IBM Security

IBM® Security Access Manager
Opening a Security Vulnerability Case - Mustgather and Remediation

IBM SECURITY SUPPORT OPEN MIC

May 2, 2019

Announcing IBM VIP Rewards

Engage. Earn points. Get Rewards.

IBM VIP Rewards is a way to engage with and recognize the ways that you, the client, add value to IBM. Complete fun challenges and get rewarded for interacting with IBM, learning new technologies and sharing your knowledge.

Learn more...
ibm.biz/vip-rewards

Join IBM VIP Rewards for Security...
ibm.biz/JoinIBMVIPRewards-Security

IBM

IBM VIP Rewards for Security

Come to IBM Security Master Skills University – May 13 - 17

Location: **Hilton Orlando Bonnet Creek – Orlando, FL**

- Learn more about your IBM Security product through advanced education sessions and hands on labs taught by the experts who build, deploy and support these products every day
- Network among a classroom of your peers that have a shared vision and passion for security
- Connect with support experts, discuss how you use your product, and share what you want to achieve with it in 2019

7 tracks will run concurrently. All registrants must select one track in order to attend.

- IBM QRadar - Basic
- IBM QRadar - Advanced
- IBM BigFix
- IBM Guardium
- IBM Resilient
- IBM Identity Governance & Intelligence (IGI)
- IBM Security Access Manager (ISAM) and Cloud Identity

Register now: ibm.com/events/2019/OrlandoMS

Conference fee: $595 USD

IBM **Security Master Skills University – Orlando - 2019**

IBM Security Learning Academy

www.SecurityLearningAcademy.com

New content published daily!

Learning at no cost!

Learning Videos • Hands-on Labs • Live Events

Panelists

Chet Holt – Presenter – ISAM L2 Support Engineer

Steven Seidenberg – Panelist – X-Force Development Manager

Kathy Hansen – Moderator – ISAM L2 Support Manager

Goals of session

- Outline the required data to be submitted when opening an ISAM security vulnerability case.
- Discuss common solutions.
- Give an overview and show implementation of Web Content Protection for advanced threat detection.

Agenda

- What to collect when opening a ticket
- Common solutions
- Web Content Protection
- Questions

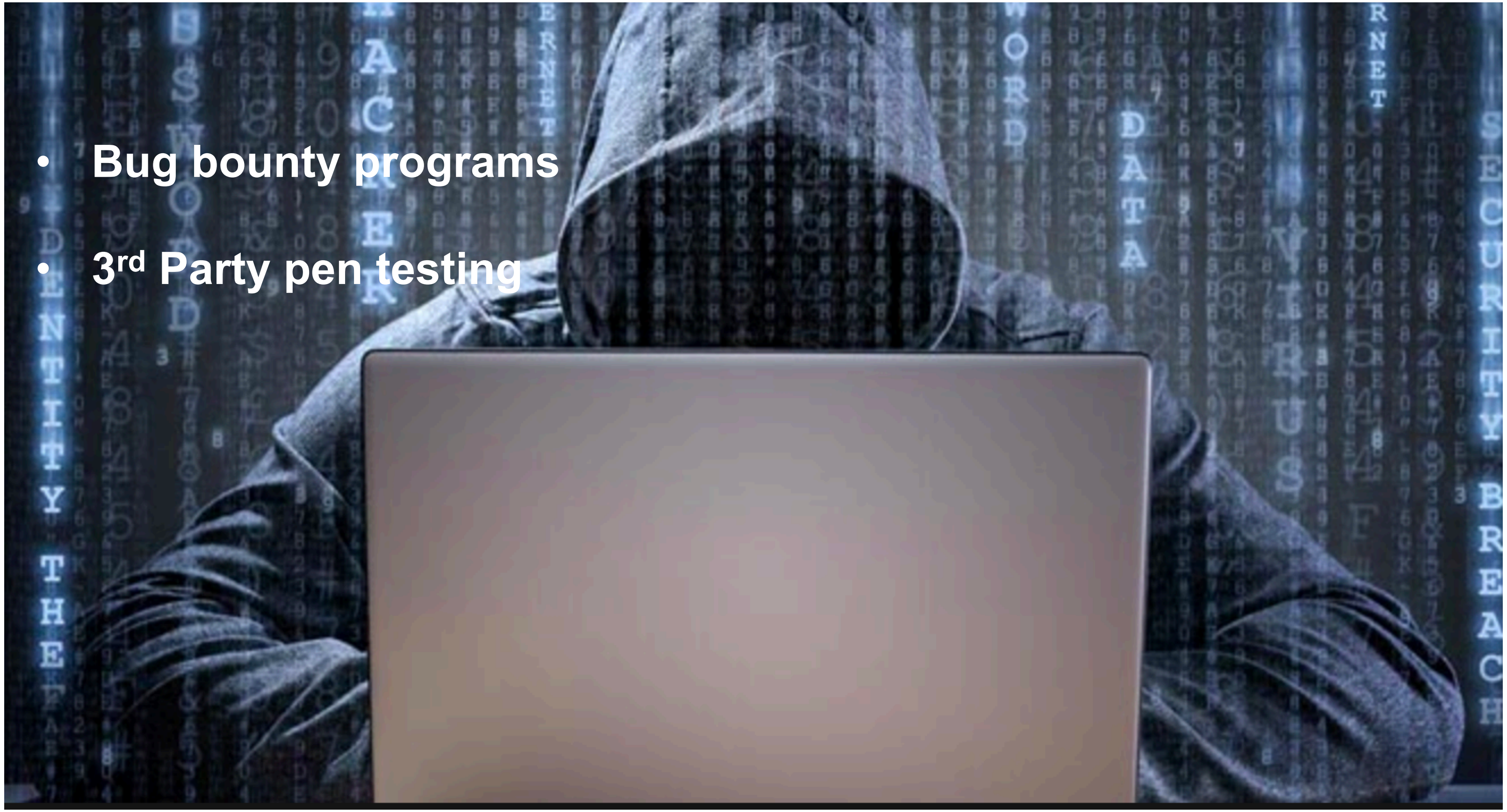
"NOW THAT YOU'RE ALL HERE, LET'S GO OVER THE AGENDA FOR THE MEETING."

