microsoft Word) ou TXT (éditeur de texte).

   Remarque : Si vous avez précédemment sauvegardé un rapport dans un format et que vous souhaitez maintenant le sauvegarder dans un autre format, vous devez le faire avec un autre nom de fichier. Par exemple : Si vous avez précédemment sauvegardé un rapport nommé Report458.pdf et que vous souhaitez maintenant le sauvegarder au format RTF, vous ne pouvez pas le sauvegarder sous le nom Report458.rtf, mais vous pouvez le faire sous le nom Report_458.rtf.

Création de rapports partiels

Vous pouvez créer un Rapport de sécurité ou un Rapport basé sur un modèle pour un sous-ensemble de résultats d'examen en cliquant avec le bouton droit de la souris sur l'adresse URL ou le dossier pour lequel vous voulez créer le rapport.

Procédure

1. Dans l'Arborescence de l'application, cliquez avec le bouton droit de la souris sur l'adresse URL ou le dossier pour lequel vous voulez créer le rapport puis sélectionnez :
   - **Rapport pour ce nœud > Sécurité**
   - **Rapport pour ce nœud > Basé sur un modèle**

La boîte de dialogue Créer un rapport qui s'ouvre contient des options de rapport pour le nœud sélectionné.

2. Continuez comme pour un rapport standard.
   - «Rapports de sécurité»
   - «Rapports basés sur un modèle», à la page 253

Versions antérieures des modèles de rapport

Des versions antérieures de certains modèles de rapport sur la conformité aux normes de l'industrie et à la réglementation sont enregistrées dans le dossier "Old Versions".

Pourquoi et quand exécuter cette tâche

La boîte de dialogue Rapports liste les dernières versions des modèles de rapport. Cependant, dans le cas de certains rapports sur la conformité aux normes de l'industrie et à la réglementation, des versions antérieures sont enregistrées dans un dossier particulier. Ce dossier se trouve dans `[dossier d'installation AppScan Standard]\Regulations\Old Versions`.

Procédure

1. Dans la boîte de dialogue Rapports, sélectionnez **Normes de l'industrie** ou **Conformité à la réglementation**.
2. Dans l'onglet Type de rapport, sélectionnez **Défini par l'utilisateur**.
3. Cliquez sur **Parcourir...** et accédez à `[dossier d'installation AppScan Standard]\Regulations\Old Versions`.

   Pour le japonais, l'emplacement par défaut est `[dossier d'installation AppScan Standard]\ja-JP\Regulations\Old Versions`.
4. Sélectionnez le fichier requis et continuez comme pour la création d'un rapport standard.

Rapports de sécurité

Le rapport de sécurité fournit des informations sur les problèmes de sécurité détectés. Vous pouvez effectuer une sélection parmi plusieurs modèles en fonction du type de contenu requis.

Pourquoi et quand exécuter cette tâche

Vous pouvez créer un rapport de sécurité englobant tout l'examen ou un rapport concernant une adresse URL ou un dossier particulier dans l'arborescence d'application.

Chaque modèle de rapport est un ensemble de rubriques appropriées aux différents destinataires au sein de votre organisation. Les rubriques contiennent les résultats d'examen de chacune des vues (Problèmes de sécurité, Tâches de résolution, Données d'application), formatés pour en faciliter l'impression, la lisibilité ainsi que la compréhension de leur signification, de la raison pour laquelle ils sont appropriés, et de la manière de les corriger.

Options du rapport de sécurité

Le tableau suivant récapitule les options de la boîte de dialogue Rapports de sécurité.

Option	Description
Modèle	Sélectionnez l'un des différents modèles de rapport ou définissez votre propre modèle, en cochant/décochant les cases dans la sous-fenêtre de droite, comme indiqué dans le tableau suivant. • **Valeur par défaut :** rapport de niveau intermédiaire contenant un récapitulatif de haut niveau et des informations sur les problèmes, sans les détails des variantes. • **Résumé :** récapitulatif de haut niveau mettant en évidence les risques de sécurité trouvés dans votre application Web et contenant les statistiques des résultats d'examen, présentés sous forme de tableaux et de graphiques. • **Détaillé :** rapport approfondi contenant le récapitulatif ainsi que des problèmes de sécurité, des conseils et recommandations de correction, des tâches de résolution et des données d'application. • **Tâches de résolution :** actions conçues pour résoudre les problèmes détectés dans l'examen. • **Développeur :** problèmes de sécurité, variantes, conseils et recommandations de correction, sans les sections Récapitulatif ou Tâches de résolution. • **Assurance qualité :** problèmes de sécurité, conseils et recommandations de correction, données d'application, sans les informations détaillées sur les variantes ni les sections Récapitulatif ou Tâches de résolution. • **Inventaire de fichiers :** données d'application uniquement. • **Tutoriel sur les modèles personnalisés :** cette option vous permet de créer un modèle personnalisé de Rapport de sécurité à l'aide des cases à cocher afin de définir le rapport que vous souhaitez, puis en cliquant sur **Créer comme modèle**. Une fois sauvegardé, ce modèle peut servir à générer des rapports, aussi bien à partir de l'interface utilisateur que de l'interface en ligne de commande. – **Sauvegarder comme modèle :** sauvegarde la configuration actuelle du Rapport de sécurité en tant que modèle personnalisé. – **Supprimer le modèle :** supprime le modèle personnalisé actuel.
Min. Gravité	Sélectionnez le niveau le plus faible de gravité pour les problèmes à inclure dans le rapport.
Type de test	Sélectionnez les types de travaux à inclure dans la liste des résultats : **Tous, Application, Infrastructure** ou tests **Composant Web tiers**.
Classer par	Indiquez si les problèmes doivent être classés par type ou adresse URL.
Limiter le nombre de variantes par problème	Vous pouvez réduire la longueur du rapport en limitant le nombre de variantes répertoriées par problème, si ce niveau de détail risque de ne pas être utile au destinataire du rapport.
Ajouter un saut de page après chaque problème	Ce paramètre s'applique uniquement à une sortie PDF. Il rend le rapport plus lisible.
Afficher une fois terminé	Si vous cochez cette case, le rapport s'ouvre dans un afficheur approprié après avoir été généré. **Remarque :** Cette opération n'est réalisable que si vous avez installé un programme pouvant ouvrir le rapport généré.

Après avoir sélectionné un modèle comme base, vous pouvez personnaliser la structure de rapport individuelle en sélectionnant/désélectionnant les zones d'informations à inclure. Dans ce cas, le nom du modèle devient "Personnalisé".

Sections du rapport de sécurité

Le tableau suivant présente un récapitulatif du contenu standard des divers rapports de sécurité. Dans tous les cas, le contenu réel peut être modifié en cochant/décochant les cases du panneau Contenu du rapport.

Remarque : Un rapport détaillé complet pouvant comprendre des centaines de pages, pensez à inclure seulement les sections appropriées aux destinataires du rapport.

Section Rapport	Description
Introduction	Courte section fournissant des informations générales sur l'examen, par exemple des détails tel que le nombre global de problèmes détectés (Elevé, Moyen, Faible et Message d'information) et les paramètres de connexion. Cette section figure dans tous les rapports.
Récapitulatif	Série de tableaux récapitulant les informations suivantes sur l'examen, ou la partie de l'examen comprise dans le rapport : • Types de problèmes (comprend le nombre problèmes trouvé pour chaque type et leur gravité) • Adresse URL vulnérables (comprend le nombre et le type de problèmes par adresse URL) • Recommandations de correction • Risques de sécurité • Causes • Classification des menaces WASC
Problèmes de sécurité	Problèmes trouvés dans votre application : • De base : si vous ne sélectionnez aucune des cases à cocher suivantes, seules les informations de base sont inclues. • Supplémentaire : comprend des informations plus détaillées, dont des captures d'écran, comme pour le contenu de l'onglet Informations sur les problèmes • Variantes : comprend des informations de variante spéciales : – Demande/réponse – Différence : différence entre la demande d'origine et la demande de test, telle qu'elle est indiquée dans la sous-fenêtre Détail > onglet Demande/Réponse
Conseils et recommandations de correction	Explications techniques des problèmes trouvés et recommandations pour les corriger. **Remarque :** Pour inclure des recommandations de correction spécifiques aux environnements .NET, Java EE et PHP, accédez à Outils > Options > Préférences et sélectionnez les options requises.
Tâches de résolution	Suggestions de tâches permettant d'améliorer la sécurité du site en fonction des problèmes trouvés. Une seule tâche peut parfois résoudre plusieurs problèmes.
Données d'application	Liste des données trouvées par AppScan dans votre application Web : adresses URL d'application, paramètres de script, liens rompus, commentaires, JavaScripts, cookies et adresses URL filtrées.

Procédure

1. Sélectionnez le contenu de l'examen sur lequel baser le rapport :
   - Pour créer un rapport pour la totalité de l'examen, cliquez sur **Outils > Rapport > Rapport de sécurité**
   - Pour créer un rapport pour une adresse URL ou un dossier inclus dans l'examen, cliquez avec le bouton droit de la souris sur l'arborescence d'application, puis sélectionnez **Rapport pour ce noeud > Sécurité**.
2. Sélectionnez le modèle pertinent, ou définissez votre propre contenu de rapport en activant/désactivant les cases à cocher dans la sous-fenêtre de droite.
3. Sélectionnez les options requises.
4. Pour sauvegarder la configuration en vue d'une réutilisation ultérieure, cliquez sur **Sauvegarder comme modèle** et définissez un nom unique pour le modèle.
5. Pour personnaliser la présentation du rapport, cliquez sur l'onglet Présentation. Pour plus d'informations, voir «Configurer la présentation d'un rapport», à la page 233.

6. Sélectionnez le format de sortie requis : PDF, HTML, TXT, RTF ou XML.
7. Cliquez sur **Sauvegarder le rapport**.

Limitation de la taille des rapports de sécurité

Conseils pour la limitation d'un rapport de sécurité à une taille raisonnable.

Pourquoi et quand exécuter cette tâche

Les rapports de sécurité peuvent être très volumineux. Si, au cours de la génération d'un rapport de sécurité, un message d'avertissement signale que le fichier contiendra plusieurs centaines de pages, ou si le processus de création du rapport dépasse le délai d'attente, vous pouvez suivre les conseils ci-après pour essayer de réduire la taille du rapport aux informations que vous jugez importantes.

Procédure

1. L'une des manières de réduire la taille d'un rapport consiste à limiter ce dernier à une partie de l'application. Vous pouvez pour cela sélectionner le noeud approprié dans l'arborescence d'application, cliquer dessus avec le bouton droit de la souris et sélectionner **Rapport pour ce noeud > Sécurité**. Un rapport est alors créé pour toutes les parties de l'application sous le noeud sélectionné.
2. Si vous constatez que les résultats de l'examen contiennent des milliers de problèmes, pensez à générer un **Récapitulatif** uniquement ou le **Rapport par défaut** en ayant décoché la case **Informations complémentaires sur les problèmes**.
3. Par défaut, *tous* les types de test sont inclus dans les rapports (Gravité min. = Informationnel). Essayez d'augmenter le paramètre de **gravité minimale** de sorte que seuls les incidents de gravité élevée ou élevée et moyenne soient inclus.
4. Vérifier que la valeur **Max. Le paramétrage** des variantes est 1, de sorte qu'il n'y a pas plus d'une seule variante pour chaque édition.
5. Gardez présent à l'esprit que les options **Variantes > Demande/Réponse** et **Conseils et recommandations de correction** peuvent faire augmenter considérablement la taille des rapports. Sélectionnez-les uniquement si nécessaire.

Rapports sur les normes de l'industrie et sur la conformité

Les rapports sur les normes de l'industrie permettent de déterminer si votre application est conforme aux normes d'un comité de secteur d'activité. Les rapports sur la conformité à la réglementation permettent de déterminer si votre application est conforme à des réglementations spécifiques ou à des normes légales.

Rapports sur les normes de l'industrie

Les rapports sur les normes de l'industrie permettent de déterminer si votre application est conforme aux normes d'un comité de secteur d'activité.

Pourquoi et quand exécuter cette tâche

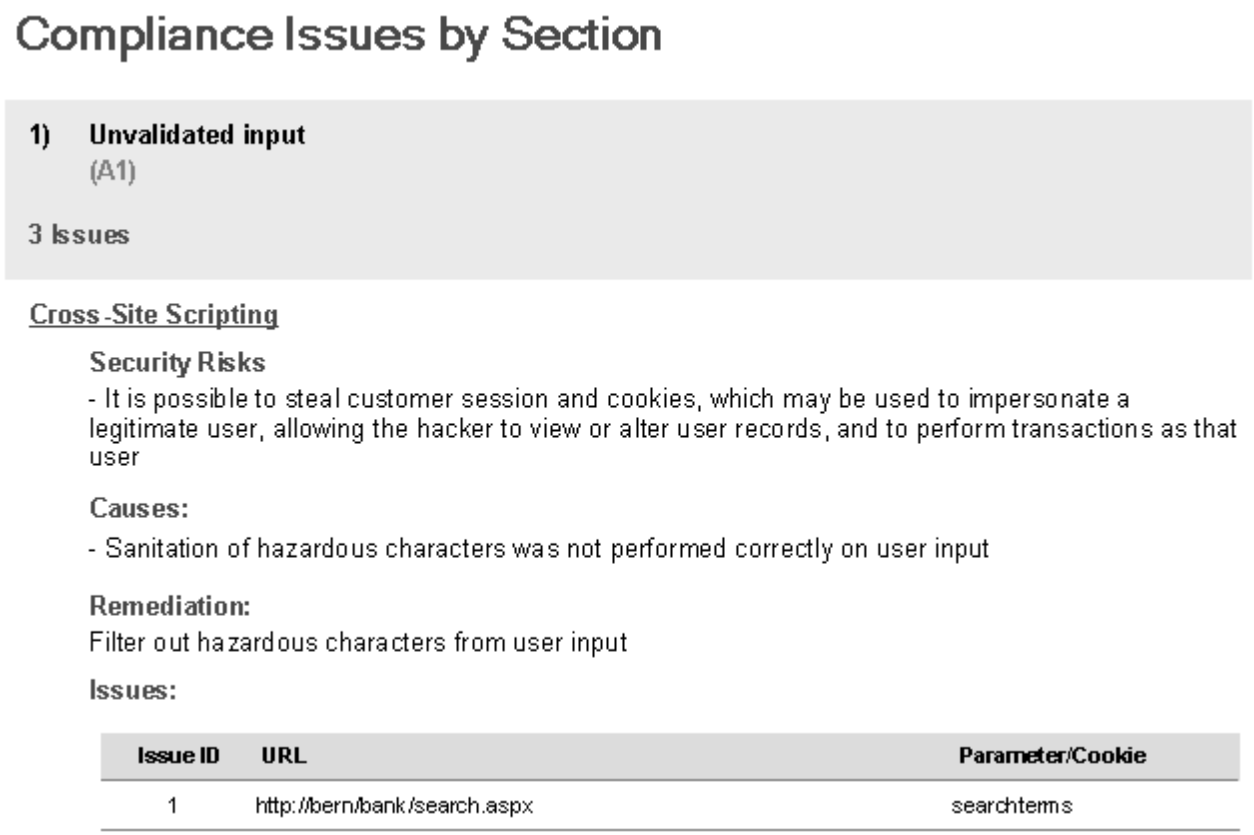
IBM met à jour la liste des modèles parmi lesquels choisir au fur et à mesure que de nouvelles normes sont créées pour les différents secteurs de l'industrie ; et votre AppScan est automatiquement mis à jour régulièrement.

Si vous ne trouvez pas la norme de l'industrie souhaitée dans la liste, vous pouvez créer votre propre modèle de rapport sur les normes de l'industrie (voir «Rapports définis par l'utilisateur», à la page 243).

Les rapports sur les normes de l'industrie comprennent les sections suivantes :

Titre de la section	Informations présentées
Description	Explication du standard.
Récapitulatif de la conformité	Liste et décompte des problèmes non conformes. Notez qu'un seul problème peut indiquer la non-conformité de plusieurs sections. Par conséquent, le nombre de problèmes par section, pour toutes les sections, peut être supérieur au nombre de problèmes uniques.
Problèmes de conformité uniques	Liste des URL non conformes, des paramètres et des cookies appropriés et des noms de test. Chaque problème n'apparaît qu'une seule fois.
Problèmes de conformité par section	Explications détaillées des raisons pour lesquelles votre application n'est pas conforme et solution pour résoudre ces problèmes.

L'illustration ci-dessous présente un modèle d'une partie d'un rapport sur les normes de l'industrie.



Procédure

1. Cliquez sur **Outils > Rapport > Normes de l'industrie**
2. Procédez de l'une des façons suivantes :
   - Sélectionnez l'un des **Modèles de rapport sur les normes de l'industrie** répertoriés.
   - Sélectionnez le bouton radio **Défini par l'utilisateur** et entrez ou accédez au fichier modèle personnalisé Normes de l'industrie (***.asreg**). Pour plus de détails, voir «Rapports définis par l'utilisateur», à la page 243.

3. Si vous souhaitez contrôler l'apparence du rapport, ouvrez l'onglet **Présentation** (voir «Configurer la présentation d'un rapport», à la page 233).
4. Cliquez sur **Prévisualisation** pour générer et visualiser le rapport dans AppScan ou cliquez sur **Sauvegarder le rapport** pour le générer et le sauvegarder dans un fichier.

Versions prises en charge

Liste des normes de l'industrie prises en charge et des versions associées.

Les rapports ci-après sur les normes de l'industrie peuvent être générés.

Normes de l'industrie	Version
Norme internationale - ISO 27001	Janvier 2013
Norme internationale - ISO 27002	Janvier 2013
NERC CIPC Electricity Sector Security Guidelines	Septembre 2013
NIST Special Publication 800-53	Révision 4
OWASP Top 10	2013, 2017
SANS/CWE - Les 25 erreurs de programmation les plus dangereuses	1.03
Classification des menaces par le consortium WASC	2.0

Rapports sur la conformité à la réglementation

Les rapports sur la conformité à la réglementation permettent de déterminer si votre application est conforme aux réglementations et normes légales.

Pourquoi et quand exécuter cette tâche

Il existe une longue liste de modèles provenant de divers pays parmi lesquels choisir, chaque modèle disposant d'un rapport de conformité pour une réglementation particulière.

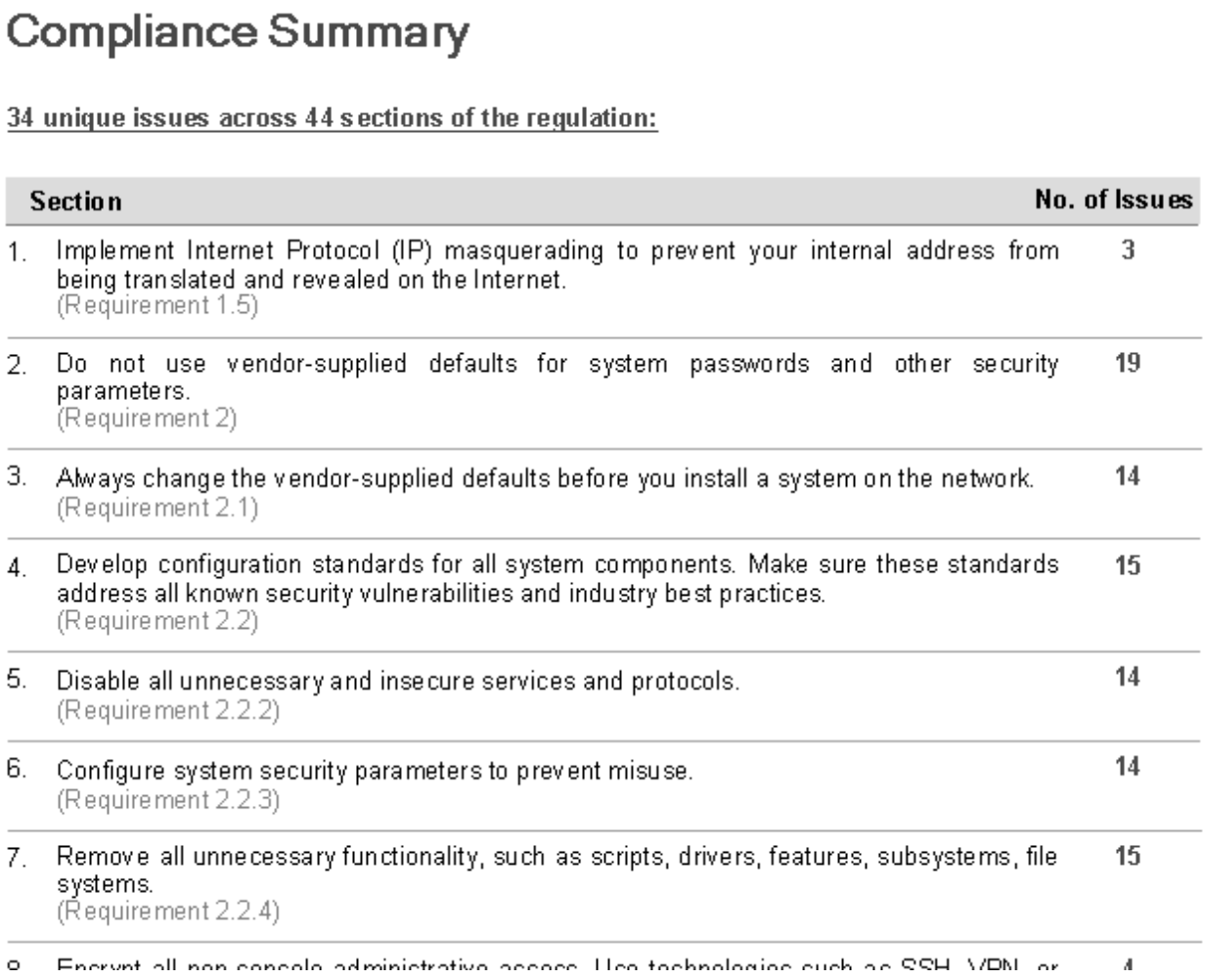
Si vous ne trouvez pas la réglementation souhaitée dans la liste, vous pouvez créer votre propre rapport de conformité à la réglementation (pour plus de détails, voir «Rapports définis par l'utilisateur», à la page 243).

Les rapports de conformité à la réglementation comprennent les sections suivantes :

Titre de la section	Informations présentées
Description	Explication de la réglementation
Récapitulatif de la conformité	Liste et décompte des problèmes non conformes. Notez qu'un seul problème peut indiquer la non-conformité de plusieurs sections. Par conséquent, le nombre de problèmes par section, pour toutes les sections, peut être supérieur au nombre de problèmes uniques.
Problèmes de conformité uniques	Liste des URL non conformes, des paramètres et des cookies appropriés et des noms de test. Chaque problème n'apparaît qu'une seule fois.

Titre de la section	Informations présentées
Problèmes de conformité par section	Explications détaillées des raisons pour lesquelles votre application n'est pas conforme et solution pour résoudre ces problèmes.

L'illustration ci-dessous présente un modèle de rapport de conformité à la réglementation.



Compliance Summary

34 unique issues across 44 sections of the regulation:

	Section	No. of Issues
1.	Implement Internet Protocol (IP) masquerading to prevent your internal address from being translated and revealed on the Internet. (Requirement 1.5)	3
2.	Do not use vendor-supplied defaults for system passwords and other security parameters. (Requirement 2)	19
3.	Always change the vendor-supplied defaults before you install a system on the network. (Requirement 2.1)	14
4.	Develop configuration standards for all system components. Make sure these standards address all known security vulnerabilities and industry best practices. (Requirement 2.2)	15
5.	Disable all unnecessary and insecure services and protocols. (Requirement 2.2.2)	14
6.	Configure system security parameters to prevent misuse. (Requirement 2.2.3)	14
7.	Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems. (Requirement 2.2.4)	15
8.	Encrypt all non-console administrative access. Use technologies such as SSH, VPN, or	4

Procédure

1. Cliquez sur **Outils > Rapport > Conformité à la réglementation**
2. Procédez de l'une des façons suivantes :
   - Sélectionnez l'un des **Modèles de rapport de conformité légale** répertoriés :
   - Sélectionnez le bouton radio **Défini par l'utilisateur** et entrez ou accédez au fichier modèle personnalisé Conformité légale (***.asreg**). Pour plus d'informations, voir «Rapports définis par l'utilisateur», à la page 243.
3. Si vous souhaitez contrôler l'apparence du rapport, ouvrez l'onglet **Présentation** (voir «Configurer la présentation d'un rapport», à la page 233).
4. Cliquez sur **Prévisualisation** pour générer et visualiser le rapport dans AppScan ou cliquez sur **Sauvegarder le rapport** pour le générer et le sauvegarder dans un fichier.

Versions prises en charge

Liste des réglementations prises en charge et des versions associées

Les rapports ci-après sur la conformité légale peuvent être générés.

Réglementation	Version prise en charge
[AUS] APRA PPG 234 - Management of Security Risk in Information and Information technology	Janvier 2012
[CANADA] PIPED Act	Janvier 2014
[CANADA] Freedom of Information and Protection of Privacy Act (FIPPA)	Septembre 2012
[CANADA] Management of Information Security Technology (MITS)	Septembre 2012
[EU] European Directive 1995/46/EC	Janvier 2012
[EU] European Directive 2002/58/EC	Mars 2012
[EU] Regulation 2016/679 of the European Parliament and of the Council (GDPR)	Avril 2016
[JAPAN] Japan's Personal Information Protection Act (JPIPA)	Janvier 2012
[UK] Data Protection Act	Décembre 2014
[US] California Assembly Bill No. 1950 and Senate Bill 1386	Mars 2012
[US] Children Online Privacy Protection Act (COPPA)	Décembre 2014
[US] DCID 6/3 Availability Basic	Janvier 2011
[US] DCID 6/3 Availability High	Janvier 2011
[US] DCID 6/3 Availability Medium	Janvier 2011
[US] DCID 6/3 Confidentiality Reqs Protection Level 1	Janvier 2011
[US] DCID 6/3 Confidentiality Reqs Protection Level 2	Janvier 2011
[US] DCID 6/3 Confidentiality Reqs Protection Level 3	Janvier 2011
[US] DCID 6/3 Confidentiality Reqs Protection Level 4	Janvier 2011
[US] DCID 6/3 Confidentiality Reqs Protection Level 5	Janvier 2011
[US] DCID 6/3 Integrity Basic	Janvier 2011
[US] DCID 6/3 Integrity High	Janvier 2011
[US] DCID 6/3 Integrity Medium	Janvier 2011
[US] DCID 6/3 Securing Advanced Technology IS	Janvier 2011
[US] Electronic Funds and Transfer Act (EFTA)	Décembre 2013
[US] Federal Financial Institutions Examination Council (FFIEC), Information Security handbook	Février 2013
[US] Federal Information Security Management Act (FISMA)	Septembre 2014
[US] The Federal Risk and Authorization Management Program (FedRAMP)	
[US] Financial Services (GLBA)	Janvier 2013
[US] Healthcare Services (HIPAA)	Décembre 2014
[US] NERC Cyber Security Standards	Septembre 2014
[US] Privacy Act of 1974	Janvier 2011

Réglementation	Version prise en charge
[US] Safe Harbor	Novembre 2012
[US] Sarbanes-Oxley Act (SOX)	Janvier 2013
[US] Title 21 Code of Federal Regulations	Novembre 2011
[US] Family Educational Rights and Privacy Act (FERPA)	Janvier 2013
[US] DISA's Application Security and Development STIG	Version 3 édition 9
[US] DoD Instruction 8500.1 - Cybersecurity	Septembre 2014
[US] DoD Instruction 8550.01 - Internet Services and Internet Based Capabilities	Septembre 2014
[US] Massachusetts 201 CMR 17.00	Janvier 2011
Basel II	Octobre 2012
Norme de sécurité des données d'application de paiement	3.0
The Payment Card Industry Data Security Standard (PCI DSS)	3.2

Rapports définis par l'utilisateur

Vous pouvez créer des modèles de rapport définis par l'utilisateur pour les rapports sur les normes de l'industrie ou les rapports sur la conformité légale.

Pourquoi et quand exécuter cette tâche

Les modèles de rapport AppScan portent l'extension de fichier **.asreg**. Les modèles fournis sont stockés dans le dossier \Regulations de votre répertoire d'installation AppScan. Les modèles que vous créez doivent être stockés dans votre dossier de fichiers utilisateur AppScan.

Vous pouvez créer un nouveau modèle à partir de zéro et l'enregistrer avec l'extension **.asreg**, ou copier un fichier existant et effectuer des modifications, le cas échéant. (La procédure ci-dessous décrit comment créer un modèle basé sur un modèle existant.)

Procédure

1. Ouvrez le dossier **[Dossier d'installation d'AppScan Standard]\AppScan\Regulations** et copiez un fichier **.asreg** existant.
2. Collez le fichier dans votre dossier de fichiers utilisateur AppScan et donnez-lui un nouveau nom.

   Remarque : Par défaut, le dossier de fichiers utilisateur AppScan est `\My Documents\AppScan`, à moins que vous n'ayez spécifié un emplacement différent dans **Outils > Options > onglet Préférences > Emplacements de fichiers > dossier Fichiers utilisateur.**
3. La balise racine est `Règles`, avec l'attribut `format_version` :

   ```
   <Regulation format_version="2.0">
   ```
4. La balise suivante doit être le titre de votre modèle :

   ```
   <Title>Our Organization's web Application Requirement Compliance Report
   </Title>
   ```
5. Entrez une description des règles ou des normes à l'aide de la balise `Description` :

   ```
   <Description>
    <Subtitle>Sub Section</Subtitle>
    <p>This regulation addresses ...</p>
   ```

```
 <p>It is important because...</p>
 <Subtitle>Sub Section 2</Subtitle>
 <p>This section of the regulation addresses ...</p>
</Description>
```

6. Par défaut, il existe une balise `<Disclaimer>` qui assure que vous ne prenez pas de responsabilité légale pour le contenu du rapport.
7. Créez une ou plusieurs sections de configurations requises (en utilisant la balise `<Section>`) pour votre modèle de règles et définissez quels problèmes AppScan sont appropriés pour chaque section, en utilisant les balises `<Cause>`, `<Risk>`, `<ThreatClass>`, et `<CWE>`.
   - Utilisez l'attribut `name` de la balise `Section` pour définir le titre de section du rapport.
   - Entre les balises d'ouverture et de fermeture `Section`, ajoutez un ou plusieurs des éléments suivants :
     - `<Cause>` (voir la «Liste des causes»). Un motif décrit une configuration incomplète ou incorrecte, une validation manquante ou un état similaire.
     - `<Risk>` (voir la «Liste des risques», à la page 246). Chaque risque est un "scénario-catastrophe".
     - `<ThreatClass>` (voir la «Liste des classes de menaces», à la page 247). Une classe de menaces est une catégorie de tests.
     - `<CWE>` par numéro.

   Exemple :

```
<Section name="My Application login must be secured">
 <Cause>inputLengthNotChecked</Cause>
 <Risk>denialOfService</Risk>
 <Risk>siteDefacement</Risk>
 <CWE>79</CWE>
</Section>
```

8. Fermez le fichier en utilisant la balise de fermeture `</Regulation>`.

Liste des causes

Cause	Description
hazardousCharactersNotSanitized	L'assainissement des caractères dangereux n'a pas été correctement exécuté sur l'entrée utilisateur.
formatStringsVulnerability	L'entrée utilisateur est utilisée directement comme une entrée de chaîne de formatage pour C/C++'s sprintf et fonctions similaires.
hiddenParameterUsed	Les valeurs de paramètre ont été 'codées en dur' dans HTML comme un paramètre de type 'masqué'.
boundsCheckingOnParamValues	La vérification des limites propres n'a pas été effectuée sur les valeurs des paramètres entrants.
incorrectDataType	Aucune validation n'a été exécutée pour vérifier que l'entrée utilisateur correspond au type de données attendu.
inputLengthNotChecked	La longueur de l'entrée utilisateur n'est pas limitée, permettant ainsi le dépassement de la mémoire tampon.
errorMessagesReturned	Des exceptions et des messages d'erreur pouvant contenir des informations de débogage sensibles sont présentés aux utilisateurs.
debugInfoInHtmlSource	Le programmeur a laissé des informations de débogage dans des pages Web.
backDoorLeftBehind	Une porte dérobée ou une option de débogage ont été laissées par les programmeurs.
clientSideValidation	La validation de l'entrée utilisateur est effectuée côté client et peut être contournée facilement.
usOfClientSideLogic	L'application Web utilise une logique côté client pour créer des pages Web.
cookiesCreatedAtClientSide	Des cookies sont créés côté client.

Cause	Description
javaScriptPassWordMechanism	L'application Web utilise une authentification par mot de passe côté client.
sqlBuiltByJavaScript	L'application Web utilise une logique côté client pour créer des requêtes SQL.
dotDotNotSanitized	L'entrée utilisateur n'est pas vérifiée pour la chaîne '..'.
weakTokenUsed	Un algorithme de jeton faible est utilisé par l'application Web.
missingPatchesForThirdPartyProds	Les derniers modules de correction ou correctifs pour produits tiers n'ont pas été installés.
tempFilesLeftBehind	Des fichiers temporaires ont été laissés dans l'environnement de production.
improperFileDirPermissions	Des droits/LCA incorrects ont été définis dans le fichier/répertoire.
nimdaWormBackdoor	Le programme Nimda a été trouvé sur le système.
sampleScriptsFound	Des modèles de scripts ou de répertoires par défaut ont été installés sur le site Web.
insecureThirdPartySoftware	Un logiciel tiers vulnérable sans module de correction connu est installé sur le site Web.
directoryBrowsingEnabled	La navigation dans le répertoire est activée.
managementConsoleAccess	La console de gestion Web est accessible depuis le Web.
insecureWebServerConfiguration	Le serveur Web ou le serveur d'applications est configuré de manière non sécurisée.
frontPageServerUnsecureInstall	Les extensions de serveur FrontPage ont été installées avec des paramètres de sécurité incorrects.
insecureWebAppConfiguration	Programmation ou configuration non sécurisée de l'application Web.
vulnSOAPserializer	Le sérialiseur SOAP utilisé par votre serveur de services Web ne valide pas correctement l'entrée SOAP.
sensitiveDataNotSSL	Les zones d'entrée sensibles, telles que les noms d'utilisateur, mots de passe et numéros de carte de crédit, sont communiquées non chiffrées.
nonSecureCookiesSentOverSSL	L'application Web envoie des cookies non sécurisés via SSL.
sessionCookieNotRAM	L'application Web stocke des informations de session sensibles dans un cookie permanent (sur le disque).
redirectionFromWithinSite	L'application Web effectue un réacheminement vers un site externe.
remoteFileInclusion	L'application Web autorise l'inclusion de fichiers à distance.
GETParamOverSSL	Des paramètres de requête pouvant contenir des informations sensibles ont été communiqués via SSL.
SensitiveCache	Il se peut que des informations sensibles aient été mises en cache par votre navigateur.
InsufficientAuthentication	Une méthode d'authentification insuffisante a été utilisée par l'application.
useOfGlobalFlashParamsInPDNFs	Paramètres globaux flash utilisés dans des fonctions natives potentiellement dangereuses.
causeNotAvailable	n/a
vulnActiveX	Le contrôle ActiveX utilisé est classé comme vulnérable. Le site Web analysé a peut-être été piraté dans le but de diffuser des logiciels malveillants.
compromisedDigiNotarSSLCert	Le certificat SSL utilisé a été marqué comme étant compromis en raison d'une violation de sécurité de DigiNotar.
paramValManipAllowed	La manipulation des valeurs de paramètre a été autorisée par la logique d'application.

Liste des risques

Nom du risque	Description
tempScriptDownload	Il est possible de télécharger des fichiers script temporaires pouvant exposer la logique de l'application et d'autres informations sensibles, telles que les noms d'utilisateur et les mots de passe.
sourceCodeDisclosure	Il est possible d'extraire le code source des scripts côté serveur, ce qui peut exposer la logique de l'application et d'autres informations sensibles, telles que les noms d'utilisateur et les mots de passe.
pathDisclosure	Il est possible d'extraire le chemin d'accès absolu de l'installation du serveur Web, ce qui peut aider un pirate à développer d'autres attaques et à obtenir des informations sur la structure du système de fichiers de l'application Web.
directoryListing	Il est possible de visualiser et de télécharger le contenu de certains répertoires virtuels de l'application Web pouvant contenir des fichiers restreints.
envVariablesExposure	Il est possible d'exposer des variables d'environnement du serveur pouvant aider un pirate à développer d'autres attaques contre l'application Web.
anyFileDownload	Il est possible de visualiser le contenu de n'importe quel fichier (par exemple, des fichiers de bases de données, d'informations utilisateur ou de configuration) sur le serveur Web (en fonction de la restriction des droits de l'utilisateur du serveur Web).
userImpersonation	Il est possible de voler la session et les cookies d'un client et de les utiliser pour emprunter l'identité d'un utilisateur légitime, ce qui peut permettre à un pirate de visualiser ou de modifier des enregistrements utilisateur et de réaliser des transactions en tant qu'utilisateur.
remoteCommandExecution	Il est possible d'exécuter des commandes à distance sur le serveur Web. Cela signifie généralement la compromission totale du serveur et de son contenu.
cacheFilesDownload	Il est possible de visualiser le contenu des fichiers cache pouvant contenir des informations sensibles concernant l'application Web.
debugErrorInformation	Il est possible de rassembler des informations de débogage sensibles.
eShoplifting	Il est possible de voler des biens et des services (eShoplifting - vol à l'étalage sur le Web).
denialOfService	Il est possible d'empêcher l'application Web de servir d'autres utilisateurs (refus de service).
privilegeEscalation	Il est possible de transférer des droits utilisateur et d'obtenir des droits administrateur sur l'application Web.
genericWorstCase	Il est possible de nuire à la logique de l'application.
configurationFile Téléchargeable	Il est possible de télécharger ou de visualiser le contenu d'un fichier de configuration pouvant contenir des informations vitales, telles que les noms d'utilisateur et les mots de passe.
sensitiveInformation	Il est possible de rassembler des informations sensibles relatives à l'application Web, telles que les noms utilisateur, les mots de passe, le nom de la machine et/ou les emplacements des fichiers sensibles.
genericWorstCaseJavaScript	Il est possible d'exploiter JavaScript. L'étendue du risque dépend du contexte de la page modifiée côté client.
genericWorstCaseJSCookie	Il est possible d'exploiter le code JSCookie. L'étendue du risque dépend du contexte et du rôle des cookies créés côté client.
emailSpoofing	Il est possible d'envoyer des messages électroniques via votre application Web à l'aide des adresses électroniques usurpées.
siteDefacement	Il est possible de télécharger, modifier ou supprimer des pages Web, des scripts et des fichiers sur le serveur Web.
databaseManipulations	Il est possible de visualiser, modifier ou supprimer des entrées de base de données et des tables (Injection SQL).

Nom du risque	Description
authBypass	Il est possible de contourner le mécanisme d'authentification de l'application Web.
siteStructureRevealed	Il est possible d'extraire des informations relatives à la structure du système de fichiers du site, ce qui facilite le mappage du site par le pirate.
publisherInformation Révélé	Il est possible d'extraire des informations de publication FrontPage sensibles.
dataResourceDownload	Il est possible d'accéder aux informations stockées dans une ressource de données sensibles.
sensitiveNotOverSSL	Il est possible de voler des données sensibles envoyées non chiffrées, telles que des numéros de carte de crédit, des numéros de sécurité sociale, etc.
loginNotOverSSL	Il est possible de voler des informations de connexion envoyées non chiffrées, telles que des noms utilisateur et des mots de passe.
unsecureCookieInSSL	Il est possible de voler des informations relatives à l'utilisateur ou à la session (cookies) qui ont été envoyées lors d'une session codée.
sessionCookieNotRAM	Il est possible de voler des informations de session (cookies) conservées sur le disque en tant que cookies permanents.
phishing	Il est possible de persuader un utilisateur naïf de fournir des informations sensibles telles qu'un nom utilisateur, un mot de passe, un numéro de carte de crédit, un numéro de sécurité sociale, etc.
cachePoisoning	Il est possible d'altérer le contenu du site par l'empoisonnement du cache Web.
attackFacilitation	Il est possible qu'un pirate utilise le serveur Web pour attaquer d'autres sites et augmente ainsi son autonomie.
maliciousContent	n/a
clientCodeExecution	Il est possible d'exécuter du code arbitraire des clients de l'application Web.
siteImpersonation	En utilisant des vecteurs d'attaque supplémentaires, un agresseur informatique malveillant a la possibilité de simuler ce site.

Liste des classes de menaces

Récapitulatif de classification des menaces par le consortium WASC, travail coopératif visant à classifier les failles et les attaques pouvant rendre vulnérable un site Web, ses données ou ses utilisateurs.

Les tableaux ci-après présentent une brève description des attaques et des menaces. Vous trouverez plus de détails sur la classification des menaces par le consortium WASC sur le site suivant :

http://projects.webappsec.org/w/page/13246978/Threat%20Classification

Attaques

Nom	Brève description
Abus de fonctionnalité	Technique d'attaque qui utilise les caractéristiques et fonctionnalités d'un site Web pour se servir des mécanismes de contrôle d'accès, les utiliser de façon frauduleuse ou les contourner.
Force brute	Processus automatique par tâtonnement pour deviner le nom d'un utilisateur, un mot de passe, un numéro de carte de crédit ou une clé cryptographique.
Dépassement de la mémoire tampon	Attaques qui altèrent le flux d'une application en écrasant des parties de la mémoire avec des données dépassant la taille allouée à la mémoire tampon.

Nom	Brève description
Usurpation de contenu	Technique d'attaque utilisée pour tromper un utilisateur et lui faire croire que le contenu qui apparaît sur un site Web est légitime et ne provient pas d'une source externe.
Prédiction des droits d'accès/session	Méthode de détournement ou d'usurpation d'identité pratiquée à l'encontre d'un utilisateur de site Web en déduisant ou devinant la valeur unique qui identifie une session ou un utilisateur spécifique.
Script intersite	Technique d'attaque qui force un site Web à relayer le code exécutable fourni par le pirate, qui se charge dans le navigateur de l'utilisateur.
Falsification de requêtes intersite	Attaque consistant à forcer une victime à envoyer une requête HTTP vers une destination cible, sans qu'elle n'en ait ni connaissance ni intention, afin d'effectuer une action en se faisant passer pour la victime.
Refus de service	Technique d'attaque destinée à empêcher un site Web de fournir le service normal aux utilisateurs.
Recherche d'empreintes	La méthodologie la plus couramment utilisée par les pirates consiste d'abord à observer la présence internet de la cible et de rassembler le plus d'informations possible. Avec ces informations, le pirate peut développer un scénario d'attaque précis, qui exploitera efficacement une vulnérabilité du type ou de la version du logiciel utilisé par l'hôte cible.
Formatage de chaînes	Attaques qui altèrent le flux d'une application en utilisant des fonctions de bibliothèque de formatage de chaîne pour accéder à davantage d'espace mémoire.
Dissimulation de réponses HTTP	La dissimulation de réponses HTTP est une technique permettant de "faire passer" 2 réponses HTTP d'un serveur à un client, via un périphérique HTTP intermédiaire qui attend (ou permet) une réponse unique du serveur.
Fractionnement de réponse HTTP	Le fractionnement de réponse HTTP est la capacité du pirate à envoyer une seule demande HTTP qui force le serveur Web à former un flux de sortie qui est ensuite interprété par la cible comme étant deux réponses HTTP au lieu d'une.
Dissimulation de demandes HTTP	Technique d'attaque qui utilise les incohérences dans l'analyse des demandes HTTP non conformes à RFC entre deux périphériques HTTP pour faire passer une demande au deuxième périphérique "au travers" du premier.
Fractionnement de demande HTTP	Le fractionnement de demande HTTP est une attaque qui force le navigateur à envoyer des demandes HTTP arbitraires, ce qui met en œuvre la technique cross-site scripting (XSS) et empoisonne le cache du navigateur.
Dépassements d'entier	Condition qui survient lorsque le résultat d'une opération arithmétique, comme une multiplication ou une addition, dépasse la taille maximale du type d'entier utilisé pour le stocker.
Injection LDAP	Technique d'attaque utilisée pour exploiter les sites Web qui créent des instructions LDAP à partir des entrées utilisateur.
Injection de commande de messagerie	Technique d'attaque utilisée pour exploiter les serveurs de messagerie et les applications de courrier Web qui construisent des déclarations IMAP/SMTP à partir d'entrées fournies par l'utilisateur qui ne sont pas correctement assainies.
Injection d'octet null	Technique d'exploitation active utilisée pour contourner les filtres de contrôle d'exactitude dans l'infrastructure Web en ajoutant des caractères de type octet nul codé dans l'URL aux données fournies par l'utilisateur.
Injection de commandes OS	Technique d'attaque utilisée pour exploiter les sites Web en exécutant les commandes du système d'exploitation via la manipulation des entrées de l'application.

Nom	Brève description
Traversée de répertoires	Technique d'attaque qui force l'accès aux fichiers, répertoires et commandes résidant potentiellement en dehors du répertoire racine des documents Web.
Emplacement de ressource prévisible	Technique d'attaque destinée à découvrir, par suppositions, les fonctionnalités et le contenu masqués d'un site Web.
Inclusion RFI	Technique d'attaque utilisée pour exploiter les mécanismes d'inclusion de fichier dynamique ("dynamic file include") dans les applications Web pour inciter l'application à inclure des fichiers distants comportant du code malveillant.
Détour du routage	Attaque "d'interception" dans laquelle des intermédiaires peuvent être injectés ou "détournés" dans le but de router des messages sensibles vers un emplacement extérieur.
Fixation de session	Technique d'attaque qui impose une valeur explicite à un identificateur de session utilisateur. Une fois l'identificateur de session utilisateur fixé, le pirate attend qu'il se connecte. Lorsque l'utilisateur est connecté, le pirate utilise la valeur d'identificateur de session prédéfinie pour découvrir son identité en ligne.
Validation de récupération de mot de passe faible	Lorsqu'un site Web permet à un pirate d'obtenir, de modifier ou de récupérer illégitimement le mot de passe d'un autre utilisateur.
Abus de tableau SOAP	Un service Web fonctionnant avec des tableaux peut être la cible d'une attaque par saturation XML si le serveur SOAP est forcé à générer un tableau de très grande dimension dans la mémoire de la machine, infligeant ainsi une condition DoS sur la machine à cause de la préallocation de mémoire.
Injection SSI	Technique d'exploitation côté serveur qui autorise un pirate à envoyer du code dans une application Web, qui sera ensuite exécuté localement par le serveur Web.
Injection SQL	Technique d'attaque utilisée pour exploiter les sites Web qui créent des instructions SQL à partir des entrées utilisateur.
Abus d'agent de réacheminement d'URL	Le réacheminement d'URL représente une fonctionnalité communément employée par les sites Web pour transmettre une requête entrante vers une autre ressource. Elle peut être utilisée pour des attaques par hameçonnage.
Injection XPath	Technique d'attaque utilisée pour exploiter les sites Web en construisant des requêtes XPath à partir des entrées utilisateur.
Agrandissement d'attribut XML	Attaque par saturation visant les analyseurs XML.
Entités externes XML	Cette technique tire parti d'une fonctionnalité du langage XML pour générer dynamiquement des documents au moment du traitement. Un message XML peut fournir des données de manière explicite ou pointer vers un URI où les données sont disponibles. Avec cette technique d'attaque, des entités externes peuvent remplacer la valeur de l'entité par des données malveillantes ou des renvois alternatifs, ou peuvent compromettre la sécurité des données auxquelles le serveur ou l'application XML a accès.
Expansion d'entité XML	Elle exploite une capacité des DTD XML qui permet la création de macros personnalisées, appelées entités, qui peuvent être utilisées dans un document. En définissant récursivement un ensemble d'entités personnalisées en tête d'un document, un attaquant peut submerger les analyseurs qui tentent de résoudre complètement les entités en les obligeant à parcourir presque indéfiniment ces définitions récursives.

Nom	Brève description
Injection XML	L'injection XML est une technique d'attaque utilisée pour manipuler ou compromettre la logique d'un service ou d'une application XML. L'injection de contenu et/ou de structures XML accidentels dans un message XML peut modifier la logique prévue de l'application. De plus, l'injection XML peut provoquer l'insertion de contenus malveillants dans le message ou document obtenu.
Injection XQuery	L'injection XQuery est une variante de l'attaque par injection SQL classique, contre le langage XQuery en XML. Elle utilise des données incorrectement validées qui sont passées aux commandes XQuery.

Failles

Nom	Brève description
Problème de configuration de l'application	Ces attaques tirent parti des failles de configuration détectées dans les applications Web.
Indexation de répertoire	L'indexation automatique de répertoire est une fonction de serveur Web qui liste tous les fichiers du répertoire concerné en l'absence du fichier de base normal (index.html/home.html/ default.htm). Des vulnérabilités logicielles combinées à une demande Web spécifique peuvent engendrer un listage involontaire des répertoires.
Droits d'accès inadéquats au système de fichiers	Menace pour la confidentialité, l'intégrité et la disponibilité d'une application Web. Le problème survient lorsque des droits d'accès incorrects au système de fichiers sont définis pour des fichiers, dossiers et liens symboliques.
Traitement incorrect des entrées	L'une des failles les plus courantes identifiées à l'heure actuelle parmi les applications. La mauvaise gestion des entrées est la principale cause des vulnérabilités critiques dans les systèmes et les applications.
Traitement incorrect des sorties	Si le traitement des sorties d'une application est incorrect, les données sortantes peuvent être à l'origine de vulnérabilités et d'actions que le développeur de l'application n'avait pas prévues.
Fuite d'informations	Faille d'une application dans laquelle cette dernière révèle des données sensibles, telles que des détails techniques de l'application Web, des informations sur l'environnement ou des données spécifiques à l'utilisateur.
Indexation non sécurisée	Menace pour la confidentialité des données du site Web. L'indexation de contenus de site Web par un processus ayant accès à des fichiers qui ne sont pas censés être accessibles publiquement constitue une fuite potentielle d'informations concernant l'existence de tels fichiers et leur contenu. Dans le processus d'indexation, ces informations sont recueillies et stockées par le processus d'indexation, et peuvent être récupérées plus tard par un agresseur déterminé, généralement au moyen d'une série de requêtes sur le moteur de recherche.
Anti-automatisation insuffisante	Lorsqu'un site Web permet à un pirate d'automatiser un processus qui ne devrait être exécuté que manuellement.
Authentification insuffisante	Lorsqu'un site Web autorise un pirate à accéder à un contenu ou à une fonctionnalité sensible sans avoir à s'authentifier correctement.
Autorisation insuffisante	Lorsqu'un site Web autorise l'accès à des contenus ou à une fonctionnalité sensibles qui devraient être assortis de restrictions d'accès renforcées.
Restauration de mot de passe insuffisante	Lorsqu'un site Web permet à un pirate d'obtenir, de modifier ou de récupérer illégalement le mot de passe d'un autre utilisateur.
Validation de processus insuffisante	Lorsqu'un site Web autorise un pirate à contourner ou à faire échouer le contrôle du débit prévu d'une application.
Expiration de session insuffisante	Se produit lorsqu'un site Web autorise un pirate à réutiliser d'anciens ID session ou données d'identification de session comme autorisation.

Nom	Brève description
Protection de la couche transport insuffisante	Expose la communication à des tiers non fiables.
Problème de configuration du serveur	Exploite les failles de configuration détectées sur les serveurs Web et les serveurs d'applications.

Rapport de l'analyse des écarts

Le rapport de l'analyse des écarts compare deux ensembles de résultats d'examen et affiche la différence dans les URL et/ou problèmes de sécurité qui y sont détectés.

Pourquoi et quand exécuter cette tâche

Vous sélectionnez des examens de référence et cible puis AppScan compare les deux ensembles de résultats pour vous permettre de voir de quelle manière la situation de sécurité s'est améliorée ou détériorée entre les deux examens.

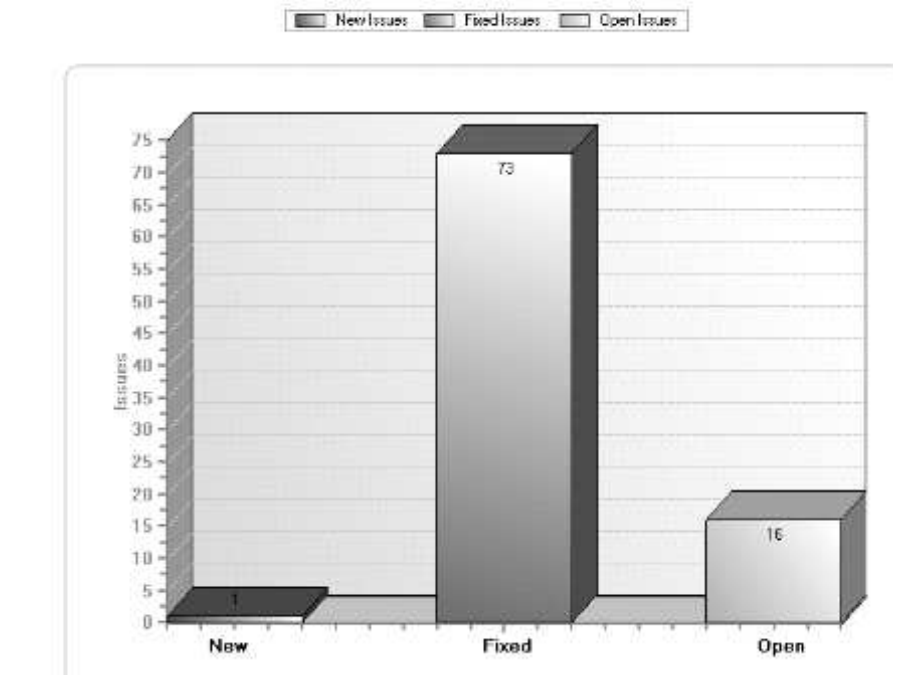
Vous pouvez comparer l'examen actuellement chargé avec un examen enregistré ou comparer deux examens enregistrés.

Lorsque vous comparez des examens, vous utilisez généralement l'examen le plus récent comme examen de référence. Le rapport de l'analyse des écarts indique alors de quelle manière les résultats de l'examen cible diffèrent de ceux de l'examen de référence.

Les rapports de l'analyse des écarts comprennent les sections suivantes :

Titre de la section	Informations présentées
Informations générales	Répertorie les noms et emplacements des examens de référence et cible.
Description	Description des informations contenues dans l'examen.
Problèmes par hôte	Tableau présentant le nombre de problèmes de niveau Elevé, Moyen, Faible, Information et Total trouvés dans chaque examen.
URL d'application	(Si inclus) Diagramme à barres présentant le nombre d'URL nouvelles, supprimées, restantes, suivi d'une liste complète de chaque type.
Problèmes de sécurité	(Si inclus) Diagramme à barres des problèmes de sécurité nouveaux/corrigés/ restants, suivi d'un diagramme à barres présentant la répartition des gravités dans les deux examens (Elevée/Moyenne/Faible/Information), suivi d'une liste complète de tous les problèmes nouveaux/corrigés/restants.

L'illustration ci-dessous présente un modèle de rapport de l'analyse des écarts.



Procédure

1. Cliquez sur **Outils > Rapport > Analyse des écarts**
2. Sélectionnez l'examen de référence (généralement le plus récent des deux examens comparés). Dans la zone Examen de base, procédez comme suit :
   - Cliquez sur le bouton radio **Examen Current**
   - Cliquez sur le bouton radio **Examen sauvegardé**, puis accédez à l'emplacement du fichier de l'examen sauvegardé.
3. Sélectionnez l'examen cible (généralement le plus ancien des deux examens comparés). Dans la zone Examen cible, procédez comme suit :
   - Cliquez sur le bouton radio **Examen Current**
   - Cliquez sur le bouton radio **Examen sauvegardé**, puis accédez à l'emplacement du fichier de l'examen sauvegardé.
4. Dans la zone Contenu du rapport, cochez une ou les deux cases selon le type d'informations que vous souhaitez que le rapport compare :
   - **URL d'application** et/ou
   - **Problèmes de sécurité**
5. Si vous souhaitez contrôler l'apparence du rapport, ouvrez l'onglet **Présentation** (voir «Configurer la présentation d'un rapport», à la page 233).
6. Cliquez sur **Prévisualisation** pour générer et visualiser le rapport dans AppScan ou cliquez sur **Sauvegarder le rapport** pour le générer et le sauvegarder dans un fichier.

Rapports basés sur un modèle

L'onglet Basé sur un modèle de la boîte de dialogue Créer un rapport permet de créer des rapports aux formats DOC et DOCX deMicrosoft Word, avec les données souhaitées et le formatage de document défini.

Plusieurs exemples de modèles sont inclus à AppScan. Ils peuvent être utilisés :

- pour générer des rapports (sans édition) ;
- comme base de création de vos propres modèles de rapport personnalisés ;
- comme outil de compréhension du processus de création de vos propres modèles de rapport.

La boîte de dialogue comporte deux panneaux :

- Le panneau de gauche répertorie les modèles actuellement disponibles. Des exemples de modèles fournis avec AppScan apparaissent en italique et avec le suffixe "(modèle)" ; tous les modèles créés par l'utilisateur apparaissent en texte régulier (non italique).
- Le panneau de droite affiche une "image d'aperçu" pour vous aider à identifier rapidement le modèle requis (voir le tableau suivant).