Protecting yourself from hackers

Protecting yourself from hackers

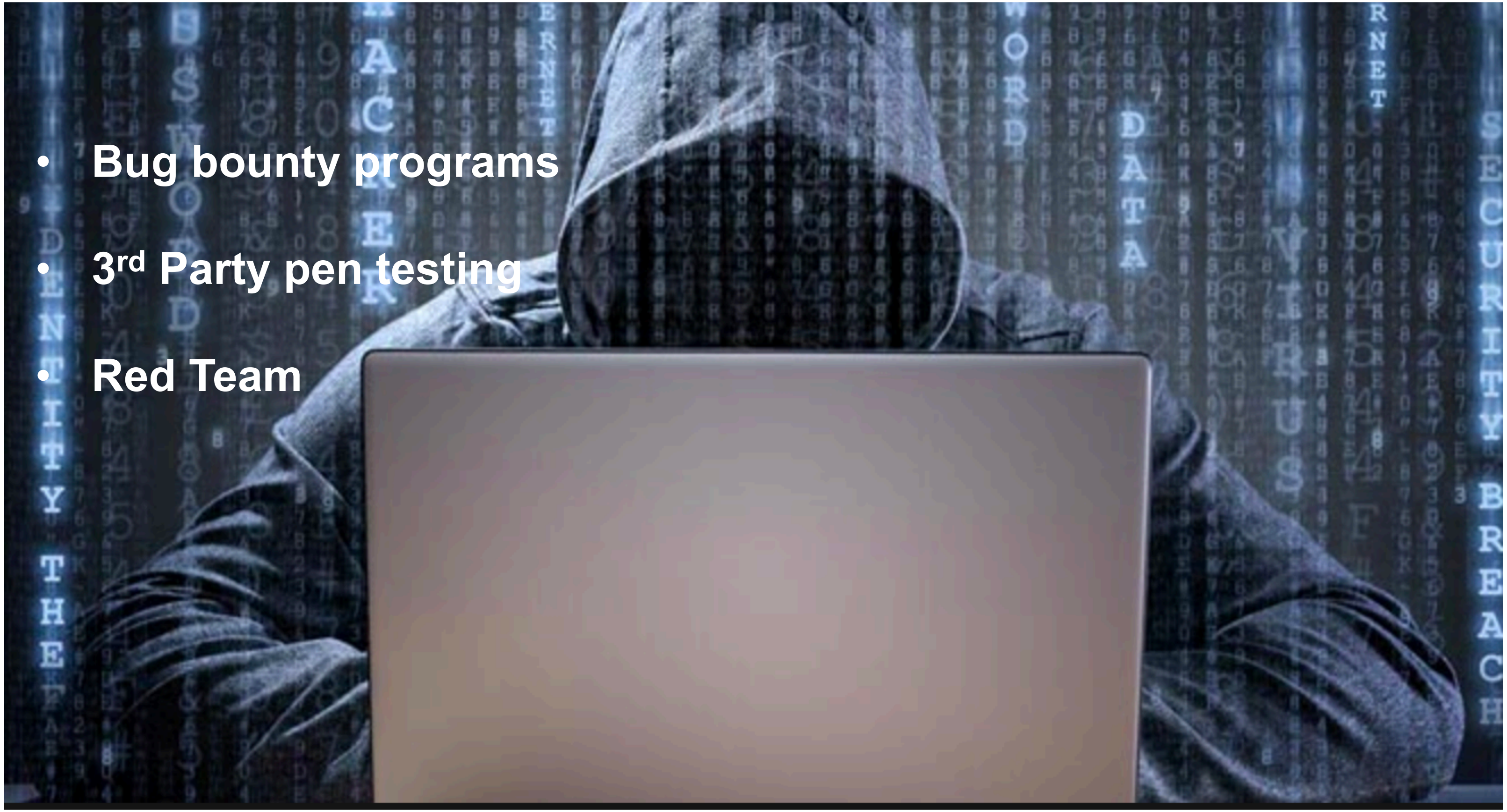
- **Bug bounty programs**

Protecting yourself from hackers



- Bug bounty programs
- 3rd Party pen testing

Protecting yourself from hackers



- Bug bounty programs
- 3rd Party pen testing
- Red Team

Protecting yourself from hackers

- Bug bounty programs
- 3rd Party pen testing
- Red Team
- Security scans

Opening a case to report a security vulnerability

The more information you can provide the better.

Attach the following to the case

- A copy of the report
- Any CVE number/information for vulnerability
- Recreate instructions
  - Curl, burp, fiddler, etc.
- Relevant screenshots
- Support file with:
  - pdweb.snoop trace
  - PAM logging if enabled (more on this later)

Common resolutions to vulnerability cases

Secure Cookie attribute

On by default for WebSEAL session cookie’s – PD-S-SESSION-ID, PD-ID

Not for PD-H-SESSION as it is by default not secure/unauthenticated

Not for any cookie that does not contain sensitive session information

What if I need Secure option on PD_STATEFUL or any other cookie from WebSEAL?

- HTTP Transformation rule
- http://www.ibm.com/support/docview.wss?uid=swg21970418
- Examples on our GitHub

Common resolutions to vulnerability cases

HttpOnly

HttpOnly Cookies – protects against XSS

Reverse proxy config file:

```
[server]
use-http-only-cookies = yes
[junction]
pass-http-only-cookie-attr = yes
```

Common resolutions to vulnerability cases

Block headers to the back-end

Scan reported HTTP Method override using X-HTTP-METHOD-OVERRIDE header through WebSEAL to the backend. Verb tunneling.

Webseald.conf

```
Use the [filter-request-headers] stanza to configure extra HTTP

headers for WebSEAL to filter before it sends a request to a junctioned

server.
```

```
Example:

header = X-HTTP-METHOD-OVERRIDE
```

Common resolutions to vulnerability cases

Illegal sub strings – method for preventing against malicious scripts being run in the browser.

```
Webseald.conf file

[illegal-url-substrings]

substring = <script

substring = <applet

substring = <embed
```

Common resolutions to vulnerability cases

Enable/disable specific protocols/ciphers

```
disable-ssl-v2 = yes
disable-ssl-v3 = yes
disable-tls-v1 = no
disable-tls-v11 = no
disable-tls-v12 = no
```

gsk-attr-name = string:<protocol identifier>:*{comma-separated cipher list on one line, in preferred order}*

jct-gsk-attr-name = = string:<protocol identifier>:*{comma-separated cipher list on one line, in preferred order}*

```
# TLSV12
# Allowed
TLS_RSA_WITH_AES_128_GCM_SHA256 TLS_RSA_WITH_AES_256_GCM_SHA384
TLS_RSA_WITH_AES_128_CBC_SHA256
TLS_RSA_WITH_AES_256_CBC_SHA256 TLS_RSA_WITH_AES_128_CBC_SHA …
```

WHEN ALL ELSE FAILS

Web Content Protection

WHEN ALL ELSE FAILS

Web Content Protection

AKA

WAF

Web Application Firewall

WHEN ALL ELSE FAILS

Web Content Protection

AKA

PAM

Protocol Analysis Module

WHEN ALL ELSE FAILS

Web Content Protection

AKA

The last line of defense

When to use Web Content Protection

When Reverse Proxy configuration cannot resolve scan failures

Higher requirement for protection needed

Pros

Up-to-date threat signatures from X-Force

Cons

Performance hit depending on configuration

- Some customers report up to 10% depending on what content that’s being examined and actions taken

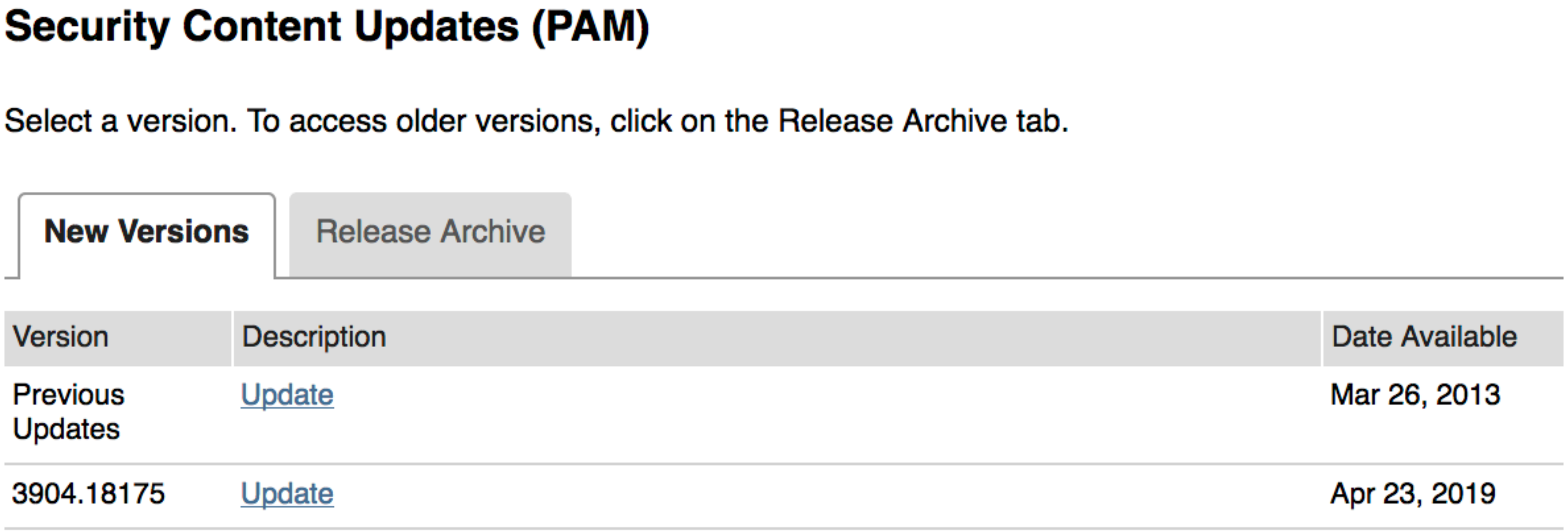
Risk of false positives

WCP – Before you begin

Always update to the latest X-Force PAM module

Techdoc - http://www.ibm.com/support/docview.wss?uid=swg21698111

Download URL - https://ibmss.flexnetoperations.com/control/isdl/product?child_plneID=123870