Bouton ou lien	**Cliquez pour :**
Importer	Importer un modèle de rapport Word dans la liste située dans le panneau de gauche (par exemple un modèle que vous avez précédemment personnalisé). Des modèles importés sont enregistrés dans : **Mes documents > AppScan > Modèles de rapport > Word** Pour plus de détails, voir «Importer un modèle personnalisé», à la page 258
Exporter	Exporter un modèle de la liste vers un emplacement différent (par exemple pour l'édition).
Supprimer	Supprimer un modèle de la liste. Cela ne supprime pas le modèle mais le déplace vers le dossier : **Mes documents > AppScan > Modèles de rapport > Word > Supprimé**
Editer dans MS Word	Ouvrir le modèle sélectionné dans MS Word pour éditer le contenu et la présentation. Pour plus de détails, voir «Tutoriel sur les modèles personnalisés», à la page 254
Afficher la référence de zone	Ouvrir une liste HTML des références de zone pouvant être utilisées pour la création de modèles de rapport Word.
Sélectionner l'image de prévisualisation du rapport	Accéder et sélectionner une image qui représentera le modèle dans le panneau de droite (lorsque le modèle est sélectionné dans le panneau de gauche).
Rétablir l'image par défaut	Réintégrer l'image par défaut (une page blanche) pour le modèle sélectionné.
Aperçu	Générer et afficher un rapport dans les résultats d'examen courants à l'aide du modèle sélectionné dans le panneau de modèles. MS Word s'ouvrira et vous pourrez éditer le contenu ou la présentation, le cas échéant. Notez qu'AppScan crée uniquement un fichier temporaire. Si vous souhaitez le sauvegarder, vous devez le faire dans Word.

Bouton ou lien	Cliquez pour :
Sauvegarder le rapport	Générer et sauvegarder un rapport dans les résultats d'examen courants (sans ouvrir MS Word pour afficher le contenu du rapport) à l'aide du modèle sélectionné dans le panneau de modèles. AppScan vous invite à spécifier un nom et un emplacement pour la sauvegarde du fichier. Le fichier s'ouvre une fois sauvegardé.

Voir aussi :

«Créer un modèle de rapport personnalisé»

«Tutoriel sur les modèles personnalisés»

«Importer un modèle personnalisé», à la page 258

«Création de rapports partiels», à la page 234

Créer un modèle de rapport personnalisé

Vous pouvez utiliser des codes de zone pour définir vos propres rapports personnalisés à générer dans MS Word.

Introduction aux "zones de fusion"

Les zones de fusion AppScan relèvent de deux catégories :

- **Répéteurs (ou boucles) :** Consistent en une balise de début et de fin. Les répéteurs ne produisent pas de données eux-mêmes, mais parcourent toutes les zones en clair placées entre les balises de début et de fin, et dessinent les données appropriées pour ces groupes.

  Exemple : `<<AS:IssueTypeRepeaterStart>>` `<<AS:IssueTypeRepeaterEnd>>` [Début du répéteur de type de problème] [Fin du répéteur de type de problème]

  Ce répéteur parcourt tous les types de problèmes des résultats de l'examen.
- **Zones en clair :** Consistent en une zone unique et produisent les données réelles. (Les zones en clair ne doivent pas nécessairement être placées dans un répéteur, mais ne peuvent pas avoir d'autres zones en clair comme "enfants".)

  Exemple : `<<AS:IssueTypeName>>` [Nom du type de problème]

  Cette zone représente les noms de tous les problèmes trouvés dans l'examen.

Un rapport peut être créé lorsque vous insérez une zone en clair entre les balises de début et de fin d'une boucle appropriée. Vous pouvez, à l'aide des deux exemples ci-dessus, créer un rapport de tous les types de problèmes trouvés par l'examen :

```
<<AS:IssueTypeRepeaterStart>> [Début du répéteur de type de problème] <<AS:IssueTypeName>> [Nom du type de problème]<<AS:Is
```

Pour mieux comprendre le fonctionnement de cette technique, voir «Tutoriel sur les modèles personnalisés» ci-dessous.

Remarque : Ouvrez la liste complète des zones de fusion valides en cliquant sur **Outils > Rapport > Basé sur un modèle > Afficher la référence de zone**.

Tutoriel sur les modèles personnalisés

Cette section décrit la manière créer un modèle personnalisé simple.

Pourquoi et quand exécuter cette tâche

Dans la présente section, nous allons créer un modèle personnalisé simple afin de générer un tableau des tâches de résolution pour tous les problèmes trouvés lors de l'examen. La sortie du modèle aura la structure illustrée ci-dessous. Bien sûr, les données réelles dépendront de l'examen que vous utiliserez pour générer le rapport.

Index	Nom	Count	Priorité
1/2	RemediationTaskA	4	Elevée
2/2	RemediationTaskB	2	Elevée
1/3	RemediationTaskC	5	Moyenne
2/3	RemediationTaskD	2	Moyenne
3/3	RemediationTaskE	7	Moyenne
2/2	RemediationTaskF	3	Faible

Les tâches de priorité élevée sont répertoriées en premier, suivies par celles de priorité moyenne, puis de priorité faible. Pour chaque tâche, le tableau indique l'index de la tâche (ex : 1/n), le nom, le nombre (nombre d'incidents auxquels s'applique la tâche) et sa priorité.

Remarque : Pour ce tutoriel, il est supposé que l'utilisateur est familiarisé avec les codes de champs. Pour obtenir des informations sur les codes de champs, reportez-vous à votre documentation MS Word.

Remarque : Ouvrez la liste complète des zones de fusion valides en cliquant sur **Outils > Rapport > Basé sur un modèle > Afficher la référence de zone**.

Procédure

1. Ouvrez la liste des champs de fusion valides en cliquant sur **Outils > Rapport > Basé sur un modèle > Afficher la référence de champ**. Vous en aurez besoin ultérieurement comme référence pour copier des noms de zone.
2. Ouvrez un document MS Word, entrez l'en-tête "Tâches de résolution", et enregistrez-le.
3. **Créez l'en-tête du tableau :** Créez un tableau avec 4 colonnes et 1 ligne ; dans la première ligne, entrez les en-têtes "Index", "Nom", "Nombre", "Priorité".
4. **Ajoutez les zones qui généreront les entrées de priorité élevée dans le tableau :**
   a. A partir du tableau de référence de zone, copiez le code : `AS:RemediationTypeRepeaterStart<Priority=High>`
   b. Dans le document Word, placez votre curseur après l'en-tête.
   c. Collez le champ de fusion dans le document *en tant que champ* (MS Word 2003 : **Insertion > Champ > Champ de fusion > Champ Nom de champ** ; MS Word 2010 : **Insertion > QuickPart > Champ > Champ de fusion > Nom de champ**).

      La zone de fusion est créée dans le document au format suivant :

      ```
      {MERGEFIELD AS:RemediationTypeRepeaterStart<Priority=High>\*  MERGEFORMAT}
      ```

      Remarque : Par défaut, Word affiche les liens tronqués ce qui, lorsqu'ils sont longs, risque de masquer des informations importantes. Pour visualiser les noms de balises en entier, sélectionnez "show field codes" en cliquant sur **[Alt]** + **[F9]** (active/désactive les codes de champs).
   d. Cliquez sur **Entrée** et créez un autre tableau avec 4 colonnes et 1 ligne. Ce tableau sera rempli avec toutes les lignes contenant des tâches de priorité élevée.
   e. Après le tableau, ajoutez le champ de fusion suivant : `AS:RemediationTypeRepeaterEnd`

      Il apparaît comme suit :

      ```
      {MERGEFIELD AS:RemediationTypeRepeaterEnd\*  MERGEFORMAT}
      ```

Vous avez entré les champs de fusion de début et de fin pour la section du document qui répertorie les tâches de résolution de priorité élevée. Ces deux champs forment une "boucle" qui crée une liste basée sur les zones insérées entre elles. Vous pouvez maintenant entrer les quatre zones qui créeront le *contenu* dans les quatre colonnes du tableau ajouté ci-dessus.

f. Dans la colonne de gauche, ajoutez le champ de fusion : `AS:RemediationTypeRepeaterIndex` Un compteur est généré (sous la forme : 1/n, 2/n, etc.) pour chacune des tâches n de cette section.

g. Dans la deuxième colonne, ajoutez la zone de fusion pour RemediationTypeName.

h. Dans la troisième colonne, ajoutez la zone de fusion pour RemediationTypeName.

i. Dans la quatrième colonne, entrez le mot "Elevée".

La section Priorité élevée du tableau est complète. Elle génère plusieurs lignes de données : une pour chaque tâche de résolution de priorité élevée dans les résultats d'examen. Votre document doit se présenter comme suit :

Index	Name	Count	Priority
{ MERGEFIELD AS:RemediationTypeRepeaterStart<Priority=High> * MERGEFORMAT }			
{ MERGEFIELD AS:RemediationTypeRepeaterIndex * MERGEFORMAT }	{ MERGEFIELD AS:RemediationTypeName * MERGEFORMAT }	{ MERGEFIELD AS:RemediationTypeCount * MERGEFORMAT }	High
{ MERGEFIELD AS:RemediationTypeRepeaterEnd * MERGEFORMAT }			

5. Répétez l'étape 4 pour les tâches de priorité Moyenne et Faible (dans la colonne Priorité, entrez respectivement "Moyenne" et "Faible"). Vérifiez que chaque ligne du tableau (Elevée, Moyenne et Faible) est précédée d'un champ de fusion de début et suivie d'un champ de fusion de fin, comme dans l'image ci-dessous.

Remarque : Le contenu de champ des trois lignes étant identique, vous pouvez copier-coller la ligne de priorité "Elevée" entre les balises de début et de fin des tâches de priorité moyenne et faible, en modifiant simplement le texte de la colonne "Priorité".

Remarque : Comme la colonne Nom contiendra des chaînes de texte, alors que les colonnes Index, Nombre et Priorité ne contiendront que des chiffres ou des mots courts, vous pouvez ajuster les largeurs de colonnes en fonction de ces données.

Index	Name	Count	Priority
{ MERGEFIELD AS:RemediationTypeRepeaterStart<Priority=High> * MERGEFORMAT }			
{ MERGEFIELD AS:RemediationTypeRepeaterIndex * MERGEFORMAT }	{ MERGEFIELD AS:RemediationTypeName * MERGEFORMAT }	{ MERGEFIELD AS:RemediationTypeCount * MERGEFORMAT }	High
{ MERGEFIELD AS:RemediationTypeRepeaterEnd * MERGEFORMAT }			
{ MERGEFIELD AS:RemediationTypeRepeaterStart<Priority=Medium> * MERGEFORMAT }			
{ MERGEFIELD AS:RemediationTypeRepeaterIndex * MERGEFORMAT }	{ MERGEFIELD AS:RemediationTypeName * MERGEFORMAT }	{ MERGEFIELD AS:RemediationTypeCount * MERGEFORMAT }	Medium
{ MERGEFIELD AS:RemediationTypeRepeaterEnd * MERGEFORMAT }			
{ MERGEFIELD AS:RemediationTypeRepeaterStart<Priority=Low> * MERGEFORMAT }			
{ MERGEFIELD AS:RemediationTypeRepeaterIndex * MERGEFORMAT }	{ MERGEFIELD AS:RemediationTypeName * MERGEFORMAT }	{ MERGEFIELD AS:RemediationTypeCount * MERGEFORMAT }	Low
{ MERGEFIELD AS:RemediationTypeRepeaterEnd * MERGEFORMAT }			

6. Ajoutez un texte explicatif et appliquez le formatage au reste du document, le cas échéant.
7. Sauvegardez le fichier.
8. Pour créer un rapport à l'aide de ce modèle, voir «Importer un modèle personnalisé», à la page 258

Hiérarchie des balises

Lorsque vous créez des rapports à l'aide de balises AppScan, vous pouvez souhaiter placer une balise "à l'intérieur" d'une autre. Par exemple, vous pouvez souhaiter une section distincte pour chaque type de problème, dans chacune de ces sections une liste des problèmes, et pour chaque problème une liste de variantes. Pour ce faire, placez les balises de début et de fin de l'"enfant" dans les balises de début et de fin du "parent", comme indiqué dans l'illustration suivante.

Les hiérarchies de répéteur (boucle) suivantes sont autorisées :

- Type de problème > Problème > Variante
- Type de résolution > Résolution
- URL vulnérable > Type de problème > Problème > Variante
- Résolution > Type de problème > Problème > Variante

Les répéteurs doivent être utilisés seuls ou dans l'une de ces hiérarchies. L'utilisation des répéteurs dans des hiérarchies autres que celles-ci peuvent causer une erreur à la création du rapport.

Voir aussi :

«Répéteurs et zones»

Répéteurs et zones

Chaque répéteur (boucle) doit contenir une ou plusieurs zones en clair qui correspondent aux entrées de données dans la boucle. (Par exemple, dans la boucle Variante, vous pouvez placer la zone VariantDifference qui indiquera la différence entre la variante et la valeur d'origine pour chaque variante dans la boucle.) Par défaut, la zone Index est ajoutée dans chaque répéteur, mais vous pouvez la supprimer ou ajouter des zones supplémentaires (comme dans le tutoriel).

Répéteurs et zones - Exemple :

```
<<AS:IssueTypeRepeaterStart>>       [Start looping through issue types]

  <<AS:IssueTypeRepeaterIndex>>     [For each type list index (e.g. 3/24) and name]
  <<AS:IssueTypeName>>

  <<AS:IssueRepeaterStart>>         [Start looping through individual issues]

    <<AS:IssueRepeaterIndex>>       [For each issue list index (e.g. 3/24)]

    <<AS:VariantID>>                [For each issue list ID and variants]
    <<AS:VariantTestRequest>>
```

```
  <<AS:IssueRepeaterEnd>>           [End issue repeater]

<<AS:IssueTypeRepeaterEnd>>         [End issue type repeater]
```

Filtres de zone

Pourquoi et quand exécuter cette tâche

Certaines zones de fusion incluent des filtres. Par exemple, la limite VariantRepeater permet de définir le nombre de variantes qui seront incluses par problème.

Remarque : Dans la zone VariantScreenShot, le filtre définit l'échelle ("Scale=50") par pourcentage (50%). Vous pouvez modifier ce paramètre par toute valeur entière jusqu'à 100 (pour la taille complète).

Procédure

1. Sélectionnez la zone.

   ```
   <<AS:VariantRepeaterStart<Limit=1> >>
   ```

2. Pour visualiser les noms de zone, cliquez sur **[Alt]+F9** (ou cliquez avec le bouton droit de la souris sur la zone et sélectionnez **Toggle Field Codes** dans le menu).

   ```
   {MERGEFIELD AS:VariantRepeaterStart<Limit=1>\*MERGEFORMAT}
   ```

3. Mettez à jour le filtre placés entre les signes supérieur et inférieur.

   ```
   {MERGEFIELD AS:VariantRepeaterStart<Limit=4>\*MERGEFORMAT}
   ```

4. Pour masquer les noms de zone complets, cliquez sur **[Alt]+F9** (ou cliquez avec le bouton droit de la souris sur la zone et sélectionnez **Toggle Field Codes** dans le menu).

   ```
   <<AS:VariantRepeaterStart<Limit=4> >>
   ```

Importer un modèle personnalisé

Pourquoi et quand exécuter cette tâche

Si vous avez créé et enregistré un modèle personnalisé (voir «Tutoriel sur les modèles personnalisés», à la page 254), vous pouvez l'ajouter à la liste apparaissant dans la liste Rapports basés sur un modèle.

Procédure

1. Dans la vue *Basé sur un modèle* de la boîte de dialogue *Rapport*, cliquez sur **Importer**.
2. Accédez à votre fichier modèle personnalisé et cliquez sur **Ouvrir**.

   Le modèle est ajouté à la liste dans le panneau de gauche et peut être utilisé pour la génération de rapports personnalisés.

Chapitre 11. Outils

La présente section explique comment utiliser les outils supplémentaires fournis avec IBM Security AppScan Standard.

Boîte de dialogue Options

La présente section décrit les options que vous pouvez contrôler pour personnaliser AppScan, à partir de la boîte de dialogue **Options** (**Outils > Options**).

Les modifications effectuées dans cette boîte de dialogue sont appliquées à AppScan via des sessions et des analyses. La boîte de dialogue comporte cinq onglets.

Onglet Options d'examen

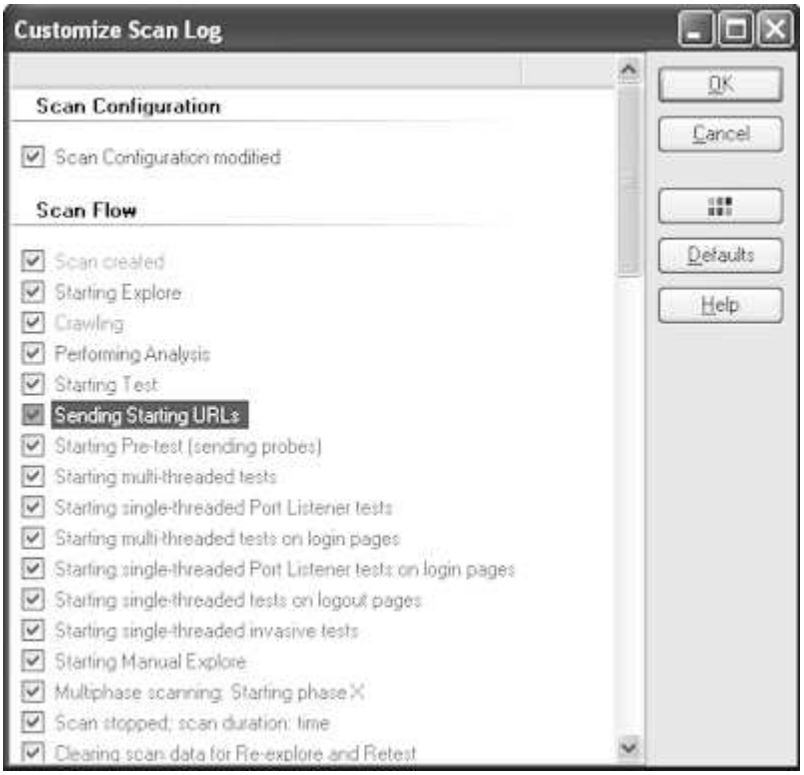
L'onglet **Outils > Options > Options d'examen** permet de contrôler le fonctionnement d'AppScan pendant un examen.

Option	Description
Surveillance des examens :	
Activer le journal d'examen	Vous pouvez activer/désactiver le journal d'examen et utiliser le bouton **Personnaliser** pour choisir quels éléments exactement apparaissent dans le journal ainsi que leur couleur. Voir «Personnaliser le journal d'examen».
Activer la consignation des demandes/réponses	Vous pouvez activer la **consignation des demandes/réponses** pour aider le support technique le cas échéant. Sachez cependant que l'activation du journal peut affecter la performance. Il doit rester désactivé tant que vous n'en avez pas besoin.
Surveiller la quantité de mémoire utilisée et l'espace disque	AppScan vérifie la mémoire physique et virtuelle et l'espace disque disponibles et envoie un avertissement si l'une ou l'autre descendent en dessous du seuil recommandé. Si vous décochez la case **Surveiller la quantité de mémoire utilisée et l'espace disque** (désactive la surveillance de la mémoire et de l'espace disque), AppScan n'exécute pas ces vérifications.
Indiquer si l'examen est terminé	Si cette option est sélectionnée, `Scan Incomplete` apparaît dans le coin inférieur gauche de la Liste des résultats lorsqu'un examen est arrêté avant la fin, pour vous rappeler que les résultats sont incomplets.
Sauvegarder automatiquement lors de l'examen	Sauvegarde un fichier de l'examen (.scan) pendant son exécution. **Intervalle en minutes :** Entrez le nombre de minutes entre deux sauvegardes ou utilisez la barre de défilement pour modifier l'intervalle.
Communications :	
Support TLS/SSL	Si votre application utilise des protocoles sécurisés pour communiquer avec des clients, configurez AppScan pour qu'il prenne en charge les protocoles appropriés. Les options sont TLS 1, 1.1, 1.2 et SSL 2. La modification de cette option nécessite que vous redémarriez AppScan.
Version HTTP	Choisissez la version HTTP du site : 1.0 ou 1.1

Personnaliser le journal d'examen

Vous pouvez choisir les éléments à faire apparaître dans le journal d'examen ainsi que leur couleur.

Le«Journal d'examen», à la page 300 répertorie des actions exécutées par AppScan lors de l'examen en cours. La boîte de dialogue **Personnaliser le journal d'examen** (**Outils > Options > onglet Options d'examen > Personnaliser**) contient une liste déroulante présentant tous les éléments pouvant être inclus au journal, une case à cocher indiquant s'ils sont actuellement inclus et un texte coloré indiquant la couleur dans laquelle ils apparaissent dans le journal.



- Pour exclure/inclure un élément à partir du journal d'examen, il suffit de désélectionner/sélectionner la case à cocher en regard de ce dernier.
- Pour modifier la couleur d'affichage d'un élément dans le journal d'examen : Sélectionnez l'élément, cliquez sur  , choisissez une couleur dans la palette de couleurs qui s'ouvre, puis cliquez sur **OK**.
- Pour restaurer les paramètres par défaut, cliquez sur l'option **par défaut**.

Activation du bouclage pour Microsoft Edge avec Windows 10

Une configuration spéciale peut s'avérer nécessaire pour pouvoir utiliser Edge comme le navigateur externe avec le système d'exploitation Windows 10.

Microsoft Windows 10 utilise une technologie d'isolement ("AppContainer") susceptible d'empêcher l'envoi de demandes depuis Edge vers votre application via AppScan. Bien que cela ne se produise pas toujours, il est recommandé d'activer le bouclage avant de procéder à un examen à l'aide d'Edge configuré comme navigateur externe.

Des instructions relatives à l'activation du bouclage sont disponibles sur la page de résolution des problèmes de Microsoft : https://msdn.microsoft.com/en-us/library/windows/apps/Hh780593.aspx

- Si vous souhaitez activer le bouclage pour Edge, utilisez la commande suivante :
  ```
  CheckNetIsolation LoopbackExempt -a -n="Microsoft.MicrosoftEdge_8wekyb3d8bbwe"
  ```
- Si vous souhaitez désactiver le bouclage pour Edge, utilisez la commande suivante :
  ```
  CheckNetIsolation.exe LoopbackExempt –d –n="Microsoft.MicrosoftEdge_8wekyb3d8bbwe"
  ```

Remarque : Pour plus de détails, voir : https://blogs.msdn.microsoft.com/fiddler/2011/12/10/revisiting-fiddler-and-win8-immersive-applications/

Onglet Préférences

L'onglet **Outils > Options > Préférences** permet de contrôler les fichiers AppScan, les recommandations de correction apparaissant dans l'interface graphique, ainsi que l'écran d'accueil.

Option	Description
Afficher l'écran d'accueil au démarrage	L'écran d'accueil apparaît lorsque AppScan est lancé. Il permet d'accéder rapidement aux examens de configuration et de chargement. Si vous constatez que vous fermez l'écran d'accueil plus souvent que vous n'utilisez ses fonctions, vous pouvez désactiver son ouverture en décochant cette case.
Rechercher les mises à jour au démarrage	A son lancement, AppScan recherchera les tests, problèmes de sécurité et correctifs mis à jour. Pour désactiver cette vérification, décochez cette case. Vous pouvez obtenir des mises à jour lorsque vous le souhaitez : **Aide > Rechercher les mises à jour**.
Installer automatiquement les mises à jour de sécurité	Si cette case est cochée, les mises à jour s'installent sans intervention, pendant que vous travaillez.
Rapport Faux positif : Chiffrer les fichiers	Ce paramètre s'applique à «Rapport Faux positif des résultats de test», à la page 222. AppScan chiffrera les fichiers zippés d'informations de variantes sélectionnés avant de les joindre à un nouveau poste de votre client de messagerie par défaut. Décochez cette case si le message électronique que vous souhaitez envoyer n'est pas destiné à l'équipe de support d'AppScan.
Exécuter Scan Expert avant l'examen	(Sélectionnée par défaut) Si cette option est sélectionnée, Scan Expert s'exécute automatiquement lorsque vous exécutez un examen complet (exploration et test), mais ne s'exécute pas lorsque vous sélectionnez uniquement l'exploration ou le test.
Inclure les vidéos de formation recommandées	Certains conseils sont accompagnés de courtes vidéos de formation qui peuvent être intégrées dans l'onglet Conseil et être visualisées en même temps que le conseil. Désélectionnez cette option si vous devez réduire la taille du fichier.
Paramètres des recommandations de correction	Si votre application n'utilise pas l'un ou plusieurs des environnements répertoriés, vous n'avez pas à lire les recommandations de correction spécifiques à ces environnements. Décochez les cases des environnements (.NET / Java EE / PHP) qui ne sont pas adaptés à votre application.
Navigateur pour l'enregistrement et la navigation	Sélectionnez le navigateur par défaut qui sera utilisé pour afficher l'URL de départ et pour procéder aux explorations manuelles. Sélectionnez l'un des deux boutons radio, puis sélectionnez un navigateur dans la liste déroulante. • **Utiliser le navigateur intégré :** Si vous sélectionnez cette option, vous avez le choix entre le navigateur IE intégré et les navigateurs Chromium d'AppScan. • **Utiliser le navigateur externe :** Si vous sélectionnez cette option, vous avez le choix entre les navigateurs pris en charge installés sur votre machine.

Onglet Enregistrement du proxy

Cet onglet permet de configurer AppScan de sorte qu'il agisse en tant que proxy pour les navigateurs externes ou qu'il explore manuellement des services Web non SOAP en utilisant un périphérique distant (comme un téléphone mobile) ou une application locale (comme un simulateur ou un émulateur).

Option	Description
Port du proxy	Indique le port utilisé par AppScan. Lorsque vous utilisez AppScan comme serveur proxy, configurez le navigateur externe ou le périphérique mobile de sorte qu'il utilise ce port. Utilisez cette case à cocher pour indiquer si AppScan sélectionne un port disponible automatiquement ou vous laisse le choisir. Le port peut changer d'une session à l'autre s'il est choisi automatiquement, ce qui vous obligera à reconfigurer votre périphérique mobile.
Connexions externes	Ce paramètre détermine quelles connexions aux domaines externes sont acceptées. **Rejeter tout** (Par défaut) Les tentatives de connexion à partir de toutes les adresses IP externes seront rejetées. Utilisez ce paramètre uniquement si vous devez procéder à une exploration à l'aide d'une application sur la même machine qu'AppScan. **Accepter la liste blanche uniquement** Les connexions à partir d'adresses IP externes qui apparaissent sur la liste blanche seront acceptées, les autres seront rejetées. **Accepter la liste blanche et me demander pour les autres** Les connexions à partir d'adresses IP externes qui apparaissent sur la liste blanche seront acceptées automatiquement. Pour toutes les autres, l'utilisateur AppScan doit répondre à une demande comportant une option d'ajout de la nouvelle adresse IP à la liste blanche. Sachez que les demandes ne sont visibles que si l'enregistreur de trafic externe est ouvert.
Liste blanche	Les connexions à partir d'adresses IP répertoriées dans cette liste seront acceptées automatiquement. Pour ajouter de nouvelles adresses IP à la liste, cliquez sur  et sélectionnez une option : • Pour ajouter une seule adresse IP, saisissez-la, ainsi qu'une description le cas échéant. **Conseil :** Si vous devez utiliser un périphérique distant mais que vous ne connaissez pas son adresse IP, ou si cette dernière change souvent, sélectionnez **Accepter la liste blanche et me demander pour les autres**. La première fois que le périphérique se connecte avec une nouvelle adresse IP, une fenêtre en incrustation s'affiche pour vous permettre d'ajouter cette dernière à la liste blanche. • Pour ajouter une *plage* d'adresses IP, ajoutez une adresse IPv4 et un masque de sous-réseau ou une adresse IPv6 et une longueur de préfixe de sous-réseau, et une description le cas échéant.

Option	Description
Certificat SSL AppScan	Comme AppScan doit agir en tant que proxy afin d'enregistrer le trafic entre le service Web et le périphérique utilisé pour l'exploration manuelle, le serveur utilisant HTTPS envoie les certificats SSL au périphérique à la place du certificat du service Web. Lorsqu'un navigateur reçoit un certificat non reconnu, il avertit généralement l'utilisateur via une fenêtre en incrustation, mais dans le cas d'un périphérique mobile, la demande est en général ignorée. Il est donc impossible d'explorer l'application à moins que le certificat AppScan soit accepté sur le périphérique qui envoie les demandes. **Ajouter** Ajoute le certificat SSL AppScan aux certificats racine sur cette machine. Effectuez cette opération pour autoriser l'envoi des demandes au service Web. Le certificat AppScan sera ajouté au certificat racine et les demandes du service Web destinées au simulateur ne seront pas rejetées. **Remarque :** Une fois le certificat ajouté, le bouton est remplacé par **Supprimer** et peut être utilisé pour supprimer le certificat de la machine AppScan. **Exporter** Sauvegarde le certificat SSL AppScan *installé sur cette machine*, sous forme de fichier ZIP, pour qu'il puisse être ajouté manuellement aux certificats racine sur un autre périphérique. Notez que cette opération n'est souvent pas nécessaire puisqu'il peut généralement être importé directement depuis le périphérique. 1. Dans AppScan, cliquez sur **Examen > Exploration manuelle > Utilisation du périphérique externe** L'enregistreur du trafic externe s'affiche à l'état "En attente des connexions entrantes". **Important :** Laissez-le ouvert pour les sous-étapes suivantes. 2. Sur le périphérique mobile, accédez au répertoire `http://appscan` 3. Dans AppScan, si le système vous demande d'autoriser une connexion entrante à partir du périphérique, cliquez sur **OK**. Lorsque le périphérique est connecté à AppScan comme proxy, un message (sur le périphérique) confirme la connexion, l'adresse IP et le port. Si le certificat est installé sur la machine AppScan, un bouton permettant de l'installer sur le périphérique est également disponible. **Remarque :** Si ce bouton est grisé, le certificat n'est pas installé sur la machine AppScan. **Remarque :** Le domaine et la demande du périphérique s'affichent alors dans les listes de l'enregistreur de trafic externe. 4. Sur le périphérique mobile, tapez **Installer le certificat SSL AppScan** Le certificat est installé. **Remarque :** Si le périphérique ne peut pas accéder à l'application que vous testez après cette procédure, installez manuellement le certificat (sur le périphérique distant ou l'application) : a. Dans AppScan, ouvrez **Outils > Options > Enregistrement du proxy** b. Cliquez sur **Exporter** et enregistrez le certificat sous forme de fichier ZIP. c. Installez le certificat en tant que certificat racine sur le périphérique ou l'application. 5. Lorsque vous avez terminé, cliquez sur **Annuler** dans l'enregistreur du trafic externe pour fermer ce dernier. **Remarque :** Cette option est active uniquement si le certificat est déjà ajouté aux certificats racine sur *cette* machine. **Avertissement :** Le certificat AppScan qui est exporté doit être identique à celui qui est installé en local. Si vous **supprimez** le certificat local avant de le **rajouter**, vous devez le réinstaller sur le périphérique car le nouveau certificat est différent du précédent.

Pour plus d'informations, voir «Utilisation d'AppScan comme proxy d'enregistrement», à la page 150.

Onglet Général

L'onglet **Outils > Options > Générales** fournit des options permettant de vérifier de quelle manière AppScan définit les priorités des problèmes, obtient des mises à jour et affiche des boîtes de dialogue.

Option	Description	
Emplacements de fichiers	Lors de l'utilisation, AppScan écrit divers fichiers sur le disque. Vous pouvez modifier les emplacements où ces fichiers sont enregistrés en cliquant sur le bouton de navigation situé à droite du type de fichier et en accédant à un autre emplacement.	
	Fichiers utilisateur	*.scan (Examen), *.exd (Données d'exploration), *.xml (Rapport, Exportation), *.scant (Modèle d'examen), *.asreg (Modèle de rapport), *.aspol (Stratégies de test) ...\My Documents\AppScan
	Fichiers journaux	*.log (Journal), *.lic (Licence), *.dmp (Vidage de mémoire), *.css (Support compressé) [Dossier d'installation AppScan Standard]\Logs
	Conseils personnalisés	*.xml (Fichier de conseil créé par l'utilisateur) ...\My Documents\AppScan\Advisories
	Fichier de classification des bruits	*.xml [Dossier d'installation AppScan Standard]\IssueManagement (Pour plus de détails, voir «Etat du problème : Ouvert ou Bruit», à la page 209.) Un clic sur le bouton – supprime le fichier de classification des bruits et restaure les classifications de bruits par défaut.
Taille du fichier journal	Définissez la taille maximale du fichier journal, en mégaoctets. Lorsque la limite est atteinte, le fichier est enregistré en tant que sauvegarde et un nouveau fichier journal est ouvert. (Au prochain enregistrement d'une sauvegarde, la sauvegarde précédente est supprimée.) Si vous avez limité l'espace sur votre disque dur, vous pouvez limiter la taille du fichier journal AppScan.	
Niveau de priorité du système d'exploitation	Par défaut, AppScan a une priorité **Normale** sur les applications en cours d'exécution. Si d'autres applications ont besoin de plus de ressources provenant de votre ordinateur, vous pouvez modifier la valeur d'AppScan par **inactif**, d'un niveau inférieur, ne lui permettant de s'exécuter que si d'autres applications n'utilisent pas les ressources. **ATTENTION :** **La modification du niveau de priorité du système d'exploitation peut affecter gravement la performance des autres applications en cours d'exécution sur le même système.**	
Réinitialiser la suppression des boîtes de dialogue	Si vous avez coché la case "Ne plus afficher" dans un avertissement AppScan, vous pouvez redéfinir les boîtes de dialogue pour les afficher à nouveau en cliquant sur le bouton Réinitialiser la suppression des boîtes de dialogue.	
Effacer l'historique	Cliquez pour effacer toutes les listes d'historique : historique de l'URL, liste des examens récents, liste des modèles récents, chaînes de recherche récentes et stratégies définies par l'utilisateur récentes.	

Option	Description
Sélectionner la langue	Si AppScan peut fonctionner sur votre poste de travail en plusieurs langues, vous pouvez sélectionner la langue de l'interface ici. Après avoir modifié ce paramètre, vous serez peut-être invité à fermer et rouvrir AppScan pour que la modification soit prise en compte.

Onglet Avancé

L'onglet **Outils > Options > Avancé** vous permet d'afficher et de changer les valeurs par défaut des paramètres avancés.

L'onglet Avancé répertorie le type (chaîne, DWord ou booléen) et la valeur en cours de nombreux paramètres et permet de modifier ces valeurs. Lorsque vous sélectionnez un paramètre en cliquant dessus, une brève description de ce paramètre et de son utilisation s'affiche en bas de la liste.

- Pour localiser un nom (ou des noms) de préférence en particulier, entrez un mot ou un fragment dans la zone de filtre en haut de la boîte de dialogue. Utilisez la flèche de recherche jusqu'à **Respecter la casse** et/ou **Mot entier.**
- Pour modifier un paramètre, cliquez sur la zone Valeur et sélectionnez ou entrez la nouvelle valeur.

  Les paramètres ayant été modifiés et n'étant plus définis sur leurs valeurs par défaut apparaissent en gras.

  Remarque : Si vous tentez d'entrer une valeur non valide, un avertissement s'affiche et la valeur n'est pas acceptée.
- Pour restaurer la valeur par défaut d'une préférence *unique*, cliquez avec le bouton droit de la souris sur Préférence et sélectionnez **Restaurer la valeur par défaut**.
- Pour restaurer la valeur par défaut de *tous* les paramètres, cliquez sur le bouton **Restaurer les valeurs par défaut** en bas de la boîte de dialogue.

Assistant de configuration des services Web

Cette extension vous permet de numériser à l'aide des fichiers de description Open API. Elle est disponible dans Outils > Extensions > Assistant Services Web (Open API), et l'extension est activée par défaut.

Cette extension AppScan prend en charge les analyses de services Web basées sur les fichiers de description des Open API (v2 et v3) (JSON ou YAML). Les étapes ci-dessous montrent le flux de travail de l'assistant. Cliquez sur le nom de l'étape pour voir les détails de cette étape.

Remarque : Cette extension explore uniquement les services web. Tout autre lien est ignoré.

Remarque : L'utilisation des clés API comme paramètres de requête HTTP n'est pas prise en charge.

Tableau 9. Flux de travail de configuration des services Web

Étape	Nom de l'étape	Description
1	Fichiers de description	Ajoutez un ou plusieurs fichiers de description Open API qui définissent le service Web.
2	Domaines	Les domaines trouvés dans les fichiers de description sont ajoutés à la liste des domaines qui peuvent être analysés. Dans cette étape, vous pouvez supprimer tous ceux qui ne doivent pas être numérisés.
3	Gestion de connexion	Définir la procédure de connexion pour le service Web.

Tableau 9. Flux de travail de configuration des services Web (suite)

Étape	Nom de l'étape	Description
4	«Séquences», à la page 267	Revoir les requêtes créées à partir des fichiers de description, et leurs paramètres, et créer des "séquences" de requêtes qui doivent être envoyées dans un ordre spécifique. **Important :** Des séquences de requêtes correctement construites sont *essentielles* pour permettre à AppScan de créer des objets qui dépendent de la création précédente d'un autre objet.
5	Paramètres	Revoir tous les paramètres trouvés dans les requêtes. Vous pouvez sélectionner les paramètres qui sont suivis et ceux qui ne le sont pas, et modifier leurs valeurs.
6	Terminée	Une fois la configuration terminée, décidez si vous voulez lancer l'analyse maintenant ou plus tard.

Tâches supplémentaires :

Après avoir terminé la configuration de l'assistant, une tâche supplémentaire possible (en fonction de votre service) peut être la configuration des en-têtes personnalisés dans la boîte de dialogue principale de configuration AppScan. Pour plus de détails, voir «Variables de la séquence», à la page 102.

Fichiers de description

Ajoutez un ou plusieurs fichiers de description Open API qui définissent le service Web.

Notez que vous ne pouvez pas ajouter de fichiers locaux, seulement des URLs. Si nécessaire, téléchargez vos fichiers de description sur votre serveur Web et fournissez l'URL.

Pour créer votre liste de fichiers de description :

1. Dans le champ URL, entrez un lien Open API et cliquez sur Ajouter. L'URL est validée et ajoutée à la liste.
2. Ajoutez d'autres URL au besoin.
3. Lorsque la liste est complète, cliquez sur **Suivant**. Les liens sont revalidés et l'étape suivante s'ouvre.

Etape suivante :«Domaines»

Domaines

Tous les domaines trouvés dans les fichiers de description sont ajoutés à la liste des domaines qui peuvent être analysés. Dans cette étape, vous pouvez supprimer tous ceux qui ne doivent pas être numérisés.

Les domaines répertoriés dans le volet de droite (" Domaines inclus ") seront analysés. Vous devez déplacer tous les domaines qui ne doivent pas être analysés vers le volet de gauche (" Domaines exclus ").

Pour exclure un domaine de l'analyse :

- Sélectionnez le domaine et cliquez sur la flèche gauche. Le domaine sélectionné est déplacé dans le volet Domaines exclus.

Etape suivante :«Gestion de connexion»

Gestion de connexion

Configurez la procédure de connexion pour le service web.

Si une connexion est nécessaire, vous devez la configurer pour qu'AppScan puisse se connecter au service.

Limitation : L'utilisation des clés API comme paramètres de requête HTTP n'est pas prise en charge.

Sélectionnez l'un des boutons radio Login :

Configurez la connexion ci-dessous
Si vous sélectionnez cette option, la partie inférieure de la boîte de dialogue devient active et vous permet de saisir ce qui suit :

1. **Demande de connexion :** Sélectionnez une demande de connexion dans la liste déroulante des demandes des fichiers de description.

   Remarque : Si le service Web implémente le contrôle d'autorisation à l'aide des clés API, une demande de connexion n'est *pas* nécessaire, alors sélectionnez **Aucun** dans la liste déroulante.
2. **Droits d'accès :** Vérifiez et, si nécessaire, modifiez les valeurs des informations d'identification de connexion.
3. **En-têtes personnalisés :** Si le service utilise des en-têtes personnalisés (tels que l'authentification au porteur dans l'en-tête d'autorisation), cliquez sur **Modifier** pour ouvrir la boîte de dialogue Ajouter un en-tête personnalisé. Pour plus d'informations, voir «Onglet En-têtes personnalisés», à la page 88.
4. **la demande de la détection En session :** Sélectionnez une demande de session dans la liste déroulante. Ceci sera utilisé par AppScan pour vérifier qu'il est connecté lors du test.

Utiliser la configuration de connexion existante
Sélectionnez si votre configuration de numérisation inclut déjà une séquence de connexion valide, vous pouvez l'utiliser.

Enregistrez la séquence de connexion dans Configuration AppScan > Gestion des connexions
Sélectionnez cette option si le fichier de description ne contient pas de demande de connexion. Vous pouvez utiliser la boîte de dialogue principale de configuration AppScan pour enregistrer la connexion en utilisant le navigateur intégré AppScan ou un périphérique externe. C'est le plus souvent le cas lorsque les utilisateurs se connectent via une interface utilisateur, ou lorsque JavaScript est impliqué dans le processus de connexion. Pour plus d'informations, voir «Vue Gestion de connexion», à la page 51.

Aucun
Sélectionnez cette option si le service ne nécessite pas de connexion.

Etape suivante :«Séquences»

Séquences

Revoir la liste des requêtes créées à partir des fichiers de description (et leurs paramètres), et définir les "Séquences" de requêtes qui doivent être envoyées dans un ordre spécifique (les objets qui dépendent d'autres objets étant créés en premier).

Demandes

Le **volet de gauche** de l'onglet Demandes affiche une liste de toutes les demandes créées à partir des fichiers de définition ; pour chacune d'elles, sa méthode et son chemin. Sélectionnez n'importe quelle demande à voir :

- **Volet supérieur droit** : Une liste des paramètres de la requête, avec leur Nom, Type, Emplacement et Valeur. Vous pouvez également cliquer sur l'icône **Modifier** pour voir sa description et modifier sa valeur, suivre le paramètre et appliquer le changement de valeur à tous les paramètres similaires.

- **Volet inférieur droit** : La requête HTTP brute, y compris les en-têtes, etc., exactement comme elle sera envoyée. Vous pouvez cliquer sur le bouton **Envoyer** pour envoyer la demande et voir la réponse dans la partie inférieure du même volet.
- Exclure une requête de l'analyse en **cliquant avec le bouton droit de la souris > Exclure la requête**. La demande est biffée. Pour l'inclure à nouveau avec le bouton droit de la souris, utilisez **Clic-Droit > Inclure la requête**.

Séquences

Des séquences correctement construites, exprimant les dépendances entre les objets, sont des outils importants dans l'analyse complète d'un service Web. Lorsqu'une demande de création d'un objet particulier dépend de la création préalable d'un autre objet, la séquence correcte des demandes doit être configurée.

Pour configurer une séquence :

1. Dans l'**onglet Demandes**, cliquez sur la première demande de la séquence pour la sélectionner.
2. Cliquez et maintenez enfoncée la **touche Ctrl**, et sélectionnez les autres requêtes dans l'ordre correct. Relâchez ensuite la touche Ctrl. Toutes les requêtes de la séquence apparaissent maintenant sélectionnées.
3. Entrez un nom pour la séquence dans le champ Nom, puis cliquez sur **Créer une séquence**.
4. Cliquez sur l'**onglet Séquences** pour voir :
   - **Volet gauche** : Toutes les séquences configurées. Chaque séquence peut être activée pour l'analyse ou désactivée pour l'enregistrer en vue d'une autre analyse, en cochant ou décochant la case **Activé**.
   - **Volet supérieur droit** : Les URL enregistrées dans la séquence sélectionnée. Vous pouvez utiliser les flèches **Haut/Bas** pour changer l'ordre des requêtes et la touche**Moins** pour supprimer les requêtes de la séquence.
   - **Volet inférieur droit** : La liste des variables trouvées dans la séquence sélectionnée. Vous pouvez cliquer avec le bouton droit de la souris sur une variable pour définir une *valeur dynamique*. Pour plus de détails, voir «Variables de la séquence», à la page 102.

Etape suivante :«Paramètres»

Paramètres

Revoir tous les paramètres trouvés dans les requêtes. Vous pouvez sélectionner les paramètres qui sont suivis et ceux qui ne le sont pas, et modifier leurs valeurs.

Cette étape affiche tous les paramètres trouvés dans les requêtes de l'application sous la forme d'une liste unique et est particulièrement utile lorsque vous souhaitez suivre ou modifier la valeur de plusieurs paramètres. Vous pouvez :

- Modifiez la valeur et l'état de suivi des paramètres individuels en cliquant sur le paramètre.
- Modifiez la valeur générale par défaut, le nom d'utilisateur et le mot de passe.

  Remarque : Si des valeurs par défaut sont définies dans les fichiers de description, elles sont utilisées sauf si elles sont modifiées ici. S'il existe des définitions dans la configuration du Remplisseur de formulaires, elles sont utilisées pour les paramètres non définis dans le fichier de description.
- Restaurer les valeurs par défaut après que les modifications aient été effectuées.

Etape suivante :«Terminée», à la page 269

Terminée

Une fois la configuration terminée, décidez si vous voulez lancer l'analyse maintenant ou plus tard.

Maintenant que votre configuration est terminée, vous pouvez :

- **Démarrer un examen automatique intégral**
- **Commencez par l'Explorateur automatique uniquement** (pour pouvoir consulter les résultats de l'Explorateur avant de continuer avec l'étape Test).
- **Démarrer l'examen plus tard**

Par défaut, l'assistant applique la stratégie de test des services Web, sauf si votre configuration spécifie une stratégie de test autre que celle par défaut. Vous pouvez changer cela en cochant ou décochant la case.

Planificateur d'examens

Vous pouvez définir des examens de sorte de démarrer automatiquement dans un examen. Les planifications d'examens peuvent se produire qu'une seule fois ou sur une base régulière. Au moment où la planification de l'examen est prévue, AppScan s'ouvre automatiquement et exécute l'examen.

Planifier un nouvel examen

Pourquoi et quand exécuter cette tâche

Vous pouvez planifier des examens à l'aide de la configuration de l'examen en cours ou d'un examen sauvegardé. Les examens planifiés reçoivent le nom de l'examen source, avec la date et l'heure, et sont enregistrés dans la même dossier que l'examen source.

Procédure

1. Dans le menu **Outils** cliquez sur **Planificateur d'examens**.

   La boîte de dialogue **Planificateur d'examens** apparaît, répertoriant tous les examens planifiés.
2. Cliquez sur **Nouveau**.

   La boîte de dialogue **Paramètres de planification** s'affiche.
3. Entrez un nom pour l'examen planifié.
4. Choisissez si vous voulez planifier l'examen en cours ou le chargement d'un examen sauvegardé (fichier ***.scan**).

   Si vous choisissez l'examen en cours et qu'il n'est pas sauvegardé, AppScan vous demande de le sauvegarder en tant que fichier d'examen à charger par le planificateur.
5. Sélectionnez la récurrence de planification : quotidienne, hebdomadaire, mensuelle ou ponctuellement à une date et heure spécifiées.
6. Sélectionnez la date et l'heure auxquelles le premier examen démarrera.
7. Vous pouvez éventuellement définir une limite d'heure pour l'examen en cochant la case **Limiter la durée de l'examen**, puis en entrant une durée maximale d'examen, en minutes.
8. Entrez votre nom de domaine, nom d'utilisateur et mot de passe.

   Ces valeurs d'authentification permettent à la tâche de s'exécuter comme si elle avait été démarrée par l'utilisateur donné ; sans elles, la tâche ne peut pas s'exécuter.
9. Cliquez sur **OK**.

   Le nom du planning apparaît dans la boîte de dialogue **Planificateur d'examens**.

Editer la configuration des examens planifiés

Procédure

1. Dans la boîte de dialogue **Planificateur d'examens** (**Outils | Planificateur d'examens)**, sélectionnez un examen planifié.
2. Cliquez sur **Editer**.

   La boîte de dialogue **Paramètres de planification** s'affiche.
3. Editez les détails comme nécessaire.
4. Cliquez sur **OK**.

Supprimer un examen planifié

Procédure

1. Dans la boîte de dialogue **Planificateur d'examens** (**Outils > Planificateur d'examens**), sélectionnez un examen planifié.
2. Cliquez sur **Supprimer**.

Planifier uniquement une étape de test

Pourquoi et quand exécuter cette tâche

Un examen intégral est constitué de deux étapes : l'exploration et le test. S'il n'est pas nécessaire d'exécuter l'étape d'exploration à chaque fois, vous pouvez configurer un examen planifié pour n'exécuter que l'étape de test. Pour ce faire, utilisez l'option *Tâches planifiées* du *Panneau de configuration* Windows.

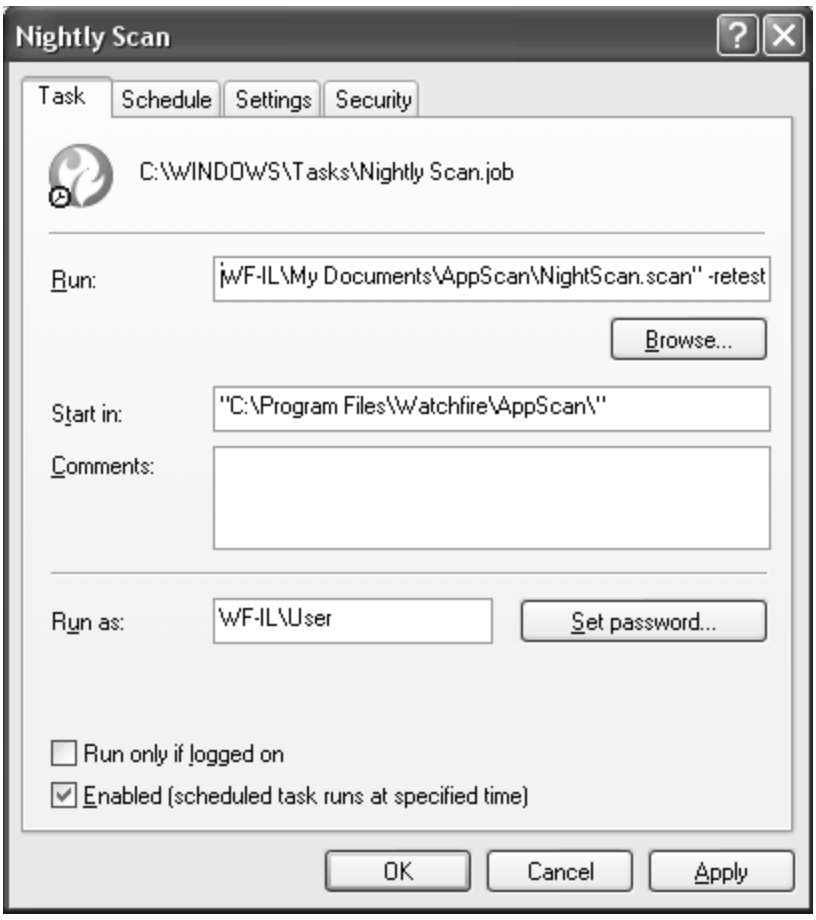
Procédure

1. Dans AppScan, «Planifier un nouvel examen», à la page 269 (**Outils > Planificateur d'examens > Nouveau**).
2. Dans le menu **Démarrer** de Windows, cliquez sur **Panneau de configuration | Tâches planifiées**.

   Remarque : Si l'option *Tâches planifiées* n'apparaît pas dans votre *Panneau de configuration* Windows, vous êtes probablement sous l'affichage *Catégories*, lequel n'affiche pas toutes les options. Si nécessaire, passez à l'*affichage classique*.

   La boîte de dialogue des tâches planifiées de Windows s'ouvre et la tâche créée dans AppScan apparaît dans la liste.
3. Cliquez avec le bouton droit de la souris sur l'examen planifié AppScan et sélectionnez **Propriétés** dans le menu en incrustation.

   La boîte de dialogue *Scheduled Task Properties* (Propriétés de la tâche planifiée) s'ouvre.



4. Dans la zone d'*exécution*, à la fin de la chaîne de texte (après les guillemets finaux), entrez : **[espace][tiret]retest**.
5. Cliquez sur **OK**.

   A l'heure planifiée, seule l'étape de test sera exécutée.

Planifier un examen par épisodes

Pourquoi et quand exécuter cette tâche

Si vous disposez de "fenêtres de temps" limitées pendant lesquelles exécuter des examens (par exemple, vous ne disposez que de trois heures par jour entre 1H00 et 4H00) et que vos examens ont besoin de plus de temps pour s'exécuter complètement, vous pouvez configurer un examen planifié pour s'exécuter par épisodes. Pour ce faire, vous devez demander à AppScan de :

- sauvegarder l'examen avec le nom de fichier d'origine (sans l'horodatage faisant partie de son nom) ;
- continuer le prochain examen planifié à l'étape où le précédent examen avait été arrêté.

Ceci est réalisé en ajoutant des paramètres de ligne de commande via l'option *Tâches planifiées* du *Panneau de configuration* Windows.

Procédure

1. Dans AppScan, «Planifier un nouvel examen», à la page 269 (**Outils > Planificateur d'examens > Nouveau**).
2. Dans la zone **Exécuter** du menu Démarrer de Windows, tapez `Task Scheduler`.

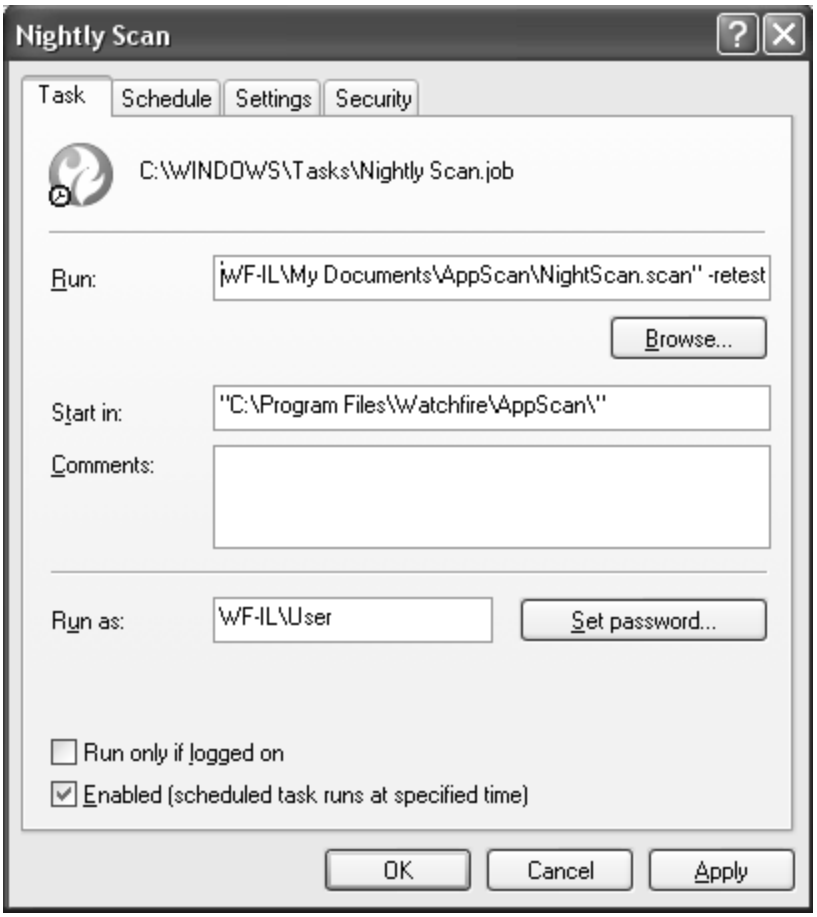
   La boîte de dialogue des tâches planifiées de Windows s'ouvre et la tâche créée dans AppScan apparaît dans la liste.

3. Cliquez avec le bouton droit de la souris sur l'examen planifié et sélectionnez **Propriétés**.
   La boîte de dialogue des propriétés de la tâche planifiée s'ouvre.
4. Dans l'onglet Déclencheurs, configurez la tâche selon vos besoins. Pour plus d'informations, reportez-vous à la documentation Microsoft Windows.

Paramètres de ligne de commande des tâches planifiées

Le tableau ci-dessous recense les paramètres de ligne de commande disponibles pouvant être utilisés dans la boîte de dialogue *Tâches planifiées* du *Panneau de configuration Windows*.

Les paramètres sont ajoutés après la chaîne principale de la zone Exécuter de l'onglet Tâche.



Paramètre de ligne de commande	Fonction
[space][number]	Ce nombre correspond au délai d'attente, en minutes, de l'examen planifié.
[space][hyphen]retest	Configure l'examen planifié pour qu'il démarre avec l'étape de test, sans exécuter l'étape d'exploration. Ce paramètre peut être utile pour tester de nouveau un site à certains intervalles en utilisant un examen source ayant déjà exploré le site.

Paramètre de ligne de commande	Fonction
[space][hyphen]continue	Configure l'examen planifié pour poursuivre à partir de l'endroit où il avait été interrompu, plutôt que de redémarrer un examen. Ce paramètre peut être utile pour tester de nouveau un site à certains intervalles en utilisant un examen source ayant déjà exploré le site. Notez que lorsque vous utilisez cette option pour réaliser un examen *par épisodes*, vous devez également utiliser le commutateur *saveName*, de sorte que l'examen planifié écrase l'original chaque fois qu'il s'exécute. (Voir «Planifier un examen par épisodes», à la page 271.)
[space][hyphen]saveName[filename]	Définit le nom sous lequel l'examen planifié sera enregistré. Lorsqu'aucun *saveName* n'est sélectionné, AppScan enregistre l'examen planifié sous le nom de fichier source suivi d'un horodatage.

Tests définis par l'utilisateur

AppScan offre une base de données composée de milliers de tests. Cependant, si votre application Web comporte des problèmes qui lui sont spécifiques, ou si vous souhaitez écrire vos propres conseils pour corriger les problèmes, vous pouvez créer vos propres tests. Ces tests sont sauvegardés et inclus à votre base de données de tests AppScan.

Chaque test recherche un problème spécifique. Par exemple, un test modifiera un chemin d'accès dans une demande, un autre test modifiera une entrée utilisateur pour inclure un caractère non valide. Pour chaque test, vous pouvez définir plusieurs conditions pour les trois éléments suivants :

- **Filtrer :** Détermine les conditions à remplir pour exécuter le test.
- **Modification :** Détermine les modifications à apporter à la demande.
- **Validation :** Détermine les conditions à remplir pour que le résultat du test soit considéré comme positif.

Pour créer et gérer des tests définis par l'utilisateur, procédez comme suit :

- Cliquez sur **Outils > Tests définis par l'utilisateur**.

  La boîte de dialogue Tests définis par l'utilisateur s'ouvre et affiche la liste des tests qui ont été définis, ainsi que leur type. La case en regard de chaque test indique si le test est actuellement activé dans les examens.

Option	Description
Case à cocher Activer	Cochez/désélectionnez la case pour inclure ou exclure un test de l'examen en cours.
	Cliquez sur cette icône pour exporter **l'ensemble des tests définis par l'utilisateur** ou **une sélection de tests définis par l'utilisateur** avec leur statut activé/effacé sous la forme d'un fichier UDT qui peut être importé dans un autre examen.
	Cliquez sur cette icône pour importer un fichier UDT précédemment sauvegardé. Les tests de ce fichier sont ajoutés à la liste de ceux en cours.
	Sélectionnez une *ligne* de test (pas la case à cocher associée) et cliquez sur **Editer** pour ouvrir l'Assistant de création de tests définis par l'utilisateur et modifier le test sélectionné.

Option	Description
	Cliquez sur cette icône pour supprimer le test sélectionné.
	Cliquez sur cette icône pour ouvrir l'assistant de création de tests définis par l'utilisateur et créer un test.

Assistant de création des tests définis par l'utilisateur

L'assistant de création des tests définis par l'utilisateur permet de créer des tests définis par l'utilisateur appliqués par AppScan lors de l'examen, en plus des tests créés automatiquement.

L'écran de bienvenue permet de définir les attributs de test de base.

Attributs de test

Nom	Le nom affecté apparaît dans les résultats et les rapports de test.
Description	La description apparaît uniquement dans la liste Tests définis par l'utilisateur dans AppScan.
Créé(e) par	Cet attribut est utilisé en interne par AppScan pour établir une distinction entre les tests définis par l'utilisateur qui portent des noms identiques et pour signaler les conflits.
Gravité	Affectez le niveau de gravité Elevé, Moyen, Faible ou Message d'information au problème.

Une fois l'opération terminée, cliquez sur **Suivant** pour passer à l'étape suivante.

Type de test

Cette étape permet de définir le type de test que créez. Il détermine les étapes de l'assistant à afficher.

Les étapes de l'assistant varient en fonction du type de test que vous sélectionnez.

Modifier le chemin (infrastructure)	Crée un test qui tente d'atteindre une URL spécifique lors de l'examen.
Modifier les paramètres et les cookies	Crée un test qui modifie la valeur d'un ou de plusieurs cookies et/ou paramètres.
Modifier la demande complète	Crée un test qui modifie le chemin de la demande d'origine : • En définissant ou en ajoutant au début ou à la fin une section Filename • En ajoutant, en supprimant ou en modifiant un cookie ou paramètre • En remplaçant le corps de la demande
Recherche de schéma (pas de modification)	Crée un test qui recherche les conditions de validation dans toutes les réponses filtrées de l'étape d'exploration d'une application ; (vous pouvez définir un filtre ou inclure *toutes* les réponses.)
Validation globale (pour tous les tests AppScan)	Crée un test qui recherche les conditions de validation dans toutes les réponses de l'étape de test d'une application. Un résultat positif est considéré comme une vulnérabilité pour ce test défini par l'utilisateur.

Une fois l'opération terminée, cliquez sur **Suivant** pour passer à l'étape suivante.

Filtre

Cette étape permet de définir les conditions à remplir pour exécuter ce test. Seules les demandes remplissant ces conditions sont testées.

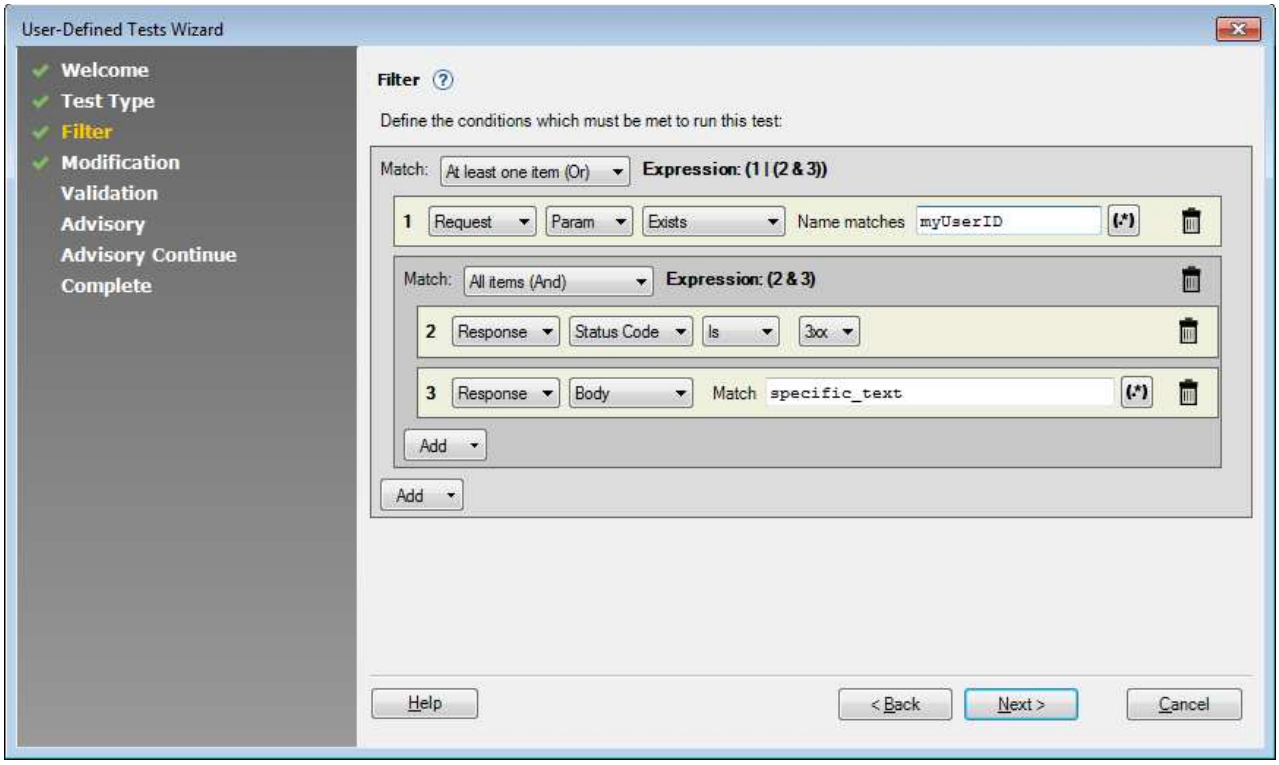
La définition de filtres qui limitent le test *uniquement* à des demandes pertinentes peut considérablement améliorer l'efficacité de la procédure.

- Cliquez sur **Ajouter** pour ajouter un filtre supplémentaire de type **Une fois** ou **Groupe**.
- Lorsque vous ajoutez plusieurs éléments, vous devez indiquer la relation logique qui les lie : **Tous**, **Tous** ou **Aucun**. Reportez-vous à l'exemple ci-dessous.

Une fois l'opération terminée, cliquez sur **Suivant** pour passer à l'étape suivante.

Exemple

Dans cet exemple, trois conditions ont été ajoutées. Le nouveau test est appliqué uniquement aux réponses qui remplissent la condition 1 (demande incluant le paramètre `myUserID`) ou qui remplissent *à la fois* les conditions 2 et 3 (code de statut de réponse égal à 3xx *et* corps de la réponse incluant `specific_text`).



L'expression prend la forme suivante :

```
( 1 | (2 & 3 )
```

Modification

Cette étape permet de définir les modifications apportées à la demande d'origine pour créer la demande de test.

Définissez la modification en ajoutant une ou plusieurs modifications à appliquer à la demande d'origine pour créer la demande de test.

- Cliquez sur **Ajouter** pour ajouter une modification.
- Si vous ajoutez plusieurs modifications, elles sont appliquées ensemble comme s'il s'agissait une seule modification. Pour les appliquer séparément, vous devez créer des tests distincts.
- Si vous souhaitez inclure une valeur dynamique dans la modification, cliquez sur l'icône Editeur de macro en regard de la zone Valeur.

Une fois l'opération terminée, cliquez sur **Suivant** pour passer à l'étape suivante.

Editeur de macro

L'éditeur de macro permet d'ajouter des valeurs dynamiques (macros) à des modifications de test défini par l'utilisateur.

Pour ajouter une valeur Modification qui inclut une ou plusieurs macros, procédez comme suit :

1. Cliquez sur l'icône **Editeur de macro** en regard de la zone Valeur.
2. Tapez le texte brut de votre choix dans la zone de saisie.
3. Placez le curseur au point d'insertion souhaité.
4. Sélectionnez une macro dans la liste qui apparaît au-dessous.
5. Cliquez sur **Insérer**.

Validation

Cette étape permet de définir les conditions indiquant que le test a abouti.

- Cliquez sur **Ajouter** pour ajouter un filtre supplémentaire de type **Une fois** ou **Groupe**.
- Lorsque vous ajoutez plusieurs éléments, vous devez indiquer la relation logique qui les lie : **Tous, Tous** ou **Aucun**.
- Dans la plupart des cas, la validation s'applique à la réponse à la demande de test ; il s'agit du comportement par défaut. En revanche, pour certaines vulnérabilités comme un script intersite stocké (Stored CSS), la validation doit être effectuée dans la réponse à une demande *différente*. Dans ce cas, sélectionnez le second bouton d'option (**Exécuter cette validation sur la réponse à la demande suivante :**), puis définissez la demande.

  Conseil : Pour contrôler davantage la définition d'URL, par exemple si vous devez remplacer le corps ou indiquer une procédure GET ou POST, cliquez sur **Editer la demande**.

Une fois l'opération terminée, cliquez sur **Suivant** pour passer à l'étape suivante.

Exemple

Pour obtenir un exemple, reportez-vous à l'étape «Filtre», à la page 274.

Conseil

Dans les étapes Conseil et Conseil - Suite, vous pouvez entrer le texte du conseil qui apparaîtra dans les résultats et les rapports de l'examen. Toutes les zones sont facultatives.

Description technique	Description technique de ce problème.
Produits concernés	Si ce problème affecte des produits tiers, répertoriez-les dans cette zone.
Tâche de résolution	Décrivez les tâches générales nécessaires pour résoudre le problème.
Recommandation de correction	Indiquez une solution ou une solution palliative pour ce problème.
Références et liens appropriés	Indiquez toutes les références ou tous les liens externes qui fournissent des informations complémentaires sur ce problème.

Une fois l'opération terminée, cliquez sur **Suivant** pour passer à l'étape suivante.

Fin de l'exécution de l'assistant

Une fois que vous avez défini le nouveau test, cliquez sur Terminer pour l'ajouter à la liste.

PowerTools

AppScan offre un accès à cinq utilitaires (PowerTools), chacun fournissant une fonction spécifique vous aidant à gérer la sécurité de votre application ou à utiliser AppScan.

Vous pouvez accéder aux outils PowerTools à partir d'within AppScan (**Outils > PowerTools**) ou indépendamment à partir du menu Démarrer de Windows.

Authentication Tester

Le PowerTool Authentication Tester est un utilitaire de test ayant recours à la technique dite de "force brute", qui révèle les combinaisons faibles nom d'utilisateur-mot de passe susceptibles d'être exploitées pour accéder à votre application Web. (Une attaque par force brute est un processus automatique par essai et erreur qui permet de deviner les données d'authentification. Elle peut amener un serveur à reconnaître un imposteur comme un utilisateur légitime.)

Avec la force brute, un utilisateur malveillant peut parcourir les combinaisons jusqu'à ce qu'il trouve des données d'identification lui donnant accès au domaine autorisé. La force brute lui permet également d'utiliser un fichier de dictionnaire, voire simplement d'essayer toutes les combinaisons possibles du jeu de caractères accepté (selon les formats de nom d'utilisateur et de mot de passe admis par le site). Une telle attaque peut générer plusieurs milliers, voire plusieurs millions de combinaisons incorrectes avant de pouvoir obtenir un droit d'accès, et sa durée se chiffre en heures, voire en semaines, ou plus.

En faisant en sorte que votre application Web exige l'utilisation de mots de passe renforcés, vous limitez fortement la faisabilité des attaques par force brute.

- Vous pouvez exécuter Authentication Tester depuis AppScan, en cliquant sur **Outils > PowerTools > Authentication Tester**
- Vous pouvez exécuter Authentication Tester seul, à partir du menu Démarrer de Windows, en cliquant sur **Tous les programmes > [Dossier d'installation AppScan Standard] > PowerTools > Authentication Tester**

Méthodes d'authentification

Dans la fenêtre principale d'Authentication Tester, vous choisissez la méthode d'authentification utilisée par votre application Web. Les options sont les suivantes :

- **Authentification de formulaire :** (l'authentification est exécutée par une page Web personnalisée)
  «Authentification de formulaire»
- **Authentification HTTP :** (l'authentification est exécutée conformément à la définition donnée dans le protocole)
  «Authentification HTTP», à la page 280

Les options d'examen disponibles varient selon la méthode sélectionnée.

Remarque : Si l'application utilise les *deux* types d'authentification (par exemple l'Authentification HTTP en général et l'Authentification de formulaire pour certaines pages administrateur), vous devez fournir à Authentication Tester le nom d'utilisateur et le mot de passe *réels* pour l'authentification HTTP, afin de lui permettre de tester l'Authentification de formulaire sur ces pages. (Pour plus de détails, voir «Authentification HTTP sur authentification de formulaire», à la page 280.)

Authentification de formulaire

Pourquoi et quand exécuter cette tâche

Si vous sélectionnez le bouton d'option **Authentification de formulaire**, exécutez les procédures suivantes :

Procédure

1. «Fourniture d'une connexion typique».
2. «Description des réponses de connexion de l'application».

Fourniture d'une connexion typique :
Pourquoi et quand exécuter cette tâche

Si vous sélectionnez **Authentification de formulaire** dans la section **Méthode d'authentification** de la fenêtre principale, le bouton **Configurer** s'affiche. Il permet de configurer Authentication Tester avec la procédure de connexion correcte.

Procédure

1. Cliquez sur **Configurer**.

   Le navigateur d'Authentication Tester s'ouvre.
2. Accédez à la page de connexion de votre application Web.
3. Exécutez la procédure de connexion en utilisant les données d'identification suivantes (vous pouvez les copier-coller depuis la partie supérieure de la fenêtre du navigateur) :

nom d'utilisateur :	BruteUsername
mot de passe :	BrutePassword

   Authentication Tester exige de modéliser la procédure de connexion au site avec ces valeurs. Pendant la phase de test, ces chaînes seront remplacées par des combinaisons possibles de nom d'utilisateur et de mot de passe lorsqu'Authentication Tester tente d'accéder au site par force brute. Lorsque vous avez terminé la procédure de connexion, Authentication Tester ne tente pas réellement de se connecter avec ces données d'identification, mais se contente d'examiner la demande de connexion.

   ATTENTION :
   Si les chaînes "BruteUsername" et "BrutePassword" ne sot pas autorisées par votre vérification côté client, aucune demande de connexion ne sera créée pour Authentication Tester. Dans ce cas, vous devez modifier les valeurs des marques de réservation des chaînes du nom d'utilisateur et du mot de passe. Voir «Onglet Authentification de formulaire», à la page 282.

   Lorsque vous avez terminé la procédure de connexion, Authentication Tester "capture" la demande de connexion, et un message de confirmation s'affiche.
4. Dans le message de confirmation, cliquez sur **OK**

   Le navigateur se ferme et la fenêtre **Détection de connexion réussie** s'ouvre. Cela permet de décrire les réponses de connexion. Voir «Description des réponses de connexion de l'application»

Description des réponses de connexion de l'application :
Pourquoi et quand exécuter cette tâche

Dans la fenêtre Détection de connexion réussie, vous activez Authentication Tester afin qu'il reconnaisse si les demandes de connexion ont réussi ou échoué. Il est nécessaire de connaître ces informations pour savoir quand l'application Web a accepté des données d'identification comme valides.

Certaines réponses de réussite par défaut s'affichent dans la liste par défaut, mais vous devez modifier cette liste afin qu'elle comprenne toutes les réponses concernant votre application.

Procédure

1. Sélectionnez le type de réponse que vous souhaitez décrire :
   - **Réponse en cas de réussite :** La réponse à une tentative de connexion valide
   - **Réponse en cas d'erreur :** La réponse à une tentative de connexion non valide

2. Entrez une chaîne de texte ou une expression régulière (regexp) correspondant à un contenu sur la page de réponse. (Veillez à mettre en concordance uniquement du contenu statique, pas des variables.)

   Par exemple, si vous savez que des données d'identification non valides reçoivent souvent la réponse suivante : `"Username and password do not match"` vous pouvez utiliser cette information pour communiquer le résultat des tests à Authentication Tester.

   L'utilisation des expressions régulières, et non de chaînes, vous permet de configurer Authentication Tester une seule fois en vue d'exécutions multiples pendant les étapes de développement de votre application Web.

   Par exemple, si la conception de la page de connexion réussie n'a pas encore été finalisée, soit avec une grande mention `Bienvenue !` en pleine page, soit avec une petite chaîne `bienvenue` en haut de la page d'accueil, vous pouvez entrer `(?i)bienvenue` pour indiquer que la recherche sur les mots est insensible à la casse.

   Conseil : Pour en savoir plus sur regexps et sur les métacaractères utilisables pour indiquer plus que des chaînes littérales, voir «À propos des métacaractères». Pour tester des expressions régulières avant d'essayer de les utiliser dans Authentication Tester, testez l'outil Expression Test PowerTool.
3. Cliquez sur **Ajouter**.

   L'expression régulière regexp est ajoutée à la liste des réponses.

   Vous pouvez ajouter autant d'expressions régulières que vous le souhaitez. Authentication Tester les utilise avec un opérateur OR : si une ou plusieurs des expressions régulières correspond à du contenu sur une page de votre site, cette page est reconnue comme une page de résultat (soit une connexion réussie, soit une page d'erreur, selon le type de réponse sélectionné).
4. Pour retirer les expressions régulières non souhaitées de la liste, sélectionnez l'expression régulière et cliquez sur **Supprimer**.
5. Cliquez sur **OK**.

   La fenêtre **Détection de connexion** réussie se ferme et vous revenez à la fenêtre principale. Vous pouvez maintenant exécuter des tests de force brute à l'aide de la configuration en cours (voir «Exécution de tests d'authentification», à la page 281).

À propos des métacaractères :

Un métacaractère désigne un ou plusieurs caractères ayant une signification spéciale et non-littérale dans le contexte d'une expression régulière. Par exemple, le caractère circonflexe (`^`) est un métacaractère ayant pour signification "rechercher au début". Si vous souhaitez rechercher l'accent circonflexe, mais pas en tant que métacaractère, vous devez le protéger (à l'aide d'un caractère d'échappement) à l'aide d'une barre oblique inversée, comme suit : `\^`.

Le tableau suivant répertorie des exemples de certains métacaractères courants d'expression régulière.

	Métacaractère Description	**Exemple**
`\`	Protège le caractère suivant (afin de l'interpréter littéralement et non comme un métacaractère).	`\!` trouve le point d'exclamation (`!`) `\.` trouve un point (.), et non un caractère
`^`	Recherche au début d'une chaîne.	`^H` trouve **Heure** mais pas **heure** ou **PHP**
.	Rechercher n'importe quel caractère (lettre, nombre, symbole, espace), sauf une nouvelle ligne.	(.*) trouve n'importe quel paragraphe

	Métacaractère Description	Exemple
( )	Rechercher un schéma de groupe.	`(mot)` permet de rechercher "Dans ce **mot**" `^(Mot)` permet de rechercher "**Mot**s dans cette ligne" `Enregistrer ((fichier)|(sauvegarde))` trouve "**Enregistrer fichier**" et "**Enregistrer sauvegarde**"
[ ]	Rechercher une plage de schémas.	`[a-z]` trouve tous les caractères alphabétiques en minuscule
*	Rechercher le schéma zéro ou plusieurs fois.	`<(.*)>` trouve toutes les balises HTML avec leur contenu
+	Rechercher le schéma une ou plusieurs fois.	`(<.l>)+` permet de rechercher **<UL><OL>**
?	Rechercher le schéma zéro ou une fois.	`log(.?)in` trouve **login** et **log in**
(?i)	Rechercher les prochains caractères à l'aide d'une recherche sensible à la casse.	`(?i)mot` trouve **mot**, **Mot, mOt, MOT**

Authentification HTTP

Pourquoi et quand exécuter cette tâche

Si vous cliquez sur le bouton d'option **Authentification HTTP** dans la section **Méthode d'authentification**, les zones **Adresse de l'URL** et **Domaine** s'affichent.

Procédure

1. Entrez l'adresse URL de la page de connexion dans la zone de texte **Adresse de l'URL**.
2. Pour tester que l'adresse URL est correcte, cliquez sur **Afficher**.
   Le navigateur s'ouvre.
   - Si une fenêtre de connexion standard HTTP s'affiche sur le navigateur, l'adresse URL est correcte.
   - Si la page s'affiche sans fenêtre de connexion HTTP, l'adresse URL est incorrecte. Corrigez-la.
3. Fermez le navigateur.
4. Si la fenêtre de connexion HTTP demande un domaine, entrez le nom de domaine correct dans la zone **Domaine**.
   Vous pouvez maintenant exécuter des tests de force brute à l'aide de la configuration en cours (voir «Exécution de tests d'authentification», à la page 281).

Authentification HTTP sur authentification de formulaire

Pourquoi et quand exécuter cette tâche

Dans certains cas, une application peut utiliser *les deux* types d'authentification. L'authentification HTTP peut en général être utilisée sur toutes les pages, tandis que l'authentification de formulaire permet de protéger des domaines d'administrateur précis. Dans ces cas, il peut être souhaitable d'exécuter les deux types de test.

Authentification HTTP : le test se déroule comme indiqué ci-dessus (voir la rubrique «Authentification HTTP»)

Authentification de formulaire : Pour ce test, vous devez fournir à Authentication Tester le nom d'utilisateur et le mot de passe réels de l'authentification HTTP. Cela lui permet de passer l'authentification HTTP et de tester l'authentification de formulaire sur ces pages.

Procédure

1. Dans la fenêtre principale d'Authentication Tester, cliquez sur le bouton d'option **Authentification de formulaire**.

2. Configurez l'authentification de formulaire (voir la rubrique «Authentification de formulaire», à la page 277).
3. Cliquez sur **Avancé**.

   La boîte de dialogue Configuration avancée s'ouvre (avec l'onglet Général dans la partie supérieure).
4. Dans la zone **Authentification HTTP sur authentification de formulaire**, cochez la case **Activer**.

   Les zones Nom d'utilisateur, Mot de passe et Domaine sont activées.
5. Tapez des données d'identification HTTP valides qui seront utilisées par Authentication Tester lors du test des pages Authentification de formulaire.
6. Si la fenêtre de connexion HTTP demande un domaine, entrez le nom de domaine correct dans la zone **Domaine**.
7. Cliquez sur **OK** pour fermer la boîte de dialogue.

   Vous pouvez maintenant exécuter des tests de force brute à l'aide de la configuration en cours (voir «Exécution de tests d'authentification»).

Exécution de tests d'authentification

Lorsque vous avez choisi la méthode d'authentification et configuré les tests de base, vous pouvez démarrer l'examen d'Authentication Tester en cliquant sur **Démarrer**.

La barre de progression de la fenêtre principale affiche ce qui suit :

- Nombre de paires nom d'utilisateur-mot de passe à tester, par rapport au nombre de paires à essayer.
- Nombre d'unités d'exécution utilisées par Authentication Tester dans cet examen.
- Etat de l'examen, s'il n'est pas en cours d'exécution : interrompu, repris, arrêté, terminé.

Si vous **interrompez** un examen et laissez Authentication Tester ouvert (sans quitter), vous pouvez reprendre plus tard l'examen en cliquant sur **Reprendre**. Si vous quittez Authentication Tester après l'avoir interrompu, l'examen est supprimé.

Si vous **arrêtez** un examen, les données collectées seront supprimées.

Résultats de l'examen

Lorsque le test est terminé, toutes les paires nom d'utilisateur-mot de passe qui ont abouti à une connexion sont listées dans le tableau des Connexions réussies.

Vous pouvez enregistrer les résultats en les exportant sous la forme d'un fichier XML. Cette fonction est pratique pour le test d'authentification pendant le développement. Elle vous permet de comparer les résultats d'Authentication Tester après avoir implémenté les correctifs.

Cliquez sur **Exporter les résultats** et nommez le fichier d'exportation. Un fichier XML listant les données d'identification qui ont abouti à une connexion est créé.

Configuration avancée

La boîte de dialogue Configuration avancée permet de personnaliser le comportement de Authentication Tester sur votre réseau local et pour l'application que vous testez.

Conseil : Si vous allez tester Authentification de formulaire et Authentification HTTP, vous pouvez entrer en même temps toutes les informations. Seules les informations concernant le type de test exécuté (Formulaire ou HTTP) sont utilisées.

Lorsque vous cliquez sur **Avancé** dans la fenêtre principale, la boîte de dialogue **Configuration avancée** s'ouvre. Elle comprend quatre onglets :

- «Onglet Général», à la page 282
- «Onglet Authentification de formulaire», à la page 282
- «Onglet Proxy», à la page 283

- «Onglet Génération de données d'identification», à la page 283

Onglet Général :

L'onglet **Général** de la fenêtre **Configuration avancée** vous permet de modifier les configurations réseau.

Option	Description
Nombre d'unités d'exécution	Définit le nombre maximum d'unités d'exécution de connexion qui seront testées simultanément par Authentication Tester. La valeur par défaut est 12. Un nombre supérieur d'unités d'exécution se traduit par un examen plus rapide. Si vous constatez qu'Authentication Tester surcharge votre réseau, vous pouvez réduire ce nombre.
Délai d'expiration de la demande (millisecondes)	Définissez le délai d'attente observé par Authentication Tester pour atteindre le serveur de l'application Web avant que la connexion soit interrompue.
Port de proxy interne	Un port disponible est affecté automatiquement au proxy interne. Si nécessaire, vous pouvez lui affecter un autre port. Vous recevez un avertissement si le port sélectionné n'est pas disponible.
Authentification HTTP sur authentification de formulaire	Si l'application Web utilise l'authentification HTTP sur l'authentification de formulaire, pour tester l'authentification de *formulaire*, vous devez sélectionner **Activer**, puis entrer des valeurs valides pour l'authentification HTTP : **nom d'utilisateur**, **mot de passe** et **domaine**. Cela permet à Authentication Tester d'accéder au serveur d'applications Web pour exécuter les tests de force brute sur le mécanisme Authentification de formulaire. Ces valeurs n'affectent pas le test de l'authentification HTTP. Elles sont appliquées uniquement si vous sélectionnez la méthode **Authentification de formulaire**.

Onglet Authentification de formulaire :

Cet onglet contient les expressions régulières Connexions réussies que vous entrez pour décrire la page envoyée en réponse à une combinaison nom d'utilisateur-mot de passe accepté. (Les informations entrées ici concernent uniquement le cas d'un test d'Authentification de formulaire).

Option	Description
Détection de connexion réussie	
Réponse en cas de réussite	Lorsque cette option est sélectionnée, les Réponses en cas de réussite déjà configurées s'affichent dans l'écran situé en dessous.
Réponse en cas d'erreur	Lorsque cette option est sélectionnée, les Réponses en cas d'erreur déjà configurées s'affichent dans l'écran situé en dessous.
Ajouter/Supprimer	Voir les rubriques «Description des réponses de connexion de l'application», à la page 278 pour savoir comment ajouter des réponses aux listes ou «À propos des métacaractères», à la page 279 pour en savoir plus sur la rédaction d'expressions régulières.
Données d'identification contrefaites par défaut	

Option	Description
Nom d'utilisateur/Mot de passe	Ces zones affichent les chaînes que vous devrez entrer lors de la création de la demande de connexion pour configurer l'Authentification de formulaire (voir la rubrique «Authentification de formulaire», à la page 277). Il n'est pas nécessaire d'indiquer des données d'identification *valides*, car elles ne sont pas utilisées pour vous connecter réellement au site. Ces zones permettent simplement d'indiquer à Authentication Tester l'emplacement des données d'identification dans la demande de connexion (en cas d'attaque par force brute contre le site). Les valeurs par défaut sont `BruteUsername` et `BrutePassword`. Si la logique côté client ne permet pas d'utiliser ces valeurs dans une demande de connexion au site (par exemple, si l'application nécessite un e-mail comme nom d'utilisateur et si la logique côté client applique cette règle lors de la création de la demande de connexion), remplacez ces valeurs par un format valide. Lorsque vous modifiez les données d'identification contrefaites par défaut, assurez-vous qu'aucune valeur n'est une sous-chaîne de l'autre. Par exemple, si vous entrez utilisateur@email.com comme nom d'utilisateur, vous ne pouvez pas choisir utilisateur comme mot de passe.

Onglet Proxy :

Si votre application Web nécessite une connexion de proxy Web, cochez la case **Activer** dans l'onglet **Proxy** et indiquez le Serveur et le Port. Si le proxy requiert une authentification, indiquez le Nom d'utilisateur et le Mot de passe, et le Domaine le cas échéant.

Onglet Génération de données d'identification :

Les options de cet onglet vous permettent de configurer les noms d'utilisateur et les mots de passe essayés par Authentication Tester pendant l'examen.

Il comporte deux zones :

- **Mode :** «Génération de données d'identification : Zone du mode»
- **Configuration :** «Génération de données d'identification : Zone de configuration»

Génération de données d'identification : Zone du mode :
Procédure

Sélectionnez le mode qui sera exécuté par Authentication Tester :

- **Matrice :** Chaque nom d'utilisateur de la liste est testé par rapport à chaque mot de passe de la liste. Sélectionnez ce mode pour un examen plus complet.
- **Parallèle :** Les noms d'utilisateur et les mots de passe sont classés par paire, par numéro d'index. Sélectionnez ce mode pour un examen plus rapide.

Génération de données d'identification : Zone de configuration :
Pourquoi et quand exécuter cette tâche

Dans cette zone, vous configurez les options utilisées par Authentication Tester pour générer les noms d'utilisateur et/ou les mots de passe à tester.

Procédure

1. Sélectionnez l'un des boutons d'option pour personnaliser **Noms d'utilisateur** ou **Mots de passe**.

   Toutes les zones et les données affichées dans la zone Configuration s'appliquent désormais à l'élément sélectionné. Pour chaque élément, la liste déroulante vous permet de configurer la structure des noms d'utilisateurs/mots de passe qui seront créés et utilisés dans l'attaque.

2. Dans la liste déroulante **Type d'élément**, sélectionnez un type d'élément à inclure dans l'attaque, puis dans la zone située en dessous, complétez les valeurs de l'élément comme indiqué dans «Types de liste».
3. Cliquez sur **Ajouter** pour ajouter la nouvelle définition à la liste dans le volet Configuration.
4. Répétez l'opération pour les autres éléments si nécessaire.
5. Organisez les types d'élément (avec les fonctions **Haut** et **Bas**) afin que chaque nom d'utilisateur ou mot de passe essayé soit créé conformément à chaque type, dans l'ordre indiqué.

Types de liste :

Elément	Description	Exemples de valeurs
Dictionnaire	Un fichier de "valeur par ligne" utilisé lors de la génération de noms d'utilisateur/mots de passe pour l'attaque. Les fichiers par défaut sont fournis pour les Noms d'utilisateur et les Mots de passe, mais vous pouvez utiliser le bouton **Parcourir** pour accéder à tout autre fichier utilisable. Le dossier de données comprend aussi un fichier de dictionnaire de mots de passe beaucoup plus long (passwords_long.txt) qui est utilisable à la place du fichier par défaut.	Chemin d'accès au fichier de dictionnaire de "valeur par ligne"
Numérique	Plage de nombres qui est incluse dans les noms d'utilisateur/mots de passe générés	0 à 999999999
Constante	Chaîne que vous souhaitez inclure dans tous les noms d'utilisateur/mots de passe générés	N'importe quelle chaîne
Plage de caractères	Plage de caractères et longueur de chaîne, pour les caractères à inclure dans les noms d'utilisateur/mots de passe générés	[espace jusqu'au tilde] -~ et une longueur de chaîne

Remarque : La plage **espace jusqu'au tilde** comprend les caractères a à z, A à Z, 0 à 9 et les symboles d'entrée ASCII. Si vous entrez " **-~**" (sans les guillemets) comme plage de caractères, Authentication Tester insère automatiquement tous les caractères inclus dans la liste des expressions régulières.

La valeur valide de la zone **Longueur** dépend de la plage. Par exemple, si la plage est 0 à 9 et si la longueur est 10, la plage est valide [0000000000, 0000000001, ...10]. Par contre, si la plage est a à z, Authentication Tester n'accepte pas 9999999999 comme une longueur valide, car le nombre de combinaisons exigerait une quantité de ressources et un temps de traitement excessifs.

Remarque : Pour utiliser un tiret comme caractère et non pour signaler une plage, faites-le précéder d'une barre oblique inversée, comme suit : **\-**

Exemples de configuration de génération de données d'identification :

Génération de données d'identification	Données d'identification obtenues
Dictionnaire : C:\web tests\data\users.txt Constant value: _ Plage de nombres : 0 à 9	user_0 user_1 user_2 ... user_9
Valeur constante : passwd Plage de caractères : a-zA-Z0-9 ; longueur : 3	passwdaaa passwdaab ... passwd999
Valeur constante : iamgod Plage de caractère : -~; longueur : 1 Plage de nombres : 1900 à 3000	iamgod 1900 iamgod!1900 ... iamgod~3000

Suppression d'un élément :

Procédure

Sélectionnez l'élément à supprimer dans le panneau inférieur : pour ce faire, cliquez sur l'élément, puis cliquez sur **Supprimer**.

Test de connexion

L'outil Test de connexion PowerTool permet de lancer une commande ping sur les sites Web sans l'aide du protocole ping, qui est bloqué par de nombreux pare-feu.

- Vous pouvez exécuter Test de connexion à partir d'AppScan, en cliquant sur **Outils > PowerTools > Test de connexion**
- Vous pouvez exécuter Test de connexion seul, à partir du menu Démarrer de Windows, en cliquant sur **Tous les programmes > [Dossier d'installation AppScan Standard] > PowerTools > Test de connexion**

Utilisation de Test de connexion

Procédure

1. Dans la zone de texte **Site Web**, entrez ou collez une URL.
2. Cliquez sur **Envoyer une commande ping au site**.

   La liste des résultats de la commande ping indique si Test de connexion a pu atteindre l'URL avec succès et, si tel est le cas, indique le nombre de millisecondes dont il a eu besoin pour l'atteindre.

Que faire ensuite

- Pour effacer la liste des résultats de la commande ping, cliquez sur **Effacer**.

Méthode HTTP :

Le menu déroulant de la **méthode HTTP** propose deux méthodes de demande HTTP.

- **HEAD :** Sélectionnez cette méthode pour obtenir les en-têtes HTTP uniquement. Il s'agit de la méthode la plus rapide.
- **GET :** Sélectionnez cette méthode pour obtenir la page entière. Certains sites n'autorisent pas les demandes HTTP utilisant la méthode Head ; dans ce cas, essayez la méthode Get.

Port :

Dans la zone de texte du port, entrez le port d'écoute du serveur Web.

La valeur par défaut pour la plupart des URL non sécurisés est **80**. Vous pouvez changer le port pour des URL spécifiques si nécessaire.

Pour utiliser SSL (Secure Sockets Layer), cochez **Sécurisé**. Le port par défaut prend la valeur **443**.

Nombres d'intervalles :

Dans la zone de texte **Nombres d'intervalles**, entrez le nombre de fois que Test de connexion devrait effectuer une commande ping sur l'URL indiquée.

- Si vous souhaitez uniquement tester si vous pouvez atteindre l'URL, utilisez une petite valeur (par exemple entre 3 et 5).
- Si vous devez surveiller les pannes de serveur, la valeur doit être plus élevée (par exemple entre 100 et 1000). Test de connexion s'exécute en arrière-plan pendant que vous effectuez d'autres tâches. Ainsi vous pouvez fixer le nombre d'intervalles à un nombre aussi élevé que vous le souhaitez.

Vous pouvez arrêter Test de connexion à tout instant avant la prochaine commande ping en cliquant sur **Arrêter**.

Délai entre les intervalles :

Dans la zone de texte **Délai entre les intervalles**, entrez le nombre de millisecondes d'attente de Test de connexion entre chaque commande ping.

- Si vous souhaitez tester si vous pouvez atteindre l'URL, la valeur pourrait être 0 (zéro).
- Si vous devez surveiller les pannes de serveur, la valeur doit être plus élevée (par exemple 2000, ce qui correspond à deux secondes).

Afficher l'en-tête du serveur :

Cochez la case à cocher **Afficher l'en-tête du serveur** pour voir le type de serveur Web sur lequel une commande ping est effectuée. Les informations sont affichées une fois le dernier intervalle atteint.

Exemple d'en-tête de serveur :

- www.ibm.com - `Microsoft-IIS/6.0`
- www.cnn.com - `Apache`
- www.sky-news.co.uk - `Microsoft-IIS/5.0`
- www.sourceforge.org - `Apache/1.3.31 (Unix) PHP/4.3.11 mod_ssl/2.8.19 OpenSSL/0.9.7a`

Coder/Décoder

L'outil Coder/Décoder PowerTool permet de coder et décoder des chaînes que vous avez intégrées, depuis et vers le format de votre choix.

- Vous pouvez exécuter Coder/Décoder à partir d'AppScan, en cliquant sur **Outils > PowerTools > Coder/Décoder**
- Vous pouvez exécuter Coder/Décoder seul, à partir du menu Démarrer de Windows, en cliquant sur **Tous les programmes > [Dossier d'installation AppScan Standard] > PowerTools > Coder/Décoder**

Utilisation de Coder/Décoder

Procédure

1. Dans la zone de texte Entrée, entrez ou collez le texte.
2. Dans le menu déroulant des méthodes, sélectionnez une méthode de codage/décodage. (Voir «Méthodes»)

   Si vous choisissez la méthode 3DES, entrez ou collez une clé de chiffrement adaptée dans la zone de texte Clé de chiffrement.
3. Cliquez sur Coder ou Décoder.

   Le texte codé ou décodé apparaît dans la boîte de dialogue de sortie.

Codage/décodage en couche : Vous pouvez renvoyer la sortie en tant qu'entrée, et coder ou décoder à nouveau, en cliquant sur Renvoyer.

Cela est utile si vous voulez effectuer les actions suivantes :

- Vérifier que le format de codage correspond au format de décodage
- Effectuer un codage multiple sur une chaîne
- Décoder une chaîne qui a subi un chiffrement multiple

Méthodes :

Méthode	Capacité	Convertir entre
URL	coder + décoder	texte <-> codage URL

Méthode	Capacité	Convertir entre
Base64	coder + décoder	texte <-> codage Base64
UTF-8 sous forme superlongue	coder + décoder	texte <-> UTF-8 sous forme superlongue (2 octets)
UU	coder + décoder	texte <-> codage UU
HTML	coder + décoder	texte <-> entités HTML
MD5	encode	texte <-> signature digitale
SHA1	encode	texte <-> signature digitale
SHA256	encode	texte <-> signature digitale
SHA384	encode	texte <-> signature digitale
SHA512	encode	texte <-> signature digitale
3DES (clé 192 bits)	coder + décoder	texte lisible <-> texte chiffré (à l'aide d'une clé définie)

Expression Test

L'écriture précise d'expressions régulières peut être un processus de tâtonnement fastidieux. L'outil Expression Test PowerTool permet d'accélérer le processus.

- Vous pouvez exécuter Expression Test à partir d'AppScan, en cliquant sur **Outils > PowerTools > Expression Test**
- Vous pouvez exécuter Expression Test seul, à partir du menu Démarrer de Windows, en cliquant sur **Tous les programmes > [Dossier d'installation AppScan Standard] > PowerTools > Expression Test**

Utilisation de Expression Test

Procédure

1. Dans la zone **Texte**, entrez ou collez le texte que l'expression régulière doit rechercher.
2. Dans la zone **Expression régulière**, entrez l'expression régulière qui, selon vous, permet de rechercher le texte.
3. Cliquez sur **Tester**.

Résultats

Le texte de la zone de texte qui correspond au schéma est mis en évidence en rouge.

Remplacements de texte

Remplacement de texte correspondant à un schéma spécifique.

Pourquoi et quand exécuter cette tâche

Si vous utilisez des expressions régulières pour remplacer du texte correspondant à un schéma spécifique, vous pouvez utiliser Expression Test pour tester si le remplacement est effectué correctement.

Procédure

1. Dans la zone **Expression régulière**, entrez l'expression régulière.
2. Dans la zone **Remplacer**, entrez le texte devant remplacer le texte correspondant au schéma de l'expression régulière.
3. Dans la zone **Texte**, entrez ou collez un exemple de texte.
4. Cliquez sur **Tester** puis vérifiez que le texte prévu correspond à l'expression régulière.
5. Cliquez sur **Remplacer**.

Résultats

Le texte qui correspondait au schéma de l'expression régulière (mis en évidence en rouge) est remplacé par le texte de la zone **Remplacer**.

Schéma de groupe

Application d'une expression régulière à un groupe de caractères ou métacaractères.

Souvent, il est nécessaire d'appliquer une expression régulière à un groupe de caractères ou métacaractères.

Pour grouper un ensemble, mettez les caractères entre parenthèses ( ).

Un nombre est attribué au groupe dans la zone Associer les groupes et le texte correspondant est affiché à côté.

S'il y a correspondance, vous pouvez voir le texte correspondant à chaque groupe dans la zone Associer les groupes.

Par exemple, un code HTML avec `<UL>first` dans le texte.

Vous entrez `(<.L>)([a-z ]*)` comme expression régulière.

Dans la zone Texte, `<UL>first` est mis en évidence en rouge.

Dans la zone **Associer les groupes**, les groupes sont divisés :

- `Groupe 1 <UL>`
- `Groupe 2 first`

Métacaractères

Informations générales sur les métacaractères.

Tout caractère unique (lettre, caractère numérique, ou symbole) dans une expression régulière correspond à lui-même, littéralement ; à moins que ce ne soit un métacaractère. Un métacaractère est un ou plusieurs caractères ayant une signification unique et n'étant pas utilisé littéralement pour la correspondance de l'expression régulière.

Par exemple, le caractère circonflexe (^) est un métacaractère ayant pour signification "rechercher au début".

Si vous voulez rechercher le caractère, plutôt que le schéma du métacaractère, insérez une barre oblique inversée (\) avant.

Par exemple, pour rechercher le circonflexe en tant que caractère de texte, l'expression régulière doit être : `\^`

Exp. rég.	Description	Exemple
\	Rechercher le prochain caractère en tant que caractère ; ne pas utiliser son schéma de métacaractère.	`\.` permet de rechercher un point (`.`) dans le texte `.` permet de rechercher le premier caractère (n'importe quel caractère)
^	Rechercher au début d'une chaîne.	^1 permet de rechercher "**1**. Cliquez sur Sauvegarder."mais pas : "dans la ligne 2**1**0"
.	Rechercher n'importe quel caractère (excepté le retour à la ligne).	Permet de rechercher les caractères a, A, 1, <, ., =, etc., quel que soit le premier caractère.
()	Rechercher un schéma de groupe.	`(mot)` permet de rechercher "Dans ce **mot**" `^(Mot)` permet de rechercher "**Mot**s dans cette ligne"
[]	Rechercher une plage de schémas.	`[a-z]` permet de rechercher des lettres, mais pas des nombres
*	Rechercher le schéma précédent aucune ou plusieurs fois.	`.*` permet de rechercher tous les caractères `<(.*)>` permet de rechercher toutes les balises HTML
+	Permet de rechercher le schéma précédent une ou plusieurs fois.	`(<.l>)+` permet de rechercher **<UL><OL>**
?	Permet de rechercher le schéma précédent aucune ou une seule fois.	`(<.l>)?` permet de rechercher **<UL>**
(?i)	Rechercher les prochains caractères à l'aide d'une recherche insensible à la casse.	`(?i)mot` permet de rechercher **mot** et **Mot**

HTTP Request Editor

L'outil HTTP Request Editor PowerTool permet d'envoyer une requête HTTP entièrement contrôlée vers votre site, et ainsi de tester la manière dont le site répond à différents types de requête HTTP.

- Vous pouvez exécuter HTTP Request Editor à partir d'AppScan, en cliquant sur **Outils > PowerTools >** HTTP Request Editor
- Vous pouvez exécuter HTTP Request Editor seul, à partir du menu Démarrer de Windows, en cliquant sur **Tous les programmes > [Dossier d'installation AppScan Standard] > PowerTools >** HTTP Request Editor

Utilisation de HTTP Request Editor

Procédure

1. Dans l'onglet **Requête**, renseignez toutes les zones nécessaires.
2. Cliquez sur **Envoyer**.
3. Ouvrez l'onglet **Réponse** de manière à voir comment l'hôte a traité la requête.

Onglet Requête

Options de vue : Les options de vue de l'onglet Requête permettent de créer une requête HTTP selon différentes façons :

- **Brute :** Créer la requête en entrant ou collant du texte.
- **Analysée :** Créer la requête en remplissant le formulaire.

Pour mettre à jour la requête HTTP brute avec des détails intégrés dans la vue Analysée, dans l'onglet Brute, cliquez sur **Mettre à jour à partir de la requête analysée**.

La requête que vous avez configurée à l'aide du formulaire analysé est affichée dans un formulaire brut.

Paramètres de requête :

Paramètre	Description
Hôte	Entrez l'adresse IP ou le nom d'hôte de votre site Web.
Port	Entrez le port TCP sur lequel votre serveur Web est à l'écoute. Default=80
Méthode	Sélectionnez une méthode dans le menu déroulant, ou entrez une valeur pour le paramètre de requête de méthode. Le menu déroulant par défaut inclut les méthodes suivantes : GET : Extraire toutes les informations identifiées par l'URI de requête. POST : Demande à ce que le serveur d'origine accepte une entité jointe dans la requête en tant que nouveau subordonné de la ressource identifiée par l'URI de requête dans la ligne de requête. La fonction réelle accomplie par cette méthode est déterminée par le serveur et dépend généralement de l'URI de requête. HEAD : Extraire des informations identifiées par l'URI de requête. Le serveur ne doit pas renvoyer un message en tant que réponse. Les métainformations dans les en-têtes HTTP reçues en réponse à une requête HEAD sont les mêmes que celles reçues en réponse à une requête GET. Utilisée pour obtenir des informations sans avoir à transférer tout le corps ; souvent utilisée pour tester la validité, l'accessibilité et les modifications des liens hypertexte.
Sécurisé	Cochez pour envoyer la requête à l'aide de HTTPS.
URL	Entrez ou collez une URL. Vous pouvez afficher la liste des liens extraits à partir de la dernière réponse dans l'onglet Réponse.
Version HTTP	Entrez le numéro de la version du protocole HTTP que la requête devrait utiliser. Valeur par défaut=1.1
Longueur du contenu automatique	Lorsque cette case est cochée, l'éditeur de requête HTTP calcule et ajoute automatiquement l'en-tête de longueur du contenu et ses valeurs correctes.

Détails du message : Créer ou modifier les paramètres, en-têtes, cookies, et leurs valeurs, pour les inclure dans la requête.

Paramètres :

Ajout de paramètres :
Procédure

1. Cliquez sur **Ajouter**.
   La boîte de dialogue Ajouter un paramètre s'ouvre.
2. Entrez un nom pour le paramètre puis entrez une valeur.
3. Sélectionnez le type :
   - **Corps :** Envoyer le paramètre dans le corps de la requête.
   - **Requête :** Envoyer le paramètre dans la partie requête de la demande.
4. Cliquez sur **OK**.
   Le paramètre est ajouté à la requête.
   Dans la vue Analysée, la table des paramètres affiche le nom, la valeur et l'emplacement que vous avez saisis.

Dans la vue Brute, le paramètre apparaît de manière différente, en fonction de l'emplacement que vous avez choisi :

- **Corps :** une paire `nom=valeur` apparaît dans le corps de la requête.
- **Requête :** `une` paire `nom=valeur` apparaît dans la partie requête de la demande (après le symbole ?)

Dans les deux cas, les paires nom=valeur sont concaténées avec `&` s'il existe plus d'une paire.

Edition de paramètres :
Procédure

Procédez de l'une des façons suivantes :

- Dans la vue Analysée : sélectionnez le paramètre, puis cliquez sur **Editer**.
- Dans la vue Brute : éditez le texte.

Retrait de paramètres :
Pourquoi et quand exécuter cette tâche

Vous pouvez supprimer des paramètres de la requête sans les supprimer de l'outil HTTP Request Editor.

Procédure

Dans la vue Analysée, décochez le nom du paramètre.

Suppression de paramètres :
Procédure

Procédez de l'une des façons suivantes :

- Dans la vue Analysée, sélectionnez le paramètre, puis cliquez sur **Supprimer**.
- Dans la vue Brute, supprimez le texte.

En-têtes :

Ajout d'en-têtes :
Procédure

1. Cliquez sur **Ajouter**.
   La boîte de dialogue Ajouter un en-tête s'ouvre.
2. Entrez un nom et une valeur pour le nouvel en-tête HTTP.
3. Cliquez sur **OK**.
   L'en-tête est ajouté à la requête.
   - Dans la vue Analysée, la table des en-têtes affiche le nom ou la valeur du nouvel en-tête HTTP.
   - Dans la vue Brute, l'en-tête apparaît de la façon suivante : `En-tête nom : valeur de l'en-tête`

Edition d'en-têtes :
Procédure

Procédez de l'une des façons suivantes :

- Dans la vue Analysée, sélectionnez le nom de l'en-tête, puis cliquez sur **Editer**.
- Dans la vue Brute, localisez l'en-tête dont vous voulez éditer et modifier le texte.

Retrait d'en-têtes :
Pourquoi et quand exécuter cette tâche

Vous pouvez supprimer des en-têtes de la requête sans les supprimer de l'outil HTTP Request Editor.

Procédure

Dans la vue Analysée, décochez la case à cocher située à côté du nom de l'en-tête.
L'éditeur de requête HTTP génère une requête avec plusieurs en-têtes par défaut (Accept, Host, User Agent). Vous pouvez supprimer ou modifier ces en-têtes comme tout autre en-tête.

Suppression d'en-têtes :
Procédure

Procédez de l'une des façons suivantes :

- Dans la vue Analysée, sélectionnez le nom de l'en-tête, puis cliquez sur **Supprimer**.
- Dans la vue Brute, localisez l'en-tête HTTP dont vous voulez supprimer le texte de la requête.

Cookies :

Ajout de cookies :
Procédure

1. Cliquez sur **Ajouter**.
   La boîte de dialogue Ajouter un cookie s'ouvre.
2. Entrez un nom pour le cookie, puis entrez une valeur.
3. Cliquez sur **OK**.
   Le cookie est ajouté à la requête.
   - Dans la vue Analysée, la table des cookies affiche le nom et la valeur que vous avez saisis.
   - Dans la vue Brute, le cookie apparaît dans l'en-tête : `Cookie : nom=valeur`

Edition de cookies :
Procédure

Procédez de l'une des façons suivantes :

- Dans la vue Analysée : sélectionnez le cookie, puis cliquez sur **Editer**.
- Dans la vue Brute : localisez l'en-tête du cookie dont vous voulez modifier et éditer le texte.

Retrait de cookies :
Pourquoi et quand exécuter cette tâche

Vous pouvez supprimer des cookies de la requête sans les supprimer de l'outil HTTP Request Editor.

Procédure

Dans la vue Analysée, décochez la case à cocher du nom du cookie.

Suppression de cookies :
Procédure

Procédez de l'une des façons suivantes :

- Dans la vue Analysée : sélectionnez le cookie puis cliquez sur **Supprimer**.
- Dans la vue Brute : localisez l'en-tête du cookie dont vous voulez supprimer le texte.

Onglet Réponse

Une fois que vous avez cliqué sur **Envoyer** dans l'onglet Requête, vous recevez une réponse du serveur Web.

Il existe trois façon différentes d'afficher une réponse :

- **Brute :** La réponse est présentée sous forme de texte brut
- **Analysée :** Liste de liens extraits à partir du HTML de la réponse, et informations SSL
- **Navigateur :** La réponse est affichée dans un navigateur Web

Remarque :

Seule la réponse réelle qui a été envoyée par le serveur Web est présentée dans le navigateur. Redirections, images, et feuilles CSS de sont pas demandées automatiquement.

Dans la vue Brute, vous avez la possibilité de rechercher du texte dans la réponse. Dans la zone de texte au bas de la fenêtre, entrez une expression régulière (par exemple : "[a-z0-9]@" pour rechercher un message électronique) puis cliquez sur **Rechercher**.

Cochez la case **Insensible à la casse** de sorte que le schéma respecte les lettres majuscules et minuscules.

GSC (Generic Service Client)

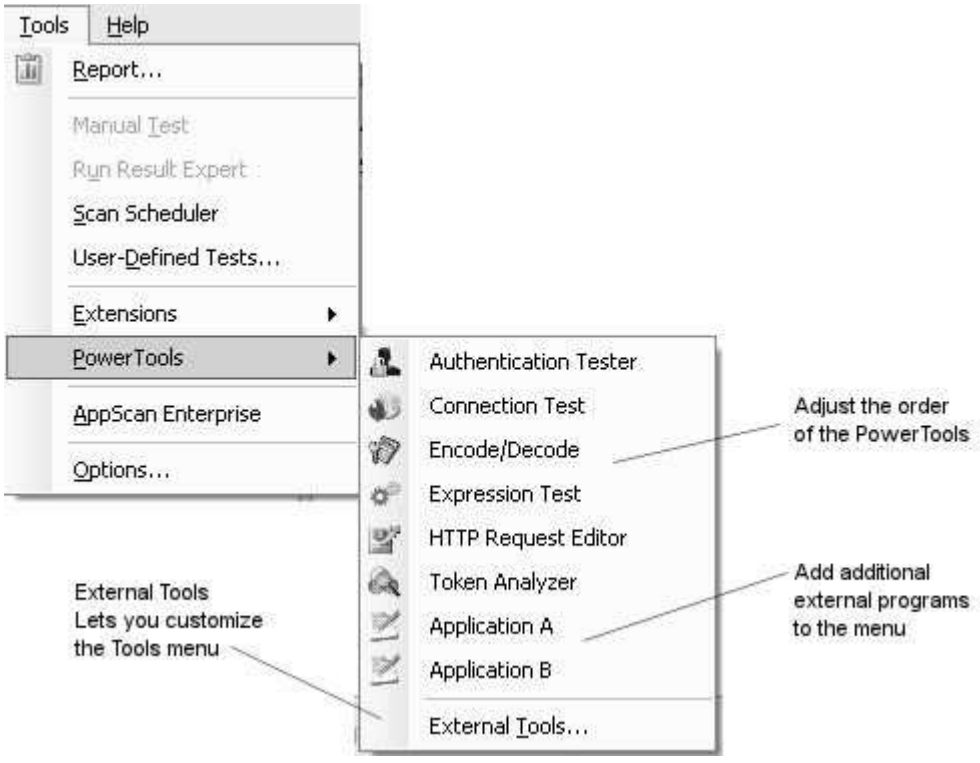
GSC (Generic Service Client) fournit une interface simple qui affiche les services disponibles, et permet d'entrer des paramètres et de visualiser les résultats. Utilisez-le pour explorer votre service Web SOAP manuellement afin qu'AppScan puisse utiliser vos entrées pour créer des tests appropriés.

Voir «Utilisation de GSC», à la page 153.

Personnaliser le menu Outils

Vous pouvez personnaliser le menu Outils pour :

- «Modifier l'ordre des autres outils», à la page 294
- «Ajouter des programmes au menu Outils», à la page 294



Modifier l'ordre des autres outils

Procédure

1. Cliquez sur **Outils > PowerTools > Outils externes**.
   La boîte de dialogue Outils externes s'ouvre.
2. Sélectionnez un élément de menu dans la liste, puis cliquez sur **Déplacer vers le haut** ou **Déplacer vers le bas**, le cas échéant.