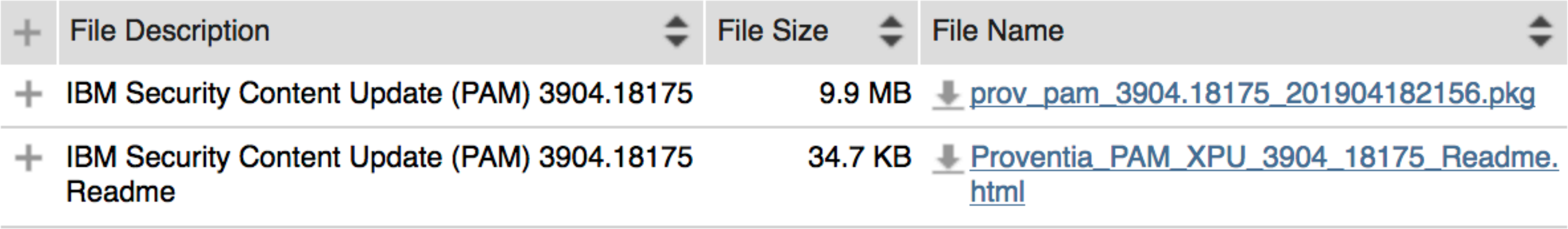
Security Content Updates (PAM)

Select a version. To access older versions, click on the Release Archive tab.

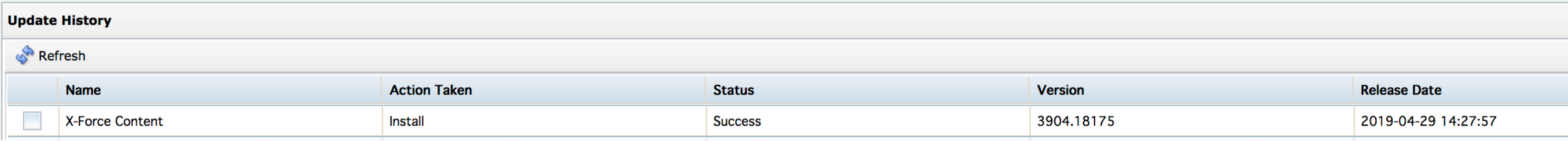
Version	Description	Date Available
Previous Updates	Update	Mar 26, 2013
3904.18175	Update	Apr 23, 2019

Updating WCP PAM module

Download the prov_pam_<version>.pkg file



+	File Description	File Size	File Name
+	IBM Security Content Update (PAM) 3904.18175	9.9 MB	prov_pam_3904.18175_201904182156.pkg
+	IBM Security Content Update (PAM) 3904.18175 Readme	34.7 KB	Proventia_PAM_XPU_3904_18175_Readme.html



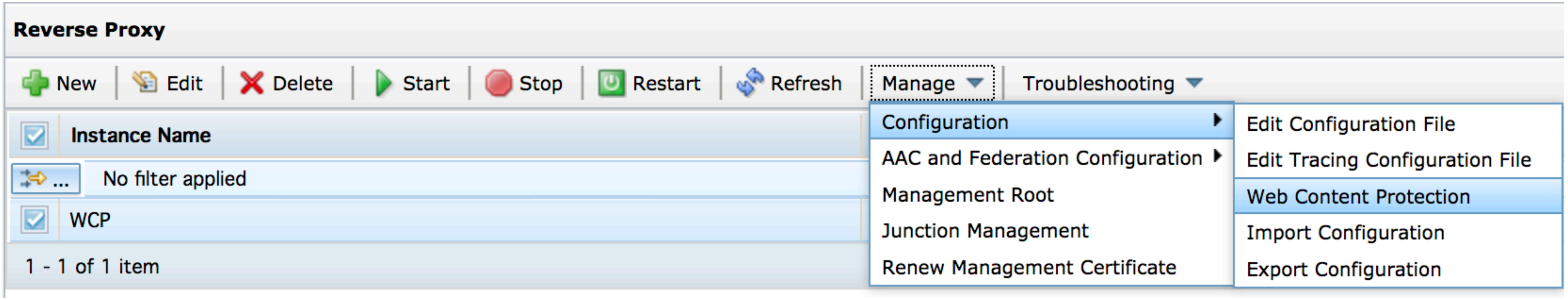
Update History

	Name	Action Taken	Status	Version	Release Date
□	X-Force Content	Install	Success	3904.18175	2019-04-29 14:27:57