Ajouter des programmes au menu Outils

Pourquoi et quand exécuter cette tâche

Vous pouvez ajouter un lien à un programme externe que vous utilisez fréquemment tout en exécutant AppScan et vous pouvez ajouter un lien au menu Outils pour l'ouvrir à partir d'AppScan.

Procédure

1. Cliquez sur **Outils > PowerTools > Outils externes**.
   La boîte de dialogue **Outils externes** s'ouvre.
2. Cliquez sur **Ajouter**
   La boîte de dialogue **Créer un outil externe** s'ouvre.
3. Dans la zone **Titre**, entrez le nom que vous souhaitez voir apparaître dans le menu **Outils**.
4. Cliquez sur le bouton **Parcourir** (...), localisez le fichier EXE du programme, puis cliquez sur **Ouvrir**.
5. Cliquez sur **OK**.
   Le titre et le chemin d'accès du fichier EXE sont ajoutés à la liste Outils externes.
6. Pour ajuster sa position dans le menu, sélectionnez le nouvel élément et cliquez sur **Déplacer vers le haut** ou **Déplacer vers le bas**, le cas échéant.

Extensions

AppScan permet de facilement écrire et intégrer des extensions. Les extensions sont des ajouts de fonctionnalité à AppScan. Elles peuvent être divers éléments allant du simple utilitaire de notification par courrier électronique à un outil complet d'exploitation de la vulnérabilité. Les extensions permettent aux utilisateurs de personnaliser AppScan selon leurs propres besoins. Elles sont écrites à l'aide du logiciel SDK d'AppScan et de l'infrastructure préfabriquée des extensions.

Plus d'informations sur l'utilisation des extensions avec AppScan, et où télécharger/héberger des extensions, sont disponibles à l'adresse : http://www.ibm.com/developerworks/rational/downloads/08/appscan_ext_framework/

Le fichier d'aide en ligne SDK **AppScanSDK.chm** se trouve dans le dossier principal de la documentation AppScan.

AppScan est livré avec l'extension Pyscan et d'autres extensions intégrées. L'intégration et la gestion d'extensions supplémentaires avec le gestionnaire d'extensions sont simples à réaliser.

Gestionnaire d'extensions

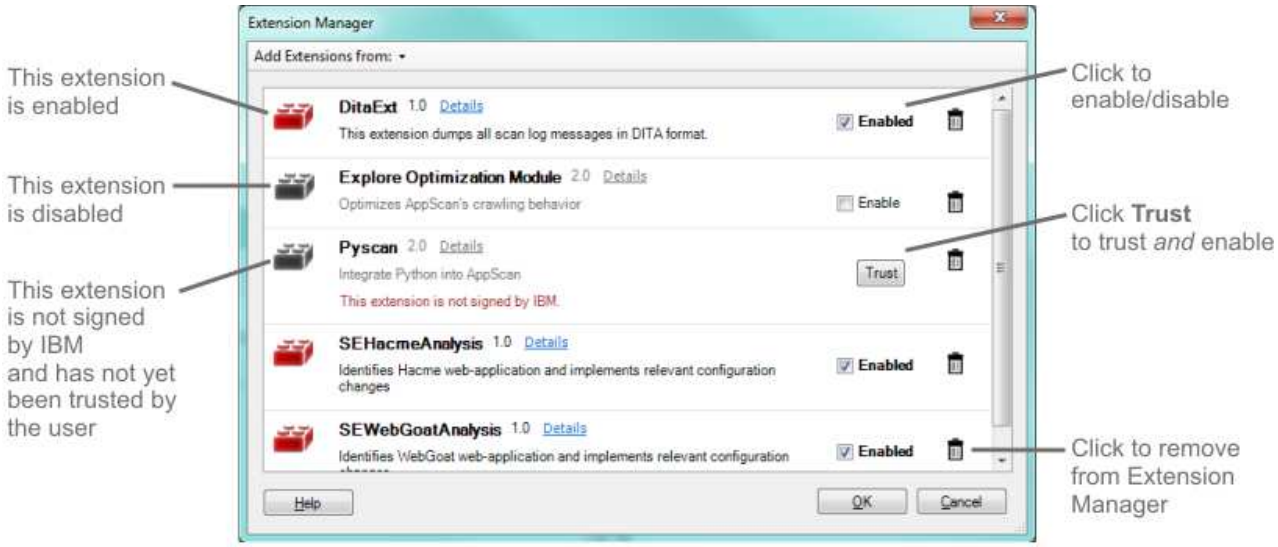
Le gestionnaire d'extensions vous permet d'ajouter ou de supprimer, d'activer ou de désactiver des extensions à utiliser avec AppScan

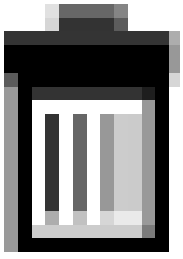
Le gestionnaire d'extensions (**Outils > Extensions > Gestionnaire d'extensions**) répertorie toutes les extensions qui ont été ajoutées.

- Vous pouvez ajouter des extensions disponibles dans IBM Security, ainsi que les vôtres.
- Vous pouvez activer et désactiver des extensions qui sont ajoutées.

- Vous pouvez choisir de "faire confiance" aux extensions (par exemple, les extensions que vous avez créées).

Si une extension est ajoutée mais qu'elle n'est pas digne de confiance et activée, l'icône sur la gauche est grisée.



Option	Explication
Ajouter des extensions depuis :	Pour ajouter une nouvelle extension, cliquez et sélectionnez la source : • **Cet ordinateur** ou • **AppScan eXtensions Framework Page**
Case à cocher **Activée**	Sélectionnez/désélectionnez la case à cocher pour activer/désactiver l'extension. Cette modification ne prendra effet que lors de la prochaine ouverture d'AppScan. Lorsqu'une extension est ajoutée, elle est automatiquement activée (et cette case est cochée), sauf s'il existe une raison pour laquelle AppScan n'a pas réussi à l'activer (par exemple, une version incompatible) ou si les extensions ne sont pas signées.
Bouton **Faire confiance**	Si une extension est installée mais n'est pas signée, AppScan ne la charge pas mais affiche le bouton **Faire confiance** à côté. Lorsque vous ouvrez AppScan, une fenêtre contextuelle vous avertit qu'il s'agit d'extensions non signées et non activées. Si vous pensez que l'extension est digne de confiance (par exemple, vous l'avez écrite vous-même), cliquez sur le bouton **Faire confiance** pour l'approuver à partir de maintenant et activez-la. **Conseil :** Si vous disposez d'une extension IBM non signée que vous avez utilisée avec une version précédente d'AppScan, vous pouvez choisir de la considérer comme étant digne de confiance ou cliquer sur **Obtenir davantage d'extensions** pour déterminer si une version signée est disponible pour la remplacer (voir «Remplacement d'extensions non signées», à la page 345).
	Cliquez pour supprimer une extension.

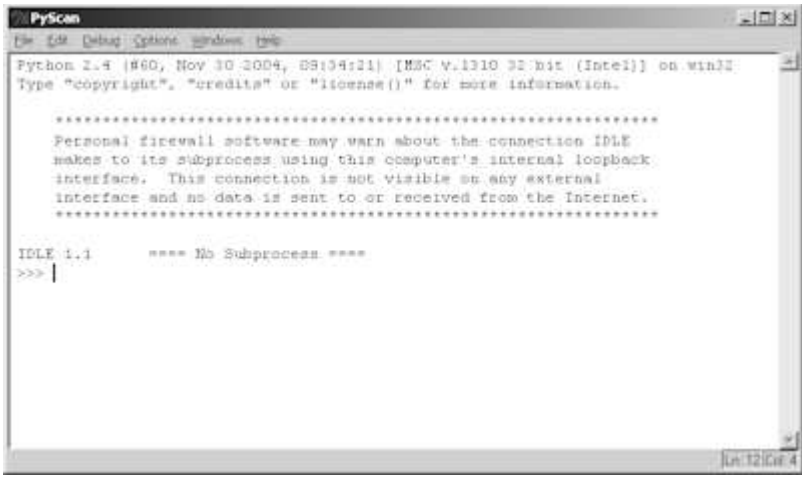
Pyscan

Pourquoi et quand exécuter cette tâche

Pyscan est une extension de Python qui permet de contrôler AppScan à l'aide de l'interface Python. Pyscan est installé et activé lors de l'installation standard d'AppScan.

Procédure

Dans la barre d'outils **Outils**, cliquez sur **Extensions** > **Pyscan**.
L'interface Pyscan s'ouvre.



Module d'optimisation de l'exploration

Cette extension facilite l'amélioration de l'efficacité de l'examen en éliminant les URL inutiles des résultats de l'exploration.

L'extension peut améliorer tout particulièrement les performances lorsque la réécriture d'URL est utilisée par le site ; en effet, celle-ci alourdit l'étape d'exploration de l'examen avec les adresses URL dupliquées qui apparaissent différentes uniquement à cause de paramètres intégrés.

Le module d'optimisation de l'exploration identifie les adresses URL redéfinies pour inclure des paramètres. Par exemple, s'il existe un grand nombre d'URL du type de celles indiquées ci-dessous, AppScan crée un dossier pour chacune dans lequel elles sont en réalité des paramètres réécrits dans l'URL pour plus de facilité.

```
http://mysite.com/2010/10/01/
http://mysite.com/2010/10/02/
http://mysite.com/2010/11/01/
http://mysite.com/2010/11/02/
http://mysite.com/2010/12/01/
http://mysite.com/2010/12/02/
```

Un cas comme celui-ci peut générer des milliers d'URL inutiles, ou une étape d'exploration sans fin.

Lorsqu'il rencontre un grand nombre d'URL qui semblent liées, le module les analyse. Il crée ensuite un paramètre personnalisé (dans ce cas, il s'agirait de `/[year]/[month]/[day]`), efface les résultats de l'exploration et lance une nouvelle étape d'exploration, débouchant vraisemblablement sur une étape de test comportant un nombre d'URL largement inférieur. Les performances de l'examen s'en trouvent largement accrues.

Remarque : **Exécuter la détection des paramètres de navigation** est une autre fonctionnalité de ce module qui peut contribuer à l'efficacité de l'examen (pour plus de détails, voir «Configuration de l'optimisation de l'exploration», à la page 299).

Exécution automatique du module

Il est conseillé d'exécuter le module au cours des examens *chaque fois que le nombre de liens reconnus dans l'étape d'exploration (y compris les liens non visités) atteint le seuil configuré*. En général, la valeur de ce seuil ("Nombre minimal de liens pour le démarrage du module") est généralement au minimum 1,000 (1000).

Remarque : Si vous lancez un examen à partir de l'interface de ligne de commande, l'optimisation de l'exploration ne s'exécute *pas* automatiquement, même si elle est configurée.

Remarque : Si votre configuration d'examen inclut des données d'exploration manuelle ou une opération en plusieurs étapes, l'optimisation de l'exploration ne s'exécute *pas* automatiquement même si elle est configurée ; vous pouvez toutefois l'exécuter manuellement (Outils > Extensions > Module d'optimisation de l'exploration > Exécuter).

Pour modifier la configuration :

1. Cliquez sur **Outils > Extensions > Optimisation de l'exploration : Configurer**.
   La boîte de dialogue de configuration de l'optimisation de l'exploration s'ouvre.
2. Cochez la case **Exécuter l'optimiseur de l'exploration automatiquement au cours des examens**.
3. Cliquez sur **OK**.

Exécution manuelle du module

Vous pouvez lancer manuellement le module sur tous les résultats d'exploration, même si le nombre d'URL reconnues est *inférieur* au seuil configuré ("Toujours exécuter automatiquement pendant les examens"). Cependant, le module est particulièrement utile lorsque le nombre d'URL est au moins de plusieurs centaines.

Pour lancer manuellement l'optimisation de l'exploration :

- Cliquez sur **Outils > Extensions > Optimisation de l'exploration : Exécuter**.
  Le module commence l'exploration, à partir de l'URL de départ configurée. À la fin de l'étape d'exploration, il analyse les résultats. Si des optimisations potentielles sont détectées, il vous offre la possibilité d'enregistrer le premier ensemble de résultats avant d'effacer ces résultats et de relancer une exploration.

Voir aussi :

«Réglage de la redondance», à la page 83

«Options par défaut du réglage de la redondance», à la page 84

Utilisation de l'optimisation de l'exploration

La présente section décrit l'exécution d'un examen lorsque l'optimisation de l'exploration est activée.

Pourquoi et quand exécuter cette tâche

Si votre site réécrit des paramètres à l'intérieur de ses URL, ou si les tentatives initiales d'exploration du site avec la fonction d'optimisation de l'exploration désactivée produisent une très grande quantité d'URL ou des examens sans fin, utilisez le module d'optimisation de l'exploration pour tenter de réduire l'examen à des proportions gérables. De plus, l'activation de l'option Exécuter la détection des paramètres de navigation peut être utile.

Procédure

1. Configurez l'URL de départ et les autres paramètres habituellement définis dans un examen standard.
2. Accédez à **Outils > Extensions > Module d'optimisation de l'exploration : Configurez** et cochez la case **Exécuter l'optimiseur de l'exploration automatiquement au cours des examens**.

   Remarque : Si votre configuration d'examen inclut des données d'exploration manuelle ou une opération en plusieurs étapes, l'optimisation de l'exploration ne s'exécute *pas* automatiquement même si elle est configurée ; vous pouvez toutefois l'exécuter manuellement (Outils > Extensions > Module d'optimisation de l'exploration > Exécuter).
3. Dans la zone de configuration d'examen, vous pouvez définir le paramètre **Exécuter la détection des paramètres de navigation** à **True**.
4. Cliquez sur **OK**.
5. Lancez un examen (**Examen > Examen intégral**).

   Si le nombre d'URL détectées pendant l'étape d'exploration (y compris les URL non explorées) atteint le seuil défini dans **Nombre minimal de liens pour le démarrage du module** (valeur par défaut : 1000), l'étape d'exploration est interrompue et le module d'optimisation de l'exploration entre dans une *phase* constituée de deux étapes (principales) :

   Identification des paramètres de navigation (si configurée)
   Le module recherche des paramètres de navigation, sur la base des paramètres Noms et Valeurs (configurés dans Outils > Extensions > Optimisation de l'exploration : Configurer). Puis, s'il parvient à identifier des paramètres de navigation, le module :
   a. Les définit dans la liste des paramètres (Configuration des examens > Paramètres et cookies > onglet principal).
   b. Règle la redondance au niveau le plus strict
   c. Réduit le niveau du réglage *par défaut* de la redondance (pour les paramètres non navigationnels) (voir «Options par défaut du réglage de la redondance», à la page 84)

   Identification de la réécriture des URL
   Le module recherche les paramètres écrits dans l'URL. S'il les trouve, il les définit dans la liste des paramètres personnalisés (Configuration des examens > Paramètres et cookies > Avancé : onglet Paramètres personnalisés).
6. A la fin de cette *phase* d'optimisation de l'exploration :
   - Si des modifications de la configuration ont été effectuées, les données d'exploration existantes sont effacées et une nouvelle étape d'exploration est exécutée. Si vous avez démarré le mode manuellement, vous avez la possibilité de sauvegarder les données en cours avant l'exécution de la nouvelle étape d'exploration.
   - Si la configuration n'a pas été modifiée, une nouvelle *phase* d'optimisation de l'exploration est lancée, avec un seuil plus élevé (non configurable par l'utilisateur), pour tenter de rassembler suffisamment de données pour identifier les paramètres et ramener les données d'exploration à une taille raisonnable.
7. Lorsque l'exécution du module a abouti (avec une ou plusieurs phases, et une ou plusieurs étapes de réexploration), l'examen reprend et se termine.
8. A la fin de l'examen, passez en revue les résultats et recherchez une indication que son déroulement s'est terminé normalement :
   - La barre d'état, en bas à gauche de l'écran, indique le nombre de tests créés et le nombre de tests envoyés. Tous les tests doivent avoir été envoyés.
   - L'arborescence d'application doit être complète, ce qui signifie que toutes les parties importantes du site ont été visitées.
   - Sur la base des paramètres de navigation ajoutés, vérifiez que tous les paramètres importants ont été contrôlés.

- Vérifiez que les paramètres personnalisés ajoutés correspondent bien à la manière dont le site écrit ses paramètres dans les URL.

Configuration de l'optimisation de l'exploration

Cette boîte de dialogue est utilisée pour activer et configurer le module d'optimisation de l'exploration.

Dans la plupart des cas, il n'est pas nécessaire de modifier d'autres configurations. Comme indiqué ci-dessous, certaines ne doivent pas être modifiées sans l'aide du support.

Cette boîte de dialogue s'ouvre dans **Outils > Extensions > Optimisation de l'exploration : Configurer**.

Remarque : Si vous modifiez ces paramètres et créez un nouvel examen, ils reviennent tous à leur valeur par défaut, sauf le paramétrage de la case à cocher.

Nom	Description
Case à cocher	
Exécuter l'optimiseur de l'exploration automatiquement au cours des examens	Si cette case est cochée, le module s'exécute automatiquement lorsque vous lancez Exploration uniquement ou Examen intégral, chaque fois que la limite "Nombre minimal de liens pour le démarrage" (ci-dessous) est atteinte. **Important :** Ce paramètre s'applique à *tous* les examens. Tous les autres paramètres de cette boîte de dialogue s'appliquent seulement à l'examen en cours. Valeur par défaut : Désélectionnée **Remarque :** Si vous lancez un examen à partir de l'interface de ligne de commande, l'optimisation de l'exploration ne s'exécute *pas* automatiquement, même si elle est configurée. **Remarque :** Si votre configuration d'examen inclut des données d'exploration manuelle ou une opération en plusieurs étapes, l'optimisation de l'exploration ne s'exécute *pas* automatiquement même si elle est configurée ; vous pouvez toutefois l'exécuter manuellement (Outils > Extensions > Module d'optimisation de l'exploration > Exécuter).
Configuration des examens	

Ancrer les règles de réécriture vers la droite	Considérons des URL comme celles-ci :
	`http://...php/1/index`
	`http://...php/2/index`
	`http://...php/3/index`
	
	Lorsque le module crée le paramètre personnalisé :
	
	Si la valeur est False, le paramètre créé est :
	
	`php/([^/.]+)`
	
	Si la valeur est True, le paramètre créé est :
	
	`php/([^/.]+)/index`
	
	Valeur par défaut : Faux

Pourcentage de la marge de fiabilité	Ne modifiez ce paramètre que si le service de support vous le demande.
Délimiteurs utilisés dans la réécriture d'URL	Ajoutez les délimiteurs personnalisés utilisés par votre application.
Profondeur maximale pour le démarrage des paires de lignes	Ne modifiez ce paramètre que si le service de support vous le demande.
Durée de phase maximale (minutes)	Durée maximale de l'exécution d'une étape d'optimisation de l'exploration.

Nom	Description
Fusionner les règles de réécriture vers la gauche	Ne modifiez ce paramètre que si le service de support vous le demande.
Nombre minimal de liens pour le démarrage du module	Nombre minimal de liens dans les données de l'étape d'exploration (y compris les URL non visitées) avant que le module d'optimisation de l'exploration démarre automatiquement, si la case Exécuter l'optimiseur de l'exploration automatiquement au cours des examens est cochée. **Remarque :** Même si ce paramètre est modifié, la notification vous suggérant d'activer le module apparaît lorsque le chiffre de 1 000 liens est atteint dans l'étape d'exploration. Valeur par défaut : 1 000
Délimiteurs de paires valeur-nom	Entrez les délimiteurs personnalisés utilisés par votre application.
Nom des paramètres de navigation	Correspondances partielles pour les noms des paramètres de navigation, séparées par un espace.
Valeurs de paramètres de navigation	Correspondances partielles pour les schémas des valeurs des paramètres de navigation, séparées par un espace.
Supprimer les délimiteurs non utilisés	Ne modifiez ce paramètre que si le service de support vous le demande. Valeur par défaut : Vrai
Détection de paramètre de navigation	Lorsque cette valeur est définie à True, le module tente d'identifier les paramètres de navigation par nom ou par valeur. Il règle la redondance au niveau le plus strict pour ces paramètres, *et réduit la valeur par défaut appliquée aux autres paramètres.* Cela permet à AppScan de tester les paramètres de navigation de manière *plus* approfondie, tout en testant en toute sécurité les paramètres non navigationnels de manière *moins* approfondie. Définir cette valeur à True permet d'améliorer nettement l'exactitude et la performance ; vous devez toutefois vérifier les résultats avec attention pour vous assurer que la couverture de l'examen n'a pas été affectée. Valeur par défaut : Faux
Changer de limite de complexité	Si un dossier spécifique contient un nombre de sous-dossiers supérieur à cette limite, AppScan considère que les sous-dossiers sont des valeurs de paramètre dynamiques et ne requièrent pas d'examen individuel. **Remarque :** La valeur saisie ici est également utilisée comme seuil d'exécution manuelle de l'optimisation de l'exploration. Si le nombre de liens reconnu est inférieur à la valeur saisie ici, le module ne s'exécute pas. Valeur par défaut : 20

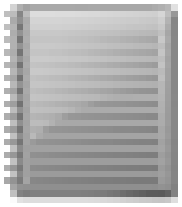
Journaux

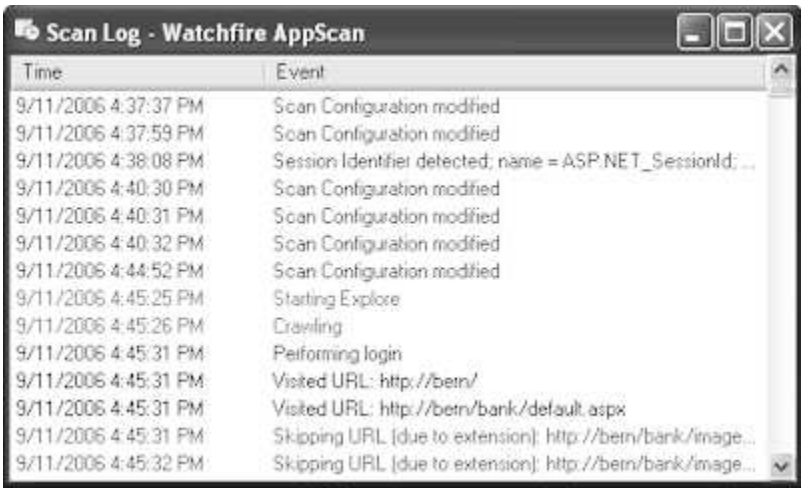
Les journaux peuvent vous aider à traiter les incidents.

Journal d'examen

Ce journal répertorie les actions effectuées par AppScan pendant l'examen en cours.

Lorsqu'un examen est exécuté, le journal d'examen est mis à jour en temps réel ce qui permet de suivre AppScan pas à pas.

- Dans la barre d'outils, cliquez sur l'icône **Journal d'examen**  .



Le journal d'examen est sauvegardé avec l'examen. Lorsqu'un examen sauvegardé est chargé, le journal d'examen existant l'est également, et les données sont ajoutées au journal au fur et à mesure que l'examen continue.

Remarque : La fenêtre Journal d'examen n'affiche pas les données précédentes sauvegardées dans le journal d'examen. Il n'est possible de consulter ces données que dans le fichier journal lui-même. Pour l'afficher, ouvrez le fichier d'examen (.SCAN) à l'aide d'un programme ouvrant les fichiers compressés, recherchez le fichier ScanLog.log et ouvrez-le dans un afficheur de texte.

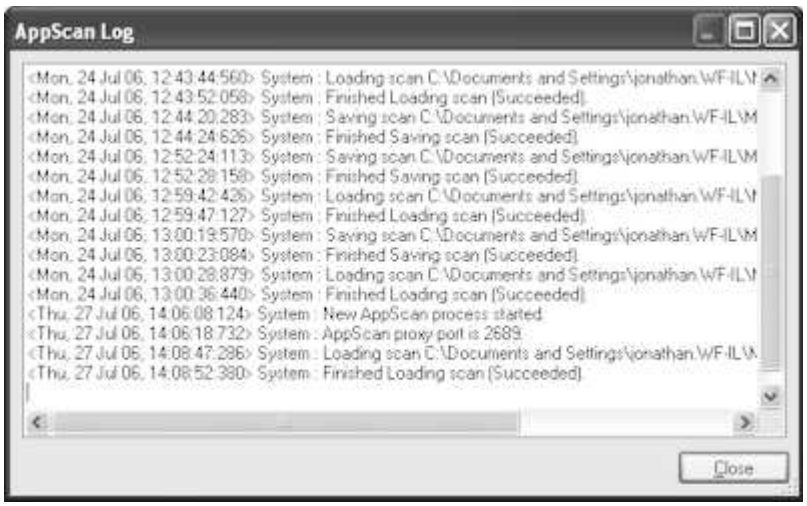
Vous pouvez personnaliser le journal d'examen en définissant exactement les éléments qu'il doit inclure ainsi que leur couleur dans la fenêtre Journal d'examen (voir «Onglet Options d'examen», à la page 259).

Si nécessaire, les messages et réponses utilisateur suggérés sont décrits dans la section «Messages du journal des examens», à la page 346

AppScan Journal

Ce journal affiche la liste des erreurs, des connexions et AppScan des messages système (événements et avertissements de l'application générale).

- Pour afficher le journal AppScan dans AppScan, cliquez sur **Aide > Journal AppScan**.



- Pour connaître l'emplacement de sauvegarde de ce journal, cliquez sur **Outils** > **Options** > **Onglet Général** > **Dossier des fichiers journaux**.

  Dans Windows 7, l'emplacement par défaut est :

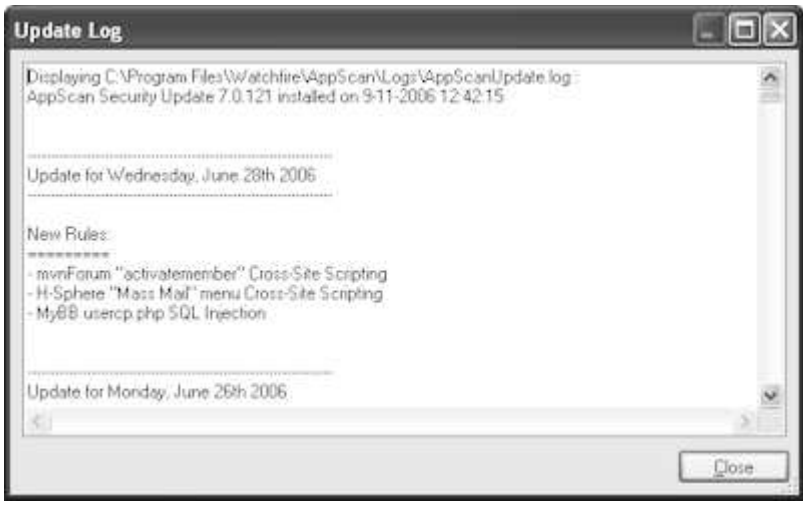
  `...\AppData\Roaming\IBM\AppScan Standard\Logs`

Si nécessaire, les messages et réponses utilisateur suggérés sont décrits dans la section «AppScan Messages des journaux», à la page 356

Journal des mises à jour

Ce journal affiche la liste de toutes les mises à jour apportées au programme depuis son installation.

- Pour afficher le journal des mises à jour, cliquez sur **Aide > Journal des mises à jour**.



- Pour connaître l'emplacement de sauvegarde de ce journal, cliquez sur **Outils** > **Options** > **Onglet Général** > **Dossier des fichiers journaux**.

  Dans Windows 7, l'emplacement par défaut est :

  `...\AppData\Roaming\IBM\AppScan Standard\Logs`

Voir aussi :

«Mises à jour», à la page 12

Consignation du trafic

Ce journal répertorie les demandes et les réponses échangées entre AppScan et le site pendant l'examen et peut se révéler utile pour le traitement des incidents.

Le Journal du trafic répertorie toutes les réponses aux demandes reçues de l'application pendant l'examen. Par défaut, AppScan n'enregistre pas le journal du trafic mais vous pouvez l'activer si le service de support vous le demande pour vous fournir une meilleure assistance.

L'activation du journal peut avoir un impact sur les performances et doit donc être effectuée uniquement en cas de besoin.

- Pour activer le Journal du trafic, cliquez sur **Outils > Options** et sélectionnez **Activer la consignation des demandes/réponses**.
- Pour connaître l'emplacement de sauvegarde de ce journal, cliquez sur **Outils** > **Options** > **Onglet Général** > **Dossier des fichiers journaux**.

  Dans Windows 7, l'emplacement par défaut est :

  ```
  ...\AppData\Roaming\IBM\AppScan Standard\Logs
  ```

Recherche de résultats

Vous pouvez filtrer la liste des résultats à partir de n'importe quelle vue à la recherche de données spécifiques.

Procédure

1. Dans la barre d'outils, cliquez sur **Rechercher** ou appuyez sur **Ctrl + F**.

   La barre **Rechercher** apparaît au bas de l'écran.
2. Dans l'**Arborescence de l'application**, sélectionnez un nœud.
   - Si vous sélectionnez le nœud **Mon application**, la recherche se fait parmi tous les résultats.
   - Si vous sélectionnez un nœud dans l'arborescence, la recherche se fait dans le nœud sélectionné et ses sous-nœuds.
3. Dans la zone de saisie **Rechercher** de la barre **Rechercher**, entrez une chaîne ou une partie de chaîne.
4. Dans la liste **Afficher**, cliquez sur un type de données.
5. Cliquez sur **Rechercher maintenant** ou appuyez sur **Entrée**.

   Les résultats apparaissent dans la **liste des résultats**, écrasant la liste précédemment affichée, et les compteurs sont mis à jour pour afficher le nouveau nombre d'éléments dans chaque catégorie. Les onglets ne contenant pas de résultat sont grisés.

   Si vous entrez une autre chaîne **Rechercher** et cliquez à nouveau sur **Rechercher maintenant**, la nouvelle recherche est réalisée sur le nœud sélectionné dans l'**Arborescence de l'application**, et non sur les résultats affichés de la précédente recherche.

   Remarque : Pour revenir à l'examen intégral, annulez le filtre sur la Liste des résultats et cliquez sur **Effacer**.

Chapitre 12. Intégrations

Cette section décrit les intégrations d'autres applications à AppScan Standard.

AppScan Enterprise

Cette section décrit les modes d'interaction entre les éditions AppScan Standard et Enterprise.

L'édition AppScan Enterprise permet un examen centralisé et fournit des contrôles d'accès utilisateur, comporte des fonctions de résolution ainsi que des tableaux de bord globaux, et fournit des rapports de conformité et une intégration transparente avec AppScan Standard. Si votre organisation utilise AppScan Enterprise, vous pouvez :

- Importer les droits d'accès utilisateur AppScan Enterprise à utiliser *en plus* de ceux octroyés par la licence AppScan Standard locale.
- Exporter ("Publier") les résultats d'examen de AppScan Standard à utiliser dans AppScan Enterprise.
- Créer un travail AppScan Enterprise.

Importation des autorisations de licence pour AppScan Enterprise

Configurez AppScan Standard afin d'effectuer un examen des sites autorisés par votre licence AppScan Enterprise.

Pourquoi et quand exécuter cette tâche

Si votre organisation dispose d'une licence AppScan Enterprise permettant l'examen de sites autres que ceux autorisés par votre licence locale AppScan Standard, vous pouvez importer ces autorisations pour les utiliser sur votre poste local *en plus* de votre licence existante. Vous pourrez également examiner toute adresse URL autorisée par l'une des licences ou par les deux.

Remarque : Cette option est disponible uniquement lorsqu'une licence AppScan Standard complète (et non une licence de démonstration) est chargée.

Procédure

1. Cliquez sur **Aide > Licence**.
   La boîte de dialogue Licence s'ouvre.
2. Cliquez sur **Ajouter une licence AppScan Enterprise**.
   La boîte de dialogue AppScan Enterprise s'ouvre.
3. Cochez la case **AppScan Enterprise**.
   Les zones deviennent actives.
4. Sélectionnez la case à cocher et entrez les nom d'utilisateur, mot de passe, domaine et URL pour le serveur AppScan Enterprise.
5. (Facultatif) Vérifiez que vous êtes connectés au réseau et cliquez sur le bouton **Tester ces paramètres**.
   AppScan contacte AppScan Enterprise Server et la licence de votre organisation s'affiche dans la partie inférieure de la boîte de dialogue.

   Remarque : Si le client local ne parvient pas à entrer en contact avec le serveur Enterprise, vous êtes notifié que l'examen est limité aux adresses IP autorisées par la licence locale.
6. Cliquez sur **OK**.
   Les autorisations correspondant à AppScan Enterprise sont chargées dans la licence AppScan, en complément de ses propres autorisations.

Publication vers AppScan Enterprise

Vous pouvez publier les résultats AppScan Standard dans AppScan Enterprise afin de pouvoir les utiliser dans ce produit.

Procédure

1. Ouvrez l'examen dont vous voulez exporter les résultats.
2. Cliquez sur **Fichier > Exporter > Publier les résultats dans AppScan Enterprise**.
   La boîte de dialogue Connexion s'ouvre.
3. Configurez vos informations de connexion AppScan Enterprise.
   Pour vous connecter avec votre ID utilisateur et votre mot de passe :
   a. Sélectionnez **Connexion avec l'ID utilisateur et le mot de passe**.
   b. Dans la zone URL :
      - **AppScan Enterprise 9.0.3.1 et versions ultérieures :** Entrez l'URL du service du serveur AppScan Enterprise.
        Format : `https://[AppScan Enterprise Server]:[Server port]/ase`
      - **AppScan Enterprise 9.0.3 et versions antérieures :** Entrez l'URL du service SOAP du serveur AppScan Enterprise.
        Format : `http://[AppScan Enterprise Server]/ase/desktop/permissions.asmx`
   c. Entrez un ID utilisateur (au format `[domain name]\[username]`) et un mot de passe valides.
   d. Cliquez sur **Connexion**.

   Pour vous connecter à l'aide d'un certificat côté client ou d'une carte à puce :
   a. Sélectionnez **Connexion avec le certificat côté client/la carte à puce**.
   b. Dans la zone URL :
      - **AppScan Enterprise 9.0.3.1 et versions ultérieures :** Entrez l'URL du service du serveur AppScan Enterprise.
        Format : `https://[AppScan Enterprise Server]:[Server port]/ase`
      - **AppScan Enterprise 9.0.3 et versions antérieures :** Entrez l'URL du service SOAP du serveur AppScan Enterprise.
        Format : `http://[AppScan Enterprise Server]/ase/desktop/permissions.asmx`
   c. Sélectionnez la case à cocher correspond au certificat requis.
   d. Cliquez sur **Connexion**.

   Remarque : Si un code PIN de carte à puce est requis pour se connecter, une boîte de dialogue s'affiche pour que vous puissiez le saisir.

   La boîte de dialogue de publication des résultats s'ouvre.
4. Définissez le Nom du travail et éventuellement le Dossier et l'Application AppScan Enterprise.

   Remarque :
   - La sélection des données s'applique uniquement à SOAP et est prise en charge depuis la version 8.7 d'AppScan Enterprise. Si vous ne sélectionnez aucun dossier, le dossier AppScan Enterprise par défaut est utilisé. Pour les services REST, la sélection des dossiers ne s'applique pas et les résultats sont sauvegardés dans l'application sélectionnée.
   - La sélection des applications est prise en charge depuis la version 9.0 d'AppScan Enterprise.
   - La boîte de dialogue Sélectionner une application inclut une option **Créer une nouvelle application sur le serveur** si vos droits le permettent.
5. Cliquez sur **Publier**.
   A l'issue du processus, un message de réussite vert apparaît dans la boîte de dialogue. Vous pouvez maintenant ouvrir le travail et le gérer depuis AppScan Enterprise.

Création d'un travail dans AppScan Enterprise

Vous pouvez créer un travail AppScan Enterprise à l'aide de votre configuration AppScan Standard.

Pourquoi et quand exécuter cette tâche

Il est possible d'exporter les configurations d'examen dans AppScan Enterprise en tant que nouveaux travaux pour les utiliser.

Remarque : Security AppScan Enterprise version 9.0 ou ultérieure est nécessaire.

Procédure

1. Ouvrez l'examen dont vous souhaitez utiliser la configuration.
2. Cliquez sur **Fichier > Exporter > Créer un travail dans AppScan Enterprise**.
   La boîte de dialogue Connexion s'ouvre.
3. Configurez vos informations de connexion AppScan Enterprise.
   Pour vous connecter avec votre ID utilisateur et votre mot de passe :
   a. Sélectionnez **Connexion avec l'ID utilisateur et le mot de passe**.
   b. Dans la zone URL :
      - **AppScan Enterprise 9.0.3.1 et versions ultérieures :** Entrez l'URL du service du serveur AppScan Enterprise.
        Format : `https://[AppScan Enterprise Server]:[Server port]/ase`
      - **AppScan Enterprise 9.0.3 et versions antérieures :** Entrez l'URL du service SOAP du serveur AppScan Enterprise.
        Format : `http://[AppScan Enterprise Server]/ase/desktop/permissions.asmx`
   c. Entrez un ID utilisateur (au format `[domain name]\[username]`) et un mot de passe valides.
   d. Cliquez sur **Connexion**.

   Pour vous connecter à l'aide d'un certificat côté client ou d'une carte à puce :
   a. Sélectionnez **Connexion avec le certificat côté client/la carte à puce**.
   b. Dans la zone URL :
      - **AppScan Enterprise 9.0.3.1 et versions ultérieures :** Entrez l'URL du service du serveur AppScan Enterprise.
        Format : `https://[AppScan Enterprise Server]:[Server port]/ase`
      - **AppScan Enterprise 9.0.3 et versions antérieures :** Entrez l'URL du service SOAP du serveur AppScan Enterprise.
        Format : `http://[AppScan Enterprise Server]/ase/desktop/permissions.asmx`
   c. Sélectionnez la case à cocher correspond au certificat requis.
   d. Cliquez sur **Connexion**.

   Remarque : Si un code PIN de carte à puce est requis pour se connecter, une boîte de dialogue s'affiche pour que vous puissiez le saisir.

   La boîte de dialogue de création d'un travail s'ouvre.
4. Définissez le Nom du travail et éventuellement le Dossier et l'Application AppScan Enterprise.

   Remarque : La sélection des dossiers est prise en charge depuis AppScan Enterprise version 8.7 et la sélection des applications depuis AppScan Enterprise version 9.0. Les dossiers de modèles d'examen ne sont pas affichés. Si vous ne sélectionnez aucun dossier, le dossier AppScan Enterprise par défaut est utilisé.

Remarque : La boîte de dialogue Sélectionner une application inclut une option **Créer une nouvelle application sur le serveur** si vos droits le permettent.

5. Si votre configuration comprend des données d'exploration manuelle, vous avez la possibilité de :
   - **Continuer l'examen intégral :** AppScan effectuera une étape d'exploration automatique avant de tester toutes les données d'exploration (manuelles et automatiques).
   - **Test uniquement :** Seules les données d'exploration manuelle existantes seront testées.
6. Cliquez sur **Créer**.

   A l'issue du processus, un message de réussite vert apparaît dans la boîte de dialogue. Vous pouvez maintenant ouvrir les résultats et les gérer depuis AppScan Enterprise.

Création d'un modèle d'examen dans AppScan Enterprise

Vous pouvez créer un modèle AppScan Enterprise à l'aide de votre configuration AppScan Standard.

Pourquoi et quand exécuter cette tâche

Vous pouvez exporter des configurations d'examen dans AppScan Enterprise sous la forme de modèles pour les utiliser dans cet environnement.

Remarque : Security AppScan Enterprise version 9.0 ou ultérieure est nécessaire.

Procédure

1. Ouvrez l'examen dont vous souhaitez utiliser la configuration.
2. Cliquez sur **Fichier > Exporter > Créer un modèle dans AppScan Enterprise**.

   La boîte de dialogue de création d'un modèle s'affiche.
3. Configurez vos informations de connexion AppScan Enterprise.
   a. Entrez un ID utilisateur (au format `[domain name]\[username]`) et un mot de passe valides.
   b. Dans la zone d'URL, entrez l'URL du serveur AppScan Enterprise au format suivant :

      `http://[AppScan Enterprise Server]/ase/desktop/permissions.asmx`
   c. Cliquez sur **Tester ces paramètres**.

   La boîte de dialogue de création d'un travail s'ouvre.
4. Définissez le nom du modèle et sélectionnez l'option correspondant au dossier et à l'application AppScan Enterprise.

   Remarque : La sélection des dossiers est prise en charge depuis AppScan Enterprise version 8.7 et la sélection des applications depuis AppScan Enterprise version 9.0. Seuls les dossiers de modèles sont affichés. Si vous ne sélectionnez aucun dossier, le dossier AppScan Enterprise par défaut est utilisé.

   Remarque : La boîte de dialogue Sélectionner une application inclut une option **Créer une nouvelle application sur le serveur** si vos droits le permettent.
5. Cliquez sur **Créer**.

   A l'issue du processus, un message de réussite vert apparaît dans la boîte de dialogue. Vous pouvez maintenant ouvrir et utiliser le modèle dans AppScan Enterprise.

Infrastructures d'automatisation

Vous pouvez utiliser des scripts créés pour votre infrastructure d'automatisation Assurance qualité (comme Selenium) afin de créer des enregistrements d'exploration manuelle pour un examen AppScan.

Si le personnel chargé de l'assurance qualité utilise une infrastructure d'automatisation pour exécuter des tests fonctionnels dans votre application Web, vous pouvez tirer parti des scripts déjà créés pour créer des examens personnalisés. Les demandes transmises par l'infrastructure d'automatisation à l'application

sont envoyées en utilisant AppScan en tant que proxy pour permettre à AppScan d'enregistrer les actions sous la forme d'une étape d'exploration pour son propre examen. AppScan teste ensuite le site en fonction de cette étape d'exploration. Cette opération est effectuée à l'aide de l'interface de ligne de commande AppScan.

En principe, vous créez et exécutez une commande par lots qui permet d'effectuer les opérations suivantes :

1. Ouvrir AppScan et configurer :
   a. Adresse URL de départ
   b. Les données d'identification utilisateur
   c. Test uniquement
   d. L'ouverture du proxy d'AppScan avec un port d'écoute spécifique
2. Exécuter le script de l'infrastructure d'automatisation en utilisant le même port.
3. Lorsque le script est terminé, fermer le proxy d'AppScan et démarrer l'étape de test.
4. Sauvegarder les résultats de l'examen et créer et sauvegarder un rapport, si nécessaire.

La section ci-après explique comment tester le site de démonstration d'AppScan avec Selenium ; toutefois, la procédure peut être facilement adaptée à n'importe quel site et à n'importe quelle infrastructure d'automatisation.

Création de la commande par lots

Cet exemple effectue un examen à l'aide d'un script Selenium pour l'étape d'exploration. Les mêmes principes peuvent s'appliquer à n'importe quelle autre infrastructure d'automatisation.

Pourquoi et quand exécuter cette tâche

L'exemple suppose que vous utilisez un script Selenium et que le port 56232 est configuré pour les communications entre Selenium et AppScan Standard. Vous pouvez évidemment modifier ses paramètres en fonction de vos besoins.

Remarque : Dans chaque exemple de code, le code ajouté lors de cette étape apparaît en gras.

Si vous voulez parcourir vous-même cet exemple, le dossier contenant le fichier utilisé ici est :

```
[AppScan Standard installation folder]\Docs\Selenium Example
```

Remarque : Si le chemin de votre dossier AppScan est différent, vous devez modifier le chemin dans le fichier JAR.

Procédure

1. Créez un fichier TXT et ouvrez-le dans un éditeur de texte.
2. Entrez la commande AppScan pour ouvrir AppScan et définissez l'URL de départ, les données d'identification de connexion, l'option Test uniquement, l'ouverture du proxy et le port d'écoute du proxy :

   ```
   START "" "[AppScan Standard installation folder]\AppScanCMD.exe"
   /starting_url "https://demo.testfire.net"
   /credentials "jsmith:demo1234"
   /test_only
   /opr
   /lp "53262"
   ```

   Conseil : vous pouvez ajouter des commandes supplémentaires si nécessaire, par exemple pour définir une stratégie de test spécifique ou créer un rapport (pour des détails, voir Chapitre 15, «Interface de ligne de commande», à la page 365).
3. Ajoutez un lot avec un délai de 15 secondes pour permettre AppScan de s'afficher :

```
START "" "[AppScan Standard installation folder]\AppScanCMD.exe"
/starting_url "https://demo.testfire.net"
/credentials "jsmith:demo1234" /test_only /opr /lp "53262"

timeout /t 15
```

4. Ajoutez votre script Selenium :

```
START "" "[AppScan Standard installation folder]\AppScanCMD.exe"
/starting_url "https://demo.testfire.net"
/credentials "jsmith:demo1234" /test_only /opr /lp "53262"

timeout /t 15

java -jar selenium-server-standalone-2.52.0.jar -trustAllSSLCertificates -htmlSuite "*firefox" "https://demo.testfire.ne
```

   Important : L'URL de départ indiquée pour Selenium doit être identique à celle définie dans le modèle AppScan.

5. Insérez dans le script Selenium le port et l'hôte du proxy AppScan auxquels Selenium doit envoyer ses demandes :

```
START "" "[AppScan Standard installation folder]\AppScanCMD.exe"
/starting_url "https://demo.testfire.net"
/credentials "jsmith:demo1234" /test_only /opr /lp "53262"

timeout /t 15

java -Dhttp.proxyHost=localhost -Dhttp.proxyPort=56232 -Dhttps.proxyHost=localhost -Dhttps.proxyPort=56232 -jar seleniu
-htmlSuite "*firefox" "https://demo.testfire.net" "mytestsuite.html" "results.html"
```

6. Ajoutez une commande à la fin pour fermer le proxy d'AppScan et démarrer l'étape de test :

```
START "" "[AppScan Standard installation folder]\AppScanCMD.exe" /scan_template
" C:\Users\<username>\Documents\AppScan\QA Automation Demo Template.scant " /test_only /opr /lp
"56232"

timeout /t 15

java -Dhttp.proxyHost=localhost -Dhttp.proxyPort=64345 -Dhttps.proxyHost=localhost
-Dhttps.proxyPort=56232 -jar selenium-server-standalone-2.52.0.jar -trustAllSSLCertificates
-htmlSuite "*firefox" "https://demo.testfire.net" "mytestsuite.html" "results.html"

"[dossier d'installation d'AppScan Standard]\AppScanCMD.exe" cpr
```

7. Sauvegardez le fichier et exécutez-le à l'aide de la ligne de commande.

Résultats

Selenium s'ouvre et explore le site, puis AppScan démarre les tests. Une fois l'examen terminé, AppScan le sauvegarde dans le même dossier que le fichier de commandes.

Important : Si le processus n'aboutit pas ou si vous l'arrêtez avant la fin de son exécution, il est possible que les paramètres de proxy de votre navigateur Internet Explorer ou Chrome soient modifiés et que vous deviez annuler la modification manuellement.

Application Security on Cloud

Cette section présente comment AppScan Standard peut interagir avec IBM Application Security on Cloud pour examiner les applications sur le cloud.

Vous devez disposer d'un compte Application Security on Cloud pour utiliser cette fonction et y avoir créé au moins une application.

Si votre site n'est pas accessible à partir d'Internet, vous devez déjà disposer d'une version AppScan Presence avec accès au site et à Internet, pour permettre à Application Security on Cloud d'établir une connexion.

Pour plus de détails, voir la Application Security on Clouddocumentation.

Téléchargement vers Application Security on Cloud

Vous pouvez télécharger un examen AppScan Standard ou un fichier modèle (SCAN ou SCANT) dans IBM Application Security on Cloud pour exécuter un nouvel examen dans le cloud.

Procédure

1. Ouvrez l'examen ou le modèle à télécharger.
2. Cliquez sur **Fichier > Exporter > Télécharger l'examen dans Application Security on Cloud**.
3. Connectez-vous avec votre ID et mot de passe de clé.
4. Cliquez sur **Sélectionner une application**, choisissez une application existante dans la liste puis cliquez sur **Sélectionner**.

   La boîte de dialogue d'exécution d'examen s'affiche.
5. Zone **Paramètres d'examen** : si vous le souhaitez, vous pouvez changer le nom de l'examen et sélectionner la case à cocher permettant d'être notifié une fois l'examen terminé.
6. Zone **Examen de site privé** : sélectionnez la case à cocher seulement si votre site n'est *pas* disponible sur Internet, puis sélectionnez votre instance d'AppScan Presence dans la liste.
7. Zone **Options de test** : sélectionnez l'un des deux boutons radio :

   Test uniquement
   Testez les parties du site déjà explorées dans AppScan Standard. Utilisez cette option si vous souhaitez tester uniquement les opérations à plusieurs étapes ou l'exploration manuelle enregistrées dans AppScan Standard. Une étape de test est exécutée sur les données d'exploration existantes dans le fichier téléchargé.

   Examen intégral
   Poursuit l'étape d'exploration (ajoute des éléments aux données d'exploration sauvegardées dans le fichier) puis exécute une étape de test. Si le fichier téléchargé contient des données d'exploration, ces dernières sont ajoutées et utilisées. Pour qu'elles ne soient pas prises en compte, sélectionnez Test uniquement.
8. Cliquez sur **Télécharger et exécuter**.

   Une mention confirme que le téléchargement a abouti. L'examen commence immédiatement mais le statut de l'examen est visible uniquement dans Application Security on Cloud.

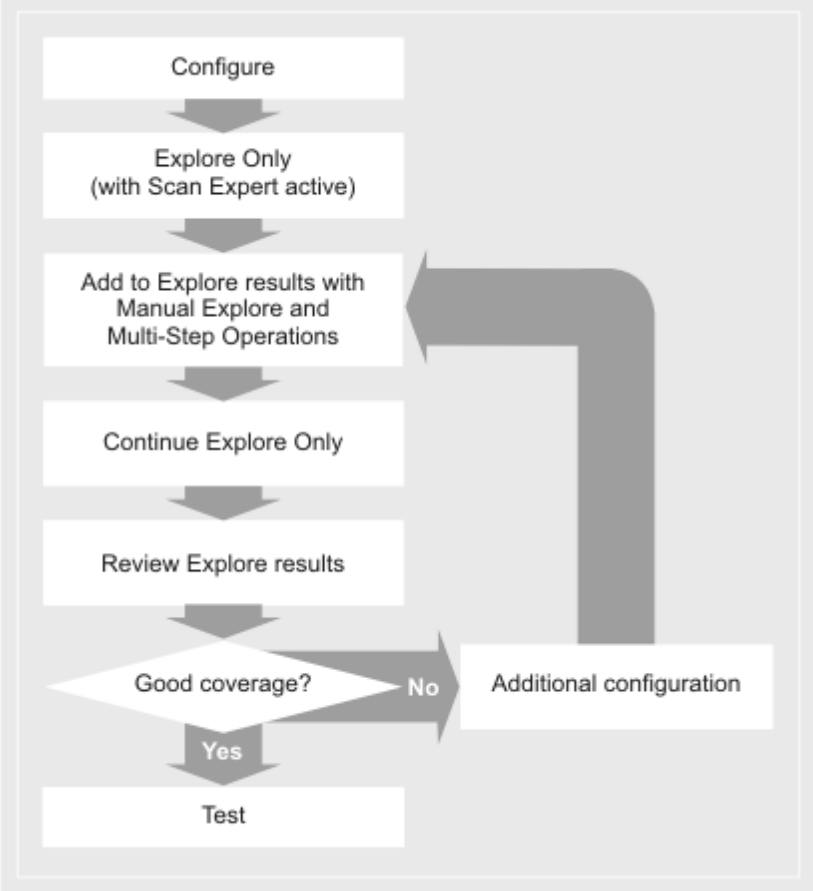
Chapitre 13. Meilleures pratiques et foire aux questions

La présente section fournit des valeurs recommandées ainsi que des scénarios d'utilisation pour les utilisateurs avancés et inclut des questions fréquemment posées (foire aux questions).

Flux de travaux pour les utilisateurs avancés

Ce flux de travaux est destiné à aider les utilisateurs expérimentés dans le domaine de la sécurité Web à réaliser un examen plus approfondi.

La réussite de l'étape de test, et donc de l'examen lui-même, dépend de la couverture obtenue lors de l'étape d'exploration. Si l'étape d'exploration omet des portions non négligeables de la logique de l'application, l'étape de test risque de ne pas révéler d'éventuelles failles importantes. Ce flux de travaux vous aide à améliorer la couverture de l'étape d'exploration.



Tâche	Description
1. Configuration initiale	A l'aide de l'assistant ou de la boîte de dialogue Configuration des examens : 1. Définissez l'URL de départ 2. Enregistrez la procédure de connexion 3. Validez le schéma En session et, si nécessaire, sélectionnez un nouveau schéma. 4. Si votre site dispose d'une fonction de blocage de compte, désactivez-la, ou configurez AppScan de sorte qu'il ne teste pas les pages de connexion. Sinon, le compte utilisé par AppScan se verrouille pendant l'étape de test et cette étape est bloquée. Pour une description détaillée de cette étape, voir «Configuration initiale», à la page 315.
2. Exploration uniquement	Exécutez une première exploration automatique : 1. Dans la barre d'outils, cliquez sur  > **Exploration uniquement**, et patientez jusqu'à la fin de l'étape d'exploration. AppScan explore le site, mais ne le teste pas encore. Au début de l'étape d'exploration, Scan Expert s'exécute et suggère éventuellement des modifications à apporter à la configuration. Le paramétrage par défaut n'autorise Scan Expert à effectuer que les modifications qui peuvent être faites automatiquement. **Remarque :** Si la réécriture URL est mise en œuvre dans le site, lancez l'optimisation de l'exploration (**Outils > Extensions > Module d'optimisation de l'exploration : Exécuter**) et, si l'extension le requiert, exécutez à nouveau l'étape d'exploration automatique (**Examen > Nouvelle exploration**). 2. Si l'exploration prend fin parce que AppScan est hors session, réenregistrez et reconfigurez la procédure de connexion, en portant une attention toute particulière à la détection en session et au suivi de l'ID de session. Pour une description détaillée de cette étape, voir «Exploration automatique initiale», à la page 316.
3. Amélioration manuelle de la couverture du site à l'aide du navigateur	Ajoutez les URL non reconnues par l'exploration automatique : 1. **Exploration manuelle :** Utilisez l'exploration manuelle pour ajouter des pages individuelles, notamment celles qui demandent une saisie spécifique. **Remarque :** Pour les rares cas dans lesquels le navigateur intégré n'arrive pas à parcourir l'application, vous pouvez configurer l'utilisation d'un autre navigateur dans AppScan. 2. **Opérations en plusieurs étapes :** Si des portions du site ne peuvent être atteintes qu'en cliquant sur des liens *dans un ordre spécifique*, enregistrez les opérations en plusieurs étapes. Pour une description détaillée de cette étape, voir «Amélioration manuelle de la couverture du site», à la page 317.
4. Continuer Exploration uniquement	Avec les nouvelles données fournies via l'exploration manuelle, l'exploration automatique doit pouvoir explorer l'application de manière plus approfondie. **Remarque :** Cliquez sur  > **Continuer Exploration automatique** (ou **Examen > Exploration uniquement**) pour conserver les premiers résultats d'exploration et les données d'exploration manuelle. Ne cliquez pas sur **Nouvel examen > Nouvelle exploration**, car cela entraînerait la suppression des données existantes.
5. Evaluation des résultats de l'exploration	Examinez les résultats obtenus pour déterminer si la logique de l'application est bien couverte par l'exploration. **Remarque :** Si vous effectuez de nouvelles modifications sur la configuration, vous devez relancer à nouveau l'exploration automatique (**Examen > Nouvelle exploration**). Pour une description détaillée de cette étape, voir «Evaluation des résultats de l'exploration», à la page 318.

Tâche	Description
6. (Si nécessaire) Opérations de configuration supplémentaires	Si la couverture du site n'est toujours pas suffisante, d'autres options de configuration sont envisageables. Pour une description détaillée de cette étape, voir «Configuration supplémentaire», à la page 321.
7. Etape de test	Cliquez sur **Test uniquement** pour passer à l'étape de test et terminer l'examen.

Configuration initiale

Pourquoi et quand exécuter cette tâche

Effectuez la procédure de la configuration de base avant de tenter d'explorer le site, manuellement ou automatiquement.

Procédure

1. **Définissez et vérifiez l'URL de départ de l'examen.**
   a. Cliquez sur **Fichier > Nouveau** et créez un nouvel examen d'application Web à l'aide de l'assistant (ou configurez-le avec la boîte de dialogue de configuration, **Configuration des examens > Vue URL et serveurs**).
   b. Saisissez l'URL de départ de l'examen.
   c. Si votre application est sensible à la casse, vérifiez que la case Chemin d'accès sensible à la casse est cochée.

      Le plus souvent, les applications qui s'exécutent sur les systèmes de type Linux sont sensibles à la casse, tandis que celles qui s'exécutent sous Microsoft Windows ne le sont pas. Les applications Java constituent une exception et sont, en général, sensibles à la casse quel que soit le système d'exploitation.
   d. Cliquez sur l'icône **Afficher dans le navigateur**, à côté de la zone d'URL, et vérifiez que la page attendue s'affiche dans le navigateur AppScan.
2. **Enregistrez la procédure de connexion.** Cela permet à AppScan de se connecter à l'application pour démarrer l'examen, ou se reconnecter en cas de déconnexion pendant l'examen.
   a. A l'étape 2 de l'assistant, (ou dans **Configuration des examens > Vue Gestion de connexion**), cliquez sur 

pour commencer à enregistrer les actions. Le navigateur s'ouvre à la page de l'URL de départ définie précédemment.
   b. Effectuez toutes les étapes par lesquelles un utilisateur doit passer pour se connecter à l'application.
   c. Recherchez sur la page une indication confirmant que vous êtes bien connecté, par exemple "Bienvenue [nom d'utilisateur]", ou un lien "Déconnexion", *disponible uniquement lorsque l'utilisateur est connecté*.
   d. Fermez le navigateur et recherchez l'icône Clé verte  confirmant que le schéma En session a été identifié.

      Si l'icône est rouge  , *aucun* schéma En session n'a été détecté, et vous devez le définir manuellement (voir «Boîte de dialogue Sélectionner un schéma de détection», à la page 61).

      Remarque : En général, la première adresse URL dont la réponse comprend le schéma en session doit être l'"URL En session", et c'est aussi l'adresse URL qui est sélectionnée automatiquement. Mais vous pouvez cependant améliorer la performance en sélectionnant une autre adresse URL (voir «Optimisation de la détection en session», à la page 62).

3. **Validez le schéma En session.** Le schéma En session est une expression régulière qui correspond au schéma ou à la chaîne affiché(e) pour l'utilisateur sur la page de connexion lorsque celle-ci a abouti, comme "Bienvenue [nom d'utilisateur]", ou un lien "Déconnexion". Même si l'icône est verte, vérifiez le schéma.
   a. A l'étape 2 de l'assistant, sélectionnez **Je souhaite configurer les options de détection en session**, puis cliquez sur **Suivant** (ou accédez à **Configuration des examens > Gestion de connexion > Vue Détails**).

      La séquence de connexion s'affiche.
   b. Cliquez deux fois sur la page signalée comme "En session" pour l'ouvrir dans le navigateur.
   c. Dans le navigateur, cliquez sur l'onglet Demande/Réponse pour voir le code source, et vérifiez que le schéma sélectionné indique effectivement le statut En session.

      Remarque : Si le contenu de la page est en JavaScript ou en CSS, il ne peut en aucun cas convenir comme page En session, et vous devez choisir une autre page.

   Si l'icône Clé est verte alors que le schéma sélectionné n'est *pas* un schéma En session, reportez-vous à la rubrique «Traitement des incidents liés à la connexion basée sur les demandes», à la page 338.
4. **Configuration du blocage de compte.** Pendant l'étape de test, AppScan effectue de nombreuses tentatives de connexion non valides. Si votre site dispose d'une fonction qui verrouille les comptes après la saisie d'un certain nombre de mots de passe, le compte d'AppScan est verrouillé et ne peut pas continuer l'examen.
   - Désactivez la fonction de blocage du compte, ou (si c'est compliqué)
   - Configurez AppScan pour qu'il ne teste pas les pages de connexion et de déconnexion (**Configuration des examens > Options de test**, désélectionnez **Envoyer les tests sur les pages de connexion et de déconnexion**).

Concepts associés:

«Flux de travaux pour les utilisateurs avancés», à la page 313
Ce flux de travaux est destiné à aider les utilisateurs expérimentés dans le domaine de la sécurité Web à réaliser un examen plus approfondi.

Exploration automatique initiale

Une fois la configuration de base effectuée, vous pouvez exécuter une première exploration automatique pour déterminer la qualité de la couverture du site AppScan à cette étape.

Pourquoi et quand exécuter cette tâche

Un examen complet est constitué d'étapes d'exploration et d'une étape de test. Pour le moment, limitez-vous à lancer une étape d'exploration.

La couverture du site basée sur votre configuration initiale peut être incomplète, mais cette étape vous permet de comprendre quelles parties du site sont reconnues et lesquelles ne le sont pas, et facilite l'amélioration de la configuration.

Procédure

1. Cliquez sur **Examen > Explorer uniquement**.

   Scan Expert est configuré pour s'exécuter automatiquement avant l'étape d'exploration.
2. Si Scan Expert suggère des modifications de la configuration, suivez ses recommandations.

   Remarque : Certaines modifications peuvent être implémentées automatiquement, d'autres nécessitent une action de votre part.
3. Laissez AppScan explorer le site jusqu'au bout. Pendant l'examen, vous voyez les données remplir l'arborescence de l'application au fur et à mesure de l'exploration du site.

4. Vérifiez que l'étape d'exploration s'est terminée normalement, et que AppScan n'a pas subi de mise hors session provoquant un arrêt précoce de l'exploration.

   Remarque : Si l'exploration a pris fin prématurément parce que AppScan était hors session, réenregistrez et reconfigurez la procédure de connexion, en portant une attention toute particulière à la détection en session et au suivi de l'ID de session.
5. (Sites utilisant la réécriture d'URL :) Si votre site utilise la réécriture d'URL, le module d'optimisation de l'exploration peut améliorer l'efficacité de l'examen en éliminant à cette étape les URL inutiles des résultats de l'exploration.
   a. Cliquez sur **Outils > Extensions > Module d'optimisation de l'exploration : Exécuter**
   b. Si le module le recommande à la fin du processus, cliquez sur **Examen > Nouvelle Exploration**.

   Avertissement : N'effectuez pas cette étape si vous n'êtes pas sûr que le site applique la réécriture d'URL.

Concepts associés:

«Flux de travaux pour les utilisateurs avancés», à la page 313
Ce flux de travaux est destiné à aider les utilisateurs expérimentés dans le domaine de la sécurité Web à réaliser un examen plus approfondi.

Amélioration manuelle de la couverture du site

Vous pouvez ajouter les URL omises par l'étape d'exploration automatique initiale, à la fois les URL individuelles (comme celles nécessitant une saisie spécifique, présentes dans certains formulaires) et les séquences ordonnées d'URL (dans les panier d'achat, par exemple).

Pourquoi et quand exécuter cette tâche

Il existe plusieurs raisons pour lesquelles AppScan ne peut pas explorer automatiquement certaines parties du site sans votre intervention préalable.

- Si l'application contient des formulaires nécessitant une saisie spécifique, vous pouvez naviguer jusqu'aux pages correspondantes à l'aide de la fonction d'exploration manuelle, et remplir les données requises. Les données sont enregistrées par la fonction de remplissage automatique de formulaires, et seront réutilisées pendant l'examen.
- Si votre application utilise JavaScript, des applets Java, ou Flash, et contient des liens qui n'apparaissent que dans certains états, à la suite d'une séquence d'états spécifique, ces liens peuvent être omis par l'exploration automatique. L'utilisation de l'exploration manuelle pour y accéder permet de s'assurer qu'ils seront testés par AppScan, ainsi que les autres liens auxquels ils mènent.
- Si l'application utilise des applets Java qui contiennent des liens, ceux-ci ne seront pas testés par AppScan tant que vous ne les explorerez pas manuellement.
- Si certaines parties du site ne peuvent être atteintes qu'en cliquant sur les liens dans un *ordre spécifique* (comme dans un panier d'achat), vous devez enregistrer une opération en plusieurs étapes (**Configuration des examens > Vue Opérations en plusieurs étapes**).

Procédure

1. **Exploration manuelle.** Utilisez cette fonction pour ajouter les URL qui n'ont pas été reconnues pendant l'exploration automatique, et qui sont accessibles sans un contexte spécifique.
   a. Sur la barre d'outils, cliquez sur **Exploration manuelle**.

      Le navigateur intégré à AppScan s'ouvre.

      Remarque : Si l'application ne s'affiche pas comme prévu dans le navigateur, elle n'est probablement pas optimisée pour le navigateur intégré d'AppScan. Dans ce cas, vous pouvez configurer AppScan pour qu'il utilise un autre navigateur. Voir «Modification du navigateur par défaut», à la page 334.

b. Parcourez l'application, en cliquant sur les liens à tester, en remplissant les données et en tentant de couvrir autant de fonctionnalités que possible.
c. Lorsque vous avez terminé, fermez la fenêtre (en cliquant sur le bouton X dans la barre de titre).

   La fenêtre d'exploration manuelle s'ouvre.
d. Enregistrez les données en vue d'examens ultérieurs en cliquant sur **Exporter**, et en les sauvegardant.
e. Pour ajouter les données à l'examen en cours, sélectionnez **Ajouter tout**, puis cliquez sur **OK**.
f. Après le chargement des nouvelles pages, cliquez sur **Examen > Continuer Exploration uniquement**.

   AppScan explore désormais les nouveaux liens révélés par l'exploration manuelle.
g. Une fois l'exploration terminée, passez en revue les données de l'application pour vérifier que l'exploration a atteint la couverture désirée.

2. **Opérations en plusieurs étapes.** Utilisez cette fonction pour enregistrer les séquences d'URL qui doivent être accédées dans un ordre spécifique.
   a. Ouvrez **Configuration des examens > Vue Opérations en plusieurs étapes**.
   b. Cliquez sur le bouton rouge **Commencer l'enregistrement**, et sélectionnez **Connecter puis enregistrer**.
   c. Connectez-vous à l'application et commencez le processus à enregistrer (par exemple, l'ajout d'un élément à un panier d'achat et le paiement).

      Remarque : Vous pouvez cliquer sur **Interrompre** si vous devez cliquer sur des liens que vous ne souhaitez pas inclure dans l'enregistrement, puis cliquez à nouveau sur **Interrompre** pour reprendre l'enregistrement.
   d. Fermez la fenêtre du navigateur.
   e. Si certains paramètres de la séquence nécessitent une valeur unique, voir «Variables de la séquence», à la page 102, ou reportez-vous à la note technique :

      "Utilisation des variables dans les opérations en plusieurs étapes"

Concepts associés:

«Flux de travaux pour les utilisateurs avancés», à la page 313
Ce flux de travaux est destiné à aider les utilisateurs expérimentés dans le domaine de la sécurité Web à réaliser un examen plus approfondi.

«Utilisation d'AppScan», à la page 143
L'exploration manuelle vous permet d'explorer des parties spécifiques de l'application en remplissant en même temps les zones et les formulaires. Cela permet de vous assurer que des zones spécifiques du site sont couvertes et qu'AppScan dispose des informations requises pour remplir correctement les formulaires.

Référence associée:

«Vue Opérations en plusieurs étapes», à la page 95
La vue Opérations en plusieurs étapes de la boîte de dialogue Configuration permet de tester les parties du site accessibles uniquement en cliquant sur les liens dans un ordre spécifique.

Evaluation des résultats de l'exploration

Avant de passer à l'étape de test, passez en revue les résultats de l'exploration, car les zones importantes du site qui auraient été omises pendant l'étape d'exploration ne seraient pas testées pendant l'étape de test.

Pourquoi et quand exécuter cette tâche

Les résultats de l'étape d'exploration sont visualisables dans les trois sous-fenêtres de vue des données. Les sections qui suivent contiennent des astuces pour évaluer si l'étape d'exploration a bien fonctionné et si elle a abouti à une couverture satisfaisante de l'application.

Remarque : En cas de modification de la configuration au cours de cette étape, vous devrez réexplorer l'application avant de lancer l'étape de test.

Procédure

1. **Journal d'examen**. Consultez-le pour vérifier que AppScan n'a pas été hors session trop souvent.
   a. Cliquez sur **Afficher > Journal d'examen**.
   b. Faites défiler les entrées du journal pour vérifier que AppScan n'a pas été hors session trop souvent.

   Si AppScan a été hors session plus de deux fois en l'espace de cinq minutes, il peut être utile de refaire l'enregistrement et de reconfigurer la connexion enregistrée en accordant une attention toute particulière à la configuration de la détection en session.
2. **Arborescence de l'application**. Il s'agit d'une représentation graphique de toutes les zones du site qui ont été reconnues et explorées. Utilisez-la pour voir si la couverture du site est satisfaisante.
   a. L'arborescence de l'application représente-t-elle précisément la structure de l'architecture et les pages principales de votre application ?
   b. L'arborescence contient-elle des URL de connexion ? (Si elle n'en contient pas, la connexion n'a jamais été envoyée.)
   c. Le nombre total d'URL visitées (angle inférieur gauche) correspond-il à la taille du site tel que vous le concevez ?
   d. Un nombre raisonnable de tests, destinés à l'étape de test, ont-ils été créés (au minimum cinq fois autant que d'URL) ?
3. **Requêtes envoyées**. Passez en revue et validez les requêtes envoyées pendant l'étape d'exploration.
   a. Dans la sous-fenêtre des données, sélectionnez la vue **Requêtes** pour afficher toutes les requêtes envoyées.
   b. Vérifiez que les URL de connexion apparaissent dans cette liste, particulièrement la requête En session et la requête de connexion contenant les données d'identification de l'utilisateur.
   c. Consultez un certain nombre des requêtes qui s'affichent après la requête de connexion dans la procédure de connexion. Vérifiez que la réponse ne contient pas d'erreur. Pour ce faire, entrez le mot "error" dans la zone de recherche de la sous-fenêtre Détails, puis sélectionnez les URL une par une dans le panneau supérieur. Si une réponse spécifique contient le mot "error", la couleur de la zone de recherche passe du rouge ("introuvable") au vert ("trouvé"), et le mot "error" est mis en évidence dans le corps de la réponse.
   d. Si ces requêtes contiennent des chaînes d'erreur, cela indique que l'utilisateur était hors session, et donc que la procédure de connexion n'a pas été enregistrée correctement. Réenregistrez-la.
4. **Vue Données d'application**. Il s'agit de la vue par défaut pendant l'étape de test, et permet d'accéder à différentes vue en cliquant sur les filtres situés en haut de la sous-fenêtre.
   a. Cliquez sur F2 ou sur l'icône des données sur la droite de la barre d'outils pour ouvrir cette vue.
   b. En haut de la sous-fenêtre Données, sélectionnez un filtre pour afficher les informations.
   c. Cliquez sur un élément de la sous-fenêtre des données pour afficher ses caractéristiques dans la sous-fenêtre Détails.
5. **Pages d'erreur personnalisées**. Les réponses 4xx sont identifiées automatiquement en tant que pages d'erreur. Si le site renvoie des réponses 2xx avec les pages d'erreur personnalisées, vous devez configurer AppScan pour qu'il les reconnaisse. Ces informations sont essentielles pour déterminer si les tests ont abouti. Les pages d'erreur personnalisées non configurées génèrent des résultats inexacts, à la fois faussement positifs et faussement négatifs. Ainsi, si vous avez trouvé, dans les étapes suivantes, des pages dont la réponse contenait le mot "error", configurez-les maintenant.
   a. Dans la sous-fenêtre Détails, cliquez sur **Afficher dans le navigateur** pour vérifier qu'il s'agit bien d'une page d'erreur.
   b. Cliquez sur **Définir comme page d'erreur**.

Remarque : Vous pouvez également définir les pages d'erreur dans **Configuration des examens > Pages d'erreur**, en cliquant sur l'icône (+) et en définissant une chaîne, une expression régulière, une URL ou une page.

6. **URL filtrées**. Passez en revue la liste des requêtes qui n'ont *pas* été envoyées, pour vérifier qu'elle ne contient pas de requête qui *auraient dû* être envoyées.
   a. Dans la sous-fenêtre Données, sélectionnez la vue **URL filtrées**, et vérifiez que les URL filtrées doivent l'être, et que leur catégorie est la bonne.
   b. Si les URL ont été filtrées par erreur à cause de leur domaine, ("Serveur Web non testé"), ajoutez le domaine à l'examen (**Configuration > URL et serveurs > Serveurs et domaines supplémentaires > +**).
   c. Si les URL ont été filtrées par erreur parce que la "Limite de chemin d'accès" est atteinte, envisagez de modifier la configuration de la façon suivante :

      - Augmentez la "Limite de chemin d'accès redondant" (**Configuration > Options d'exploration > Limite de chemin d'accès redondant**)

      - Ajustez le réglage de la redondance par défaut (**Paramètres et cookies > Valeurs par défaut du réglage de la redondance**)

      - Ajustez le réglage de la redondance pour les paramètres individuels
7. **Navigation basée sur des paramètres.** Si le site ou une partie du site envoie une URL, tandis que différents paramètres contrôlent le contenu et la structure, reportez-vous à la rubrique «Sites utilisant une navigation basée paramètres», à la page 322.
8. **Paramètres**. Dans la sous-fenêtre Données, passez en revue les paramètres reconnus pendant l'étape d'exploration.
   a. Dans la sous-fenêtre Données, sélectionnez la vue **Paramètres** pour afficher tous les paramètres détectés pendant l'étape d'exploration.
   b. Si nécessaire, mettez à jour les définitions (**Configuration > Paramètres et cookies**).
9. **Demandes ayant échoué.** Il s'agit des requêtes dont les réponses ont le statut 4xx ("Error"). Passez en revue cette liste pour vérifier si des requêtes légitimes ont reçu des réponses d'erreur inattendues.
   a. Dans la sous-fenêtre Données, sélectionnez la vue **Demandes ayant échoué**.
   b. **404 Introuvable :** Cliquez sur **Afficher dans le navigateur** pour vérifier que l'URL n'existe pas.
   c. **Délai d'expiration ou échec de la connexion :** Vérifiez si l'examen nécessite un délai plus élevé (**Configuration > Communication et proxy > Délai d'expiration**), si le serveur ou l'environnement du site doit être amélioré, ou si les problèmes de communication sont dus à des demandes envoyées simultanément (**Configuration > Communication et proxy > Nombre d'unités d'exécution**, et réduisez le paramètre à "1"), ou à un trop grand nombre de demandes envoyées à un moment donné (**Configuration > Communication et Proxy > Limite de débit de demande**).
   d. **401 ou 407 Authentification requise :** Certaines zone de l'application demandent une authentification HTTP (à définir dans **Configuration > Authentification via la plateforme**).
   e. **Autres statuts 4xx :** Vérifiez si le site a renvoyé une erreur parce que l'utilisateur n'est pas connecté. Si nécessaire, réenregistrez la procédure de connexion (**Configuration > Gestion de connexion**).
10. Si, après avoir passé en revue les résultats initiaux de l'exploration, vous pensez que la couverture est insuffisante, reportez-vous à la section qui suit pour déterminer d'éventuelles modifications de la configuration. Voir «Configuration supplémentaire», à la page 321.

Concepts associés:

«Flux de travaux pour les utilisateurs avancés», à la page 313
Ce flux de travaux est destiné à aider les utilisateurs expérimentés dans le domaine de la sécurité Web à réaliser un examen plus approfondi.

«Sites utilisant une navigation basée paramètres», à la page 322
Les sites dans lesquels l'accès à toutes les pages s'effectue à l'aide d'une adresse URL nécessitent une configuration d'examen spécifique.

Tâches associées:

«Configuration supplémentaire»
Les modifications suivantes peuvent être envisagées si la couverture du site lors de l'étape d'exploration initiale est insuffisante.

Configuration supplémentaire

Les modifications suivantes peuvent être envisagées si la couverture du site lors de l'étape d'exploration initiale est insuffisante.

Pourquoi et quand exécuter cette tâche

Si la couverture du site dans l'étape d'exploration initiale est insuffisante, ou dure plus d'une trentaine de minutes, vous pouvez modifier les définitions de paramètre et de cookie suivantes :

Procédure

1. Cliquez sur la vue **Configuration > Paramètres et cookies**.
2. **Suivi.** Si votre site effectue le suivi des cookies (par exemple, les identificateurs de session qui sont mis à jour à chaque connexion d'un utilisateur), vous devez vérifier qu'ils sont définis correctement.
   a. Vérifiez que les cookies et les paramètres du site ont été identifiés et figurent dans l'onglet avec la mention "Suivi".
   b. Si nécessaire, définissez des paramètres et des cookies supplémentaires en cliquant sur l'icône  . Pour plus d'informations, voir «Définition de paramètre», à la page 78.
3. **Réglage de la redondance.** Un réglage fin de la redondance peut réduire de façon significative la durée de l'examen, sans réduire la couverture ni la précision de l'examen. Réglez la redondance en vérifiant qu'aucune requête en double n'est envoyée inutilement, mais que les requêtes nécessaires le sont. Pour plus de détails, voir «Réglage de la redondance», à la page 83.
   a. Si le cookie ou le paramètre à configurer n'est pas dans la liste, cliquez sur l'icône  et définissez-le.
   b. Vérifiez les paramètres des cookies et des paramètres.
4. **Vérification de l'ID session.** Une définition d'ID de session précise est importante pour permettre à AppScan de créer des requêtes spécifiques pendant l'étape d'exploration.
   a. Vérifiez que les paramètres de suivi de tous les ID de session sont définis correctement en tant que Valeur de connexion.
   b. Vérifiez que tous les paramètres définis comme Valeur de connexion sont des ID de session.
5. Si vous avez modifié les définitions de paramètre et de cookie, réexplorez l'application. Il peut être également nécessaire d'enregistrer à nouveau l'exploration manuelle et les opérations en plusieurs étapes.

   «Vue Paramètres et cookies», à la page 76
   Vue Paramètres et cookies de la boîte de dialogue Configuration.

   «Définition de paramètre», à la page 78

   «ID session», à la page 81

   «Réglage de la redondance», à la page 83
   Un réglage précis de la redondance peut réduire de façon significative la durée de l'examen.

   «Flux de travaux pour les utilisateurs avancés», à la page 313
   Ce flux de travaux est destiné à aider les utilisateurs expérimentés dans le domaine de la sécurité Web à réaliser un examen plus approfondi.

Sites utilisant une navigation basée paramètres

Les sites dans lesquels l'accès à toutes les pages s'effectue à l'aide d'une adresse URL nécessitent une configuration d'examen spécifique.

Un site sur lequel la navigation est "basée sur les paramètres" est un site où une seule adresse URL (contrôleur) est envoyée, mais avec différents paramètres qui renvoient des contenus et structures différents. (Ce type de site est parfois qualifié de "megascript".)

- Sur certains sites, l'adresse URL reste la même pour toutes les "pages" comme dans l'exemple suivant :

  `http://site.com/content.aspx?PageName=page1`

  `http://site.com/content.aspx?PageName=page2`
- Sur d'autres sites, la direction des liens est indiquée via une page de proxy unique, à l'aide d'un paramètre GET. Par exemple:

  `http://site.com?default.aspx/redirect=page1`

  redirige vers :

  `http://site.com/page1.aspx`

  Le problème est le même pour AppScan que dans le cas précédent, puisque la même URL est envoyée à chaque fois.
- Pour les liens de publication ASP.NET 2.0, chaque lien génère une demande POST vers la page sur laquelle il se trouve.

  A nouveau, le problème posé à AppScan est identique.

Dans tous les cas, les demandes pour toutes les "pages" sont envoyées à la même adresse URL. Ceci nécessite un traitement spécial de la part d'AppScan puisque la configuration par défaut produira un examen incomplet.

Pour examiner un site avec une navigation à base de paramètres, appliquez la procédure ci-dessous.

1. Lors de la création de l'examen, sélectionnez le modèle de navigation basée sur les paramètres plutôt que le modèle d'examen standard.
2. Vérifiez que le ou les paramètres de navigation de votre site sont correctement définis : Sélectionnez **Examen > Configuration des examens > Paramètres et cookies** et vérifiez que l'expression régulière définissant le dernier paramètre de la liste inclut le ou les paramètres de navigation de votre site. Si nécessaire, modifiez l'expression régulière. (Voir «Vue Paramètres et cookies», à la page 76.)
3. (Facultatif et avancé :) Configurez la page Résultats basés sur le contenu de la boîte de dialogue Configuration des examens pour que AppScan puisse présenter une arborescence d'application significative. (Voir «Vue Résultats basés sur le contenu», à la page 103.)
4. Effectuez les autres modifications de la configuration nécessaires et continuez comme pour un examen standard.
5. (Facultatif) Lorsque vous affichez les résultats d'examen dans l'arborescence d'application, sélectionnez la vue basée sur le contenu au lieu de la vue basée sur l'URL par défaut. (Voir «Arborescence de l'application», à la page 21.)

Voir aussi :

«Modèle de navigation basée sur des paramètres», à la page 139

«Exigences pour les sites dont la navigation est basée sur des paramètres», à la page 323

Exigences pour les sites dont la navigation est basée sur des paramètres

Description des modifications de la configuration requises pour l'examen d'un site avec navigation à base de paramètres.

Par défaut, AppScan a une Limite de chemin d'accès redondant égale à 5 (nombre maximal de fois qu'une demande peut être envoyée à la même adresse URL. Voir «Vue Options d'exploration», à la page 71). Sur les sites standard, ceci évite de répéter inutilement des tests. Cependant, lorsque la navigation sur le site est basée sur des paramètres, cette limite faible empêchera concrètement AppScan d'effectuer un examen minutieux du site et, si l'examen est exécuté à l'aide du modèle d'examen standard, la reconnaissance et le test du site seront très limités.

L'augmentation de la Limite de chemin d'accès redondant ou la désactivation pure et simple de ce paramètre ne suffit pas à résoudre le problème. En fait, ceci peut conduire AppScan à effectuer indéfiniment une boucle ou, au moins, à créer un examen avec des tests si nombreux que la mémoire d'AppScan sera saturée. Il existe deux raisons à cela :

1. Pendant l'étape d'exploration, lors du hachage d'une demande, AppScan inclura tous les paramètres et les cookies détectés dans la demande. En l'absence de limite de chemin redondant, toutes les combinaisons de ces valeurs seront prises en considération.

   Par exemple, chaque page d'une section du site contient des centaines de liens vers un script qui extrait de la base de données des informations sur un élément à vendre. Ces liens contiennent un paramètre appelé `item_id` qui n'est pas utile à la génération de nouvelles pages et sert uniquement à extraire des informations sur l'élément. AppScan en arrivera à réclamer des milliers d'instances de la page d'informations de cet élément, à moins que le paramètre `item_id` ne puisse être exclu du hachage.
2. Dans l'étape de test, la gravité du problème s'accentue. Imaginons qu'une demande contient les deux paramètres `par1` et `par2`, et qu'AppScan rencontre quatre liens incluant ces paramètres :

   ```
   http: // site.com/content.aspx?par1=a&par2=c
   http: // site.com/content.aspx?par1=a&par2=d
   http: // site.com/content.aspx?par1=b&par2=c
   http: // site.com/content.aspx?par1=b&par2=d
   ```

   S'il existe 400 tests applicables à chaque paramètre, AppScan enverra au total 1 600 tests (800 pour `par1` lorsque `par2=c` et `par2=d` et 800 pour `par2` lorsque `par1=a` et `par1=b`) ! Par conséquent, en plus de l'exclusion de ces paramètres du hachage de l'étape d'exploration, il est nécessaire d'indiquer à AppScan de tester une seule fois chaque paramètre : soit 400 tests pour `par1` et 400 tests pour `par2`.

Par conséquent, pour l'examen d'un site avec une navigation basée sur des paramètres, la procédure à suivre est la suivante :

1. **Etape d'exploration :** Ignorez les valeurs de tous les paramètres à l'exception des paramètres de navigation.
2. **Etape de test :** Ne créez pas de nouveaux tests lorsque la valeur d'un paramètre est modifiée, sauf pour les paramètres de navigation.

Voir aussi :

«Sites utilisant une navigation basée paramètres», à la page 322

«Modèle de navigation basée sur des paramètres», à la page 139

Examen des environnements de production opérationnels

Les risques et les suggestions ci-dessous doivent être pris en compte avant l'examen d'un site opérationnel à l'aide d'AppScan.

Lorsque vous examinez un site opérationnel, vous pouvez utiliser le modèle de site de production prédéfini. Ce modèle contient une stratégie de test de site de production sélectionnée ainsi que des paramètres de configuration conçus pour minimiser le risque de dégradation d'un site opérationnel ou de refus de service aux utilisateurs réels.

Si vous choisissez d'utiliser votre propre configuration ou stratégie de test, les sections suivantes vous permettent de configurer votre examen de façon efficace.

Il se peut que la base de données soit remplie d'informations inutiles envoyées pendant l'examen.

Pour limiter l'impact produit, prenez les précautions suivantes :

- Désactivez la fonction de remplissage automatique des formulaires (Configuration des examens > Remplissage automatique des formulaires > première case à cocher).

  Ceci empêche AppScan de remplir les formulaires automatiquement en soumettant des données pouvant saturer une base de données, un tableau d'affichage ou un forum en ligne, ou en envoyant des courriers électroniques indésirables à un compte d'administrateur ou de modérateur. Sachez cependant que ceci neutralise la capacité d'AppScan Standard à atteindre des zones du site accessibles via une soumission de formulaires. Dans ce mode de fonctionnement, AppScan examine uniquement les zones du site accessibles en suivant des liens (avec ou sans paramètres).
- Créez un compte de test qui sera utilisé par AppScan.

  L'utilisation d'un compte de test facilite le suivi des modifications de la base de données (par exemple, pour s'assurer que des services ne sont pas commandés), ainsi que le nettoyage du site par les administrateurs une fois l'examen terminé.

  Lorsque vous créez le compte, il est recommandé de :
  - Limiter l'accès à la base de données pour les enregistrements de test afin de permettre la restauration des enregistrements modifiés.
  - Vérifier que les nouveaux enregistrements créés par le compte de test seront supprimés.
  - Vérifier que les bons de commande (ou autres transactions) issus du compte de test seront ignorés.
  - Donner l'accès au compte pour les enregistrements de test uniquement si les transactions ont un impact (par exemple, s'il s'agit d'actions).
  - Donner l'accès au compte de test uniquement pour tester les forums, si le site comporte des forums, afin que les clients réels ne voient pas les tests créés pendant l'étape de test.
  - Définir plusieurs comptes de test avec des privilèges différents, si le site possède plusieurs comptes ayant des privilèges différents. Ceci garantit un examen plus exhaustif du site.
  - Ne pas créer de compte de test avec un accès de niveau administrateur.

Risque de saturation de la messagerie électronique

Lorsqu'il teste des pages utilisant la notification par courrier électronique, AppScan génère un grand nombre de requêtes, ce qui peut surcharger le serveur de messagerie du site.

Voici quelques suggestions pour éviter cela :

- Modifiez temporairement les adresses électroniques pour les pages testées afin d'envoyer les courriers électroniques vers des adresses non valides.
- Si possible, configurez AppScan de manière à exclure ces pages de l'examen de l'environnement de production.
- Examinez un seul serveur Web à la fois et empêchez-le de se connecter au serveur SMTP pendant l'examen.
- Si vous décidez de garder la fonction de remplissage automatique de formulaires active, configurez-la de façon à insérer une valeur unique dans la zone de courrier électronique afin que les destinataires puissent identifier aisément les courriers générés par AppScan.

Examen via un proxy

Lorsque cela est possible, évitez d'effectuer un examen via un proxy. Bien que ce mode d'examen soit pris en charge, le recours à un proxy risque de nuire à la clarté des résultats.

Risque de verrouillage de l'examen pour l'application

Certaines applications sont configurées pour verrouiller les utilisateurs après un certain nombre de tentatives de connexion avortées. Si ceci se produit lors de l'examen, AppScan ne pourra manifestement pas mener celui-ci à terme.

Pour éviter cela :

- Désactivez **Envoyer les tests sur les pages de connexion et de déconnexion** (Configuration des examens > Options de test).

Risque d'échec d'une application

Pour éviter qu'AppScan n'entraîne l'échec de votre application en ligne, vous pouvez désactiver les tests invasifs dans la stratégie de test. Les tests de refus de service, de dépassement de la mémoire tampon et les autres tests risquant de causer l'échec de l'application ou du serveur Web ne sont pas envoyés.

Important : Les applications Web comportent souvent des points vulnérables que seuls les tests invasifs permettent de découvrir. Il est, par conséquent, déconseillé de faire totalement l'impasse sur les tests invasifs. Testez vos applications pour ces vulnérabilités en coordination avec le propriétaire ou l'administrateur de votre site Web, en planifiant les examens, par exemple, pendant les heures creuses où l'application n'est pas sollicitée.

Pour désactiver les tests invasifs dans la stratégie de test :

1. Sélectionnez **Configuration > Stratégie de test**.
2. Cliquez sur la colonne **Invasif** afin de regrouper tous les tests invasifs.
3. Faites défiler la liste des tests invasifs (ceux pour lesquels "Oui" est défini pour la valeur Invasif) et désélectionnez tous les tests sélectionnés afin de les exclure de l'examen.

Compréhension de l'option Optimisation du test

Cette section décrit comment l'option Optimisation du test fonctionne et comment mieux l'intégrer au cycle de vie de votre développement.

Description du fonctionnement

Généralement, un examen AppScan Standard complet standard envoie des milliers de tests et son exécution peut prendre plusieurs heures, voire plusieurs jours. Au cours des premières étapes de développement, ou pour avoir une évaluation globale rapide du contexte de sécurité actuel de votre produit, vous pouvez utiliser Optimisation du test pour obtenir les résultats requis dans un délai plus court.

Nos filtres de test intelligents s'appuient sur l'analyse statistique et filtrent certains tests (ou même des variantes de test spécifiques) pour générer un examen plus court qui identifie uniquement les vulnérabilités les plus fréquentes, graves et importantes. Les groupes de correctif et les correctifs iFixes AppScan permettent de vous maintenir à jour grâce aux filtres d'optimisation les plus récents. Grâce à l'option Optimisation du test, vous pouvez réduire considérablement la durée de l'examen, lorsque vous accordez davantage d'importance à la vitesse qu'à la profondeur de l'examen.

La fonction Optimisation du test s'applique à n'importe quel modèle que vous sélectionnez pour l'examen, à l'aide des résultats de votre dernière analyse statistique.

Nous vous recommandons d'utiliser l'option Optimisation du test au cours des premières étapes de développement et pour l'automatisation, mais également d'exécuter un examen complet lorsque vous avez plus de temps, afin de vous assurer d'avoir une image *complète* du contexte de sécurité de votre site.

Il est possible d'activer l'option Optimisation du test depuis l'assistant de configuration et la boîte de dialogue Configuration principale.

Foire aux questions

Q : L'option Optimisation du test s'applique-t-elle à toutes les stratégies de test ?

R : Oui. L'option Optimisation du test filtre les stratégies de test en fonction de notre analyse statistique des résultats de test, qui est régulièrement mise à jour.

Q : L'option Optimisation du test filtre-t-elle des tests *entiers* ?

R : Pas toujours. Parfois, elle filtre uniquement des variantes de test spécifiques.

Q : Puis-je, d'une manière ou d'une autre, savoir exactement quels tests ou variantes ont été filtrés par la stratégie de test que j'ai sélectionnée ?

R : Ce n'est pas possible actuellement.

Q : L'option Optimisation du test change-t-elle les autres paramètres de configuration, et puis-je voir ces modifications dans la boîte de dialogue de configuration ?

R : Aucune modification de configuration n'est apportée actuellement. Cela pourrait être le cas dans les versions AppScan futures, mais les modifications éventuelles seront indiquées.

Q : Si son examen est plus rapide, pourquoi ne puis-je pas utiliser l'option Optimisation du test à chaque fois ?

R : L'option Optimisation du test est parfaite quand vous avez besoin de résultats plus rapides, mais elle n'est pas aussi approfondie qu'un examen complet. Nous vous recommandons les examens optimisés lorsque la vitesse est importante, mais que vous pouvez également les consolider avec des examens complets à intervalles réguliers.

Q : Puis-je m'attendre à ce que les résultats de deux examens optimisés effectués sur le même site soient identiques ?

R : Puisque notre équipe analyse et met à jour constamment les paramètres, chaque mise à jour d'AppScan a amélioré les paramètres d'optimisation. Par conséquent, même si le site reste inchangé, les résultats peuvent ne pas être identiques. Néanmoins, il est peu probable qu'un test qui a décelé un problème dans l'ancien examen soit exclu du nouvel examen.

Contenus Flash

Cette section propose des suggestions pour l'analyse de contenus Adobe Flash.

AppScan Explore et teste les structures Adobe ActionScript 1.0, 2.0 et 3.0, et Adobe Flex 2.0 et 3.0. L'analyse et l'exécution de contenus Flash sont activées depuis la vue Options d'exploration de la boîte de dialogue Configuration des examens.

Configurations requises

Pour permettre à AppScan d'exécuter des contenus Adobe Flash lors des analyses, vous devez disposer d'une version Adobe Flash Player pour Internet Explorer prise en charge installée sur l'ordinateur. Les versions 9.0.124.0 à 14.0.0.125 sont prises en charge.

Remarque : L'outil Flash Player est livré sous forme de plug-in ActiveX spécifique au navigateur utilisé. AppScan nécessite Adobe Flash Player for Internet Explorer.

- Si votre version est trop ancienne, vous pouvez télécharger la version la plus récente de Flash Player depuis le site http://get.adobe.com/flashplayer/
- Si vous disposez d'Adobe Flash Player version 10.1 ou ultérieure, vous risquez d'obtenir un message indiquant que ce produit doit être configuré pour pouvoir fonctionner avec AppScan. Voir «Configuration de Flash Player», à la page 7

Remarque : Dans les deux cas, ("Version Flash Player prise en charge non installée", ou "Flash Player non configuré") une alerte apparaît dans la boîte de dialogue de configuration *et Flash ne pourra pas s'exécuter* au cours des analyses.

Limitations des analyses de contenus Flash

Les limitations des analyses de contenus Flash suivantes doivent être prises en compte :

- Etant donné que AppScan analyse les contenus Flash via un proxy, les URL de l'hôte local ne sont pas analysées.
- Les problèmes détectés sont propres à la version du navigateur Adobe Flash pour Internet Explorer qui est installée sur votre machine. Il se peut donc que :
  - Votre lecteur soit vulnérable au problème signalé alors qu'un lecteur destiné à un autre navigateur, ou une version plus récente de ce même lecteur, n'y est pas exposé
  - Votre lecteur Internet Explorer n'est *pas* vulnérable à certains problèmes, et par conséquent AppScan ne les signale pas, alors qu'ils *affectent* les lecteurs destinés à d'autres navigateurs ou des versions antérieures de ce même lecteur

Couverture incomplète des URL

Ci-dessous figurent des suggestions pour les situations où vous avez effectué une analyse et qu'à l'étude des résultats, il semble que AppScan n'ait pas identifié des URL associées à vos contenus Flash.

Pour quelle raison AppScan identifie-t-il certaines URL des contenus Flash et en ignore-t-il d'autres ?

Plusieurs possibilités sont à examiner :

- Vérifiez que la version de votre film Flash est prise en charge (celles non prises en charge sont listées dans la vue Données d'application sous "URL filtrées").
- Lisez le film dans le navigateur Internet Explorer sur la machine ayant effectué l'analyse pour vérifier qu'il est lu correctement.
- Vérifiez que l'option Exécution de JavaScript (activée par défaut) n'a pas été désactivée. (**Configuration des examens > Options d'exploration > Exécuter JavaScript pour reconnaître les adresses URL et des contenus dynamiques**).

La couverture des contenus Flash semble incomplète

Plusieurs possibilités sont à examiner :

1. Vérifiez que les informations de remplissage des formulaires sont complètes (**Configuration des examens > Remplissage automatique de formulaires**).

2. Essayez d'augmenter la valeur affectée à l'option **Configuration des examens > Options d'exploration > Flash > Limite de clic**.
3. Essayez de faire passer la valeur affectée à l'option **Configuration des examens > Options avancées > Flash : délai maximal entre échantillonnages** au-dessus de sa valeur par défaut de 160 ms.
4. Essayez de faire passer la valeur affectée à l'option **Configuration des examens > Options avancées > Flash : Couverture** de 1 à 2.
5. Essayez de lire le film dans Internet Explorer pour vérifier qu'il peut être lu correctement.
6. Si la lecture du film échoue, définissez l'option **Niveau de débogage** du navigateur Flash à Trace 3, relancez l'analyse et envoyez le journal du navigateur ([AppScan Standard dossier d'installation]\Logs\AppScanFlashBrowser.log) à votre fournisseur de support.

Vulnérabilités non détectées

Les suggestions suivantes sont destinées aux situations où AppScan a reconnu les URL et les a ajoutées à l'arborescence de l'application mais n'a pas détecté de vulnérabilités dans celles-ci.

Pour quelles raisons AppScan ne détecte-t-il pas de vulnérabilités dans les URL Flash qu'il a reconnues ?

Les explications possibles sont les suivantes :

- Le film peut tout simplement ne pas contenir de paramètres suspects. Consultez les informations dans **Données d'application > Paramètres de script** pour déterminer les paramètres Flash qui ont été reconnus.
- Vérifiez que tous les tests Flash (ActionScript 2 et 3) sont activés. (Ouvrez **Configuration des examens > Stratégie de test**, recherchez "ActionScript" et vérifiez que tous les tests sont bien sélectionnés).
- Il se peut simplement que le film ne soit pas vulnérable.

Quelles sont mes autres possibilités ?

Si vous soupçonnez néanmoins que des vulnérabilités Flash ont été ignorées, activez le mode de support étendu, répétez l'analyse et envoyez les résultats à votre fournisseur de support. Voir «Mode de support étendu», à la page 333.

Foire aux questions

Cette rubrique traite des questions d'application générales.

Quelles sont les différentes méthodes disponibles pour l'examen des services Web ?

L'examen d'un site commence par une exploration qui, en fonction des données rassemblées, est suivie d'un test. Les "données d'exploration" peuvent être rassemblées en utilisant une ou plusieurs méthodes d'exploration. Dans tous les cas, ces données, une fois rassemblées sont utilisées par AppScan pour créer et envoyer des tests au site pendant l'étape de test.

Exploration d'applications web (sites avec interface utilisateur)

- Dans le cas d'applications (sites) sans services web, il suffit souvent de fournir à AppScan l'adresse URL de départ et les données d'authentification pour lancer le test sur le site.
- Si nécessaire, vous pouvez parcourir manuellement le site *via AppScan* afin d'accéder à des zones accessibles uniquement à l'aide d'entrées utilisateur spécifiques.
- Pour les pages accessibles uniquement via des pages sélectionnées dans un ordre spécifique, vous pouvez enregistrer une opération incluant plusieurs étapes à utiliser par AppScan.

- Alors que l'Assistant de configuration vous permet de configurer et de démarrer votre numérisation en quelques étapes, pour les sites complexes, la boîte de dialogue Configuration vous permet d'affiner et de personnaliser de nombreux autres paramètres.

Exploration de services Web

- Vous pouvez configurer AppScan comme proxy d'enregistrement pour l'appareil (tel qu'un téléphone mobile ou un simulateur) que vous utilisez pour explorer le service. AppScan peut alors analyser les données d'exploration et créer des tests. Vous pouvez également utiliser AppScan pour enregistrer le trafic à l'aide d'un outil externe, tel qu'un testeur fonctionnel de services Web. Voir «Utilisation d'AppScan comme proxy d'enregistrement», à la page 150.
- Si vous avez des fichiers de description Open API (JSON ou YAML) pour votre service Web, vous pouvez utiliser l'extension Web Services Wizard pour configurer une analyse et les séquences en plusieurs étapes nécessaires pour utiliser le service. AppScan analysera alors automatiquement le service.
- Si vous ne pouvez pas utiliser les deux premières méthodes et que vous disposez d'un fichier WSDL pour votre service Web (tel qu'un service Web SOAP), l'installation AppScan comprend en option un outil séparé qui permet aux utilisateurs de visualiser les différentes méthodes intégrées au service Web, de manipuler les données d'entrée et d'examiner les commentaires du service. Vous devez tout d'abord indiquer à AppScan l'adresse URL du service. Le "Generic Service Client" (GSC) intégré utilise le fichier WSDL pour afficher les différentes méthodes disponibles dans un format arborescent et créer une interface graphique conviviale pour envoyer des requêtes au service. Vous pouvez utiliser cette interface pour entrer des paramètres et en visualiser les résultats. Le processus est "enregistré" par AppScan et utilisé afin de créer des tests pour le service lorsqu'AppScan effectue l'examen du site. GSC peut aussi être utilisé comme client pour les requêtes REST, sans analyser un fichier WSDL, comme un simple client HTTP. Voir «Utilisation de GSC», à la page 153.

Quelle est la différence entre une exploration manuelle et une opération à plusieurs étapes ?

Exploration manuelle

L'exploration manuelle d'un site consiste à collecter les données pouvant être utilisées par AppScan pour s'assurer que, lors du test du site, les parties de l'application ou les services n'ayant pas été pris en compte lors de l'étape d'exploration automatique seront couverts. Cela peut être nécessaire si une entrée utilisateur spécifique est requise, ou si le site répond uniquement à un type d'outil ou de périphérique différent. Vous pouvez procéder à une exploration manuelle via AppScan, l'utiliser en tant que proxy d'enregistrement ou via le service GSC (Generic Service Client).

Voir Chapitre 5, «Exploration manuelle», à la page 143

Opération en plusieurs étapes

Une opération à plusieurs étapes est requise pour l'exploration des parties du site accessibles uniquement en cliquant sur des liens *dans un ordre spécifique*, comme une boutique en ligne où l'utilisateur ajoute des articles dans un panier avant de les payer. Prenez en compte les trois pages suivantes :

1. L'utilisateur ajoute un ou plusieurs articles à un panier
2. L'utilisateur remplit les détails pour le règlement et la livraison
3. L'utilisateur reçoit la confirmation que la commande est terminée

La page 2 peut uniquement être atteinte via la page 1. La page 3 peut uniquement être atteinte via la page 1 suivie de la page 2. Il s'agit d'une séquence. Pour pouvoir tester les pages 2 et 3, AppScan doit envoyer la séquence correcte de demandes HTTP avant chaque test.

Voir «Vue Opérations en plusieurs étapes», à la page 95

Quelle est la différence entre la lecture basée sur les actions et la lecture basée sur les demandes ?

Lorsqu'une procédure est enregistrée pour une utilisation en tant que connexion ou en tant qu'opération à plusieurs étapes, deux méthodes de lecture sont disponibles :

Lecture basée sur les demandes
Envoie les demandes HTTP brutes à partir de l'enregistrement. Cette méthode est généralement plus rapide.

Lecture basée sur les actions
Exécute à nouveau les actions de clic et de frappe de l'utilisateur. Vous pouvez être amené à choisir cette méthode lorsque le site inclut un grand nombre d'éléments JavaScript ou lorsque certaines demandes de la lecture basée sur les demandes ont été marquées d'un caractère X rouge lors d'une tentative de validation. Cette méthode peut augmenter la durée de l'examen.

Voir Configurer > Explorer > «Onglet Vérifier et valider», à la page 55 et Configurer > «Vue Opérations en plusieurs étapes», à la page 95

Chapitre 14. Identification et résolution des incidents

Cette section fournit des suggestions de traitement des incidents par l'utilisateur.

Fonctions de traitement des incidents

AppScan fournit de nombreuses informations pouvant être utilisées pour mieux localiser et résoudre des incidents.

- **AppScan Journal** - Affiche des informations relatives aux fonctionnalités d'AppScan, y compris la manière dont il se connecte à votre proxy et sur le port sur lequel il se met à l'écoute après chaque redémarrage.
- **Journal de trafic** - Lorsqu'il est activé, AppScan écrit dans ce journal tout le trafic envoyé à votre site Web et reçu de votre site Web.

  Remarque : L'activation du journal de trafic ralentit l'application et augmente la consommation d'espace disque.
- **Fichier de vidage** - Dans le cas d'une panne, AppScan crée un fichier de vidage de mémoire et vous indique son chemin et son nom de fichier. Ce fichier contient toutes les informations disponibles relatives au cas d'utilisation ayant occasionné la panne et doit être envoyé au support d'AppScan Standard pour y être examiné.
- **Mode de support** - Permet de reproduire l'incident puis de comprimer les fichiers de données et de les envoyer au support technique.
- **Fichiers comprimés** - AppScan crée une archive des fichiers de données que vous pouvez envoyer au support technique. Ces fichiers comprennent : scan file (*.scan), AppScanDbg.log, AppScanSys.log et AppScanTraffic.log.
- **Rapport Faux positif** - Permet d'envoyer les retours d'information à IBM Security AppScan Standard relatifs à des tests spécifiques, principalement à ceux dont les résultats sont positifs mais que vous suspectez devoir être négatifs dans votre application. AppScan compresse les informations sur les variantes sélectionnées et joint le fichier zip à un nouveau message électronique, ouvert dans le client de messagerie par défaut.

Traitement des incidents liés aux licences

Pourquoi et quand exécuter cette tâche

Si vous souhaitez utiliser IBM Security AppScan Standard pour l'examen de votre site, vous devez disposer d'une licence valide. Si vous êtes sûr que votre licence est valide, mais que AppScan ne l'accepte pas, exécutez la procédure ci-dessous.

Procédure

1. Vérifiez que le serveur sur lequel AppScan est utilisé dispose d'une connexion réseau avec le serveur de licences.

   Remarque : Les licences d'AppScan Standard Edition sont installées dans le serveur de clés de licence IBM Rational, qui peut ne pas être le même que le serveur sur lequel AppScan s'exécute. Pour qu'AppScan puisse fonctionner, le serveur sur lequel il est installé doit avoir une connexion réseau avec le serveur de clés de licence. Chaque fois qu'un utilisateur ouvre AppScan, une licence est extraite (et restituée à la fermeture d'AppScan).
2. Ouvrez la licence avec un éditeur de texte (tel que le Bloc-notes MS).

   Important : Ne modifiez pas le fichier de licence !

3. Vérifiez que la licence n'est pas arrivée à expiration.
4. Vérifiez que le site que vous souhaitez examiner fait partie des restrictions de la licence (l'adresse IP ainsi que le nom d'hôte).
5. Vérifiez que l'adresse MAC et le numéro de série du disque indiqués sur la licence sont identiques à ceux indiqués sur la machine.

Que faire ensuite

Si cette procédure ne résout pas le problème, référez-vous au document suivant : Comment obtenir et appliquer les licences AppScan Standard, ou contactez le support AppScan.

Espace disque insuffisant

Pourquoi et quand exécuter cette tâche

La taille des fichiers temporaires créés lors d'un examen AppScan peut atteindre la taille de l'examen lui-même. Tous les dossiers temporaires doivent donc disposer de cette capacité. La taille d'un examen dépend du site examiné, du modèle, de la configuration et des problèmes trouvés.

- Par défaut, AppScan place les fichiers temporaires dans `C:\ProgramData`.
- Les composants tiers d'AppScan placent les données aux emplacements définis pour les variables d'environnement utilisateur de Windows TEMP et TMP.

Procédure

1. Essayez de libérer de l'espace disque pour les trois chemins.
2. Si nécessaire, changez les chemins.
   - Pour changer le chemin temporaire AppScan, définissez le nouveau chemin dans :
     Outils > Options > Avancé > TempFilesDir

     Remarque : Le chemin doit être local et utiliser des caractères ASCII uniquement.
   - Pour changer les chemins temporaires tiers, modifiez les valeurs TEMP et TMP dans les variables d'environnement utilisateur de Windows.

Traitement des incidents liés à la signature numérique

Pourquoi et quand exécuter cette tâche

A chaque fois que vous ouvrez AppScan, il vérifie la signature numérique de ses règles de sécurité (fichier DLL). Cette vérification peut échouer pour plusieurs raisons :

- Le fichier DLL est endommagé.
- Le fichier DLL a été altéré (éventuellement par un pirate informatique).
- Le certificat suivant, qui est installé par défaut lors de l'installation de Windows, est manquant dans la liste des certificats "Autorités de certification racines de confiance" du magasin Windows :
  `VeriSign Class 3 Public Primary Certification Authority - G5`

Procédure

1. Vérifiez que le certificat racine suivant est installé :
   `VeriSign Class 3 Public Primary Certification Authority - G5`
2. Désinstallez et réinstallez AppScan.
3. Si cette procédure ne résout pas le problème, contactez le service d'assistance technique.

   Remarque : Le message d'avertissement vous permet de continuer si vous êtes sûr que votre système n'est pas compromis.

Importation d'un modèle d'examen existant

Cette section décrit comment importer le modèle d'examen à partir d'un examen enregistré dans une version d'AppScan antérieure à la version 8.6.

Dans AppScan version 8.6, le format du fichier d'examen a été revu et les examens enregistrés dans des versions antérieures ne peuvent pas être ouverts dans la version actuelle. Si nécessaire, vous pouvez importer le modèle en vue d'une utilisation dans un nouvel examen.

Pour importer le modèle d'examen, procédez comme suit :

1. Modifiez l'extension du fichier d'examen de SCAN en ZIP.
2. Ouvrez le fichier ZIP, puis localisez `templateconfig.xml` et procédez à son extraction.
3. Changez son extension de XML en SCANT.
4. Ouvrez-le avec AppScan.

Génération de rapports de résultats faux positifs

Si vous pensez qu'un résultat AppScan particulier est faux (faux positif), vous pouvez envoyer la demande envoyée par AppScan ainsi que la réponse reçue de votre application Web par courrier électronique au service d'assistance d'IBM Security AppScan Standard. Voir «Rapport Faux positif des résultats de test», à la page 222.

Traitement des incidents liés à la fonction Rapport faux positif

Les conseils suivants sont fournis pour vous aider si vous rencontrez des difficultés à utiliser la fonction **Rapport Faux positif** pour envoyer des commentaires en retour avec des informations sur les variantes au service d'assistance AppScan.

Problème	Cause	Solution
Le destinataire ne peut pas lire le document joint.	Le message envoyé est chiffré. Aucun autre destinataire ne dispose de la clé privée nécessaire pour lire le message électronique.	Pour désactiver le chiffrement : Dans le menu **Outils** > commande **Options** > onglet **Général** > option **Rapport Faux positif**, décochez la case **Chiffrement des pièces jointes**.

Mode de support étendu

Le mode de support étendu consigne toutes les activités AppScan en vue de leur compression et envoi à votre fournisseur de support pour une assistance à la résolution d'une procédure problématique.

Pourquoi et quand exécuter cette tâche

Si vous avez besoin d'aide pour résoudre une procédure problématique, votre fournisseur de support peut vous demander d'exécuter AppScan en mode de support étendu afin de consigner toutes les activités et d'intégrer toutes les données dans un seul fichier.

Important : N'activez pas le mode de support étendu sans y être invité par le service d'assistance autorisé. Ce mode a un impact sur les performances d'AppScan performance.

Procédure

1. Activez le mode de support étendu : **Aide > Support > Mode de support étendu**
   Un message vous avise que le mode de support étendu a été activé et consignera toutes vos actions.
2. Cliquez sur **OK**.

Un indicateur dans la barre d'état signale que AppScan s'exécute en mode de support étendu :


3. Reproduisez la procédure problématique.
4. A l'issue de l'opération, désactivez le mode de support étendu : **Aide > Support > Mode de support étendu**

   OU

   Si AppScan a cessé de fonctionner à la suite de la procédure, rouvrez-le et, quand le programme vous demandera si vous désirez continuer à opérer en mode de support étendu, sélectionnez l'option **Désactiver**.
5. Sélectionnez les options requises :

Option	Description
Chiffrer	Toutes les données de support sauvegardées, y compris le fichier d'examen s'il est inclus, sont chiffrées. **Important :** N'optez pas pour le chiffrement, sauf si vous l'envoyez à l'assistance AppScan, car elle seule pourrait l'ouvrir.
Inclure un fichier d'examen	Vous pouvez inclure le fichier d'examen en cours, ou un autre fichier d'examen pertinent sauvegardé, dans le fichier de support.

6. Cliquer sur :

Option	Description
Enregistrer	Sauvegarde les données de support existantes en tant que fichier .SUPPORT (en chiffrant et en incluant le fichier d'examen dans la configuration le spécifie). Les données de support sont effacées de l'interface AppScan et AppScan repasse en mode normal. Le chemin par défaut est : `...\My Documents\AppScan\Support\`
Ne pas sauvegarder	Les données de support sont effacées de l'interface AppScan et AppScan repasse en mode normal.
Annuler	Les données de support ne sont *pas* effacées de l'interface AppScan et AppScan reste en Mode support étendu.

Modification du navigateur par défaut

Vous pouvez configurer AppScan pour utiliser un navigateur différent du navigateur intégré.

Pourquoi et quand exécuter cette tâche

Par défaut, AppScan ouvre son navigateur intégré lorsque vous enregistrez la procédure de connexion, ou une opération en plusieurs étapes, ou lorsque vous cliquez sur le bouton **Afficher dans le navigateur**.

Si le navigateur intégré ne parvient pas à accéder à certaines parties du site, ou si votre site n'est pas optimisé pour lui, vous pouvez configurer AppScan pour qu'il utilise un autre navigateur que celui que vous avez installé sur votre machine.

Procédure

1. Cliquez sur **Outils > Options**, et sélectionnez **Utiliser un navigateur externe**.

2. Sélectionnez un navigateur dans la liste déroulante des navigateurs pris en charge *qui sont installés sur votre machine*. Les navigateurs pris en charge sont les suivants :
   - Microsoft Internet Explorer
   - Mozilla Firefox
   - Google Chrome
   - Microsoft Edge
3. Si l'une des deux options de configuration suivantes a été modifiée, les valeurs d'en-tête définies sont utilisées, et non celles du nouveau navigateur sélectionné. Si nécessaire, vous pouvez restaurer les valeurs par défaut.
   - **Configuration > Configuration avancée > Communication : Valeur d'en-tête de requête langage Accept**
   - **Configuration > Options d'exploration > Valeur d'en-tête agent d'utilisateur**

   Les manières dont les paramètres ont été modifiés *par l'utilisateur* sont les suivantes :
   - Vous avez ouvert le navigateur pour enregistrer la procédure de connexion ou une opération en plusieurs étapes, ou vous avez cliqué sur "Afficher dans le navigateur".
   - Vous les avez modifiés manuellement.
   - Vous avez chargé un examen enregistré.