pam.log

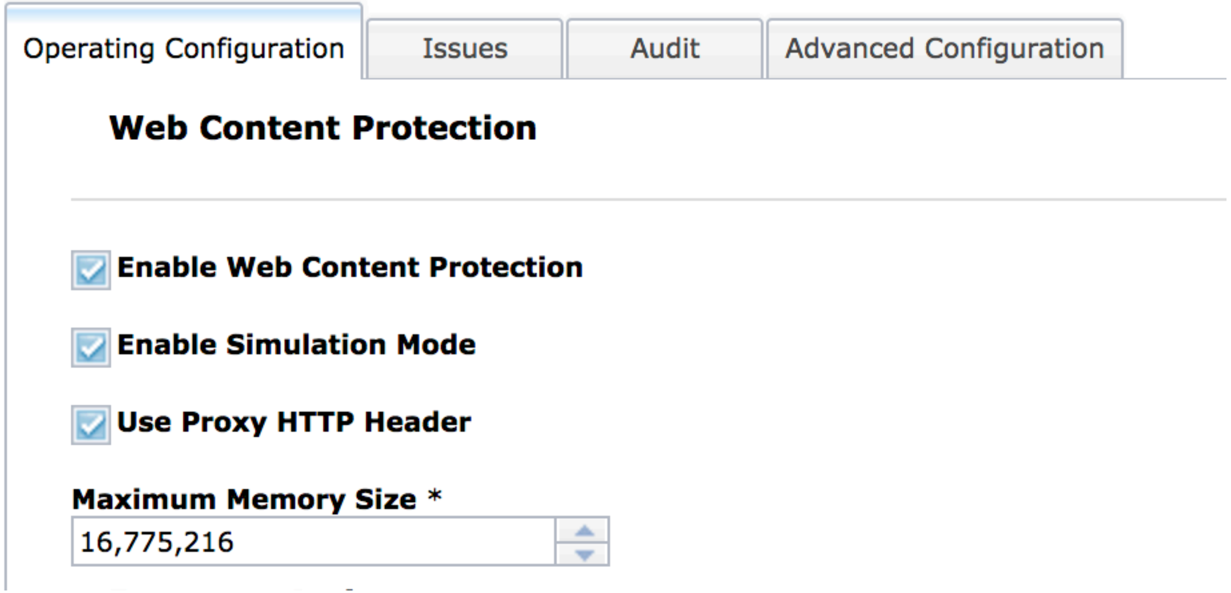
```
<message time="1556555396" value="PAM base=0x7f4c81aee210 guard=0x2d10c6d0 label='7.0-2019.04.18-17.56-XPU_3904.18175 (multithread)'"/>
```