   Pour ajuster ces deux paramètres au navigateur que vous venez de définir, supprimez simplement les valeurs, et (si nécessaire) réenregistrez la connexion ou l'opération en plusieurs étapes. A partir de ce moment, AppScan utilise automatiquement l'en-tête du navigateur défini.

   Remarque : Les limitations suivantes s'appliquent au nouveau navigateur :
   - Si le navigateur sélectionné est configuré pour utiliser un fichier de configuration de proxy, cette sélection est ignorée et c'est le navigateur intégré qui s'ouvre.
   - Si vous enregistrez une opération en plusieurs étapes à l'aide de l'option "Connecter puis enregistrer", le navigateur intégré est utilisé.
   - Si une autre instance AppScan est ouverte et que vous tentez d'ouvrir un navigateur externe, c'est le navigateur intégré qui s'ouvre.
   - Dans **Gestion de connexion > onglet Détails**, si vous sélectionnez une URL et que vous cliquez sur **Afficher dans le navigateur** ou **Sélectionner**, le navigateur intégré s'ouvre.
   - Si vous sélectionnez Firefox, AppScan crée automatiquement un profil Firefox nommé "AppScan" (s'il n'en existe pas déjà un). Si Firefox était ouvert au moment où cela a été fait, vous devez le fermer pour que la modification prenne effet.

Concepts associés:

«Flux de travaux pour les utilisateurs avancés», à la page 313
Ce flux de travaux est destiné à aider les utilisateurs expérimentés dans le domaine de la sécurité Web à réaliser un examen plus approfondi.

Tâches associées:

«Amélioration manuelle de la couverture du site», à la page 317
Vous pouvez ajouter les URL omises par l'étape d'exploration automatique initiale, à la fois les URL individuelles (comme celles nécessitant une saisie spécifique, présentes dans certains formulaires) et les séquences ordonnées d'URL (dans les panier d'achat, par exemple).

Référence associée:

«Vue Configuration avancée», à la page 120
L'onglet **Avancé** de la boîte de dialogue **Configuration des examens** permet de modifier des paramètres avancés du registre qui affectent des examens spécifiques (Examen > Configuration des examens > onglet Avancé) et devrait être utilisé uniquement par des utilisateurs AppScan expérimentés ou conformément aux instructions de l'équipe de support en vue de traiter un problème.

«Vue Options d'exploration», à la page 71
Vue Options d'exploration de la boîte de dialogue Configuration.

Traitement des incidents liés à la connexion

Astuces pour identifier les problèmes de détection de session dans la vue Configuration des examens > Gestion de connexion.

Lorsque vous fermez le navigateur après avoir enregistré la procédure de connexion, l'icône Clé verte  confirme que AppScan a détecté un schéma En session utilisable pendant les examens pour vérifier son statut En session. Si l'une des autres icônes s'affiche à la place, AppScan risque de ne pas disposer d'informations suffisantes pour se connecter au site pendant l'examen.

Configuration des examens > Gestion de connexion permet d'enregistrer la séquence de connexion de deux façons : en tant qu'actions et en tant que demandes. Tant que l'*une* de ces deux méthodes aboutit, AppScan est en mesure de se connecter au site. Le tableau ci-dessous peut vous aider à identifier les problèmes si les deux méthodes ont échoué.

Le tableau suivant récapitule les messages et les actions de l'utilisateur possibles pour le traitement des incidents.

Icône	Message	Actions utilisateur possibles
	**Utilisation d'une connexion basée sur les actions** Connexion basée sur les actions : Succeeded (Réussite) Connexion basée sur les demandes : Succeeded (Réussite)	Aucune action requise. La connexion basée sur les actions sera utilisée et la connexion basée sur les demandes sera disponible comme méthode de rétromigration.
	**Utilisation d'une connexion basée sur les actions** Connexion basée sur les actions : Succeeded (Réussite) Connexion basée sur les demandes : Echec	Aucune action requise. La connexion basée sur les actions sera utilisée. Pour résoudre les problèmes liés à la connexion basée sur les demandes, voir «Traitement des incidents liés à la connexion basée sur les demandes», à la page 338
	**Utilisation d'une connexion basée sur les demandes** Connexion basée sur les actions : Echec Connexion basée sur les demandes : Succeeded (Réussite)	Aucune action requise. Bien que la connexion basée sur les actions soit la méthode préférée, étant donné que la connexion basée sur les demandes aboutit, cette dernière sera utilisée. Pour résoudre les problèmes liés à la connexion basée sur les actions, voir «Traitement des incidents liés à la connexion basée sur les actions», à la page 338 **Remarque :** Si l'une des pages de connexion est très lente, il peut être plus pratique d'utiliser la connexion basée sur les demandes, car de nombreuses connexions sont généralement requises pendant un examen.
	**Séquence de connexion pas encore enregistrée**	Cliquez sur  et enregistrez une connexion ou, si la connexion n'est pas requise, dans l'onglet Connexion/Déconnexion > méthode Connexion, sélectionnez **Aucune** pour désactiver la détection de session.

Icône	Message	Actions utilisateur possibles
	**Séquence de connexion pas encore validée**	Si des modifications ont été apportées à l'une des séquences, vous devez cliquer sur le bouton **Valider** pour valider la nouvelle séquence de connexion.
	**Modèle de détection en session non défini**	Commencez par réenregistrer la connexion, mais cette fois-ci, après vous être connecté, cliquez sur un lien supplémentaire avant de fermer l'enregistreur de connexion. Ce lien doit pointer vers une page dont la réponse inclura des données ou des liens disponibles uniquement lorsque les utilisateurs seront en session. De cette manière, AppScan pourra peut-être identifier automatiquement un schéma valide. Si cela ne fonctionne pas, définissez vous-même un schéma en session. Pour plus de détails, voir «Boîte de dialogue Sélectionner un schéma de détection», à la page 61
	**Demande en session identique à une demande de connexion**	En général, la séquence de connexion doit se terminer immédiatement après la connexion d'AppScan à l'application. Cependant, dans de rares cas, la demande En session contient également la demande de connexion (avec le nom d'utilisateur et le mot de passe). Alors, chaque fois qu'AppScan réexécute la demande En session (pour vérifier la connexion), il se connecte et, par conséquent, ne peut pas détecter sa déconnexion. La solution consiste à réenregistrer la séquence de connexion, puis une fois la connexion établie, à cliquer sur un autre lien de la page. La séquence de connexion comporte maintenant une étape supplémentaire. Tant que cette nouvelle demande n'inclut pas les données d'identification, AppScan peut utiliser la séquence pour vérifier le moment de sa déconnexion et l'icône Clé devient verte.
	**Page de session redirigée**	Si la page sélectionnée comme première page En session redirige vers une autre page, le modèle En session sélectionné par AppScan risque d'être incorrect. • Vérifiez que le **modèle de détection En session** en cours indique le statut En session. • Si vous n'êtes pas sûr, essayez d'ajouter la page de redirection comme étape supplémentaire dans la séquence de connexion basée sur les demandes.

Icône	Message	Actions utilisateur possibles
	**Page de session non identifiée**	Dans l'onglet Demande, ouvrez la page finale de la séquence de connexion, recherchez un modèle (dans l'onglet Navigateur ou dans l'onglet Demande/Réponse) *unique* pour les utilisateurs connectés (tel qu'un lien "déconnecter"), et sélectionnez-le comme modèle En session. • Pour résoudre les problèmes liés à la connexion basée sur les actions, voir «Traitement des incidents liés à la connexion basée sur les actions» • Pour résoudre les problèmes liés à la connexion basée sur les demandes, voir «Traitement des incidents liés à la connexion basée sur les demandes» • Pour prendre connaissance d'un flux de travaux avancé pour le traitement des incidents, voir «Flux de travaux avancé pour le traitement des incidents liés à la connexion», à la page 339
	**La détection de session est désactivée**	Aucune action requise. Il est possible d'activer la détection de session en sélectionnant l'une des trois méthodes de connexion suivantes : Enregistrée, Invite ou Automatique.

Traitement des incidents liés à la connexion basée sur les actions

Ces étapes vous aideront à identifier les problèmes liés à la connexion basée sur les actions.

Procédure

1. Dans **Gestion de connexion > Détails > Actions**, vérifiez que le nom d'utilisateur (uid) et le mot de passe (passw) sont corrects (cliquez deux fois sur la valeur du mot de passe pour voir la valeur entrée), et corrigez-les manuellement si nécessaire.
2. Cliquez sur  pour exécuter la séquence dans le lecteur. Cela vous permettra peut-être de visualiser le moment où la séquence a échoué.

   Remarque : Si l'une des pages de connexion est très lente, il peut être plus pratique d'utiliser la connexion basée sur les demandes, car de nombreuses connexions sont généralement requises pendant un examen.
3. Cliquez sur  et réenregistrez la séquence, mais cette fois :
   a. Entrez le nom d'utilisateur et le mot de passe dans l'éditeur de texte et copiez-collez-les dans la page Web.
   b. Au lieu de cliquer sur le bouton Soumettre de votre site, cliquez sur la touche **Entrée** de votre clavier.

   Si aucune de ces étapes ne résout le problème, essayez d'utiliser la séquence basée sur les demandes.

Traitement des incidents liés à la connexion basée sur les demandes

Si le schéma Détection En session affiché dans l'onglet Détails n'identifie *pas* correctement le statut En session, vous pouvez sélectionner un autre schéma à l'aide de la séquence Demandes.

Procédure

1. Dans **Gestion de connexion > Détails > Demandes**, sélectionnez l'URL marquée comme étant En session (mise en évidence en vert), puis cliquez sur le bouton **Sélectionner** en bas de la boîte de dialogue pour choisir un schéma différent.

   Le navigateur s'ouvre, vous pouvez alors sélectionner un nouveau schéma dans le navigateur ou dans l'onglet Corps de la réponse. Fermez ensuite le navigateur et cliquez sur **Valider**.
2. Si vous ne pouvez pas identifier un schéma En session sur la page finale, procédez comme suit :
   a. Sélectionnez la demande *au-dessus* de la demande consultée.
   b. Cliquez deux fois dessus et vérifiez qu'elle ne contient pas les données d'identification.
   c. Si elle ne les contient pas, cliquez sur **Sélectionner**, et tentez d'identifier un autre schéma.
3. Si vous ne trouvez pas de schéma En session, répétez l'étape précédente pour la prochaine demande. Vous pouvez la répéter autant de fois que nécessaire, jusqu'à atteindre une demande contenant les données d'identification.
4. Si vous ne parvenez pas à identifier un schéma En session parmi ces pages et qu'une ou plusieurs adresses URL sont répertoriées *après* la page En session, suivez la même procédure pour rechercher un schéma En session sur *cette* page.
5. S'il n'existe *pas* d'URL supplémentaires, essayez d'enregistrer la séquence de connexion une nouvelle fois, mais cliquez sur un lien supplémentaire une fois votre connexion établie, de préférence sur un paramètre personnalisé, et recherchez un schéma En session sur cette page.
6. En cas d'échec, essayez de sélectionner un schéma Hors session :
   a. Sélectionnez l'URL qui était initialement marquée comme la demande En Session.
   b. Ouvrez un navigateur (en dehors d'AppScan) et envoyez cette demande seule (non précédée du reste de la séquence de connexion).
   c. Comparez les deux réponses et essayez d'identifier une expression dans le corps de la réponse à partir de l'étape B, qui n'existe pas dans la page En session (par exemple, "Vous n'êtes pas connecté").

      Remarque : Si la demande vous redirige vers une autre page, vous ne pouvez pas utiliser la réponse affichée dans le navigateur, vous devez utiliser la réponse à la demande réelle, ce qui peut être fait à l'aide d'un analyseur.
   d. Au bas de l'onglet Détails, cliquez sur le bouton de liste déroulante En session et sélectionnez **Hors session**, puis collez le schéma identifié dans la zone **Modèle de détection**.

Que faire ensuite

Si cette procédure ne résout pas le problème, référez-vous à la note technique en ligne suivante :

http://www.ibm.com/support/docview.wss?&rs=3378&uid=swg21283302#Overview%20of%20In-Session%20Detection

Flux de travaux avancé pour le traitement des incidents liés à la connexion

Etapes permettant aux utilisateurs avancés de résoudre les problèmes de connexion.

Pourquoi et quand exécuter cette tâche

Les étapes ci-après permettent d'identifier et de résoudre systématiquement les problèmes de connexion. Après chaque étape suggérée dans le flux de travaux, essayez de réexécuter l'examen pour déterminer si le problème est résolu.

Procédure

1. **Configurez le navigateur basé sur les actions pour qu'il soit visible**

   Dans **Outils > Options > Avancé > Gestion de sessions > Afficher la fenêtre du lecteur basé sur les actions**, définissez le paramètre sur **True** pour pouvoir afficher les actions du navigateur.

2. **Vérifiez que le site est opérationnel et que les données d'identification sont correctes**

   Ouvrez l'URL de départ dans un navigateur standard et vérifiez qu'il est possible de se connecter manuellement avec les données d'identification que vous avez fournies.

3. **Ajustements de la configuration avancée** Dans **Configuration > URL et serveurs**, cliquez sur **Afficher dans le navigateur** et vérifiez que le navigateur AppScan peut se connecter.
   - Si une fenêtre en incrustation indiquant une erreur de script apparaît, effectuez l'une ou l'ensemble des opérations suivantes :
     - Dans **Configuration > Configuration avancée > Communication : Supprimer l'en-tête de codage ACCEPT**, définissez le paramètre sur **False** et cliquez sur **Appliquer**.
     - Dans **Configuration > Configuration avancée > Général : Filtre d'extensions de fichier proxy**, supprimez l'ensemble du contenu dans la zone Valeur et cliquez sur **Appliquer**.
     - Allez dans **Configuration > Configuration avancée > Gestion de sessions : Filtre du type de contenu de séquence**, supprimez l'ensemble du contenu dans la zone Valeur et cliquez sur **Appliquer**.
   - Si, dans le navigateur AppScan, le site ne se comporte pas de la même façon que dans votre navigateur standard, effectuez les opérations suivantes :
     - Dans **Configuration > Options d'exploration > Agent d'utilisateur**, cliquez sur l'icône **Editer**, supprimez l'ensemble du contenu, puis cliquez sur **Appliquer**.

4. **Site utilisant l'authentification HTTP**

   Si le site utilise l'authentification HTTP (si une fenêtre en incrustation dans laquelle vous devez vous authentifier s'ouvre), effectuez les opérations suivantes :

   a. Dans la vue **Configuration > Gestion de connexion**, associez **Méthode de connexion** à la valeur **Aucune**.

   b. Dans la vue **Configuration > Authentification HTTP**, indiquez le nom d'utilisateur et le mot de passe, et si nécessaire, le domaine.

      Remarque : Si le nom d'utilisateur contient une barre oblique (/), le contenu placé avant la barre oblique est le domaine, et le contenu placé après la barre oblique est le nom d'utilisateur. Sinon, ne renseignez pas la zone Domaine.

5. **Connexion automatique**

   Si vous utilisez la connexion automatique, effectuez les opérations suivantes :

   a. Dans l'onglet **Configuration > Gestion de connexion > Connexion/Déconnexion**, vérifiez que la méthode de connexion est **Automatique**.

   b. Indiquez le nom d'utilisateur et le mot de passe.

   c. Dans l'onglet **Configuration > Gestion de connexion > Détails**, cliquez sur **Configuration de la détection automatique en session**.

      Lorsqu'AppScan tente de se connecter au site automatiquement, trois types de problème peuvent survenir :

      - Si AppScan ne parvient pas à remplir les zones de connexion, cela peut signifier qu'il n'arrive pas à les identifier :
        1) Ouvrez l'URL de départ dans un navigateur standard.
        2) Cliquez avec le bouton droit de la souris sur la zone Nom d'utilisateur et sélectionnez **Inspecter**.
        3) Dans le panneau du code source HTML, localisez la valeur d'ID de la zone Nom d'utilisateur et copiez-la dans le presse-papiers.

4) Dans AppScan, allez dans **Configuration > Remplissage automatique de formulaires** et collez la valeur d'ID dans la zone Paramètres de nom d'utilisateur.
5) Répétez les étapes ii à iv pour la valeur d'ID de mot de passe.

- Si AppScan clique sur les mauvais boutons, passez à la connexion enregistrée.
- Si AppScan ne parvient pas à identifier un schéma en session, voir . «Boîte de dialogue Sélectionner un schéma de détection», à la page 61

6. **Connexion enregistrée**

   Si vous utilisez une connexion enregistrée, effectuez les opérations suivantes :

   a. Dans l'onglet **Configuration > Gestion de connexion > Connexion/Déconnexion**, vérifiez que la méthode de connexion est **Enregistrée**.
   b. Enregistrez la séquence de connexion.
   c. Ouvrez la liste **Onglet Détails > Actions** et cliquez sur le bouton **Lire**.

      AppScan tente de se connecter au site. Les problèmes suivants peuvent survenir :

      - Si AppScan remplit les paramètres de nom d'utilisateur et de mot de passe trop rapidement, accédez à la liste **Gestion de connexion > Détails > Actions** et augmentez la période d'**attente** entre les actions.
      - Si AppScan manque des actions, remplacez le clic de souris par Tabulation/Entrée, ou inversement.

   d. Dans la liste **Onglet Détails > Actions**, cliquez sur **Valider**.

      AppScan lit la séquence et tente d'identifier un schéma En session. Si aucun schéma En session n'est trouvé, ajoutez une étape supplémentaire à la séquence, après l'étape de connexion, pour atteindre une page contenant davantage d'informations (par exemple "Bienvenue [nom_utilisateur]" ou "[ID_utilisateur]", qu'AppScan pourra utiliser comme schéma En session.

7. **Passez à la connexion basée sur les demandes**

   Si aucune des étapes ci-dessus ne fonctionne, essayez d'utiliser la connexion basée sur les demandes dans un navigateur externe :

   a. Dans **Outils > Options > Options d'examen**, sélectionnez la case à cocher **Utiliser un navigateur externe** et sélectionnez un navigateur.
   b. Dans **Configuration > Gestion de connexion**, définissez la méthode de connexion sur **Enregistrée**.
   c. Cliquez sur **Enregistrer > Utiliser un navigateur externe**.
   d. Connectez-vous au site et fermez le navigateur.

Etapes d'exploration longues ou sans fin

Pour certains types de sites, l'étape d'exploration peut être très longue ou ne jamais se terminer.

La cause de ce problème peut être que le site réécrit les paramètres dans l'URL, créant des dizaines, voire des centaines d'URL "dynamiques" pour des pages qui sont sensiblement les mêmes.

Exemple :

```
http://...php/1/index
http://...php/2/index
...
http://...php/100/index
```

Bien que ces URL apparaissent dans l'arborescence d'application comme 100 noeuds distincts, et que des tests sont créés pour chacune d'entre elles, il est probablement inutile de les tester toutes séparément.

Le module d'optimisation de l'exploration peut identifier leur schéma et créer un paramètre personnalisé qui va permettre à AppScan de les traiter comme une même URL.

Voir «Module d'optimisation de l'exploration», à la page 296

Traitement des incidents liés aux films Flash

Cette section propose des solutions pour traiter les incidents liés à la fonction d'examen Flash.

Problème	Action
Après avoir installé une nouvelle version d'AppScan, le message d'erreur suivant s'affiche à chaque fois que je l'ouvre : `FlashBrowser has encountered a problem and needs to close.`	1. Fermez AppScan. 2. Supprimez tous les fichiers nommés **`user.config`** dans les dossiers du type (Windows 7) : `C:\Users\<USER_NAME>\AppData\Local\IBM_Corporation\FlashBrowser.exe_Url_<CODE>` 3. Redémarrez AppScan
AppScan n'a pas détecté d'URL dans le film.	1. Vérifiez que votre système répond à la configuration système requise. 2. Vérifiez que l'option "Lire les fichiers Flash pour détecter les vulnérabilités potentielles" (**Configuration des examens > Options d'exploration**) est sélectionnée.
AppScan identifie les URL dans certains films Flash, mais pas dans d'autres.	1. Vérifiez que la version du film Flash est prise en charge. (Les films non pris en charge sont listés dans la vue "Données d'application" sous "URL filtrées".) 2. Lisez le film problématique dans Internet Explorer sur la machine ayant effectué l'analyse. Vérifiez qu'Internet Explorer peut le lire correctement, et que la barre d'état d'IE indique 'Terminé' à la fin du film. 3. Vérifiez que l'exécution JavaScript est activée dans **Configuration des examens > Options d'exploration**.
La couverture de l'examen est incomplète.	1. Vérifiez que les informations dans **Configuration des examens > Remplissage automatique de formulaires** sont complètes. 2. Dans Configuration avancée, augmentez la valeur de Flash : Durée entre les exemples. 3. Dans Configuration avancée, définissez "Flash : Couverture" sur 2. 4. Affectez la valeur True à **Options avancées > ShowDebugFlashExecution**, redémarrez AppScan, et vérifiez que le film est lu correctement dans le "conteneur Player" qui s'ouvre.
AppScan ne détecte aucune vulnérabilité dans les films Flash.	1. Vérifiez que tous les tests ActionScript 2 et 3 sont activés dans Stratégie de test. 2. Vérifiez dans **Vue Données d'application > Paramètres de script** qu'il ne manque aucun paramètre Flash. 3. Il se peut simplement qu'un film spécifique ne soit pas vulnérable.
Je constate un changement dans les performances du film Flash lui-même après qu'il a été exploré avec AppScan. Pourquoi ?	AppScan modifie de façon réversible la configuration de Flash Player versions 10.1 et ultérieures. Pour plus d'informations et pour savoir comment annuler ces modifications, voir «Restauration des paramètres Adobe Flash Player», à la page 344.
Où puis-je trouver le journal Flash ?	Voir «Messages du journal Flash», à la page 362.

Problème	Action
Si je prends contact avec le service de support, quelles informations dois-je fournir ?	1. Activez le mode de support étendu. 2. Réexaminez le film. 3. Envoyez le fichier AppScanFlashBrowser.log qui se trouve dans le répertoire des journaux AppScan.

Certains films Flash ne sont pas examinés

L'exécution Flash est activée, mais AppScan n'arrive pas à charger certains films Flash pendant l'examen.

Cause

Il y a une différence dans la séquence d'initialisation utilisée par Adobe Flash Player lorsqu'il exécute un film Flash ou un fichier Flash SWF intégré à un film Flash.

Comportement 1 : Film Flash

Dans le cas d'un film Flash, Adobe Flash Player exécute les actions suivantes :

1. Initialisation de l'objet Flash Stage
2. Appel du constructeur du film Flash lui-même (objet Sprite ou Movie Clip)

Comportement 2 : Fichier SWF intégré

Dans le cas d'un fichier SWF intégré à un film Flash, Adobe Flash Player exécute les actions suivantes :

1. Appel du constructeur du film Flash lui-même (objet Sprite ou Movie Clip)
2. Initialisation de l'objet Flash Stage

En conséquence, tout film Flash faisant référence à l'objet Stage dans le constructeur génère une exception de type "pointeur null", parce que Stage n'est pas encore initialisé.

Pour balayer les fichiers SWF pendant un examen, AppScan Standard les charge dans son propre conteneur Flash. Cela ne devrait pas avoir d'impact sur la façon dont les fichiers Flash se comportent, à cause de la divergence de comportement mentionnée ci-dessus, mais lorsque le film est chargé dans le conteneur AppScan Standard, Adobe Flash Player prend par défaut le comportement 2 (au lieu du comportement 1 attendu). Si le constructeur du film inclut des références à l'objet Stage, AppScan Standard trouve un pointeur null et n'arrive pas à charger le film.

Solution palliative

Etant donné la fonctionnalité actuelle d'Adobe Flash Player, la seule solution de contournement de ce problème est d'effectuer une petite modification dans les fichiers SWF du site examiné. Cette modification n'affecte pas la fonctionnalité du film Flash, et ne pose aucun risque pour la sécurité du fichier SWF en question.

Exemple de code :

Structure habituelle du fichier SWF problématique :

```
package {

  import flash.display.*;
  import flash.events.*;

  public class TestSample extends MovieClip {
```

```
  public function TestSample(){

   // Begin initialization tasks
   // There may be one or more references to the Stage object here

   // For example: stage.addEventListener(MouseEvent.CLICK,MouseClicked);

   // End of initialization tasks

  }
  // other functions – no change required

 }

}
```

La solution consiste à copier les tâches d'initialisation :

```
package {

 import flash.display.*;
 import flash.events.*;

 public class TestSample extends MovieClip {

  public function TestSample(){
   this.addEventListener(Event.ADDED_TO_STAGE, solutionToFlashProblem);
  }

  private function solutionToFlashProblem(e:Event):void
  {

   // Begin initialization tasks
   // There may be one or more references to the Stage object here
   // For example: stage.addEventListener(MouseEvent.CLICK,MouseClicked);

   // End of initialization tasks

  }
  // other functions – no change required
 }
}
```

Les opérations effectuées ont consisté à copier le contenu du constructeur dans une fonction de rappel qui sera appelée lorsque la classe en cours sera ajoutée à l'objet Stage. Lorsque cela se produira, l'objet Stage sera initialisé et Flash Player suivra le comportement 1.

Restauration des paramètres Adobe Flash Player

Pourquoi et quand exécuter cette tâche

Lorsqu'un examen a été effectué avec l'exécution Flash active, le fonctionnement de Flash Player 10.1 (et des versions suivantes) est légèrement altéré, et il se comporte comme Flash 10.0 dans un domaine. Il s'agit d'une fonction de la version 10.1 (contrairement à la version 10.0) qui est arrêtée par Flash Player lorsque sa fenêtre n'est pas la fenêtre active. Cette fonction est désactivée pendant l'examen.

Après l'examen, vous pouvez annuler la modification qui a été faite. Cependant, ce paramétrage sera appliqué à nouveau la prochaine fois qu'un examen sera réalisé pendant l'exécution de Flash.

Procédure

1. Ouvrez le dossier Flash Player. Par défaut, il s'agit généralement de :
   `C:\WINDOWS\system32\Macromed\Flash`
2. Localisez le fichier `mms.cfg` et ouvrez-le dans un éditeur de texte (Bloc-notes Microsoft, par exemple).

3. Localisez la ligne :
   `FullFramerateWhenInvisible=True`
4. Supprimez cette ligne (ou affectez-lui la valeur False).
5. Sauvegardez le fichier.
6. Redémarrez votre navigateur pour que la modification prenne effet.

Traitement des incidents liés aux opérations en plusieurs étapes

Vous trouverez ici des suggestions pour le traitement des incidents liés aux opérations en plusieurs étapes basées sur les actions.

Si AppScan ne parvient pas à analyser votre enregistrement en plusieurs étapes basé sur les actions, effectuez les étapes de traitement des incidents suivantes :

1. Dans **Configuration > Opérations en plusieurs étapes**, sélectionnez la séquence et cliquez sur **Valider**. Le navigateur s'ouvre et relit la séquence. Vérifiez qu'il effectue toutes les étapes prévues. Si les actions enregistrées ne correspondent pas à la version en cours du site, réenregistrez la séquence.
2. Lorsque le navigateur se ferme, vérifiez qu'une coche verte est affichée à côté de chaque action dans la séquence. Si une ou plusieurs actions sont associées à une croix rouge, déterminez si l'action est requise pour l'exécution de l'étape suivante dans la séquence (par exemple, cliquer sur une fenêtre en incrustation qui n'apparaît pas dans la lecture). Si elle n'est pas requise, supprimez-la en la sélectionnant, puis en cliquant sur le - .
3. Après chaque étape de la séquence, AppScan insère une action WAIT d'une durée de 0 seconde. Essayez d'augmenter la durée de l'action WAIT avant une action qui échoue.
4. Vérifiez que les options de réglage de la redondance et du suivi pour tous les paramètres et cookies dans la demande de test sont correctes. Si tel n'est pas le cas, corrigez-les ou supprimez-les de la liste dans **Configuration > Paramètres et cookies > onglet principal**.
5. Augmentez le délai d'attente de non-interaction dans **Configuration > Configuration avancée > Basée sur les actions : Délai d'attente de non-interaction pour la lecture d'opérations en plusieurs étapes** .

Remplacement d'extensions non signées

Si vous voulez utiliser une extension non signée déjà utilisée dans une version précédente de AppScan, vous pouvez choisir de la considérer comme étant digne de confiance ou déterminer si une version signée disponible peut lui être substituée.

Pourquoi et quand exécuter cette tâche

Lorsqu'il s'ouvre, AppScan vérifie que les extensions activées sont signées ou ont été considérées manuellement comme étant "dignes de confiance" par l'utilisateur. Les extensions non signées qui n'ont pas été considérées comme étant "dignes de confiance" ne sont pas chargées.

Si vous disposez d'une extension IBM non signée que vous avez utilisée avec une version antérieure de AppScan, vous pouvez choisir de la considérer comme étant digne de confiance en cliquant sur le bouton **Faire confiance** en regard de celle-ci, ou déterminer si une version signée disponible peut lui être substituée, comme indiqué ci-après.

Procédure

1. Ouvrez le gestionnaire d'extensions (**Outils > Extensions > Gestionnaire d'extensions**).
   Les extensions qui ont été activées par l'utilisateur (case cochée) mais qui ne sont pas signées sont associées à un bouton Faire confiance.

Remarque : Pour considérer l'extension comme étant digne de confiance sans la remplacer, il suffit de cliquer sur le bouton Faire confiance. L'extension est désormais considérée comme étant digne de confiance.

2. Cliquez sur le lien **Obtenir davantage d'extensions** dans la partie supérieure de la boîte de dialogue.
3. Dans la page qui s'ouvre, cliquez sur l'onglet Extensions et déterminez si une version signée de l'extension est disponible.
4. Sauvegardez l'extension sur votre machine.
5. Dans le gestionnaire d'extensions, sélectionnez la version non signée (mettez-la en évidence) et cliquez sur **Supprimer**.
6. Cliquez sur **Installer**, sélectionnez la nouvelle extension et cliquez sur **Ouvrir**.

   La nouvelle extension est installée et activée. Vous devez redémarrer AppScan pour que la modification prenne effet.

Référence associée:

«Gestionnaire d'extensions», à la page 294
Le gestionnaire d'extensions vous permet d'ajouter ou de supprimer, d'activer ou de désactiver des extensions à utiliser avec AppScan

Messages du journal des examens

Les sections suivantes décrivent les messages du journal d'examen (Afficher > Journal d'examen).

Tous les messages du journal d'examen sont documentés dans cette section. Le cas échéant, des explications et actions utilisateur suggérées sont incluses.

CRWAD0201I Examen créé

Explication : Un nouvel examen a été créé. Toutes les données d'examen précédentes ont été supprimées.

Action de l'utilisateur : n/a

CRWAD0202I Démarrage de l'exploration

Explication : Démarrage de l'étape d'exploration de l'examen.

Action de l'utilisateur : n/a

CRWAD0203I Exploration

Explication : Exploration de l'application dans le cadre de l'étape d'exploration

Action de l'utilisateur : n/a

CRWAD0204I Analyse des résultats d'exploration

Explication : Analyse des résultats d'exploration en vue de créer des tests

Action de l'utilisateur : n/a

CRWAD0205I Démarrage du test

Explication : Démarrage de l'étape de test de l'examen

Action de l'utilisateur : n/a

CRWAD0206I Envoi des URL de départ

Explication : Envoi de l'URL de départ et de toute opération en plusieurs étapes enregistrée

Action de l'utilisateur : n/a

CRWAD0214I Démarrage de l'exploration manuelle

Explication : n/a

Action de l'utilisateur : n/a

CRWAD0215I Examen en plusieurs phases : Démarrage de la phase <numéro>

Explication : n/a

Action de l'utilisateur : n/a

CRWAD0216I Examen arrêté ; durée de l'examen : <durée>

Explication : n/a

Action de l'utilisateur : n/a

CRWAD0217I Données d'exploration et de test effacées

Explication : n/a

Action de l'utilisateur : n/a

CRWAD0218I Données de test effacées

Explication : n/a

Action de l'utilisateur : n/a

CRWAD0219I Limite de temps atteinte. Arrêt de l'examen...

Explication : Le délai défini pour l'étape d'exploration de Scan Expert est atteint, l'exploration a été arrêtée et Scan Expert est passé à l'étape d'évaluation. (Si AppScan est configuré pour appliquer automatiquement les modifications avant de passer à l'examen principal, cette procédure sera respectée. L'"arrêt de l'examen" fait uniquement référence à l'étape d'exploration de Scan Expert.)

Action de l'utilisateur : Pour modifier ce délai, sélectionnez Configuration des examens > Scan Expert.

CRWAD0220I Démarrage de l'exécution de Flash

Explication : n/a

Action de l'utilisateur : n/a

CRWAD0221I Un lecteur Flash pris en charge (version 9.0.124.0 ou ultérieure, pour Internet Explorer) n'est pas installé. Flash ne pourra pas s'exécuter.

Explication : L'analyse est configurée afin d'inclure l'exécution des fichiers Flash, mais aucune version prise en charge d'Adobe Flash Player n'est installée sur cette machine et les fichiers Flash ne seront pas exécutés.

Action de l'utilisateur : Pour qu'AppScan exécute des fichiers Flash au cours de l'analyse, vous devez installer une version prise en charge.

Vous pouvez télécharger la version la plus récente d'Adobe Flash Player depuis le site http://get.adobe.com/flashplayer/

CRWAD0222I Flash Player non configuré. Flash ne pourra pas s'exécuter.

Explication : L'analyse est configurée afin d'inclure l'exécution des fichiers Flash, mais Adobe Flash Player n'est pas configuré pour fonctionner avec AppScan et les fichiers Flash ne s'exécuteront pas au cours de l'analyse.

Action de l'utilisateur : Pour que AppScan exécute des fichiers Flash au cours de l'analyse, un administrateur doit configurer un navigateur Flash. Voir «Configuration de Flash Player», à la page 7.

CRWAD0301I URL visitée : <URL>

Explication : n/a

Action de l'utilisateur : n/a

CRWAD0302I Lien <URL> extrait du contenu dynamique de l'URL <URL>

Explication : Une URL a été extraite à des fins de test depuis un contenu JavaScript ou Flash.

Action de l'utilisateur : n/a

CRWAD0303I URL ignorée (en raison de l'extension) : <URL>

Explication : L'examen est configuré pour exclure les fichiers ayant cette extension ; cette adresse URL peut par conséquent être ignorée.

Action de l'utilisateur : Ceci peut être modifié dans Configuration | Exclusion de chemins et de fichiers.

CRWAD0304I URL ignorée (en raison de l'exclusion) : <URL>

Explication : L'examen est configuré pour exclure cette adresse URL.

Action de l'utilisateur : Ceci peut être modifié dans Configuration | Exclusion de chemins et de fichiers.

CRWAD0305I URL ignorée (hôte non inclus dans l'examen) : <URL>

Explication : L'examen n'est pas configuré pour inclure cet hôte.

Action de l'utilisateur : Ceci peut être modifié dans Configuration | URL et serveurs.

CRWAD0306I URL ignorée (limite de chemin d'accès dépassée) : <URL>

Explication : n/a

Action de l'utilisateur : La limite de chemin d'accès peut être modifiée dans Configuration | Options d'exploration.

CRWAD0307I URL ignorée (limite de profondeur dépassée) : <URL>

Explication : n/a

Action de l'utilisateur : La limite de profondeur peut être modifiée dans Configuration | Options d'exploration.

CRWAD0308I URL ignorée (limite de lien dépassée) : <URL>

Explication : n/a

Action de l'utilisateur : La limite de lien peut être modifiée dans Configuration | Options d'exploration.

CRWAD0309I Test <ID> <Nom du type de problème> créé pour l'URL : <URL> <param>

Explication : n/a

Action de l'utilisateur : n/a

CRWAD0310I Page visitée : [adresse URL]

Explication : n/a

Action de l'utilisateur : n/a

CRWAD0311I Page visitée : <URL>

Explication : n/a

Action de l'utilisateur : n/a

CRWAD0312I Aucun service de décodage n'a été trouvé pour le domaine <Hôte>

Explication : n/a

Action de l'utilisateur : n/a

CRWAD0313I Une adresse URL de service de décodage WebSphere Portal <URL> a été localisée.

Explication : n/a

Action de l'utilisateur : n/a

CRWAD0401I Demande de connexion détectée :<URL>

Explication : n/a

Action de l'utilisateur : n/a

CRWAD0402I Demande de déconnexion détectée : <URL>

Explication : n/a

Action de l'utilisateur : n/a

CRWAD0403I Identificateur de session détecté ; nom = <nom> ; valeur = <valeur>

Explication : n/a

Action de l'utilisateur : n/a

CRWAD0404I Identificateur de session régénéré ; nom = <nom> ; valeur = <valeur>

Explication : n/a

Action de l'utilisateur : n/a

CRWAD0405I La session est arrivée à expiration

Explication : n/a

Action de l'utilisateur : n/a

CRWAD0406I Connexion en cours

Explication : n/a

Action de l'utilisateur : n/a

CRWAD0407I Schéma En session non détecté

Explication : n/a

Action de l'utilisateur : Le schéma En session est défini dans Configuration | Gestion de connexion | Détails.

CRWAD0408I Dépassement du délai d'attente de l'opération

Explication : n/a

Action de l'utilisateur : n/a

CRWAD0409I Erreur de communication

Explication : n/a

Action de l'utilisateur : n/a

CRWAD0410I Demande inutile supprimée : [adresse URL]

Explication : n/a

Action de l'utilisateur : n/a

CRWAD0411I Exécution JavaScript dans la connexion enregistrée activée

Explication : n/a

Action de l'utilisateur : n/a

CRWAD0412I Le paramètre [nom] doit être suivi lors de la connexion, mais est prédéfini comme non suivi.

Explication : Le paramètre indiqué intervient dans la séquence de connexion et AppScan a tenté de l'ajouter à la liste des paramètres et des cookies (**Configuration des examens > Paramètres et cookies**) et de le définir sur "Suivi" (pour le suivre lors de l'examen). Cependant, il est déjà répertorié et configuré sur "Sans

suivi" de sorte qu'AppScan n'a pas modifié sa configuration.

Action de l'utilisateur : Si vous le souhaitez, vous pouvez modifier manuellement le statut de ce paramètre sur "Suivi".

CRWAD0413I Le cookie [nom] doit être suivi lors de la connexion, mais est prédéfini comme non suivi.

Explication : Le cookie indiqué intervient dans la séquence de connexion et AppScan a tenté de l'ajouter à la liste des paramètres et des cookies (**Configuration des examens > Paramètres et cookies**) et de le définir sur "Suivi" (pour le suivre lors de l'examen). Cependant, il est déjà répertorié et configuré sur "Sans suivi" de sorte qu'AppScan n'a pas modifié sa configuration.

Action de l'utilisateur : Si vous le souhaitez, vous pouvez modifier manuellement le statut de ce cookie sur "Suivi".

CRWAD0414I Nouveau paramètre suivi [nom] ajouté :

Explication : Le paramètre indiqué a été ajouté à la liste des paramètres et des cookies (**Configuration des examens > Paramètres et cookies**) et défini sur "Suivi". Son suivi sera donc effectué lors de l'examen.

Action de l'utilisateur : n/a

CRWAD0415I Nouveau cookie suivi [nom] ajouté :

Explication : Le cookie indiqué a été ajouté à la liste des paramètres et des cookies (**Configuration des arrêts > Paramètres et cookies**) et défini sur "Suivi" pour que son suivi soit effectué lors de l'examen.

Action de l'utilisateur : n/a

CRWAD0416I Format de détection En session défini sur : [format de schéma]

Explication : Le format du schéma recherché par AppScan pour vérifier qu'il est En session (voir **Configuration des examens > Gestion de connexion > Détails**) a été modifié.

Action de l'utilisateur : n/a

CRWAD0417I Schéma de détection En session défini sur : [Schéma]

Explication : n/a

Action de l'utilisateur : n/a

CRWAD0418I URL En session définie sur : [URL]

Explication : L'URL de la séquence de connexion utilisée par AppScan pour vérifier qu'il est connecté a été définie d'après cette URL (**Configuration des examens > Gestion de connexion > Détails**).

Action de l'utilisateur : n/a

CRWAD0419I Nom d'utilisateur de connexion défini sur : '<nom>' = '<valeur>'

Explication : n/a

Action de l'utilisateur : n/a

CRWAD0420I Mot de passe de connexion défini sur : 'nom' = 'valeur'

Explication : n/a

Action de l'utilisateur : n/a

CRWAD0421I Schéma de détection de page de déconnexion défini sur : 'schéma'

Explication : n/a

Action de l'utilisateur : n/a

CRWAD0501I Le test <ID> (<nom>) est POSITIF sur : <URL> <param>

Explication : n/a

Action de l'utilisateur : n/a

CRWAD0502I Le test <ID> (<nom>) est négatif sur : <URL> <param>

Explication : n/a

Action de l'utilisateur : n/a

CRWAD0503I La demande de test <URL> a échoué en raison d'une erreur de communication : <Description de l'erreur>

Explication : Les explications possibles sont les suivantes :

- La connexion est impossible
  - L'hôte distant refuse la connexion
  - L'hôte distant est arrêté
  - Le réseau n'est pas disponible
- Le délai de connexion est dépassé
  - Aucune réponse n'a été reçue du serveur dans la limite de temps
- La connexion est fermée (à distance)
  - L'application a tenté de garder active une connexion dont le délai d'attente est déjà dépassé

  - La connexion a été réinitialisée par l'homologue distant
- La connexion est fermée (en local)
  - La connexion a été interrompue par le fournisseur de connecteur sous-jacent
  - L'opération de chevauchement a été abandonnée à cause de la fermeture du connecteur
  - Trop de connecteurs sont ouverts dans le fournisseur de connecteur sous-jacent
- Inconnu(e)
  - Toute autre raison

Action de l'utilisateur : n/a

CRWAD0504I URL détectée dans la réponse du test : <URL> ; Ajout aux URL non visitées

Explication : La nouvelle adresse URL sera explorée lors de l'étape suivante de l'examen s'il en existe une. Si la limite de phase a été atteinte, l'URL apparaîtra dans les résultats comme non visitée.

Action de l'utilisateur : n/a

CRWAD0505I Le test <ID> (<nom>) sur <URL> a été filtré par un test adaptatif.

Explication : n/a

Action de l'utilisateur : Le filtrage des tests adaptatifs peut être modifié dans Configuration | Options de test.

CRWAD0506I Envoi du test <ID> (<nom>) sur : <URL> <param>

Explication : n/a

Action de l'utilisateur : n/a

CRWAD0507I Analyse de page démarrée à [adresse URL]

Explication : n/a

Action de l'utilisateur : n/a

CRWAD0508I Analyse de page terminée à [adresse URL]

Explication : n/a

Action de l'utilisateur : n/a

CRWAD0509I Echec de l'analyse de page à [adresse URL] avec l'erreur : (erreur)

Explication : n/a

Action de l'utilisateur : n/a

CRWAD0510I Résultat du test de recherche de logiciels malveillants <URL> : Non vulnérable (<brève description>)

Explication : n/a

Action de l'utilisateur : n/a

CRWAD0601I Impossible de se connecter à l'hôte : <nom du serveur>

Explication : n/a

Action de l'utilisateur : n/a

CRWAD0602I Connexion établie à l'hôte : <nom du serveur>

Explication : n/a

Action de l'utilisateur : n/a

CRWAD0603I L'examen s'est arrêté car les hôtes requis ne répondent plus

Explication : n/a

Action de l'utilisateur : n/a

CRWAD0604I Arrêt de l'examen en raison d'une fin de session détectée

Explication : AppScan a détecté qu'il est hors session, sur la base du schéma défini dans Configuration | Gestion de la connexion | Détails, et n'est pas parvenu à se connecter. L'examen a été arrêté.

Action de l'utilisateur : n/a

CRWAD0605I AppScan a détecté que sa session s'est arrêtée.

Explication : AppScan a détecté que sa session s'est arrêtée, compte tenu du schéma défini dans Configuration | Gestion de connexion | Détails.

Action de l'utilisateur : n/a

CRWAD0606I Impossible de se connecter à AppScan Enterprise

Explication : n/a

Action de l'utilisateur : n/a

CRWAD0607I Non concordance de la configuration SSL sur l'hôte : {1}, le protocole SSL est rétabli par défaut : {0}.

Explication : Lorsque AppScan ne parvient pas à se connecter à l'hôte à l'aide du protocole SSL le plus sécurisé sélectionné par l'utilisateur, il tente d'utiliser les autres protocoles sélectionnés, en commençant par l'option la plus sécurisée suivante. Ce message indique

qu'une correspondance a été trouvée. Ce problème peut survenir lorsque le système d'exploitation ne prend pas en charge un protocole SSL qui est pris en charge par AppScan et par l'hôte.

Action de l'utilisateur : Ce problème peut être résolu en installant des kits de mise à jour ou en utilisant un autre système d'exploitation.

CRWAD0701I Démarrage du test manuel

Explication : n/a

Action de l'utilisateur : n/a

CRWAD0702I Problème de sécurité ajouté au test manuel

Explication : n/a

Action de l'utilisateur : n/a

CRWAD0801I Examen sauvegardé : <chemin d'accès complet>

Explication : n/a

Action de l'utilisateur : n/a

CRWAD0802I Problème de sécurité <Nom du type de problème> supprimé par l'utilisateur

Explication : L'utilisateur a supprimé ce problème en le sélectionnant, en cliquant avec le bouton droit de la souris et en sélectionnant Supprimer.

Action de l'utilisateur : n/a

CRWAD0803I Nouveau test du problème de sécurité <Nom du type de problème>

Explication : n/a

Action de l'utilisateur : n/a

CRWAD0804I Retest non pris en charge pour le test <ID> [<nom>]

Explication : La fonction de retest ne prend en charge que les tests de type "boîte noire".

Action de l'utilisateur : Pour envoyer à nouveau ce test, réexécutez le module approprié (JSA ou Test for Malware par exemple).

CRWAD0805I Chargement de l'examen depuis le fichier [chemin d'accès complet]. Examen créé dans [version], génération [numéro de génération]

Explication : n/a

Action de l'utilisateur : n/a

CRWAD0806I Problème de sécurité <Nom du type de problème> défini comme vulnérable par l'utilisateur

Explication : n/a

Action de l'utilisateur : n/a

CRWAD0807I Problème de sécurité <Nom du type de problème> défini comme non vulnérable par l'utilisateur

Explication : n/a

Action de l'utilisateur : n/a

CRWAD1001I Démarrage de Scan Expert

Explication : n/a

Action de l'utilisateur : n/a

CRWAD1002I Scan Expert a terminé l'opération

Explication : n/a

Action de l'utilisateur : n/a

CRWAD1003I Démarrage de l'évaluation de Scan Expert

Explication : n/a

Action de l'utilisateur : n/a

CRWAD1004I Evaluation de Scan Expert terminée

Explication : n/a

Action de l'utilisateur : n/a

CRWAD1005I Application automatique des résultats de test Scan Expert

Explication : Met à jour automatiquement la configuration des examens en fonction des résultats de test de Scan Expert.

Action de l'utilisateur : n/a

CRWAD1006I L'application des résultats de test Scan Expert est terminée

Explication : Fin de la mise à jour automatique de la configuration des examens en fonction des résultats de test Scan Expert.

Action de l'utilisateur : n/a

CRWAD1007I L'examen Scan Expert a évalué : <nom>

Explication : n/a

Action de l'utilisateur : n/a

CRWAD1008I L'examen Scan Expert n'est pas parvenu à évaluer : <nom>

Explication : n/a

Action de l'utilisateur : n/a

CRWAD1009I Application de la recommandation Scan Expert : <nom>

Explication : n/a

Action de l'utilisateur : n/a

CRWAD1010I Scan Expert : Optimisation de l'exploration : interruption de l'examen pour analyser...

Explication : n/a

Action de l'utilisateur : n/a

CRWAD1011I Scan Expert : Optimisation de l'exploration : démarrée automatiquement

Explication : Le module d'optimisation de l'exploration est configuré pour démarrer automatiquement lorsque vous lancez un examen.

Action de l'utilisateur : Ce paramètre est modifiable dans **Outils > Optimisation de l'exploration : Configurer**.

CRWAD1012I Scan Expert : Optimisation de l'exploration : démarrée manuellement

Explication : n/a

Action de l'utilisateur : n/a

CRWAD1013I Scan Expert : Optimisation de l'exploration : nombre maximal de répétitions par itération atteint. Reprise de l'examen pour collecter davantage d'URL

Explication : n/a

Action de l'utilisateur : n/a

CRWAD1014I Scan Expert : Optimisation de l'exploration : activation du mode hautes performances pour cette phase

Explication : n/a

Action de l'utilisateur : n/a

CRWAD1015I Scan Expert : Optimisation de l'exploration : phase terminée. Pour la phase suivante, la limite d'URL est définie sur {0}

Explication : n/a

Action de l'utilisateur : n/a

CRWAD1016I Scan Expert : Optimisation de l'exploration : redémarrage de l'examen...

Explication : A la suite des modifications de configuration effectuées par le module d'optimisation de l'exploration, il a été nécessaire de supprimer les données d'exploration existantes et de relancer l'étape d'exploration.

Action de l'utilisateur : n/a

CRWAD1017I Scan Expert : Optimisation de l'exploration : reprise de l'examen...

Explication : Aucune modification de la configuration nécessitant l'effacement des données existantes avant de continuer n'a été effectuée. L'examen reprend là où il s'était arrêté.

Action de l'utilisateur : n/a

CRWAD1018I Scan Expert : Optimisation de l'exploration : URL insuffisantes (le nombre doit être supérieur à {0})

Explication : Le paramètre Limite de complexité définit le nombre d'URL qui doivent être contenues dans le même segment réécrit avant que le module d'optimisation de l'exploration tente de définir ce segment en tant que paramètre et relance l'étape d'exploration. Ce seuil n'a pas été atteint.

Action de l'utilisateur : Vous pouvez réduire le paramètre Limite de complexité dans **Outils | Extensions | Optimisation de l'exploration : Configurer**.

CRWAD1019I Scan Expert : Optimisation de l'exploration : abandon...

Explication : L'optimisation de l'exploration a été abandonnée par l'utilisateur.

Action de l'utilisateur : n/a

CRWAD1020I Scan Expert : Optimisation de l'exploration : Etape 1, identification des paramètres de navigation...

Explication : Le module d'optimisation de l'exploration tente d'identifier les paramètres de

navigation. S'il les identifie, il règle la redondance au niveau le plus strict.

Action de l'utilisateur : n/a

CRWAD1021I Scan Expert : Optimisation de l'exploration : analyse de {0} URL uniques

Explication : n/a

Action de l'utilisateur : n/a

CRWAD1022I Scan Expert : Optimisation de l'exploration : temps imparti pour l'analyse dépassé

Explication : La durée autorisée pour l'optimisation de l'exploration est dépassée.

Action de l'utilisateur : Vous pouvez modifier ce paramètre dans **Outils | Extensions | Optimisation de l'exploration : Configuration**.

CRWAD1023I Scan Expert : Optimisation de l'exploration : analyse terminée

Explication : n/a

Action de l'utilisateur : n/a

CRWAD1024I Scan Expert : Optimisation de l'exploration : échec de l'analyse.

Explication : n/a

Action de l'utilisateur : n/a

CRWAD1025I Scan Expert : Optimisation de l'exploration : application des modifications de configuration...

Explication : n/a

Action de l'utilisateur : n/a

CRWAD1026I Scan Expert : Optimisation de l'exploration : aucune optimisation n'a été détectée

Explication : n/a

Action de l'utilisateur : n/a

CRWAD1027I Scan Expert : Optimisation de l'exploration : valeurs par défaut du réglage de la redondance modifiées

Explication : n/a

Action de l'utilisateur : n/a

CRWAD1028I Scan Expert : Optimisation de l'exploration : règle de réécriture détectée : {0}

Explication : n/a

Action de l'utilisateur : n/a

CRWAD1029I Scan Expert : Optimisation de l'exploration : paramètre de navigation détecté : '{0}'

Explication : Le module d'optimisation de l'exploration a détecté un paramètre de navigation. Il va l'ajouter à la liste des paramètres et des cookies, et augmenter le réglage de la redondance au niveau le plus strict.

Action de l'utilisateur : n/a

CRWAD1030I Scan Expert : Optimisation de l'exploration : Etape 2, identification de la réécriture d'URL...

Explication : Le module d'optimisation de l'exploration tente d'identifier la réécriture d'URL. S'il la détecte, il crée les paramètres personnalisés nécessaires (**Configuration des examens | Paramètres et cookies | onglet Avancé**) et lancez une nouvelle étape d'exploration.

Action de l'utilisateur : n/a

CRWAD1101I <Messages du journal des extensions>

Explication : Ce message a été écrit dans le journal par une extension.

Action de l'utilisateur : Les extensions sont gérées dans Outils | Extensions | Gestionnaire d'extensions.

CRWAD1201I Démarrage de l'exploration des séquences d'opérations en plusieurs étapes

Explication : n/a

Action de l'utilisateur : Les opérations en plusieurs étapes sont gérées dans Configuration | Opérations en plusieurs étapes.

CRWAD1202I Exploration des séquences d'opérations en plusieurs étapes terminé

Explication : n/a

Action de l'utilisateur : n/a

CRWAD1203I Exploration de la séquence d'opérations en plusieurs étapes : <nom>

Explication : n/a

Action de l'utilisateur : n/a

CRWAD1204I Démarrage du test des séquences d'opérations en plusieurs étapes

Explication : n/a

Action de l'utilisateur : n/a

CRWAD1205I Test des séquences d'opérations en plusieurs étapes terminé

Explication : n/a

Action de l'utilisateur : n/a

CRWAD1206I Test de la séquence d'opérations en plusieurs étapes : <nom>

Explication : n/a

Action de l'utilisateur : n/a

CRWAD1207I Optimisation détectée pour la séquence [nom] : les demandes n° [1] à [2] doivent être exécutées avant la demande n° [n]

Explication : AppScan a déterminé que les étapes spécifiées dans la séquence seront lues dans l'ordre de demande de test n. Les étapes antérieures dans cette séquence (avant l'étape [n°1]) seront omises lors du test de cette demande.

Action de l'utilisateur : Si nécessaire, vous pouvez réviser et éditer la séquence vous-même dans **Configuration des examens > Opérations en plusieurs étapes**.

CRWAD1208I Optimisation détectée pour la séquence [nom] : aucune exécution à effectuer avant de tester la demande n° [n]

Explication : AppScan a déterminé qu'aucune exécution en plusieurs étapes n'est nécessaire avant de tester la demande [n]. Les étapes antérieures dans la séquence seront donc omises lors du test de cette demande.

Action de l'utilisateur : Si nécessaire, vous pouvez réviser et éditer la séquence vous-même dans **Configuration des examens > Opérations en plusieurs étapes**.

CRWAD1209I Impossible d'optimiser la requête [n] dans la séquence : [nom]

Explication : Toutes les tentatives d'envoi de la requête [n] ont échoué (avec ou sans les requêtes antérieures de la séquence en plusieurs étapes). La tentative d'optimisation ayant échoué, cette requête ne sera pas testée.

Action de l'utilisateur : Si AppScan fait erreur en ignorant cette demande, désélectionnez la case **Autoriser l'optimisation de la lecture** dans **Configuration > Opérations en plusieurs étapes**.

CRWAD1301I Génération des informations sur les problèmes

Explication : n/a

Action de l'utilisateur : Vous pouvez contrôler quels modules d'informations sur les problèmes s'exécutent automatiquement dans la vue Configuration > Informations sur les problèmes.

CRWAD1302I Fin de la génération des informations sur les problèmes

Explication : n/a

Action de l'utilisateur : n/a

CRWAD1303I Démarrage du module d'informations sur les problèmes : <nom>

Explication : n/a

Action de l'utilisateur : n/a

CRWAD1304I Fin du module d'informations sur les problèmes : <nom>

Explication : n/a

Action de l'utilisateur : n/a

CRWAD1305I Echec du module d'informations sur les problèmes : <nom>

Explication : n/a

Action de l'utilisateur : n/a

CRWAD1401I <nombre> demandes de service Web ont été explorées

Explication : n/a

Action de l'utilisateur : n/a

CRWAD1601I Glass box a détecté le paramètre [nom du paramètre] dans [adresse URL]

Explication : n/a

Action de l'utilisateur : n/a

CRWAD1602I Glass box a ajouté la nouvelle adresse URL [adresse URL]

Explication : n/a

Action de l'utilisateur : n/a

CRWAD1603I Impossible de se connecter au serveur glass box : [nom du serveur]

Explication : n/a

Action de l'utilisateur : n/a

CRWAD1604I Le test glass box <ID> (<nom>) est POSITIF sur : <URL> <paramètre>

Explication : n/a

Action de l'utilisateur : n/a

CRWAD1605I Le test glass box <ID> (<nom>) est négatif sur : <URL> <paramètre>

Explication : n/a

Action de l'utilisateur : n/a

CRWAD1606I La demande de test glass box <URL> a échoué en raison d'une erreur de communication : <Description de l'erreur>

Explication : Les explications possibles sont les suivantes :

- La connexion est impossible
  - L'hôte distant refuse la connexion
  - L'hôte distant est arrêté
  - Le réseau n'est pas disponible
- Le délai de connexion est dépassé
  - Aucune réponse n'a été reçue du serveur dans la limite de temps
- La connexion est fermée (à distance)
  - L'application a tenté de garder active une connexion dont le délai d'attente est déjà dépassé
  - La connexion a été réinitialisée par l'homologue distant
- La connexion est fermée (en local)
  - La connexion a été interrompue par le fournisseur de connecteur sous-jacent
  - L'opération de chevauchement a été abandonnée à cause de la fermeture du connecteur
  - Trop de connecteurs sont ouverts dans le fournisseur de connecteur sous-jacent
- Inconnu(e)
  - Toute autre raison

Action de l'utilisateur : n/a

CRWAD1607I Envoi du test glass box <ID> (<nom>) sur : <URL> <paramètre>

Explication : n/a

Action de l'utilisateur : n/a

CRWAD1608I Extraction des résultats de la collecte glass box

Explication : n/a

Action de l'utilisateur : n/a

CRWAD1609I Extraction des résultats des paramètres non référencés de glass box

Explication : n/a

Action de l'utilisateur : n/a

CRWAD1610I Glass box : La surveillance des paramètres non référencés a été lancée.

Explication : n/a

Action de l'utilisateur : n/a

CRWAD1611I Glass box : La surveillance des paramètres non référencés a été arrêtée.

Explication : n/a

Action de l'utilisateur : n/a

CRWAD1612I Glass box : La surveillance de la collecte a été lancée.

Explication : n/a

Action de l'utilisateur : n/a

CRWAD1613I Glass box : La surveillance de la collecte a été arrêtée.

Explication : n/a

Action de l'utilisateur : n/a

CRWAD1614I Détection du système d'exploitation ou de la version du système d'exploitation ou du serveur Web de l'agent glass box.

Explication : Message d'information indiquant qu'AppScan a détecté cette information sur l'hôte de l'agent glass box.

Action de l'utilisateur : n/a

CRWAD1615I Lecteur basé sur les actions démarré.

Explication : n/a

Action de l'utilisateur : n/a

CRWAD1616I Fin d'exécution du lecteur basé sur les actions [SUCCESS]

Explication : n/a

Action de l'utilisateur : n/a

CRWAD1617I Fin d'exécution du lecteur basé sur les actions [FAILED]

Explication : n/a

Action de l'utilisateur : n/a

CRWAD1618I Echec de la connexion du lecteur basé sur les actions, retour à une connexion basée sur les demandes.

Explication : AppScan n'est pas parvenu à se connecter à l'aide de l'enregistrement de connexion reposant sur une action, et désormais, il utilisera la version reposant sur une demande.

Action de l'utilisateur : Essayez de réviser ou de réenregistrer la séquence de connexion basée sur les actions pour résoudre le problème.

AppScan Messages des journaux

Les sections suivantes fournissent des explications sur les messages consignés dans le journal AppScan (Aide > Journal AppScan)

Actuellement, seuls les messages les plus importants du journal AppScan sont documentés dans cette section. Le cas échéant, des explications et actions utilisateur suggérées sont incluses.

CRWAD3000E Entrée de registre AppScan <nom de clé> incorrecte.

Explication : n/a

Action de l'utilisateur : n/a

CRWAD3002I Option de configuration avancée définie. ID : <ID> = valeur <valeur>.

Explication : n/a

Action de l'utilisateur : n/a

CRWAD3003E Option de configuration avancée non définie à la suite d'une erreur. ID : <#>, valeur <valeur>.

Explication : AppScan n'a pas pu appliquer une modification de la configuration avancée faite par l'utilisateur à cause d'un format non valide (ID et valeur définis).

Action de l'utilisateur : Localisez le paramètre de configuration par son ID et corrigez la valeur.

CRWAD3010I Version d'AppScan : <#> (Numéro de génération : <#>, Version des règles de sécurité : <#>)

Explication : n/a

Action de l'utilisateur : n/a

CRWAD3100I Nouveau processus AppScan démarré.

Explication : n/a

Action de l'utilisateur : n/a

CRWAD3101I Fermeture d'AppScan.

Explication : n/a

Action de l'utilisateur : n/a

CRWAD3102I Le port du proxy AppScan est <numéro de port>.

Explication : n/a

Action de l'utilisateur : n/a

CRWAD3103I Le port du proxy flash d'AppScan est <numéro de port>.

Explication : n/a

Action de l'utilisateur : n/a

CRWAD3104I Démarrage de l'étape d'exploration sur l'hôte ou les hôtes <hôte(s)>.

Explication : n/a

Action de l'utilisateur : n/a

CRWAD3105I Reprendre la phase d'exploration.

Explication : n/a

Action de l'utilisateur : n/a

CRWAD3106I Phase d'exploration arrêtée par l'utilisateur.

Explication : n/a

Action de l'utilisateur : n/a

CRWAD3107I Phase d'exploration terminée.

Explication : n/a

Action de l'utilisateur : n/a

CRWAD3108I Effacement des données d'exploration et de test.

Explication : n/a

Action de l'utilisateur : n/a

CRWAD3109I Création d'une nouvelle analyse.

Explication : n/a

Action de l'utilisateur : n/a

CRWAD3200I Démarrage de l'étape de test sur l'hôte ou les hôtes <hôte(s)>.

Explication : n/a

Action de l'utilisateur : n/a

CRWAD3201I Reprendre la phase de test.

Explication : n/a

Action de l'utilisateur : n/a

CRWAD3202I Phase de test arrêtée par l'utilisateur.

Explication : n/a

Action de l'utilisateur : n/a

CRWAD3203I Phase de test terminée.

Explication : n/a

Action de l'utilisateur : n/a

CRWAD3204I Suppression des données de la phase de test.

Explication : n/a

Action de l'utilisateur : n/a

CRWAD3205I Importation des données d'exploration depuis <chemin>.

Explication : n/a

Action de l'utilisateur : n/a

CRWAD3300W Echec de l'importation de données d'exploration depuis le fichier : <chemin du fichier>.

Explication : n/a

Action de l'utilisateur : n/a

CRWAD3407E La vérification de la licence a échoué ! Message d'erreur RCL (le cas échéant) : <message>

Explication : Motifs possibles : 1) La licence a expiré, 2) Aucune licence flottante n'est disponible, 3) Il est impossible de se connecter au serveur de clés de licence pendant plus de 3 jours. Le message RCL (Rational Common Licensing) peut contenir plus de détails sur le motif du problème.

Remarque : Dans certains cas, le message RCL peut être indisponible.

Action de l'utilisateur : n/a

CRWAD3409W Licence non disponible pour l'hôte <hôte>.

Explication : n/a

Action de l'utilisateur : Mettez votre licence à jour (Aide > Licence) pour inclure l'hôte indiqué ou supprimez l'hôte de la liste des hôtes supplémentaires (Configuration des examens > URL et serveurs > Serveurs et domaines supplémentaires).

CRWAD3410W Serveur de licences non disponible. Exécution en mode déconnecté autorisée pendant 3 jours. Message RCL : <message>

Explication : Lorsqu'AppScan ne parvient pas à se connecter au serveur de clés de licence pour vérifier la validité d'une licence flottante, il peut continuer de s'exécuter en mode déconnecté pendant 3 jours. Passé ce délai, s'il n'arrive toujours pas à se connecter pour vérifier la licence, les examens sont désactivés pour tous les sites, excepté demo.testfire.com. Le message RCL (Rational Common Licensing) peut contenir plus de détails sur le motif du problème.

Action de l'utilisateur : n/a

CRWAD3411I Licence extraite.

Explication : n/a

Action de l'utilisateur : n/a

CRWAD3500E Une erreur interne AppScan est survenue. Un fichier de vidage a été créé dans <chemin du fichier>. Contactez le support.

Explication : Une erreur interne critique est survenue, ce qui a entraîné l'arrêt d'AppScan. Le fichier de vidage de mémoire peut aider à déterminer la cause du problème.

Action de l'utilisateur : Prenez contact avec le service de support et fournissez au fichier de vidage toute autre information appropriée.

CRWAD3501E Une erreur interne AppScan est survenue. Tentative de sauvegarde de l'examen.

Explication : Une erreur interne critique s'est produite. AppScan a tenté de sauvegarder l'examen avant sa fermeture. Si la sauvegarde a réussi, le chemin de l'examen sauvegardé apparaîtra ultérieurement dans le journal.

Action de l'utilisateur : n/a

CRWAD3502E Sauvegarde de la récupération automatique réussie. L'examen récupéré a été sauvegardé sur : <chemin du fichier>

Explication : AppScan a réussi à sauvegarder un examen après une erreur critique. L'examen se trouve au chemin indiqué.

Action de l'utilisateur : Tentez de charger le fichier d'examen sauvegardé et poursuivez l'examen.

CRWAD3503E Echec de la tentative de sauvegarder l'examen avant de s'arrêter.

Explication : AppScan n'est pas parvenu à sauvegarder un fichier d'examen avec récupération automatique avant de s'arrêter.

Action de l'utilisateur : Contactez le support.

CRWAD3600E Le fichier de règles est endommagé.

Explication : Le fichier de règles de sécurité qui définit les tests AppScan est endommagé.

Action de l'utilisateur : Contactez le support.

CRWAD3601E Le fichier de règles défini par l'utilisateur est endommagé.

Explication : Le fichier de règles de sécurité, qui définit les tests définis par l'utilisateur, est endommagé.

Action de l'utilisateur : Contactez le support.

CRWAD3602W Certains problèmes de sécurité dans l'examen chargé ont été supprimés car des règles manquent.

Explication : n/a

Action de l'utilisateur : n/a

CRWAD3707I Le serveur <nom> ne répond pas.

Explication : n/a

Action de l'utilisateur : n/a

CRWAD3708I Le serveur <nom> répond à nouveau.

Explication : n/a

Action de l'utilisateur : n/a

CRWAD3709I Le proxy <nom> ne répond pas.

Explication : n/a

Action de l'utilisateur : n/a

CRWAD3703E Connexion impossible au serveur {0} pour la raison suivante : le certificat SSL n'est pas valide.

Explication : AppScan a été configuré par l'utilisateur pour rejeter les connexions aux serveurs dont le certificat SSL n'est pas valide. Le certificat SSL du serveur d'applications n'est pas valide, une connexion n'a donc pas pu être établie.

Action de l'utilisateur : Si vous n'êtes pas concerné par une attaque de l'homme du milieu ou autre, vous pouvez désactiver cette modification de configuration. Accédez à **Outils > Options > onglet Avancé**, recherchez l'entrée pour HttpsIgnoreCertErrors et changez cette valeur à False.

CRWAD3710I Le proxy <nom> répond à nouveau.

Explication : n/a

Action de l'utilisateur : n/a

CRWAD3800E Erreur fatale : le fichier d'examen <chemin du fichier> est endommagé.

Explication : Impossible de charger un fichier d'examen.

Action de l'utilisateur : Contactez le support.

CRWAD3801E AppScan n'est pas parvenu à charger la session. Il se peut que le fichier de session soit endommagé ou ne soit pas valide.

Explication : L'ouverture du fichier d'examen a abouti

mais AppScan n'est pas parvenu à charger une session à partir de celui-ci.

Action de l'utilisateur : Contactez le support.

CRWAD3806I Sauvegarde de l'examen dans le fichier suivant : <chemin complet>

Explication : n/a

Action de l'utilisateur : n/a

CRWAD3807I Sauvegarde de l'examen dans le fichier <chemin complet> terminée

Explication : n/a

Action de l'utilisateur : n/a

CRWAD3808I Chargement de l'examen depuis le fichier suivant : <chemin complet>

Explication : n/a

Action de l'utilisateur : n/a

CRWAD3809I Chargement de l'examen depuis le fichier <chemin complet> terminé

Explication : n/a

Action de l'utilisateur : n/a

CRWAD3810I Chargement de l'examen avec la version <version d'origine>, mise à jour vers la version en cours <version en cours>

Explication : n/a

Action de l'utilisateur : n/a

CRWAD3811E Chargement de l'examen avec la version {0}, ultérieure à la version en cours {1}

Explication : L'examen chargé a été créé dans une version (spécifiée) ultérieure à la version en cours (spécifiée). Le chargement de l'examen peut échouer.

Action de l'utilisateur : n/a

CRWAD3813E Echec de la sauvegarde de l'examen <chemin du fichier> car l'espace disque est insuffisant.

Explication : La taille des fichiers temporaires créés lors d'un examen AppScan peut atteindre la taille de l'examen lui-même. Tous les dossiers temporaires doivent donc disposer de cette capacité. La taille d'un examen dépend du site examiné, du modèle, de la configuration et des problèmes trouvés.

Action de l'utilisateur : Voir «Espace disque insuffisant», à la page 332

CRWAD3814E Impossible de sauvegarder l'examen <chemin du fichier>, car le fichier d'examen est accessible en lecture seule.

Explication : n/a

Action de l'utilisateur : n/a

CRWAD3816E AppScan n'est pas parvenu à charger l'examen car l'espace disque est insuffisant. Libérez <#> Mo sur l'unité <identificateur d'unité> et essayez à nouveau.

Explication : La taille des fichiers temporaires créés lors d'un examen AppScan peut atteindre la taille de l'examen lui-même. Tous les dossiers temporaires doivent donc disposer de cette capacité. La taille d'un examen dépend du site examiné, du modèle, de la configuration et des problèmes trouvés.

Action de l'utilisateur : Voir «Espace disque insuffisant», à la page 332

CRWAD3817W Régénération de la base de données des résultats SDK depuis le moteur de base de données.

Explication : La base de données des résultats SDK est introuvable. AppScan la régénère à partir du moteur de base de données.

Action de l'utilisateur : n/a

CRWAD3818E Chargement de l'examen avec la version de base de données {n} ; cette version n'est pas prise en charge.

Explication : L'examen a été sauvegardé à l'aide d'une version de base de données AppScan non prise en charge et il ne peut pas être chargé dans la version AppScan en cours.

Action de l'utilisateur : n/a

CRWAD4105E L'unité d'exécution critique (<nom de l'unité d'exécution>, ID de l'unité d'exécution : <ID d'unité d'exécution>) a pris fin de façon inattendue.

Explication : Une erreur interne critique s'est produite.

Action de l'utilisateur : Contactez le support.

CRWAD4106E L'unité d'exécution non critique (<nom de l'unité d'exécution>, ID de l'unité d'exécution : <ID d'unité d'exécution>) a pris fin de façon inattendue.

Explication : Une erreur interne critique s'est produite.

Action de l'utilisateur : Contactez le support.

CRWAD4300I Démarrage du mode de support étendu AppScan.

Explication : n/a

Action de l'utilisateur : n/a

CRWAD4301I Le mode de support étendu AppScan est déjà <activé/désactivé>.

Explication : n/a

Action de l'utilisateur : n/a

CRWAD4302I Mode de support étendu AppScan arrêté.

Explication : n/a

Action de l'utilisateur : n/a

CRWAD4303I Echec du conditionnement des informations de support étendu dans le fichier suivant : <chemin complet>

Explication : n/a

Action de l'utilisateur : n/a

CRWAD4500E AppScan s'est arrêté car l'espace disque est insuffisant. [Espace libre : <#> Mo, Espace requis : <#> Mo]

Explication : La taille des fichiers temporaires créés lors d'un examen AppScan peut atteindre la taille de l'examen lui-même. Tous les dossiers temporaires doivent donc disposer de cette capacité. La taille d'un examen dépend du site examiné, du modèle, de la configuration et des problèmes trouvés.

Action de l'utilisateur : Voir «Espace disque insuffisant», à la page 332

CRWAD4501E AppScan s'est arrêté car l'utilisation de la mémoire a atteint la limite prédéfinie. [Utilisation de la mémoire : <#> Mo, Utilisation maximale de la mémoire : <#> Mo]

Explication : n/a

Action de l'utilisateur : Augmentez la limite de mémoire (Outils > Options avancées) ou prenez contact avec le support technique.

CRWAD4502E AppScan s'est arrêté car le système dispose d'une quantité de mémoire virtuelle faible. [Mémoire virtuelle : <#> Mo, Mémoire virtuelle disponible : <#> Mo]

Explication : n/a

Action de l'utilisateur : Fermez d'autres applications pour libérer de la mémoire.

CRWAD4503E Quantité de mémoire système faible - Il se peut qu'AppScan ne puisse pas continuer à fonctionner correctement. [Utilisation de la mémoire : <#> Mo, Mémoire physique totale : <#> Mo]

Explication : n/a

Action de l'utilisateur : Fermez d'autres applications pour libérer de la mémoire.

CRWAD5002E Echec de l'importation de la configuration XML. Erreur d'analyse (si disponible) : %s

Explication : La configuration n'a pas pu être envoyée au moteur. Il n'est pas possible de poursuivre l'examen.

Action de l'utilisateur : Contactez le support.

CRWAD5003I Application de la configuration modifiée de l'examen au moteur.

Explication : n/a

Action de l'utilisateur : n/a

CRWAD5004E Echec de l'analyse syntaxique de la configuration XML.

Explication : La configuration n'a pas pu être envoyée au moteur. Il n'est pas possible de poursuivre l'examen.

Action de l'utilisateur : Contactez le support.

CRWAD5100E Erreur AppScan grave : %s

Explication : n/a

Action de l'utilisateur : n/a

CRWAD5101E Une exception logicielle est survenue :<message> Pile d'appels : <pile>

Explication : n/a

Action de l'utilisateur : n/a

CRWAD5400I Version du serveur glass box <URL> : Version de l'agent : <#> ; Version GBootStrap : <#> ; Version des règles de l'agent : <#>

Explication : n/a

Action de l'utilisateur : n/a

CRWAD5401E Connexion impossible au serveur glass box {0} car le serveur sur lequel l'agent est installé ou l'adresse URL de l'application d'agent n'est pas accessible.

Explication : AppScan n'a pas réussi à se connecter au serveur glass box pour l'une des raisons indiquées. L'adresse URL de l'agent peut être incorrecte, ou GBootStrap n'est pas en cours d'exécution, ou le serveur est arrêté.

Action de l'utilisateur : Vérifiez que le serveur est en cours d'exécution et que l'adresse URL de l'agent que vous avez entrée est correcte. Utilisez votre navigateur Web pour ouvrir l'adresse URL de l'agent pour vérifier que GBootStrap s'exécute correctement. Si cette procédure ne résout pas le problème, contactez le service d'assistance technique.

CRWAD5402E Connexion impossible au serveur glass box {0} car les données d'identification de connexion à l'agent glass box n'ont pas été indiquées ou ne sont pas correctes.

Explication : Les données d'identification fournies pour accéder à l'agent glass box n'ont pas été indiquées ou ne sont pas correctes.

Action de l'utilisateur : Veuillez fournir le nom d'utilisateur et le mot de passe corrects définis lors de l'installation de l'agent glass box.

CRWAD5403E Connexion impossible au serveur glass box {0} car aucun agent n'est installé à l'adresse URL de l'agent glass box spécifié.

Explication : L'adresse URL mène vers un site qui n'est pas la racine GBootStrap de l'agent glass box.

Action de l'utilisateur : Vérifiez l'URL. Par défaut, il s'agit généralement de :

```
http://<server_name>:<port_number>/GBootStrap/
```

CRWAD5404E Connexion impossible au serveur glass box {0} car l'instrumentation de l'agent glass box n'a pas démarré.

Explication : L'agent glass box n'est pas instrumenté sur le serveur spécifié.

Action de l'utilisateur :

1. Arrêtez puis redémarrez le serveur en utilisant le raccourci du bureau, si ce dernier a été créé lors de l'installation de l'agent.
2. Réinstallez manuellement l'agent de la glass box (voir «Installation de l'agent glass box», à la page 166).

CRWAD5405E Connexion impossible au serveur glass box {0} car la version du client {1} est antérieure à celle du fichier de l'agent glass box {2} ou à celle de la version de l'application de l'agent glass box {3}.

Explication : La version d'AppScan sur la machine locale n'est pas à jour.

Action de l'utilisateur : Installez la dernière version d'AppScan.

CRWAD5406E Connexion impossible au serveur glass box {0} car la version du fichier de l'agent glass box {1} et la version de l'application de l'agent glass box {2} sont antérieures à la version du client glass box {3}.

Explication : La version de l'agent glass box n'est pas à jour.

Action de l'utilisateur : Installez la dernière version de l'agent glass box sur le serveur.

CRWAD5407E Connexion impossible au serveur glass box {0} car la version de l'application de l'agent glass box {1} est antérieure à la version du client glass box {2}.

Explication : Vous avez peut-être installé manuellement l'agent glass box et omis de déployer GBootStrap.war.

Action de l'utilisateur : Suivez exactement les instructions d'installation manuelle de l'agent glass box sur votre serveur. Voir «Installation de l'agent glass box», à la page 166.

CRWAD5408E Connexion impossible au serveur glass box {0} car la version du fichier de l'agent glass box {1} est antérieure à la version du client glass box {2}.

Explication : La version du fichier JAR de l'agent glass box est antérieure à la version AppScan.

Action de l'utilisateur : Vous avez simplement omis de redémarrer le serveur après avoir installé l'agent. Essayez de redémarrer le serveur. Si cela n'a pas de résultat, réinstallez l'agent glass box.

CRWAD5409E Connexion impossible au serveur glass box {0} car la version des règles de l'agent glass box {1} est antérieure à la version des règles du client glass box {2}.

Explication : Les règles de la glass box ne sont pas à jour.

Action de l'utilisateur :

1. Accédez à **AppScan > Aide > Rechercher les mises à jour**.
   - Si un téléchargement est disponible, il est téléchargé automatiquement sur la machine et installé.
   - Si un téléchargement n'est pas disponible, consultez Fix Central pour trouver la version la plus récente et installez-la.
2. Pour mettre à jour les règles d'agent sur le serveur, ouvrez **Outils > Gestion de l'agent glass box**, puis cliquez deux fois sur le serveur souhaité. Dans la boîte de dialogue qui s'affiche, cliquez sur **Mettre à jour les règles**.
3. Redémarrez le serveur d'applications pour que la modification prenne effet.

CRWAD5410E Connexion impossible au serveur glass box {0} car les règles de l'agent glass box ont été mises à jour et un redémarrage est requis pour terminer le processus de mise à jour.

Explication : Les règles de l'agent glass box ont été mises à jour, et le serveur doit à présent être redémarré pour charger les nouvelles règles d'instrumentation.

Action de l'utilisateur : Redémarrez le serveur.

CRWAD5411E Connexion impossible au serveur glass box {0} car la version des règles du client glass box {1} est antérieure à la version des règles de l'agent glass box {2}.

Explication : Les règles de l'agent glass box ont été mises à jour, et le serveur doit à présent être redémarré pour charger les nouvelles règles d'instrumentation.

Action de l'utilisateur :

1. Accédez à **AppScan > Aide > Rechercher les mises à jour**.
   - Si un téléchargement est disponible, il est téléchargé automatiquement sur la machine et installé.
   - Si un téléchargement n'est pas disponible, consultez Fix Central (http://www.ibm.com/support/fixcentral/) pour trouver la version la plus récente et installez-la.
2. Redémarrez le serveur d'applications pour que la modification prenne effet.

CRWAD5412E Connexion impossible au serveur glass box {0} car le certificat SSL n'est pas valide.

Explication : AppScan a été configuré par l'utilisateur pour rejeter les connexions aux serveurs dont le certificat SSL n'est pas valide. Le certificat SSL du serveur glass box n'est pas valide, une connexion n'a donc pas pu être établie.

Action de l'utilisateur : Si vous n'êtes pas concerné par une attaque de l'homme du milieu ou autre, vous pouvez désactiver cette modification de configuration. Accédez à **Outils > Options > onglet Avancé**, recherchez l'entrée pour HttpsIgnoreCertErrors et changez cette valeur à False.

Messages du journal Flash

Le tableau qui suit indique comment utiliser le journal Flash pour le traitement des incidents.

Le journal Flash contient des messages qui peuvent vous aider à traiter les incidents. Il se trouve à l'emplacement suivant :

```
...[AppScan Standard installation folder]\Logs\AppScanFlashBrowser.log
```

Messages d'erreur

Message d'erreur	Action possible de l'utilisateur
`Explore Failed: Couldn't reach initial state!`	Tentez d'augmenter la valeur du paramètre **Configuration > Configuration avancée > Délai d'attente de chargement du film**

Message d'erreur	Action possible de l'utilisateur
Movie (NAME) load failed! (TIME) miliseconds timeout, (COUNT) try(s).	Tentez d'augmenter la valeur du paramètre **Configuration > Configuration avancée > Délai d'attente de chargement du film**
current state failed, since Movie is not ready!	Tentez d'augmenter la valeur du paramètre **Configuration > Configuration avancée > Délai d'attente de chargement du film**
Exception while sending status! (MESSAGE). Microsoft .NET framework Hotfix required! Contact IBM Support. Hotfix reference http://support.microsoft.com/kb/971521	Prenez contact avec le support pour obtenir ce correctif logiciel.
Movie(NAME) version (NUMBER) not supported!	Recompilez le film pour qu'il soit au moins à la version 7.
Exception in Document Completed at URL(URL)! (MESSAGE)	Prenez contact avec le support pour obtenir la bonne version de mshtml.dll.
Flash Player not Found!	Voir «Mise à niveau de Flash Player», à la page 7
Flash Player version not Supported!	Voir «Mise à niveau de Flash Player», à la page 7
Flash Player not configured!	Voir «Configuration de Flash Player», à la page 7
Exception while trying to load SWF file!	Voir «Certains films Flash ne sont pas examinés», à la page 343

Messages d'avertissement

Message d'avertissement	Action possible de l'utilisateur
Explore movie (NAME) stopped! Click limit (VALUE) reached.	Tentez d'augmenter la valeur du paramètre **Configuration des examens > Options d'exploration > Limite de clic**.
Explore movie (NAME) Stopped! Screen limit (VALUE) reached.	Tentez d'augmenter la valeur du paramètre **Configuration des examens > Options d'exploration > Limite d'écran**.
Exception while loading unsupported Flash Movie! (MESSAGE)	Republiez le film avec Flash version 7 ou supérieure.
Parsing data from bridge failed due to unsupported movie(NAME)!	Republiez le film avec Flash version 7 ou supérieure.
Exception while parsing data from bridge in unsupported movie(NAME)!	Republiez le film avec Flash version 7 ou supérieure.
Movie (NAME) not supported!	Republiez le film avec Flash version 7 ou supérieure.
Document Complete event not received from Browser!	Lisez le film dans une version autonome d'Internet Explorer. Si le message "Done" ne s'affiche pas à gauche dans la barre d'état, le lien situé dans la page HTML du fichier SWF est peut-être brisé.
Movie (NAME) failed to load in (TIME) miliseconds for (NUMBER) try(s)! Reloading...	Tentez d'augmenter la valeur du paramètre **Configuration > Configuration avancée > Délai d'attente de chargement du film**
No Browse Dialog found!	Revérifiez les chaînes définies dans **Configuration avancée > Flash : Chaîne de téléchargement vers l'amont de fichier** ou **Flash : Chaîne de téléchargement vers l'aval de fichier**. Supprimez les chaînes qui n'identifient pas une commande de téléchargement.

Message d'avertissement	Action possible de l'utilisateur
`Exception while trying to create file for upload! (MESSAGE)`	Aucun fichier n'a été configuré en vue d'un envoi par téléchargement. Configurez-en un dans **Configuration avancée > Flash : Chemin de téléchargement vers l'amont de fichier**.

Traitement des incidents glass box

Ouvrez une page Web répertoriant les messages d'agent glass box et d'autres conseils de traitement des incidents.

http://www.ibm.com/support/docview.wss?uid=swg21567723

Chapitre 15. Interface de ligne de commande

La présente section décrit la syntaxe et les options disponibles avec l'interface de ligne de commande.

Certaines fonctions d'AppScan peuvent être exécutées à l'aide de l'interface de ligne de commande (CLI), en tapant une commande à l'invite plutôt qu'en utilisant l'interface graphique. Cela peut s'avérer très utile lorsque vous devez contrôler automatiquement AppScan à partir d'un script ou d'un fichier de traitement par lots.

Important : L'utilisation de l'interface de ligne de commande requiert les privilèges d'administrateur.

Structure des commandes

Les commandes de l'interface CLI d'AppScan comportent trois parties :

1. La commande d'utilitaire : `AppScanCMD`
2. La commande spécifique à exécuter, par exemple : `exec`
3. L'option requise pour la commande sélectionnée, par exemple :
   `/base_scan <full path>/d <full path>`

Dans l'exemple ci-dessus, la commande complète est :

```
AppScanCMD exec /base_scan <full path> /d <full path>
```

(Cette commande exécute un nouvel examen à l'aide de la configuration de l'examen de base sélectionné et enregistre les résultats dans l'emplacement spécifié.)

Remarque : Les commandes peuvent être entrées sans préfixe (par exemple `exec`), avec un signe moins (par exemple `-exec`) ou avec une barre oblique (par exemple `/exec`). Par souci de simplicité, les exemples de cette section sont tous sans préfixe.

Remarque : Les options de commande doivent comporter comme préfixe *soit* un signe moins (par exemple `-base_scan`) *soit* une barre oblique (par exemple `/base_scan`). Par souci de simplicité, les exemples suivants ont tous une barre oblique comme préfixe.

Commandes

Cette section décrit les commandes spécifiques de l'application pouvant être exécutées à l'aide de l'interface CLI.

Commande Exec

La commande `exec` crée un nouvel examen avec l'URL de départ définie (dans `/starting_url`, `/base_scan` ou `/scan_template`), l'exécute et l'enregistre. Elle peut aussi être utilisée pour générer et sauvegarder un rapport de l'examen.

Pour exécuter la commande `exec`, entrez `exec`, `ex` ou `e` à l'invite de commande suivi des options de commande requises, tel que décrit ci-dessous.

Remarque : Si aucune commande n'est spécifiée, la commande exec s'exécute par défaut.

Paramètres

Les paramètres suivants peuvent être inclus dans la commande exec.

Paramètre	Explication
`/starting_url | /surl | /su <full_path>`	Définit l'URL de départ de l'examen. Si l'URL de départ est définie dans le modèle d'examen ou dans l'examen de base, il n'est pas nécessaire de la définir ici.
`/credentials | /cred | /cr <username:password>`	Spécifie la connexion automatique et définit le nom d'utilisateur et le mot de passe. Ceci remplace toute connexion configurée dans le fichier SCANT (s'il est utilisé).
`/base_scan | /base | /b <full_path>`	Définit un examen source (doit inclure un chemin complet), dont la configuration sera utilisée pour le nouvel examen.
`/dest_scan | /dest | /d <full_path>`	Définit la destination de l'enregistrement du nouvel examen (doit inclure un chemin complet). Si aucun chemin n'est indiqué, l'examen est enregistré dans un répertoire temporaire, et AppScanCMD vous indique son nom et son emplacement exact.
`/scan_template | /stemplate | /st <full_path>`	Définit le fichier de modèle d'examen.

`/old_host | /ohost | /oh <full_path>`
 	
`/new_host | /nhost | /nh <full_path>`
	Ces deux paramètres vous permettent de chercher et de remplacer un hôte par un autre, dans un examen de base.

`/login_file | /lfile | /lf <full_path>`	Importe une séquence de connexion sauvegardée.
`/multi_step_file | /mstepfile | /mf <full_path>`	Importe un fichier d'opérations en plusieurs étapes.
`/manual_explore_file | /mexplorefile | /mef <full_path>`	Importe un fichier d'exploration manuelle (au format EXD, HAR, DAST.CONFIG ou CONFIG). **Remarque :** Dans AppScan Standard Version 9.0.1, les fichiers EXD incluent des données de réponse. Pour importer ces données, ajoutez l'indicateur `/ir`. Si cet indicateur n'est *pas* ajouté, les données de réponse ne seront pas importées et une étape d'exploration sera exécutée (les demandes enregistrées seront envoyées) afin de rassembler de *nouvelles* réponses à analyser pour le test.
`/policy_file | /pfile | /pf <full_path>`	Importe un fichier de stratégie de test.
`/additional_domains | /adomains | /ad <domain>`	Définit des domaines autres que l'URL de départ à inclure dans l'examen. S'il existe plusieurs domaines supplémentaires, séparez-les par une virgule ou ajoutez plusieurs instances du paramètre.
`/report_file | /rf <full_path>`	Spécifie la destination et le nom du rapport généré (doit inclure le chemin d'accès complet). Cette zone est facultative. Si elle n'est pas définie, aucun rapport n'est généré. Si `/rt` a pour valeur `rc_ase`, aucun fichier de rapport n'est nécessaire puisque la sortie est publiée dans AppScan Enterprise.
`/report_template | /rtemplate| /rtm <CliDefault | GuiDefault | Summary | DetailedReport | Developer | QA | SiteInventory>`	Indique les types d'informations qui figureront dans le rapport (voir «Rapports de sécurité», à la page 235). Modèle par défaut (si aucun modèle n'est indiqué) : `CliDefault`. Ce modèle *n'est pas* identique au modèle par défaut de la boîte de dialogue Rapports. Pour utiliser ce modèle, indiquez `GuiDefault`.

Paramètre	Explication
/report_type | /rt <xml|pdf|rtf|txt|html|rc_ase>	Définit le format du rapport. La valeur par défaut est XML. rc_ase fait référence aux rapports AppScan Enterprise et la sortie est publiée dans AppScan Enterprise à l'aide des paramètres existants (pour les voir, cliquez sur **Fichier > Exporter > Publier les résultats dans AppScan Enterprise > Paramètres de connexion**).
/ase_application_name | /aan <AppScan Enterprise application name>	Indique l'application AppScan Enterprise dans laquelle le rapport sera publié. Uniquement avec /report_type rc_ase
/min_severity | /ms <low|medium|high|informational>	Définit la gravité minimale des résultats à inclure aux rapports (rapports non xml seulement). La valeur par défaut est "low".
/test_type|/tt <All | Application | Infrastructure | ThirdParty>	Définit le type de test à inclure dans le rapport. La valeur par défaut est "All".

Indicateurs

Les indicateurs suivants peuvent être inclus dans la commande exec. Le fait de les inclure revient à les faire passer de False à True.

Indicateur	Explication
/continue | /c	Continue l'examen.
/explore_only | /eo	Exécute l'étape d'exploration uniquement.
/include_responses | /ir	Lorsque vous importez des données d'exploration manuelle (fichier EXD) contenant des données de réponse, incluez les réponses (avec /mef). **Remarque :** Dans AppScan Standard Version 9.0.1, les fichiers EXD incluent des données de réponse. Si vous ajoutez cet indicateur et que le fichier contient des données de réponse, il est utilisé lors de l'analyse pour le test. Si le fichier n'inclut *pas* de données de réponse, une étape d'exploration sera exécutée (les demandes enregistrées seront envoyées) afin de rassembler de *nouvelles* réponses à analyser pour le test.
/merge_manual_explore_requests | /mmer	Applique les paramètres de réglage de redondance d'étape d'exploration aux données d'exploration manuelle, pour éviter les demandes en double (avec /mef).
/multi-step | /mstep	Teste uniquement les opérations en plusieurs étapes.
/open_proxy | /oprxy| /opr /listening_port|/lport|/lp <port number> /save_only|/saveo|/so	Ouvre le proxy d'enregistrement AppScan. Par défaut, le port défini dans Outils > Options > Enregistrement du proxy est utilisé. Pour définir un autre port, utilisez /listening_port <port number>. Pour sauvegarder un fichier SCAN sans exécuter d'examen, utilisez /save_only|/saveo|/so Les fichiers SCAN sont des fichiers ZIP contenant plusieurs fichiers de composant, notamment des séquences d'exploration manuelle qui sont sauvegardées en tant que fichiers Manual_Explore_#.exd individuels (où "#" est un numéro séquentiel). Les fichiers EXD peuvent être importés dans un autre examen.

Indicateur	Explication
/scan_log | /sl	Affiche le journal de l'examen pendant l'examen.
/test_only | /to	Exécute l'étape de test uniquement.
/verbose | /v	Ajoute les lignes de progression dans la sortie.

Quelques exemples de commande complète sont présentés ci-dessous.

Exemple 1

Cette commande démarre un examen avec l'URL de départ définie, à l'aide du modèle d'examen standard.

```
appscancmd e /su http://demo.testfire.net.scan
```

Exemple 2

Cette commande démarre une étape d'exploration uniquement, avec l'URL de départ définie, à l'aide du modèle d'examen standard.

```
appscancmd e /su http://demo.testfire.net.scan /eo
```

Exemple 3

Cet examen inclut une exploration manuelle, des opérations en plusieurs étapes, une connexion enregistrée et une stratégie de test.

```
appscancmd e
/st D:\demo.testfire.net.scant
/d D:\demo.testfire.net.scan
/mef D:\ManualExplore.exd
/mf D:\MyMultistepOperation.seq
/lf D:\LoginSequence.login
/pf D:\MyTestPolicy.policy
```

Exemple 4 : Domaines additionnels

Plusieurs domaines supplémentaires peuvent être définis dans un paramètre `-additional_domains`, séparés par des virgules, ou dans des paramètres distincts.

```
appscancmd e
/st D:\demo.testfire.net.scant
/d D:\demo.testfire.net.scan
/mef D:\ManualExplore.exd
/ad demo.testfire.net1,demo.testfire.net2,demo.testfire.net3
/sl
```

OU

```
appscancmd e
/st D:\demo.testfire.net.scant
/d D:\demo.testfire.net.scan
/mef D:\ManualExplore.exd
/ad demo.testfire.net1
/ad demo.testfire.net2
/ad demo.testfire.net3
/sl
```

Exemple 5 : Modification des hôtes et des ports

Vous pouvez modifier l'hôte et le port du modèle d'examen ou de l'examen de base.

```
appscancmd e
/st D:\demo.testfire.net.scant
/d D:\demo.testfire.net.scan
/mef D:\ManualExplore.exd
/oh http://demo.testfire.net:80
/nh http://demo.testfire.net2:8090
```

Commande Report

La commande `report` charge un examen spécifié et génère un rapport de sécurité (pour plus d'informations, voir «Rapports de sécurité», à la page 235).

Pour exécuter cette commande, entrez `report`, `rep` ou `r` à l'invite de commande suivi des options de commande requises, tel que décrit ci-dessous. (Les paramètres d'examen de base et de destination sont obligatoires ; les autres paramètres sont facultatifs.)

Commandes	Explication
`/base_scan | /base | /b <full_path>`	Spécifie l'examen source à partir duquel le rapport doit être généré (doit inclure le chemin d'accès complet).
`/report_file | /rf <full_path>`	Spécifie la destination et le nom du rapport généré (doit inclure le chemin d'accès complet). **Conseil :** Si `/rt` a pour valeur `rc_ase`, aucun fichier de rapport n'est nécessaire puisque la sortie est publiée dans AppScan Enterprise.
`/report_template | /rtemplate| /rtm <CliDefault | GuiDefault | Summary | DetailedReport | Developer | QA | SiteInventory | CustomTemplateName>`	Indique les types d'informations qui figureront dans le rapport. Modèle par défaut (si aucun modèle n'est indiqué) : `CliDefault`. Ce modèle *n'est pas* identique au modèle par défaut de la boîte de dialogue Rapports. Pour utiliser ce modèle, indiquez `GuiDefault`. Si vous avez enregistré des modèles personnalisés, vous pouvez les indiquer aussi. Pour plus de détails, voir «Rapports de sécurité», à la page 235
`/report_type | /rt <xml|xml_report|pdf|rtf|txt|html|rc_ase>`	Spécifie le format de sauvegarde des résultats ou du rapport : **`xml`** Résultats d'examen complets, sauvegardés dans un fichier XML (il *ne s'agit pas* d'un rapport) **`xml_report`** Rapport structuré complet, sauvegardé dans un fichier XML **`pdf|rtf|txt|html`** Rapport structuré complet, sauvegardé au format PDF, RTF, TXT ou HTML **`rc_ase`** Publie la sortie dans AppScan Enterprise à l'aide des paramètres définis dans **Fichier > Exporter > Publier dans AppScan Enterprise > Paramètres de connexion**
`/ase_application_name | /aan <AppScan Enterprise application name>`	Indique l'application AppScan Enterprise dans laquelle le rapport sera publié. Uniquement avec `/report_type rc_ase`
`/min_severity | /ms <low|medium|high|informational>`	Définit la gravité minimale des résultats à inclure aux rapports (rapports non xml seulement). La valeur par défaut est "Information", ce qui signifie que tous les niveaux de gravité sont inclus dans le rapport.
`/test_type|/tt <All | Application | Infrastructure | ThirdParty>`	Définit le type de test à inclure dans le rapport. La valeur par défaut est "All".

Indicateurs

Les indicateurs suivants peuvent être inclus dans la commande du rapport.

Indicateur	Explication
/verbose | /v	Ajoute les lignes de progression dans la sortie.

Exemple 1

Cette commande publie les résultats de l'examen de base spécifié dans AppScan Enterprise.

```
report
-base_scan  "D:\demo.testfire.net.scan"
-report_type rc_ase
```

Exemple 2

Cette commande démarre un examen avec l'URL de départ définie, à l'aide du modèle d'examen standard.

```
report
-base_scan  "D:\demo.testfire.net.scan"
-report_file D:\SecurityReport.pdf
-report_type pdf
-Scan_Log
-min_severity "informational"
```

Commande Delta analysis report

La commande `delta analysis report` compare deux ensembles de résultats d'examens (pour plus de détails, voir «Rapport de l'analyse des écarts», à la page 251).

Pour exécuter cette commande, entrez `delta_analysis_report`, `delta_report` ou `dar` à l'invite de commande suivi des options de commande requises, tel que décrit ci-dessous.

Commandes	Explication
/base_scan | /base | /b <full_path>	Spécifie l'examen source à partir duquel le rapport doit être généré (doit inclure le chemin d'accès complet).
/target_scan | /target | /ts <full_path>	Spécifie l'examen cible auquel l'examen de base sera comparé (doit inclure le chemin d'accès complet).
/report_file | /rf <full_path>	Spécifie la destination et le nom du rapport généré (doit inclure le chemin d'accès complet).
/report_type | /rt <xml|pdf|rtf|txt|html>	Spécifie le format de sauvegarde du rapport.

Indicateurs

Les indicateurs suivants peuvent être inclus dans la commande du rapport.

Indicateur	Explication
/verbose | /v	Ajoute les lignes de progression dans la sortie.

Cette commande permet de générer un rapport XML comparant les résultats de deux examens spécifiés.

```
das
-b  "D:\demo.testfire.net_1.scan"
-ts  "D:\demo.testfire.net_2.scan"
-rf D:\DeltaAnalysisReport.xml
-rt xml_report
```

Autres commandes

Commande close_proxy

La commande `close_proxy` permet de fermer le proxy d'enregistrement AppScan s'il a été précédemment ouvert.

Pour exécuter la commande `close_proxy`, entrez `close_proxy`, `cprxy` ou `cpr` à l'invite de commande.

Commande help

La commande `help` imprime la syntaxe de commande décrite dans la présente section.

Pour exécuter la commande `help`, entrez `help` ou `h` à l'invite de commande.

Codes d'état de sortie

Lorsque AppScan s'exécute dans des scripts ou des fichiers de traitement par lots, le code d'état de sortie indique si une opération a réussi.

Code	Signification
0	Terminé avec succès
1	Le démarrage d'AppScan a échoué
2	Erreur de ligne de commande
3	Licence non valide
4	Le chargement a échoué.
5	L'examen a échoué.
6	Le rapport a échoué.
7	La sauvegarde a échoué.
8	Erreur générale

Lancement d'AppScan à partir de la ligne de commande

Procédure

A partir de la ligne de commande, tapez : `AppScan.exe` [<nomfichier>]

- Cette commande lance l'exécutable AppScan pour lancer l'interface graphique, et vous pouvez ajouter un paramètre facultatif pour appeler un fichier **.scan** ou .**scant**.
- Si vous incluez un nom de fichier dans la commande, l'examen donné ou le modèle d'examen est chargé dès que l'application démarre.

Chapitre 16. Menus, barres d'outils et raccourcis clavier

La présente section récapitule les menus principaux et les barres d'outils.

Menu Fichier

Utilisé pour la création, l'ouverture et la sauvegarde d'examens.

Commande	Cliquez pour :
Nouveau	Créer un nouvel examen.
Ouvert	Ouvrir un examen sauvegardé (.scan) ou un modèle d'examen (.scant). **Conseil :** Vous pouvez également ouvrir ces fichiers en glissant-déposant le dossier vers AppScan.
Enregistrer	Sauvegarder l'examen en cours ou le modèle d'examen.
Sauvegarder sous	Sauvegarder l'examen en cours ou le modèle d'examen sous un nouveau nom.
Exporter > Résultats de l'examen sous forme de XML	Exporter tous les résultats de l'examen sous forme d'un fichier XML destiné à être utilisé avec AppScan Enterprise. Il existe deux options, selon votre version d'AppScan Enterprise : • Pour ASE 9.0.3.1 et versions ultérieures • Pour les versions antérieures (existantes)
Exporter > Résultats d'examen au format de base de données	Exporter tous les résultats de l'examen sous forme de base de données relationnelle. L'option de la base de données exporte les résultats dans une structure de base de données Firebird. Il s'agit d'une source ouverte, et suit les normes ODBC et JDBC.
Exporter > Données d'examen croisé	Si vous avez défini des problèmes spécifiques en tant que Bruit (faux positif), vous pouvez exporter ces informations pour les utiliser dans des examens exécutés sur d'autres postes de travail. (Vous n'avez pas besoin de procéder à cette opération sur votre propre poste de travail car les informations sont automatiquement enregistrées et appliquées aux examens futurs.)
Exporter > Publier les résultats dans AppScan Enterprise	Exporter les résultats d'un examen AppScan Standard vers AppScan Enterprise, exécuter une étape de test sur ces derniers et compiler le résultat dans un rapport.
Exporter > Créer un travail dans AppScan Enterprise	Exporte un examen AppScan Standard vers AppScan Enterprise. Requiert AppScan Enterprise version 9.0 ou ultérieure.
Exporter > Créer un modèle d'examen dans AppScan Enterprise	Exporte une configuration AppScan Standard vers AppScan Enterprise sous la forme d'un modèle. Requiert AppScan Enterprise version 9.0 ou ultérieure.
Exporter > Télécharger l'examen dans Application Security on Cloud	Télécharge un fichier de configuration AppScan Standard (SCAN ou SCANT) vers Application Security on Cloud. Vous pouvez utiliser la configuration pour exécuter un examen complet ou utiliser les résultats existants de l'étape d'exploration sauvegardés dans le fichier et exécuter l'option Test uniquement.
Importer > Données d'exploration	Charger une exploration manuelle Les formats pris en charge sont EXD, HAR, DAST.CONFIG et CONFIG. **Remarque :** La v1 et la v2 des fichiers HAR (Archive HTTP) générés en externe sont prises en charge.
Importer > Données d'examen croisé	Si vous avez défini des problèmes spécifiques en tant que Bruit (faux positif) sur un autre poste de travail et les avez exportés, vous pouvez importer ces informations pour les utiliser dans des examens exécutés sur votre poste de travail afin que ces problèmes ne soient pas inclus aux résultats de l'analyse.

Commande	Cliquez pour :
Configuration de page	Définir la taille, la source, l'orientation et les marges du papier pour la commande Imprimer.
Aperçu avant impression	Ouvrir une fenêtre d'aperçu affichant l'arborescence de l'application ou la Liste des résultats (selon la position du curseur) telles qu'elles apparaîtront lorsqu'elles seront imprimées à l'aide de la commande Imprimer.
Imprimer	Imprimer le contenu en cours de l'arborescence de l'application *et* de la liste de résultats. (Tous les nœuds visibles lorsque vous faites défiler vers le haut ou vers le bas l'arborescence de l'application et la liste de résultats sont inclus, mais les nœuds fermés à l'écran apparaîtront également fermés sur la sortie imprimée.)
Noms de fichiers	Fichiers récemment utilisés.
Quitter	Quitte AppScan.

Menu Edition

Utilisé pour la personnalisation des résultats de l'examen.

Commande	Cliquez pour :
Supprimer	Supprimer le problème ou la résolution sélectionnés.
Gravité	(Vue Problèmes uniquement) Personnaliser le niveau de gravité du problème sélectionné.
Etat	(Vue Problèmes uniquement) Désigner le problème sélectionné comme "Bruit" (ce qui signifie que, bien qu'il soit classé comme problème par AppScan, il ne l'est pas dans le contexte de votre application.) Les problèmes désignés comme Bruit peuvent être supprimés des résultats ou affichés barrés (menu Affichage > Afficher les problèmes marqués comme bruit).
Priorité	(Vue Résolution uniquement) Modifier le niveau de priorité d'une résolution.
Rechercher	Rechercher des chaînes, des ID, un code HTTP, etc., dans les résultats de l'examen en cours. (Les options dépendent de l'une des trois vues actuellement sélectionnées.)

Remarque : La gravité et la priorité sont mutuellement exclusives ; une seule est visible à la fois, selon la vue sélectionnée.

Menu Affichage

Utilisé pour déterminer comment la fenêtre principale s'affiche et quelles données sont affichées.

Commande	Cliquez pour :
Problèmes de sécurité	Afficher la vue Problèmes de sécurité.
Tâches de résolution	Afficher la vue Tâches de résolution.
Données d'application	Afficher la vue Données d'application (demandes ayant échoué, URL visitées, paramètres de script, etc.).
Classer par >	Sélectionner une méthode de tri pour la Liste des résultats : Gravité/Résultat/Nom. Sélectionner **Ordre inverse** pour répertorier les résultats par ordre décroissant plutôt que croissant.
Présentation >	Sélectionner une présentation horizontale ou verticale des panneaux de la fenêtre principale.
Ecran d'accueil	Ouvrir l'écran d'accueil AppScan

Commande	Cliquez pour :
Afficher les problèmes marqués comme bruit	Les problèmes trouvés par AppScan qui ne sont pas appropriés dans le contexte de votre application et pouvant être marqués comme Bruit. Cet élément de menu bascule entre l'affichage de ces problèmes avec du texte barré ou aucun affichage. Lorsque cette option est sélectionnée, Bruit apparaît barré ; lorsqu'elle est désélectionnée, Bruit ne s'affiche pas. Voir «Etat du problème : Ouvert ou Bruit», à la page 209.
Variantes non vulnérables	Ouvre la liste des variantes définies comme non vulnérables. Voir «Variantes non vulnérables», à la page 226.
Journal d'examen	Ouvrir le journal de toutes les actions exécutées par AppScan lors de l'examen en cours. Voir «AppScan Journal», à la page 301.
Personnaliser la barre d'outils >	Sélectionner **Grandes icônes** pour afficher les icônes de la barre d'outils plus grandes. Sélectionner si la barre d'outils affiche le nom de chaque icône, des icônes sélectionnées (par défaut) ou d'aucune icône. (Dans tous les cas, lorsque vous passez la souris sur une icône, une infobulle affiche son nom.)

Menu Examen

Utilisé pour contrôler l'examen.

Commande	Cliquez pour :
Examen intégral	Démarrer un examen intégral (étape d'exploration et étape de test) ou reprend l'exécution d'un examen interrompu.
Pause	Interrompre un examen en cours (qu'il s'agisse d'un examen intégral, d'une exploration uniquement ou d'un test uniquement). Vous pouvez reprendre l'examen ultérieurement. Vous pouvez également sauvegarder un examen interrompu pour poursuivre ultérieurement.
Nouvel examen >	Exécuter de nouveau l'examen en cours ou une étape de l'examen. Sélectionnez l'un des éléments du sous-menu : Nouvel examen (intégral) : Supprimer tous les résultats de l'examen et exécuter un examen intégral à l'aide de la configuration en cours. Nouvelle exploration : Supprimer tous les résultats d'examen et exécuter une étape d'exploration uniquement à l'aide de la configuration en cours. Nouveau test : Supprimer les résultats du test et exécuter une nouvelle étape de test à l'aide de la configuration en cours et des résultats de l'exploration.
Exploration uniquement	Exécuter une étape d'exploration uniquement, sans poursuivre avec l'étape de test.
Exploration manuelle	Explorer votre site manuellement. Voir «Utilisation d'AppScan», à la page 143
Exploration des services Web (WSDL)	Ouvrir GSC (Generic Service Client) de sorte que l'application peut être explorée manuellement. Les demandes et réponses sont alors utilisées lors de l'étape de test.
Test uniquement	Exécuter une étape de test uniquement (ou poursuivre un test interrompu), sans exécuter auparavant l'étape d'exploration. Cette option est uniquement active lorsqu'il existe déjà des résultats d'exploration.

Commande	Cliquez pour :
Tester les opérations en plusieurs étapes uniquement	Si vous avez configuré une ou plusieurs opérations en plusieurs étapes (voir «Vue Opérations en plusieurs étapes», à la page 95), et si elles constituent un sous-ensemble significatif de votre site pour lequel vous souhaitez procéder à un examen, vous pouvez tester ces séquences uniquement. Pour plus de détails, voir «Examiner uniquement les opérations en plusieurs étapes», à la page 192. Scan Expert ne s'exécute pas automatiquement avant cette fonction, même s'il a été configuré pour s'exécuter avant les examens. Si nécessaire, exécutez-le séparément avant l'examen des opérations en plusieurs étapes uniquement (Outils > Exécuter une évaluation Scan Expert).
Retester les problèmes détectés	Cette option envoie uniquement les tests ayant détecté des problèmes. C'est un moyen rapide de voir si les problèmes détectés au cours du dernier examen ont été corrigés.
Effacer toutes les données d'examen	Supprimer tous les résultats d'exploration et de test, en conservant uniquement la configuration des examens.
Modifier hôte/schéma/port	Si vous avez déjà enregistré une procédure de connexion, des opérations en plusieurs étapes et/ou une exploration manuelle et que l'hôte, le schéma ou le port de l'URL de départ est modifié, les demandes et les réponses de ces enregistrements doivent être mises à jour et vérifiées. Cliquez sur **Examiner > Modifier hôte/schéma/port** pour ouvrir une boîte de dialogue dans laquelle vous pouvez modifier l'URL et demander à AppScan de mettre à jour, de vérifier et de confirmer automatiquement les modifications nécessaires. La boîte de dialogue affiche les étapes en cours d'exécution et indique quand chaque étape aboutit. Si la procédure de mise à jour échoue, la boîte de dialogue vous indique quelle étape a échoué et vous permet de sauvegarder les modifications et de continuer la procédure manuellement ou d'annuler toutes les modifications. **Important :** Dans certains cas, il est possible qu'AppScan ne mette pas à jour les réponses correctement et que ce dysfonctionnement entraîne l'échec partiel ou total de l'examen. Dans ce cas, vous devez réenregistrer les procédures qui posent problème. **Remarque :** Bien que les données d'exploration *manuelle* soient mises à jour, les données d'exploration *automatique* et les résultats de l'examen sont supprimés lorsque vous modifiez l'URL de départ. **Remarque :** Cette option peut être utilisée pour modifier *uniquement* l'hôte, le schéma ou le port de l'URL de départ. Si vous devez apporter *d'autres* modifications à l'URL de départ ou modifier l'hôte, le schéma ou le port pour l'un des domaines *supplémentaires* dans l'examen, vous ne pouvez pas utiliser cette option. A la place, sauvegardez l'examen en tant que modèle et utilisez le modèle pour créer un examen.
Exécuter une évaluation Scan Expert	Scan Expert évalue si la configuration en cours est optimale pour l'application en cours d'examen. (Voir «Scan Expert», à la page 164) Cette option exécute une évaluation intégrale : Scan Expert explore brièvement l'application, analyse ses réponses et suggère des modifications à apporter à la configuration pour obtenir de meilleurs résultats.
Exécuter uniquement l'analyse Scan Expert	Cette option exécute uniquement l'étape d'analyse et n'est active que s'il existe déjà des résultats d'examen sur lesquels baser l'analyse. Scan Expert analyse les résultats en cours afin de déterminer si la configuration est optimale.
Configuration des examens	Définit les propriétés d'un examen. Voir «Boîte de dialogue Configuration des examens», à la page 46

Menu Outils

Fournit divers outils de génération de rapports et de personnalisation, y compris les PowerTools IBM Security.