Web Content Protection Configuration



Web Content Protection Configuration

Enable Web Content Protection



Web Content Protection

☑ **Enable Web Content Protection**

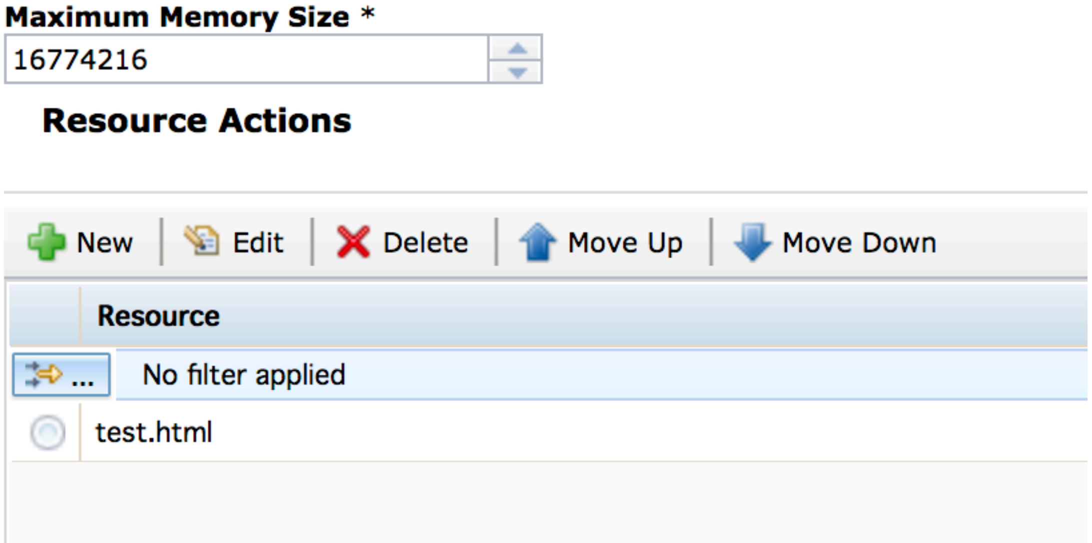
☑ **Enable Simulation Mode**

☑ **Use Proxy HTTP Header**

Maximum Memory Size *
16,775,216

Web Content Protection Configuration

- Configure Resource Actions



Maximum Memory Size *

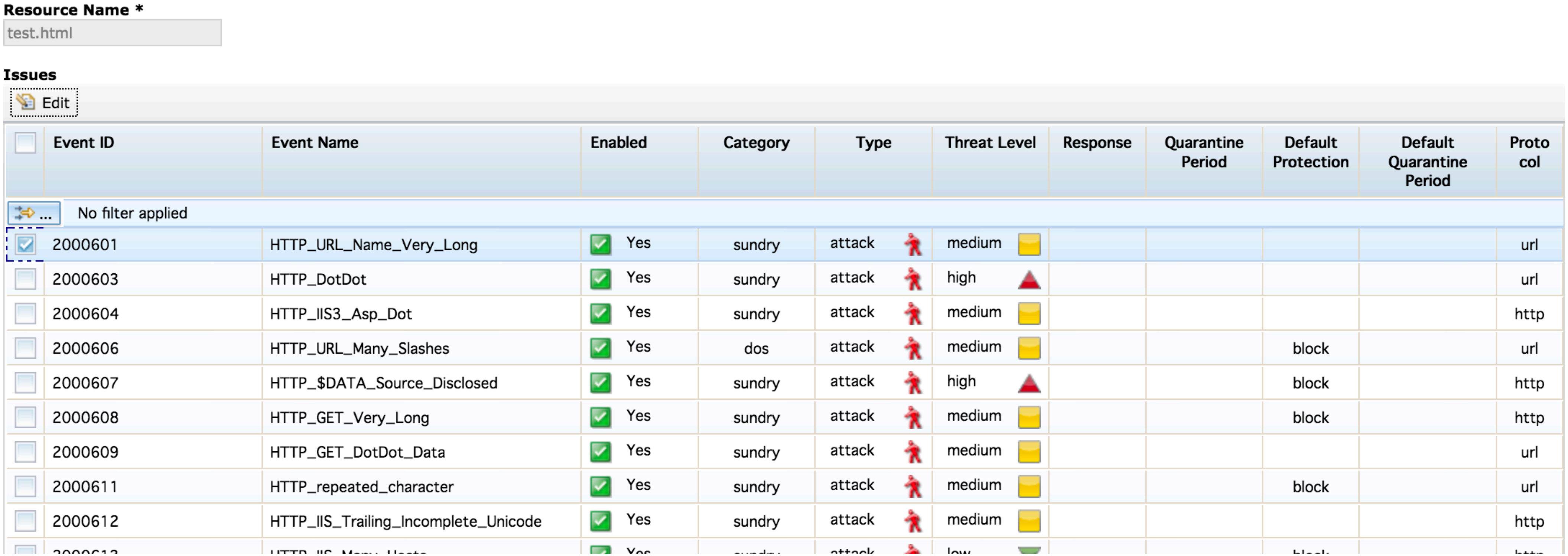
16774216

Resource Actions

	Resource
...	No filter applied
○	test.html

Web Content Protection Configuration

- Configure a Resource Action – Threat signatures



Resource Name *

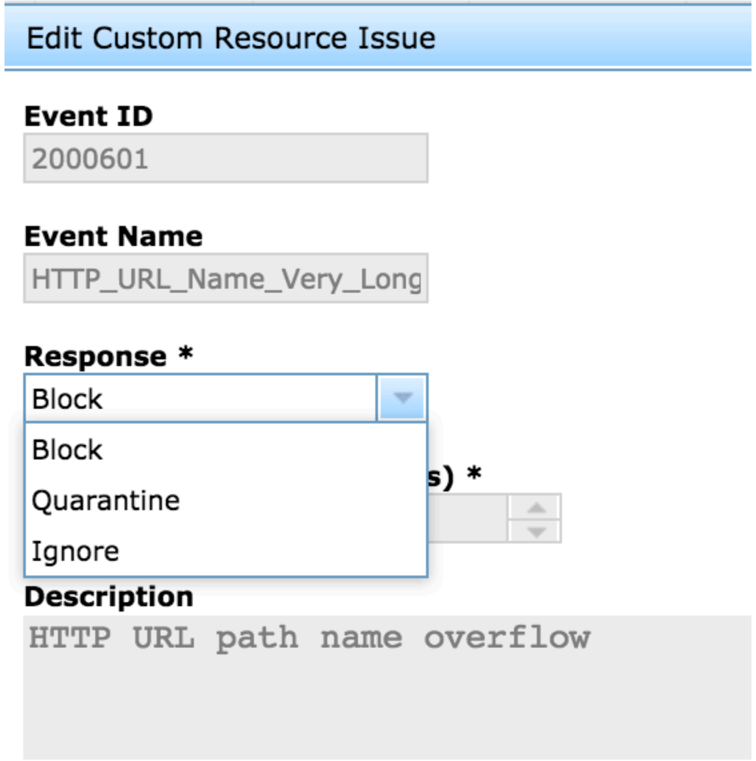
test.html

Issues

□	Event ID	Event Name	Enabled	Category	Type	Threat Level	Response	Quarantine Period	Default Protection	Default Quarantine Period	Proto col
☑	2000601	HTTP_URL_Name_Very_Long	✓ Yes	sundry	attack	medium 🟨					url
□	2000603	HTTP_DotDot	✓ Yes	sundry	attack	high ▲					url
□	2000604	HTTP_IIS3_Asp_Dot	✓ Yes	sundry	attack	medium 🟨					http
□	2000606	HTTP_URL_Many_Slashes	✓ Yes	dos	attack	medium 🟨			block		url
□	2000607	HTTP_$DATA_Source_Disclosed	✓ Yes	sundry	attack	high ▲			block		http
□	2000608	HTTP_GET_Very_Long	✓ Yes	sundry	attack	medium 🟨			block		http
□	2000609	HTTP_GET_DotDot_Data	✓ Yes	sundry	attack	medium 🟨					url
□	2000611	HTTP_repeated_character	✓ Yes	sundry	attack	medium 🟨			block		url
□	2000612	HTTP_IIS_Trailing_Incomplete_Unicode	✓ Yes	sundry	attack	medium 🟨					http
□	2000613	HTTP_IIS_Many_Hosts	✓ Yes	sundry	attack	low ▼			block		http