Commande	Cliquez pour :
Créer	Créer un rapport de l'examen en cours. Voir Chapitre 10, «Rapports», à la page 233.
Test manuel	Créer et envoyer manuellement une variante de test à une URL sélectionnée. Voir «Tests manuels», à la page 223.
Générer les informations sur tous les problèmes	(Cette option est active uniquement si des résultats d'examen ont été générés :) Générer/Mettre à jour les Informations sur les problèmes dans l'onglet Informations sur les problèmes pour *tous* les problèmes. Voir «Onglet Informations sur les problèmes», à la page 212. **Conseil :** Pour générer des Informations sur les problèmes *pour un résultat spécifique uniquement*, cliquez avec le bouton droit de la souris sur le panneau Résultat, et sélectionnez **Générer les informations sur le problème**.
Planificateur d'examens	Définir l'heure et la fréquence de l'exécution automatique d'un examen.
Tests définis par l'utilisateur	Définir de nouveaux tests pour des examens. Voir «Tests définis par l'utilisateur», à la page 273.
Agents glass box	Définir les agents glass box sur le serveur pour inclure la fonction glass box dans les examens. Voir «Examen glass box», à la page 165.
Extensions >	
Assistant Services Web (Open API)	Ouvrez l'assistant pour configurer une analyse de services Web basée sur un ou plusieurs fichiers de description Open API (v2 et v3) (JSON ou YAML). Voir Assistant Services Web
Démarrer Pyscan	Ouvrir Pyscan pour contrôler AppScan à l'aide de l'interface Python. Voir «Pyscan», à la page 296.
Gestionnaire d'extensions	Ouvrir le gestionnaire d'extensions pour gérer les applications complémentaires. Voir «Gestionnaire d'extensions», à la page 294.
PowerTools >	
Authentication Tester	Exécuter l'outil Authentication Tester PowerTool pour des tests d'authentification de force brute.
Test de connexion	Exécuter l'outil Connection Test PowerTool pour exécuter une commande ping sur les sites Web sans utiliser le protocole ping (bloqué par de nombreux pare-feu).
EncodeDecode	Exécuter l'outil EncodeDecode PowerTool pour le codage/décodage de chaînes entre divers formats.
ExpressionTest	Exécuter l'outil ExpressionTest PowerTool pour vérifier des expressions régulières.
HTTP Request Editor	Exécuter l'outil HTTP Request Editor PowerTool pour éditer et envoyer des demandes HTTP et visualiser les réponses du site.
Outils externes...	Cliquer pour ouvrir une boîte de dialogue à partir de laquelle vous pouvez : • Modifier l'ordre des outils PowerTool dans le menu Outils. • Ajouter des programmes externes supplémentaires pouvant être ouverts à partir du menu Outils.
Options	Personnaliser les opérations AppScan. Voir «Boîte de dialogue Options», à la page 259.

Menu Aide

Utilisé pour accéder à la documentation, obtenir de l'aide et obtenir une nouvelle licence.

Commande	**Cliquez pour :**
Aide AppScan	Ouvrir l'aide en ligne ; comme F1.
Mise en route AppScan	Ouvrir le Guide d'initiation au format PDF (requiert Adobe Acrobat Reader).
Vidéos de formation et de support AppScan	Ouvrir une page Web répertoriant des vidéos de formation et de support.
Contrôles d'accessibilité	Ajoute le menu Accessibilité comme premier menu (avant le menu Fichier) dans la barre de menus.
Documentation d'accessibilité	Ouvre l'aide en ligne dans la page Contrôles d'accessibilité.
Bibliothèque de publications AppScan	Ouvre la page Bibliothèque de publications IBM Security AppScan du site Web IBM, qui contient un lien vers le document Guide d'utilisation AppScan. Il s'agit d'une version PDF imprimable du fichier d'aide (requiert Adobe Acrobat Reader).
Site Web AppScan	Ouvrir le site Web IBM Security AppScan Standard dans un explorateur.
Licence	Installer ou demander une nouvelle licence. Importez les autorisations de licence AppScan Enterprise.
Support >	Accéder à la page Mode de support étendu, Chiffrer les fichiers de support ou Ressources de support. Le Mode de support étendu crée des journaux détaillés des actions exécutées pour que l'équipe de support IBM puisse traiter les incidents. Cette opération pouvant ralentir AppScan, elle ne doit être activée que lorsque cela est nécessaire.
Log AppScan	Ouvrir le fichier journal du système.
Rechercher les mises à jour	Envoyer une demande pour qu'une nouvelle reconnaissance de l'évaluation de la sécurité soit intégrée à votre version de AppScan.
Journal des mises à jour	Ouvrir un journal des installations de mise à jour directes.
A propos d'IBM Security AppScan	Afficher les informations générales sur le produit.

Barre d'outils principale

Les icônes de la barre d'outils permettent d'accéder rapidement aux fonctions fréquemment utilisées (également disponibles à partir des menus).

Icône	Nom	Cliquez pour :
	Examen >	(Uniquement disponible si un examen est chargé et configuré.) Ouvrir un court menu Examen avec les options suivantes :  Examen intégral : démarrer un examen intégral (étapes d'exploration et de test) ou reprendre l'exécution d'un examen interrompu.  Exploration uniquement : exécuter une étape d'exploration uniquement (ou continuer une exploration ayant été interrompue), sans suivre avec une étape de test.  Test uniquement : exécuter une étape de test uniquement (ou poursuivre un test interrompu) sans exécuter l'étape d'exploration au préalable. Cette option est uniquement active s'il existe déjà des résultats d'exploration.
	Pause	(Actif uniquement lorsqu'un examen est en cours d'exécution.) Interrompre un examen en cours (qu'il s'agisse d'un examen intégral, d'une exploration uniquement ou d'un test uniquement). Vous pouvez reprendre l'examen ultérieurement. Vous pouvez également sauvegarder un examen interrompu pour poursuivre ultérieurement.
	Exploration manuelle	Ouvrir le navigateur sur l'URL de l'application et naviguer manuellement vers le site, en remplissant les paramètres requis. AppScan ajoute ensuite ces données d'exploration à ses propres données d'exploration collectées automatiquement lors de la création de tests pour le site. Pour plus d'informations, voir «Utilisation d'AppScan», à la page 143.
	Configuration	Ouvrir la boîte de dialogue Configuration des examens pour configurer l'examen. Pour plus d'informations, voir «Boîte de dialogue Configuration des examens», à la page 46.
	Rapport	Créer un rapport à l'aide des données d'examen actuelles. Pour plus d'informations, voir «Présentation des rapports», à la page 233.
	Examen sur le cloud	Télécharge un fichier de configuration AppScan Standard (SCAN ou SCANT) vers Application Security on Cloud. Vous pouvez utiliser la configuration pour exécuter un examen complet ou utiliser les résultats existants de l'étape d'exploration sauvegardés dans le fichier et exécuter l'option Test uniquement.
	Rechercher	Rechercher les résultats. Pour plus de détails, voir «Recherche de résultats», à la page 303.
	Journal d'examen	Afficher le journal d'examen pendant ou après un examen. (Celui-ci répertorie toutes les actions effectuées par AppScan pendant l'examen, lorsqu'elles sont réalisées.)
	PowerTools	Ouvrir l'une des applications PowerTools fournies avec AppScan pour vous aider à effectuer diverses tâches. Pour plus d'informations, voir «PowerTools», à la page 277.

Sélecteur de vue

Les trois icônes sur la droite de la barre d'outils basculent entre les trois vues : Données d'application, Problèmes de sécurité et Tâches de résolution.

Icône	Nom	Cliquez pour afficher :
	Vue Données	Vue Données d'application Pour plus de détails, voir Chapitre 7, «Résultats : Données d'application», à la page 199.
	Vue Problèmes	Vue Problèmes de sécurité Pour plus de détails, voir Chapitre 8, «Résultats : Problèmes de sécurité», à la page 207.
	Vue Tâches	Vue Tâches de résolution Pour plus de détails, voir Chapitre 9, «Résultats : Tâches de résolution», à la page 229.

Barre d'outils du navigateur

Icônes de la barre d'outils du navigateur AppScan intégré utilisées pour afficher et sauvegarder des captures d'écran de réponses d'application.

Bouton	Description
	Précédent
	Suivant
	Arrêter
	Régénérer
	Accéder à l'adresse URL de départ par défaut.
	Définir la page en cours comme URL de départ.
	Capturer cette page (disponible uniquement lorsque le navigateur est ouvert à partir de l'onglet Capture d'écran dans le «Panneau des détails», à la page 24).

Raccourcis-clavier

AppScan utilise les raccourcis clavier suivants :

Raccourci	Fonction
F1	Ouvre l'aide en ligne AppScan
F2	Ouvre la vue Données.
F3	Ouvre la vue Problèmes.
F4	Ouvre la vue Tâches.
F5	Démarre un examen complet.
[Maj] + F5	Met l'examen en pause.
F10	Ouvrir la boîte de dialogue Configuration

Raccourci	Fonction
[Ctrl] + N	Créer un nouvel examen
[Ctrl] + O	Ouvre un examen existant.
[Ctrl] + S	Enregistre l'examen en cours.
[Ctrl] + P	Imprimer le contenu en cours de l'Arborescence d'application et de la Liste des résultats (Tous les nœuds visibles lorsque vous faites défiler vers le haut ou vers le bas l'Arborescence d'application et la Liste des résultats sont inclus, mais les nœuds fermés à l'écran apparaîtront également fermés sur la sortie imprimée.)
[Ctrl] + W	Ouvrir l'écran d'accueil

Contrôles d'accessibilité

Décrit tous les raccourcis-clavier et contrôles.

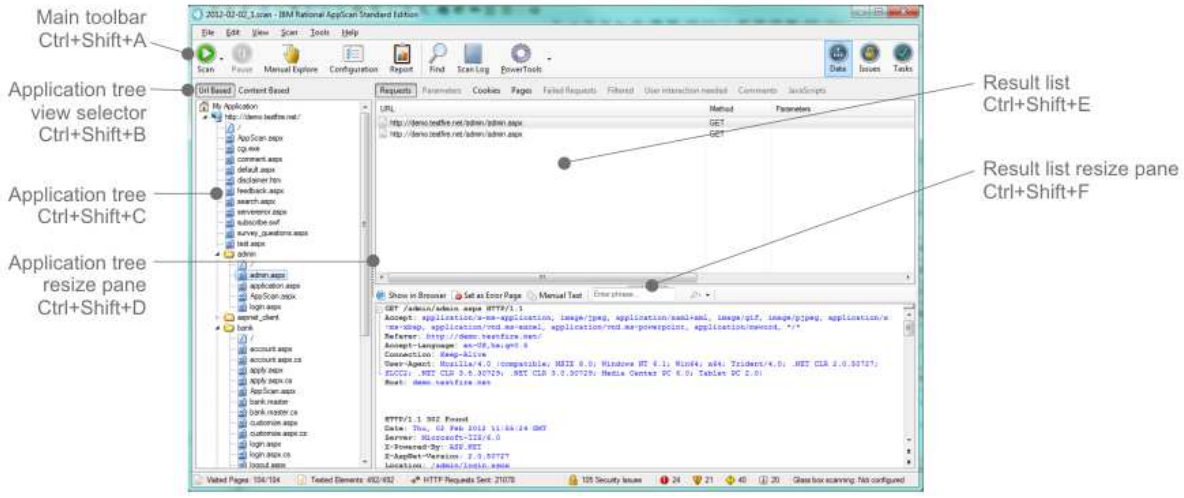
Pour activer l'accessibilité totale via le clavier, cliquez sur **Aide > Contrôles d'accessibilité**. Le menu Accessibilité s'affiche alors à gauche du menu Fichier, et un contrôle supplémentaire via le clavier (décrit ci-dessous) est activé.

Menu Accessibilité

Le menu Accessibilité s'affiche uniquement lorsque **Aide > Contrôles d'accessibilité** est coché, mais les raccourcis listés fonctionnent même lorsqu'il n'est pas activé. Les trois premières sections contrôlent les vues de l'interface utilisateur. Les autres sections sont des raccourcis-clavier des autres menus.

Toutes les vues

Les raccourcis suivants s'appliquent à toutes les vues.

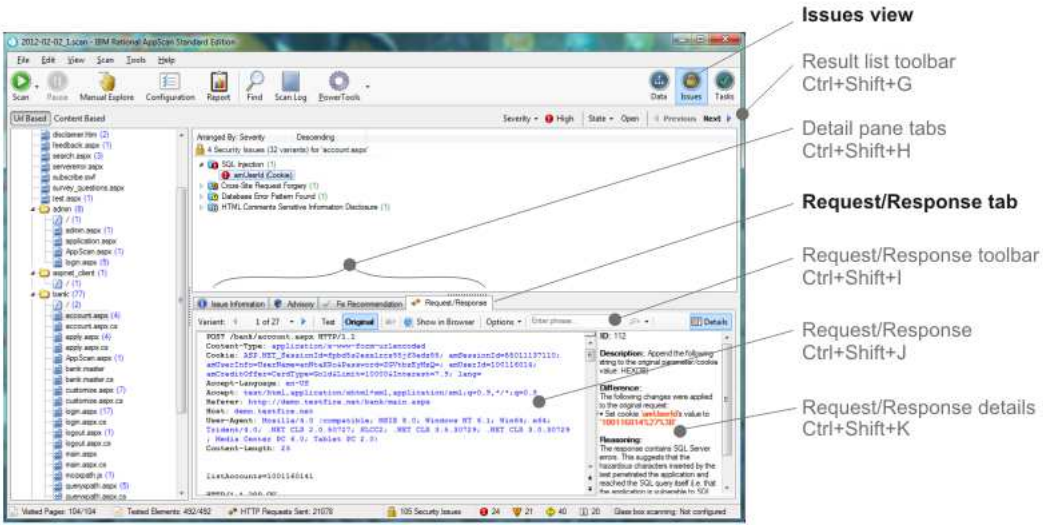


Commande	Raccourci	Description
Barre d'outils principale	Ctrl+Maj+A	Sélectionne la barre d'outils principale. Utilisez les flèches droite et gauche pour sélectionner une icône de la barre d'outils. **Remarque :** Les trois icônes Afficher le sélecteur à l'extrémité droite de la barre d'outils sont également sélectionnées.

Commande	Raccourci	Description
Sélecteur de vue Arborescence d'application	Ctrl+Maj+B	Sélectionne le Sélecteur de vue Arborescence d'application. Utilisez les flèches droite et gauche pour alterner entre les vues basées sur une adresse URL et une vue basée sur le contenu.
Arborescence de l'application	Ctrl+Maj+C	Sélectionne l'Arborescence d'application. Utilisez les flèches haut et bas pour naviguer. Utilisez les flèches droite et gauche pour ouvrir et fermer les nœuds.
Redimens. d'arboresc. d'appli.	Ctrl+Maj+D	Sélectionne la bordure entre la sous-fenêtre Arborescence d'application et la liste Résultats. Utilisez les touches flèches pour dimensionner les sous-fenêtres.
Liste des résultats	Ctrl+Maj+E	Sélectionne la liste Résultats. Utilisez les flèches haut et bas pour naviguer. Utilisez les flèches droite et gauche pour ouvrir et fermer les nœuds.
Sous-fenêtre de redimens. de la liste Résultats	Ctrl+Maj+F	Sélectionne la bordure entre la liste Résultats et la sous-fenêtre Détails. Utilisez les touches flèches pour dimensionner les sous-fenêtres.

Vue Problèmes

Les raccourcis suivants s'appliquent uniquement aux vues Problèmes.

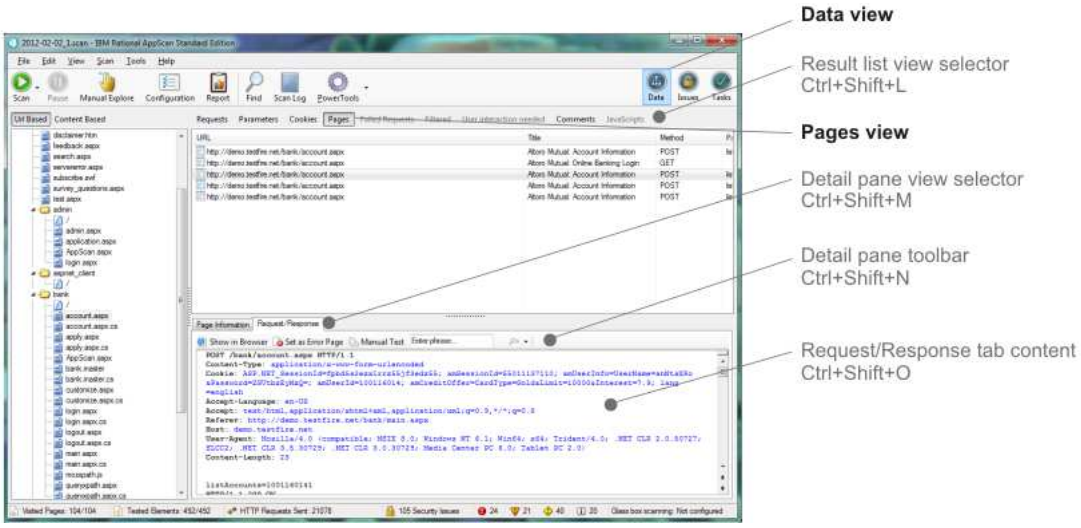


Commande	Raccourci	Description
Barre d'outils de la liste Résultats	Ctrl+Maj+G	Dans la Vue Problèmes : Sélectionne la liste Résultats. Utilisez les flèches haut et bas pour naviguer. Utilisez les flèches droite et gauche pour ouvrir et fermer les nœuds.
Panneau Détails	Ctrl+Maj+H	Sélectionne les onglets du panneau Détails.
Sous-fenêtre Détail > barre d'outils Demande/ Réponse	Ctrl+Maj+I	Dans la Vue Problèmes : Ouvre la barre d'outils de l'onglet Demande/Réponse dans la sous-fenêtre Détail et sélectionne sa barre d'outils.
Sous-fenêtre Détail > Demande/ Réponse	Ctrl+Maj+J	Dans la Vue Problèmes : Ouvre et sélectionne l'onglet Demande/Réponse dans la sous-fenêtre Détail.

Commande	Raccourci	Description
Sous-fenêtre Détail > Détails Demande/ Réponse	Ctrl+Maj+K	Dans la Vue Problèmes : Ouvre et sélectionne la section Détails (sous-fenêtre de droite) de l'onglet Demande/Réponse dans la sous-fenêtre Détail.

Vue Données

Les raccourcis suivants s'appliquent uniquement à la Vue Données.



Commande	Raccourci	Description
Sélecteur de vue Liste des résultats	Ctrl+Maj+L	Dans la Vue Données : Sélectionne la barre d'outils de la liste Résultats. Utilisez les flèches droite et gauche pour sélectionner Demandes, Paramètres et Cookies.
Sélecteur de vue de sous-fenêtre Détail	Ctrl+Maj+M	Dans la Vue Données > Pages : Permet de sélectionner Informations de page ou Demande/Réponse. Utilisez les flèches droite et gauche pour alterner.
Sous-fenêtre Détail > barre d'outils Demande/ Réponse	Ctrl+Maj+N	Dans la Vue Données > Pages : Sélectionne la barre d'outils de la liste Demande/Réponse. Utilisez les flèches droite et gauche pour naviguer.
Sous-fenêtre Détail > Onglet Demande/ Réponse	Ctrl+Maj+O	Dans la Vue Données > Pages : Sélectionne le contenu de l'onglet Demande/Réponse.

Autres raccourcis clavier

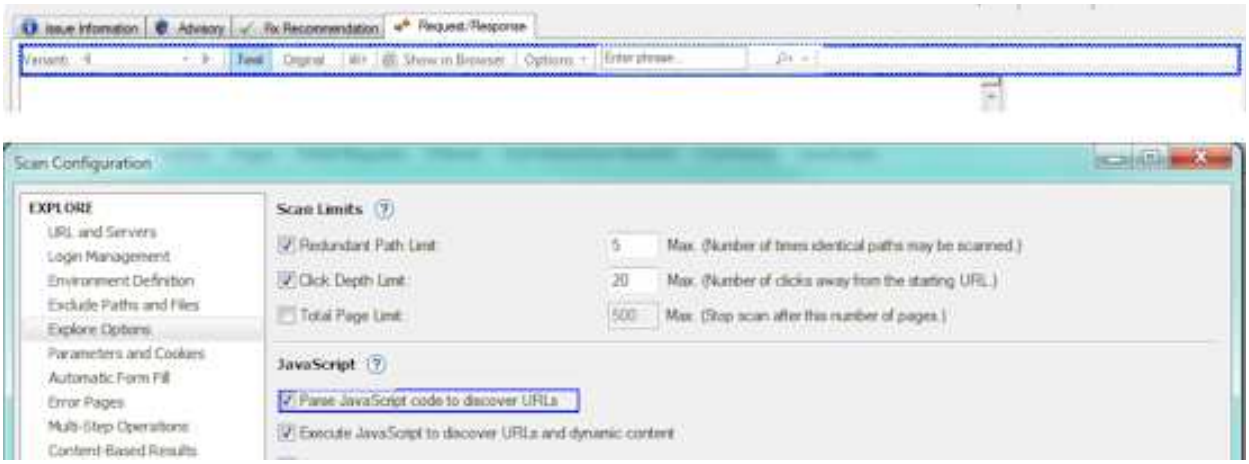
Les autres raccourcis existent aussi dans les autres menus, et sont listés dans la section «Raccourcis-clavier», à la page 380

Contrôle clavier supplémentaire

Lorsque **Aide > Contrôles d'accessibilité** est activé :

- Lorsque vous utilisez un raccourci d'accessibilité pour sélectionner une autre partie de l'interface utilisateur, la nouvelle sélection est brièvement encadrée en rouge.

- A tout moment, en cliquant sur F7, vous pouvez voir quel élément est sélectionné, à la fois dans l'interface utilisateur principale et dans la boîte de dialogue Configuration. La sélection en cours est brièvement encadrée en bleu.



Chapitre 17. Glossaire

Ce glossaire explique les termes et acronymes utilisés dans la documentation et l'interface utilisateur AppScan Standard.

Pour d'autres termes et définitions, voir le site Web de terminologie IBM (s'ouvre dans une nouvelle fenêtre).

A

contrôle d'accès
En sécurité informatique, processus permettant de vérifier que les utilisateurs ne peuvent accéder qu'aux ressources d'un système informatique auxquelles ils sont autorisés à accéder.

connexion basée sur les actions
Ce type de réexécution de la connexion reproduit les actions effectuées lorsque vous avez enregistré la séquence de connexion et constitue généralement la méthode de connexion préférée.

lecteur basé sur les actions
Navigateur comportant deux sous-fenêtres dans lequel la connexion basée sur les actions est réexécutée à des fins de vérification et de traitement des incidents. La sous-fenêtre de gauche affiche la liste des actions et met en évidence celle qui est en cous d'exécution ; celle de droite affiche le résultat de l'action en cours.

conseil
Document qui contient des informations et une analyse sur une menace ou une vulnérabilité.

cycle de vie de l'application
Succession d'étapes par lesquelles passe un produit, de son développement à sa production.

serveur d'applications
Programme serveur dans un réseau réparti qui fournit l'environnement d'exécution pour une application.

test d'application
Type de test mettant en évidence une logique d'application et les problèmes résultant d'un développement d'application non sécurisé.

arborescence de l'application
Affichage de l'arborescence d'une structure d'application Web, comprenant des répertoires et des fichiers.

attaque
Tentative, par une personne non autorisée, de compromettre l'opération d'un logiciel ou d'un système en réseau. Voir aussi pirate.

cyber-attaquant
Utilisateur (personne ou programme informatique) tentant d'endommager un système informatique ou d'accéder à des informations qui ne sont pas destinées à un accès public. Voir aussi, pirate informatique, attaque.

authentification
Processus de validation de l'identité d'un utilisateur ou d'un serveur.

Authentication Tester
Utilitaire de test de force brute (brute-force-like). L'un des outils PowerTools. Il détecte les combinaisons nom d'utilisateur-mot de passe faibles qui peuvent être utilisées pour accéder à l'application Web d'un utilisateur.

autorisation
Droit octroyé à un utilisateur pour utiliser ou communiquer avec un système informatique.

B

programme d'arrière-plan
Ensemble des composants de support d'un système informatique, tels que le système de gestion de base de données.

boîte noire
Lorsque la sortie d'une application est examinée sans référence à son code interne, on peut décrire l'application comme une "boîte noire", et le test comme un "test de type boîte noire", car il considère l'application comme une boîte noire dont le contenu est invisible. Voir aussi "boîte blanche" et "glass box".

lien rompu
Lien renvoyant une réponse non valide lorsqu'il est sélectionné.

force brute
Attaque par un programme qui essaie toutes les données d'identification possibles pour compromettre la sécurité d'un système.

mémoire tampon
Segment de mémoire réservé utilisé pour mettre en attente des données lors de son exécution.

dépassement de la mémoire tampon
Technique d'exploitation qui altère le flux d'une application en écrasant des parties de la mémoire. Les dépassements de la mémoire tampon sont une cause fréquente de problèmes au niveau logiciel.

C

sensible à la casse
Capacité de distinguer entre les lettres majuscules et minuscules.

CGI Voir Common Gateway Interface.

codage de caractères
Ensemble de caractères consistant en un code plaçant la séquence de caractères par paire d'un ensemble donné et d'un autre élément, tel qu'une séquence de nombres, d'octets ou d'impulsions électriques. Le codage facilite le stockage et la transmission de texte par des réseaux de télécommunication.

nœud enfant
Nœud situé dans un autre nœud.

client Poste de travail de l'utilisateur qui est connecté à un réseau. Voir aussi hôte.

côté client
Appartenance à une opération exécutée sur l'application client et non sur le serveur.

injection de code
Technique d'introduction d'un nouveau code dans une application. L'injection de code peut être utilisée par un pirate pour introduire un code dans un programme informatique afin de modifier le cours de l'exécution.

Common Gateway Interface (CGI)
Norme Internet de définition de scripts communiquant des informations d'un serveur Web vers un programme d'application par le biais d'une requête HTTP, et inversement.

délai d'attente de communication
Fin prévue d'une tâche incomplète après attente d'un temps donné.

connexion simultanée
Connexion se produisant en même temps que d'autres connexions.

schéma de condition
Généralement, un schéma définit par l'expression régulière. L'expression régulière peut être utilisée pour trouver des éléments correspondant au schéma.

cookie Information stockée par le serveur sur une machine cliente et à laquelle il accède au cours des sessions suivantes. Les cookies permettent aux serveurs d'obtenir des informations spécifiques sur les clients.

explorer
Rechercher des informations parmi des pages Web sur Internet ou sur un intranet.

attaque par script intersite (XSS)
Technique d'attaque qui force un site Web à répercuter les données fournies par un client et qui s'exécute dans le navigateur Web de l'utilisateur.

page d'erreur personnalisée
Fonction de la plupart des logiciels de serveur Web permettant à l'utilisateur de remplacer des messages d'erreur par défaut par des messages personnalisés conçus pour l'application.

CVE Common Vulnerabilities and Exposures. Liste des normes de l'industrie fournissant des noms usuels affectés à des expositions et vulnérabilités de sécurité publiquement connues.

CVSS Common Vulnerability Scoring System. Infrastructure ouverte permettant d'attribuer un score pour le risque associé aux vulnérabilités.

CWE Common Weakness Enumeration. Liste des normes de l'industrie fournissant des noms usuels pour les faiblesses logicielles publiquement connues.

D

système de gestion de base de données (SGBD)
Système logiciel contrôlant la création, l'organisation et la modification d'une base de données et l'accès aux données qui y sont stockées.

service de base de données
Service fournissant le stockage et l'extraction des données d'une base de données.

DBMS
Voir système de gestion de base de données.

commande de débogage
Fonction ou commande aidant à identifier des erreurs de programmation lors du processus de développement de l'application.

delta Différence, ou valeur incrémentielle, entre deux instances.

attaque par refus de service (DoS)
En sécurité informatique, attaque contre un réseau qui interrompt un ou plusieurs hôtes, ces hôtes n'étant plus en mesure de fonctionner correctement. Le service réseau est interrompu pendant un certain temps.

profondeur
Nombre de clics requis pour qu'un utilisateur ou un moteur de balayage automatique passe d'une page source à une page cible.

indexation de répertoire
Fonction de serveur Web qui affiche le contenu d'un répertoire lorsqu'il n'y a pas de page d'index.

traversée de répertoires
Technique utilisée pour exploiter des sites Web en accédant à des fichiers et des commandes sous le répertoire principal du document.

domaine
Sous-réseau de clients et de serveurs sous le contrôle d'une base de données de sécurité.

DoS Voir attaque par refus de service.

fichier de vidage
Contenu de la mémoire sans formatage de rapport.

E

navigateur intégré
Navigateur Web intégré dans AppScan et s'ouvrant à l'aide d'une barre d'outils spéciale pour pouvoir être utilisé avec des images.

attaque de codage
Technique d'exploitation qui facilite l'attaque en modifiant le format des données fournies par l'utilisateur afin d'ignorer les filtres de contrôle d'exactitude.

chiffrement
Processus consistant à transformer les données en un format non intelligible afin que les données originales ne puissent pas être obtenues ou puissent être obtenues uniquement à l'aide d'un processus de déchiffrement.

exclusion
Paramètre ou processus dont les valeurs sont exclues lors des tests.

exécutable
Fichier programme prêt à s'exécuter dans un environnement particulier.

paramètre d'exploration
Paramètre qui configure les paramètres gérant l'exploration d'une application par AppScan.

Etape d'exploration
Etape d'une analyse AppScan lors de laquelle la logique et les objets d'une application sont identifiés, avant le test.

export Sauvegarder une copie d'une base de données, d'une image ou d'un document courant dans le format de fichier requis par une autre application.

mode de support étendu
Mode permettant à l'utilisateur d'enregistrer les options d'utilisation et le comportement ainsi que de sauvegarder les données dans un fichier afin de l'envoyer au support technique.

F

faux positif
Résultat de test classé comme positif (indiquant que le site est vulnérable aux attaques) et que l'utilisateur décide de classer comme négatif (il ne s'agit pas d'une vulnérabilité).

recommandation de correction
Détails spécifiques et techniques relatifs à la correction d'une application Web afin de la sécuriser contre le problème découvert.

Flash Technique de programmation activant l'affichage de films et d'animations dans un navigateur Web en toute transparence.

propriété du formulaire
Valeur utilisée lorsque des formulaires sont renseignés automatiquement.

nom de chemin absolu
Nom d'un répertoire ou d'un fichier exprimé sous la forme d'une chaîne de répertoires et de fichiers et commençant par le répertoire principal.

G

glass box
Contrairement aux "tests de type boîte noire", qui considèrent l'application comme une "boîte noire" dont le contenu est invisible, le test de type "glass box" "regarde à l'intérieur de la boîte" en examinant le code de l'application. Cela signifie que les tests de type glass box peuvent détecter des failles de sécurité introuvables par les tests de type boîte noire.

interface graphique (GUI)
Type d'interface présentant une représentation visuelle d'une scène réelle, le plus souvent un bureau, en combinant des graphiques haute définition, des unités de pointage, des barres de menus et d'autres menus, des fenêtres en cascade, des icônes et les relations objet-action.

GUI Voir interface graphique.

H

codage en dur
Pratique de développement d'application de sortie d'intégration ou de configuration de données directement dans le code source d'un programme ou d'un autre objet exécutable.

caractère dangereux
Caractère utilisé pour procéder à des attaques d'application Web, telles que des injections XSS ou SQL.

paramètre masqué
Paramètre de formulaire HTML non rendu dans la page Web.

hôte Ordinateur connecté à un réseau et qui fournit un point d'accès à ce réseau. L'hôte peut être un client, un serveur, ou un client et un serveur simultanément. Voir aussi client

élément de formulaire HTML
Elément permettant à l'utilisateur d'entrer des informations, telles que des zones de texte, des menus déroulants, des boutons d'option ou des cases à cocher, dans un formulaire.

requête HTTP
Requête envoyée au site lors de l'étape d'exploration ou de test de l'analyse.

réponse HTTP
Réponse envoyée par le serveur.

I

ID Voir identificateur.

identificateur (ID)
Un ou plusieurs caractères utilisés pour identifier ou nommer un élément de données et éventuellement indiquer certaines propriétés de cet élément de données.

import
Lire un fichier dans un format non natif de l'application en cours.

rapport sur les normes de l'industrie
Rapport des problèmes trouvés sur l'application Web de l'utilisateur et informations appropriées en fonction de la norme industrielle sélectionnée. Les rapports AppScan aux normes de l'industrie incluent les rapports SANS Top 20, OWASP Top 10 et WASC Threat Classification.

détection en session
Détection du schéma En session dans les réponses reçues par AppScan afin de vérifier qu'il est toujours connecté.

schéma en session
Schéma identifié dans la page de connexion, tel qu'un lien de déconnexion, qu'AppScan peut utiliser pour vérifier qu'il est toujours connecté.

anti-automatisation insuffisante
Ce qui se passe lorsqu'un site Web permet à un cyber-attaquant d'automatiser un processus qui devrait uniquement être exécuté manuellement.

URL interactive
Adresse URL incluant des formulaires à remplir manuellement par l'utilisateur.

test invasif
Test facultatif qui, s'il est exécuté sur l'application, peut créer une situation de déni de service.

problème
Risque pour la sécurité auquel une application Web est vulnérable, ou informations potentiellement sensibles visibles par des utilisateurs non autorisés.

J

Java applet
Applet écrit en Java et pouvant s'exécuter dans un navigateur Web à l'aide d'une machine virtuelle Java (JVM).

machine virtuelle Java (JVM)
Implémentation logicielle d'un processeur qui exécute un code Java compilé (applets et applications).

L

extraction de liens
Analyse syntaxique ou exécution d'un code pour la reconnaissance et l'exécution de liens à partir d'une application Web.

séquence de connexion
Séquence d'entrées utilisateur permettant à AppScan de se connecter à votre application Web pour l'examiner. Il est recommandé d'enregistrer la connexion manuellement. AppScan réexécute ensuite cette séquence chaque fois qu'il doit se connecter au cours d'un examen. Lorsque vous enregistrez une séquence de connexion, AppScan analyse les actions et les demandes. Lors de la réexécution de la séquence de connexion, il tente (par défaut) de reproduire la connexion basée sur les actions. En cas d'échec, il revient à la connexion basée sur les demandes.

M

logiciel malveillant
Logiciel malveillant ou code exécutable téléchargé ou reçu sous la forme d'un fichier apparemment inoffensif.

manipulation
Modification, par un cyber-attaquant, d'un élément de données, d'un groupe d'éléments, d'une action ou d'un groupe d'actions sur la base d'une ou de plusieurs propriétés. Par exemple, la modification d'une entrée en supprimant un argument obligatoire ou la réalisation d'étapes irrégulières.

exploration manuelle
Processus d'exploration manuelle d'une application Web permettant d'accéder aux parties du site dépendantes des entrées d'un utilisateur réel et de les tester.

métacaractère
Caractère ASCII ayant une signification particulière lors du traitement d'un schéma. Ces caractères sont utilisés pour représenter des schémas de caractère à octet unique ou multi-octet pouvant être associés lors du traitement.

demande multiparties
Demande contenant plusieurs types de contenu. Pour réduire la consommation de mémoire superflue, certains types de contenu sont automatiquement exclus par filtrage des demandes multiparties au cours de l'examen. Vous pouvez configurer les types devant être exclus par filtrage dans **Configuration > Configuration avancée > Filtre du type de contenu à plusieurs parties**.

examen en plusieurs phases
Examen comprenant deux phases ou plus.

opération en plusieurs étapes
Séquence de demandes qui doivent être envoyées dans un ordre précis pour atteindre certaines parties de l'application. (Exemple : Ajouter un article au panier > Entrer les informations de règlement > Recevoir la confirmation de commande.) L'enregistrement de telles opérations en plusieurs étapes dans le cadre de la configuration des examens garantit l'examen de ces parties du site.

N

service réseau
Service transmettant des données ou fournissant une conversion de données dans un réseau.

NTLM
Voir Windows NT LAN Manager.

dépassement numérique
Résultat d'un calcul arithmétique dépassant l'espace désigné pour le contenir.

P

nœud parent
Nœud contenant le nœud courant.

analyse syntaxique
Processus de décomposition d'une chaîne d'informations, telle qu'une commande ou un fichier, en parties constituant cette chaîne.

chemin
Partie de l'adresse URL pointant vers l'emplacement d'une ressource Internet.

filtrage de chemin
Processus de filtrage ou d'inclusion de pages selon un ensemble de critères.

traversée de répertoires
Technique d'attaque qui altère l'emplacement d'une ressource ou d'un document dans une adresse URL et impose l'accès à des fichiers, répertoires et commandes situés en dehors du répertoire racine du document Web.

schéma
Méthode de description d'un texte à identifier à l'aide d'une ou de plusieurs expressions régulières.

PCI Voir Peripheral Component Interconnect.

test d'effraction
Méthode d'évaluation de la sécurité d'une application Web par la simulation d'une attaque par un pirate.

Peripheral Component Interconnect (architecture PCI)
Bus local fournissant un chemin de données à fort débit entre le processeur et les services attachés.

droit Autorisation d'exécution d'activités, telles que la lecture et l'écriture de fichiers locaux, la création de connexions réseau et le chargement d'un code natif.

code confidentiel (PIN)
Dans le support de chiffrement, numéro unique affecté par une organisation à un individu et utilisé comme preuve de son identité. Les codes confidentiels sont généralement attribués par les organismes financiers à leurs clients.

phase Processus incluant l'étape d'exploration et l'étape de test d'un examen.

limite de phase
Nombre maximal de phases autorisées dans un examen. La limite est configurable.

PIN Code confidentiel (Personal Identification Number).

plateforme
Combinaison d'un système d'exploitation et de matériel constituant l'environnement d'exploitation dans lequel s'exécute un programme.

port Point terminal pour la communication entre les applications, généralement associé à une connexion logique. Un port fournit des files d'attente pour envoyer et recevoir des données. Chaque port a un numéro qui permet de l'identifier.

programme d'écoute des ports
Mécanisme permettant au produit de valider certains tests en écoutant des connexions hors limite.

emplacement de ressource prévisible
Technique d'attaque destinée à découvrir les fonctionnalités et le contenu masqués d'un site Web. L'attaque cherche le contenu à des emplacements standard non destinés à une consultation publique, notamment les fichiers temporaires, les fichiers de sauvegarde, les fichiers de configuration ou les fichiers échantillon.

escalade des droits d'accès
Référence à des examens exécutés à l'aide de droits utilisateur différents permettant de contrôler si des ressources disposant de privilèges sont accessibles aux utilisateurs ayant des droits d'accès insuffisants.

invite Message ou symbole affiché exigeant des informations ou une action utilisateur. L'utilisateur doit y répondre pour permettre au programme de continuer à s'exécuter.

proxy Passerelle d'application d'un réseau à un autre pour une application réseau spécifique telle que Telnet ou FTP, dans laquelle le serveur Telnet proxy d'un pare-feu exécute une authentification de l'utilisateur, puis laisse le flux de trafic via le proxy comme si cet utilisateur n'existait pas. La fonction s'exécute dans le pare-feu et non sur le poste de travail client, occasionnant plus de charge dans le pare-feu.

R

limite de chemin d'accès redondant
Nombre maximal de fois où des examens identiques peuvent être examinés afin de réduire le temps d'analyse et d'éliminer les résultats en double.

expression régulière
Ensemble de caractères, de métacaractères et d'opérateurs définissant une chaîne ou un groupe de chaînes dans un schéma de recherche.

rapport sur la conformité légale
Rapport des problèmes trouvés sur une application Web et ne correspondant pas à une règle ou à

une norme légale sélectionnée. Les règles comprennent des actes, des lois et des projets de loi légaux du Canada, de l'Union européenne, du Japon, du Royaume-Uni et des Etats-Unis, ainsi que des règles de MasterCard et Visa. Des modèles personnalisés de rapport sur la conformité légale peuvent également être créés.

chemin d'accès relatif
Chemin d'accès commençant par le répertoire de travail en cours.

résolution
Suggestion de correction d'un problème.

connexion basée sur les demandes
Ce type de réexécution de la connexion reproduit les demandes envoyées lorsque vous avez enregistré la séquence de connexion.

restriction
Type de filtre limitant un examen uniquement aux adresses URL répertoriées.

Result Expert
Fonction facultative pouvant être exécutée après un examen en vue d'ajouter des paramètres CVSS, des captures d'écran et d'autres informations à l'onglet Informations sur les problèmes des résultats de l'examen.

ingénierie inverse
Analyser une unité ou un système pour prendre connaissance des détails de sa conception, sa construction et son mode opératoire.

analyse du risque
Analyse des problèmes de sécurité trouvés dans une application Web.

évaluation des risques
Evaluation des avantages et conséquences d'une action ou d'un scénario.

gestion des risques
Allocation optimale des ressources en vue de parvenir à un investissement approprié des mesures défensives au sein d'une organisation.

rôle Ensemble de droits.

S

assainir
Dans le cadre de la sécurité d'une application Web, nettoyer une entrée utilisateur de ses caractères dangereux avant de l'utiliser.

examen
Processus d'exploration et de test par AppScan d'une application et de présentation des résultats.

configuration des examens
Ensemble de paramètres AppScan définissant l'application ou le service et l'environnement de l'utilisateur ainsi que des méthodes d'examen choisies par l'utilisateur.

Scan Expert
Fonction facultative explorant le comportement de l'application et du réseau, et recommandant des modifications de configuration pour optimiser l'examen.

module d'analyse Scan Expert
Vérification unique effectuée par Scan Expert lors de son analyse.

évaluation Scan Expert
Evaluation Scan Expert de la configuration utilisateur.

modèle d'examen
Configuration d'examen pouvant être chargée pour être utilisée avec un examen.

planificateur
Serveur d'arrière-plan multitâche et multiprocesseurs conçu pour gérer la planification et le lancement de travaux, selon un calendrier simple.

audit de sécurité
Evaluation technique mesurable systématique ou manuelle d'un système ou d'une application.

risque pour la sécurité
Succès potentiel d'une menace et dommage pouvant en découler.

séquence
Liste d'adresses URL enregistrées.

session
Connexion logique ou virtuelle entre deux postes, logiciels ou unités d'un réseau permettant à ces deux éléments de communiquer et d'échanger des données. Voir aussi transaction

données d'identification de session
Chaîne de données fournie par le serveur Web et stockée dans un cookie ou une adresse URL, identifiant un utilisateur et autorisant ce dernier à exécuter diverses actions.

fixation de session
Technique d'attaque qui permet à un cyber-attaquant de fixer (définir) l'identificateur de session d'un utilisateur et d'assumer son identité en ligne.

détournement de session
Compromission d'une session utilisateur par un pirate. Le pirate peut réutiliser cette session volée pour se présenter comme l'utilisateur.

ID session
Voir identificateur de session

identificateur de session (ID session)
Compromission d'une session utilisateur par un pirate. Le pirate peut réutiliser cette session volée pour se présenter comme l'utilisateur.

jeton de session
Identificateur envoyé par le navigateur en tant que paramètre ou cookie afin d'effectuer une corrélation entre un utilisateur et sa session en cours sur l'application Web. Voir aussi identificateur de session, jeton temporaire.

évaluation de la gravité
Niveau affecté par l'examen à un problème et indiquant le risque de sécurité qu'il représente.

shell Interface logicielle entre les utilisateurs et un système d'exploitation. Les shells font généralement partie de l'une des deux catégories suivantes : un shell de ligne de commande, qui fournit une interface de ligne de commande au système d'exploitation ; et un shell graphique, qui fournit une interface graphique.

code source
Programme informatique dans un format lisible. Le code source est converti en code binaire pouvant être utilisé par un ordinateur.

usurpation
Technique de simulation de l'adresse d'envoi d'une transmission afin d'obtenir un accès illégal à un système sécurisé.

SQL Voir Structured Query Language.

injection SQL
Voir injection Structured Query Language.

étape Partie d'une étape d'examen dans laquelle AppScan explore ou teste le site.

protocole apatride
Protocole ne conservant pas de relation entre des commandes. HTTP est un exemple de protocole apatride.

Structured Query Language (SQL)
Langage normalisé servant à définir et manipuler les données dans une base de données relationnelle.

injection Structured Query Language (injection SQL)
Technique d'attaque utilisée pour exploiter les sites Web en altérant les instructions SQL en arrière-plan via la manipulation des entrées de l'application.

syntaxe
Règles de construction d'une commande ou d'une instruction.

T

correctif de test
Correctif temporaire fourni à des clients spécifiques pour obtenir la réponse de test à un incident rapporté.

stratégie de test
Stratégie qui limite l'examen à certaines catégories et certains types de tests.

demande de test
Requête envoyée à l'application lors de l'étape de test de l'examen. Les demandes de test sont conçues pour révéler les vulnérabilités de sécurité.

étape de test
Etape de l'examen pendant laquelle les objets et la logique de l'application analysée sont soumis à un barrage total des techniques d'utilisation malveillantes générales, erronées et simulées résultant d'un inventaire complet des vulnérabilités de sécurité.

unité d'exécution
Flux d'instructions informatiques contrôlant un processus. Dans certains systèmes d'exploitation, une unité d'exécution est l'unité d'opération la plus petite d'un processus. Plusieurs unités d'exécution peuvent s'exécuter simultanément et effectuer des travaux différents.

menace
Problème de sécurité ou acte malveillant, tel que le déploiement d'un virus ou la pénétration illégale dans un réseau.

classe de menaces
Groupe de problèmes de sécurité, classés par catégories WASC-TC. Pour chaque classe de menaces, il existe de nombreux tests spécifiques ; et pour chaque test, de nombreuses variantes.

transaction
Demande faite à une application et réponse (de l'application) générée par cette demande.

jeton temporaire
Jeton dont la valeur change (il s'agit généralement d'un jeton de session). L'envoi d'un jeton temporaire arrivé à expiration pouvant provoquer la déconnexion d'AppScan de l'application qu'il teste, il doit donc les maintenir à jour. Voir aussi jeton de session.

U

adresse URL (Uniform Resource Locator)
Adresse unique d'une ressource d'information qui est accessible sur un réseau tel qu'Internet. L'adresse URL inclut le nom abrégé du protocole utilisé pour accéder à la ressource d'information et l'information utilisée par le protocole pour localiser la ressource d'information.

UNIX Système d'exploitation hautement portable disposant de fonctions de multiprogrammation s'exécutant dans un environnement multi-utilisateurs. Le système d'exploitation UNIX a été

initialement développé pour être utilisé sur des petits ordinateurs, mais a été adapté pour des grands systèmes et des micro-ordinateurs. Le système d'exploitation AIX est une implémentation IBM du système d'exploitation UNIX.

URL Voir adresse URL.

test défini par l'utilisateur
Test créé par un utilisateur en plus des tests créés et exécutés automatiquement.

V

validation
Processus consistant à vérifier qu'un test particulier est parvenu à atteindre son objectif ou a échoué.

vulnérabilité
Exposition de la sécurité dans un système d'exploitation, un logiciel système ou un composant de logiciel d'application.

W

application Web
Application accessible par un navigateur Web et fournissant certaines fonctions lors de l'affichage statique d'informations, par exemple en permettant à l'utilisateur d'analyser une base de données. Les composants communs d'une application Web comprennent des pages HTML, des pages JSP et des servlets.

navigateur Web
Programme client lançant des requêtes à un serveur Web et affichant les informations renvoyées par le serveur.

contenu Web
Fichiers et autres ressources composant un site Web. Le contenu Web peut comporter des fichiers d'images, des fichiers audio, des fichiers HTML, des fichiers JSP, des feuilles de style, des entrées de base de données ou tout autre élément pouvant être contenu dans un site Web.

sécurité Web
Théorie et pratique de la sécurité des informations par rapport au World Wide Web, au protocole HTTP et au logiciel d'application Web.

serveur Web
Programme capable de servir les demandes HTTP (Hypertext Transfer Protocol).

service Web
Application exécutant des tâches spécifiques et accessibles par le biais de protocoles ouverts tels que HTTP et SOAP.

Web Services Description Language (WSDL)
Spécification basée sur XML décrivant des services réseau comme un ensemble de points finaux opérant sur des messages contenant des informations orientées document ou orientées procédure.

boîte blanche
Examen permettant d'analyser le code source d'une application, tel que le code JavaScript dans le cas d'une analyse statique. Voir aussi "black box" et "glass box".

Windows NT LAN Manager (NTLM)
Protocole utilisé dans de nombreux protocoles réseau Microsoft pour l'authentification.

WSDL
Voir Web Services Description Language.

X

XSS Voir attaque par script intersite.

Chapitre 18. Remarques

:NONE.

Il est probable que IBM n'offre pas les produits, services ou fonctions évoqués dans le présent document dans d'autres pays. Pour plus de détails, référez-vous aux documents d'annonce disponibles dans votre pays, ou adressez-vous à votre partenaire commercial IBM. Toute référence à un produit, logiciel ou service IBM n'implique pas que seul ce produit, logiciel ou service IBM puisse être utilisé. Tout autre élément fonctionnellement équivalent peut être utilisé, s'il n'enfreint aucun droit de IBM. Il est de la responsabilité de l'utilisateur d'évaluer et de vérifier lui-même les installations et applications réalisées avec des produits, logiciels ou services non expressément référencés par IBM.

IBM peut détenir des brevets ou des demandes de brevet couvrant les produits mentionnés dans le présent document. La remise de ce document ne vous donne aucun droit de licence sur ces brevets ou demandes de brevet. Si vous désirez recevoir des informations concernant l'acquisition de licences, veuillez en faire la demande par écrit à l'adresse suivante :

IBM Director of Licensing IBM Corporation North Castle Drive, MD-NC119 Armonk, NY 10504-1785 US

Pour plus d'informations sur les licences concernant les produits utilisant un jeu de caractères double octet, contactez IBM Intellectual Property Department dans votre pays ou envoyez vos demandes par écrit à l'adresse suivante :

Intellectual Property Licensing Legal and Intellectual Property Law IBM Japan Ltd. 19-21, Nihonbashi-Hakozakicho, Chuo-ku

INTERNATIONAL BUSINESS MACHINES CORPORATION FOURNIT LE PRESENT DOCUMENT "EN L'ETAT" ET DECLINE TOUTE RESPONSABILITE, EXPLICITE OU IMPLICITE, RELATIVE AUX INFORMATIONS QUI Y SONT CONTENUES, Y COMPRIS EN CE QUI CONCERNE LES GARANTIES DE VALEUR MARCHANDE OU D'ADAPTATION A VOS BESOINS. Certaines juridictions n'autorisent pas l'exclusion des garanties implicites, auquel cas l'exclusion ci-dessus ne vous sera pas applicable.

Le présent document peut contenir des inexactitudes ou des coquilles. Ce document est mis à jour périodiquement. Chaque nouvelle édition inclut les mises à jour. IBM peut, à tout moment et sans préavis, apporter des améliorations et/ou modifier les produits et/ou logiciels décrits dans ce document.

Les références à des sites Web non IBM sont fournies à titre d'information uniquement et n'impliquent en aucun cas une adhésion aux données qu'ils contiennent. Les éléments figurant sur ces sites Web ne font pas partie des éléments du présent produit IBM et l'utilisation de ces sites relève de votre seule responsabilité.

IBM pourra utiliser ou diffuser, de toute manière qu'elle jugera appropriée et sans aucune obligation de sa part, tout ou partie des informations qui lui seront fournies.

Les licenciés souhaitant obtenir des informations permettant : (i) l'échange des données entre des logiciels créés de façon indépendante et d'autres logiciels (dont celui-ci), et (ii) l'utilisation mutuelle des données ainsi échangées, doivent adresser leur demande à :

IBM Director of Licensing IBM Corporation North Castle Drive, MD-NC119 Armonk, NY 10504-1785 US

Ces informations peuvent être soumises à des conditions particulières, prévoyant notamment le paiement d'une redevance.

Le logiciel sous licence décrit dans ce document et tous les éléments sous licence disponibles s'y rapportant sont fournis par IBM conformément aux dispositions du document IBM Customer Agreement, des Conditions internationales d'utilisation des logiciels IBM ou de tout autre accord équivalent.

Les données de performance présentées ici ont été obtenues dans des conditions de fonctionnement spécifiques. Les résultats peuvent donc varier.

Les informations concernant des produits non IBM ont été obtenues auprès des fournisseurs de ces produits, par l'intermédiaire d'annonces publiques ou via d'autres sources disponibles. IBM n'a pas testé ces produits et ne peut confirmer l'exactitude de leurs performances ni leur compatibilité. Elle ne peut recevoir aucune réclamation concernant des produits non IBM. Toute question concernant les performances de produits non IBM doit être adressée aux fournisseurs de ces produits.

Les instructions relatives aux intentions d'IBM pour ses opérations à venir sont susceptibles d'être modifiées ou annulées sans préavis, et doivent être considérées uniquement comme un objectif.

Le présent document peut contenir des exemples de données et de rapports utilisés couramment dans l'environnement professionnel. Ces exemples mentionnent des noms fictifs de personnes, de sociétés, de marques ou de produits à des fins illustratives ou explicatives uniquement. Toute ressemblance avec des noms de personnes, de sociétés ou des données réelles serait purement fortuite.

LICENCE DE COPYRIGHT :

Le présent logiciel contient des exemples de programmes d'application en langage source destinés à illustrer les techniques de programmation sur différentes plateformes d'exploitation. Vous avez le droit de copier, de modifier et de distribuer ces exemples de programmes sous quelque forme que ce soit et sans paiement d'aucune redevance à IBM, à des fins de développement, d'utilisation, de vente ou de distribution de programmes d'application conformes aux interfaces de programmation des plateformes pour lesquels ils ont été écrits. Ces exemples de programmes n'ont pas été rigoureusement testés dans toutes les conditions. Par conséquent, IBM ne peut garantir expressément ou implicitement la fiabilité, la maintenabilité ou le fonctionnement de ces programmes. Les exemples de programmes sont fournis "EN L'ETAT" sans garantie d'aucune sorte. IBM ne sera en aucun cas responsable des dommages liés à l'utilisation de ces exemples de programmes.

Toute copie totale ou partielle de ces programmes exemples et des œuvres qui en sont dérivées doit comprendre un

Marques

IBM, le logo IBM et ibm.com sont des marques ou des marques déposées d'International Business Machines Corp. dans diverses juridictions à travers le monde. Les autres noms de produits et services peuvent être des marques d'IBM ou d'autres sociétés. La liste actualisée de toutes les marques d'IBM est disponible à la page Web "Copyright and trademark information" à l'adresse www.ibm.com/legal/copytrade.shtml.

Dispositions applicables à la documentation du produit

Les droits d'utilisation relatifs à ces publications sont soumis aux dispositions suivantes :

Applicabilité

Ces dispositions viennent s'ajouter à celles du site Web IBM.

Usage personnel

Vous pouvez reproduire ces publications pour votre usage personnel, non commercial, sous réserve que toutes les mentions de propriété soient conservées. Vous ne pouvez distribuer ou publier tout ou partie de ces publications ou en faire des œuvres dérivées sans le consentement exprès de IBM.

Usage commercial

Vous pouvez reproduire, distribuer et publier ces publications uniquement au sein de votre entreprise, sous réserve que toutes les mentions de propriété soient conservées. Vous ne pouvez reproduire, distribuer, afficher ou publier tout ou partie de ces publications en dehors de votre entreprise, ou en faire des œuvres dérivées, sans le consentement exprès de IBM.

Droits

Excepté les droits d'utilisation expressément accordés dans ce document, aucun autre droit, licence ou autorisation, implicite ou explicite, n'est accordé pour ces publications ou autres informations, données, logiciels ou droits de propriété intellectuelle contenus dans ces publications.

IBM se réserve le droit de retirer les autorisations accordées ici si, à sa discrétion, l'utilisation des informations s'avère préjudiciable à ses intérêts ou que, selon l'appréciation de IBM, les instructions susmentionnées n'ont pas été respectées.

Vous ne pouvez télécharger, exporter ou réexporter ces informations qu'en total accord avec toutes les lois et règlements applicables dans votre pays, y compris les lois et règlements américains relatifs à l'exportation.

IBM N'OCTROIE AUCUNE GARANTIE SUR LE CONTENU DE CES PUBLICATIONS. LES DOCUMENTS SONT LIVRES EN L'ETAT. IBM DECLINE TOUTE RESPONSABILITE, EXPLICITE OU IMPLICITE, RELATIVE AUX INFORMATIONS QUI Y SONT CONTENUES, Y COMPRIS EN CE QUI CONCERNE LES GARANTIES DE VALEUR MARCHANDE OU D'ADAPTATION A VOS BESOINS.

Déclaration IBM de confidentialité sur Internet

Les Logiciels IBM, y compris les Logiciels sous forme de services (“Offres Logiciels”) peuvent utiliser des cookies ou d'autres technologies pour collecter des informations sur l'utilisation des produits, améliorer l'acquis utilisateur final, personnaliser les interactions avec celui-ci, ou dans d'autres buts. Bien souvent, aucune information personnelle identifiable n'est collectée par les Offres Logiciels. Certaines Offres Logiciels vous permettent cependant de le faire. Si la présente Offre Logiciels utilise des cookies pour collecter des informations personnelles identifiables, des informations spécifiques sur cette utilisation sont fournies ci-dessous.

Cette Offre Logiciels n'utilise pas de cookies ou d'autres techniques pour collecter des informations personnelles identifiables.

Si les configurations déployées de cette Offre Logiciels vous permettent, en tant que client, de collecter des informations permettant d'identifier les utilisateurs par l'intermédiaire de cookies ou par d'autres techniques, vous devez solliciter un avis juridique sur la réglementation applicable à ce type de collecte, notamment en termes d'information et de consentement.

Pour plus d'informations sur l'utilisation à ces fins des différentes technologies, y compris celle des cookies, voir les Points principaux de la Déclaration IBM de confidentialité sur Internet à l'adresse http://www.ibm.com/privacy, la Déclaration IBM de confidentialité sur Internet à l'adresse http://www.ibm.com/privacy/details à la section nommée “Cookies, pixels espions et autres technologies”, et à la section “IBM Software Products and Software-as-a-Service Privacy Statement” à l'adresse http://www.ibm.com/software/info/product-privacy (en anglais).

Imprimé en France