Web Content Protection Configuration

- Configure Resource Action – Update Action



Edit Custom Resource Issue

Event ID
2000601

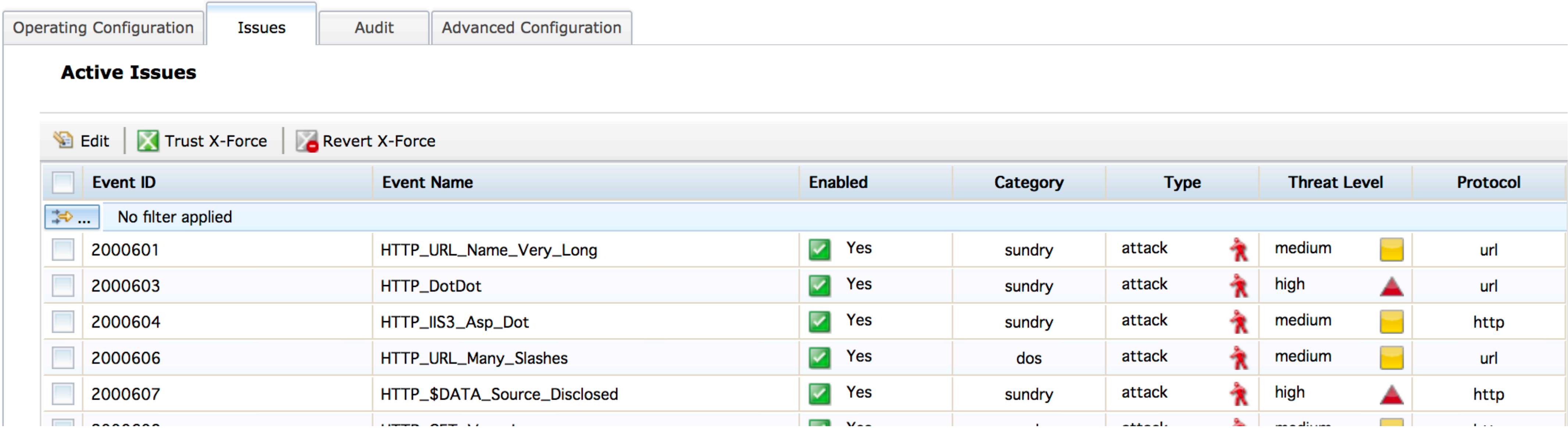
Event Name
HTTP_URL_Name_Very_Long

Response *
Block

Description
HTTP URL path name overflow

Web Content Protection Configuration

- Default Resource Action
- If request sent to PAM does not match any of the patterns in the list it gets the default policy:

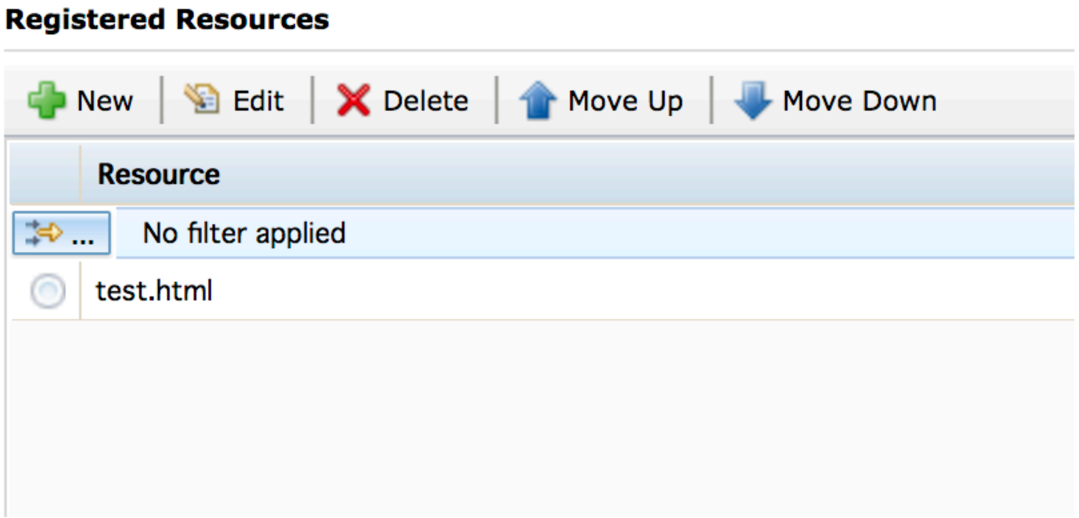


Active Issues

□	Event ID	Event Name	Enabled	Category	Type	Threat Level	Protocol
...	No filter applied						
□	2000601	HTTP_URL_Name_Very_Long	✓ Yes	sundry	attack	medium 🟨	url
□	2000603	HTTP_DotDot	✓ Yes	sundry	attack	high ▲	url
□	2000604	HTTP_IIS3_Asp_Dot	✓ Yes	sundry	attack	medium 🟨	http
□	2000606	HTTP_URL_Many_Slashes	✓ Yes	dos	attack	medium 🟨	url
□	2000607	HTTP_$DATA_Source_Disclosed	✓ Yes	sundry	attack	high ▲	http

Web Content Protection Configuration

- Configure Registered Resources



Registered Resources

	Resource
...	No filter applied
○	test.html

Web Content Protection

- Sample request and pam.log entry

```
$ curl -i -k https://192.168.198.171:444/ -H "Accept:*/*" -H "Content-Type:application/json" -d
'{"uid":"clefleur<script>alert(document.cookie)</script>","canale": "email"}' -X POST
```

Connection reset by WebSEAL

```
curl: (52) Empty reply from server
```

Pam.log entry

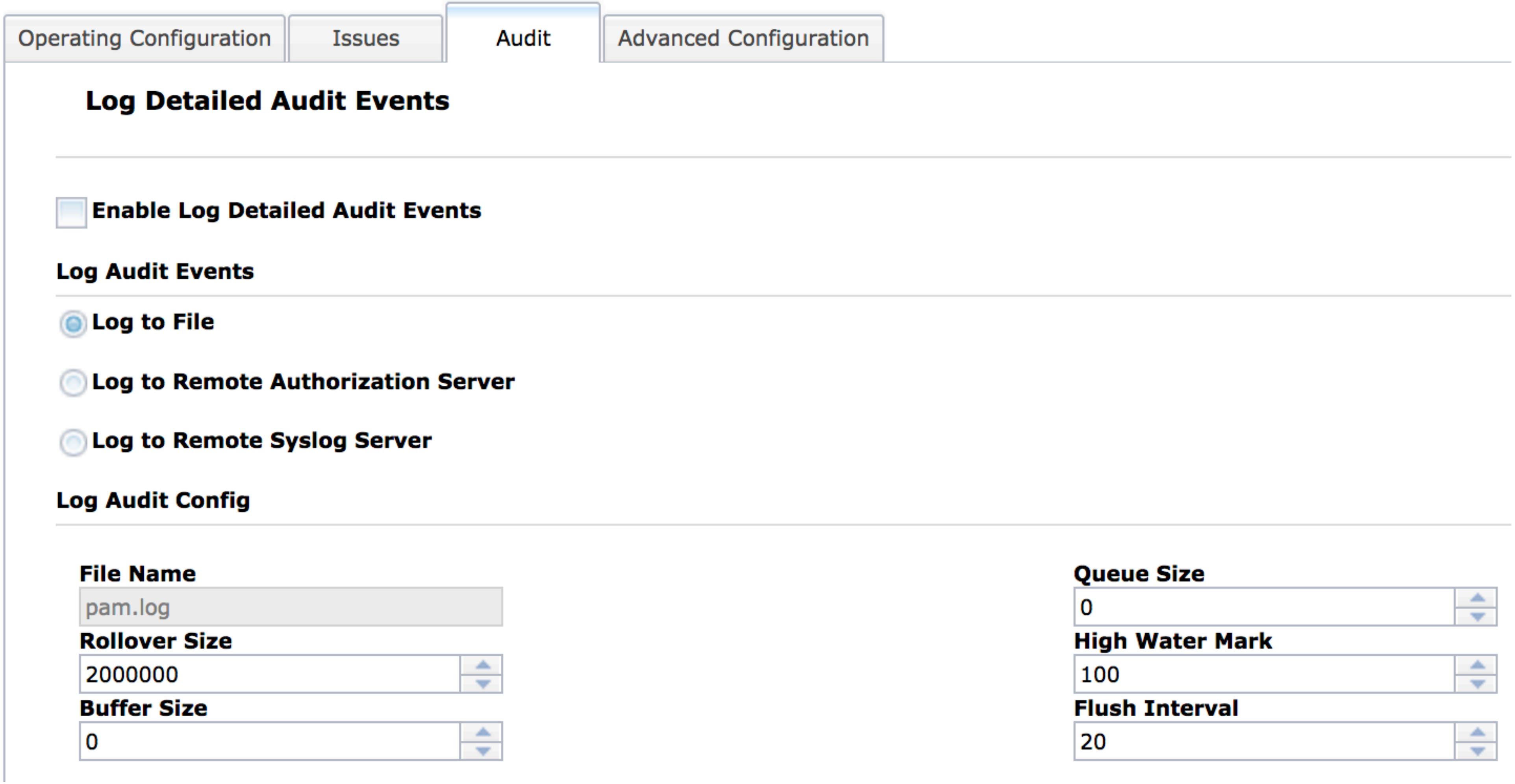
```
<issue id="2141016" name="Json_Embedded_JavaScript" start="1551207034" intruder="192.168.198.1"
victim="192.168.198.163:444"><events action="Block" mode="enforcing"><event resource="/"/><event
resource="/"/></events></issue>
```

Web Content Protection Flow

The process flow works as such :

- When PAM is enabled (even in simulation mode) and the Reverse Proxy receives a request it will check the URI against registered resources to confirm whether it should be passed to the PAM layer.
- If it is passed to the PAM layer then PAM will search for a [pam-resource:<uri_pattern>]' stanza that matches – This is the resource action
  - If one matches, this custom rule set will be used on the resource
  - If there is no match the default PAM rule set will be applied to the resource
- If it is not passed to the PAM layer then ISAM will move on

Web Content Protection Audit / Logging



Log Detailed Audit Events

□ Enable Log Detailed Audit Events

Log Audit Events

● Log to File

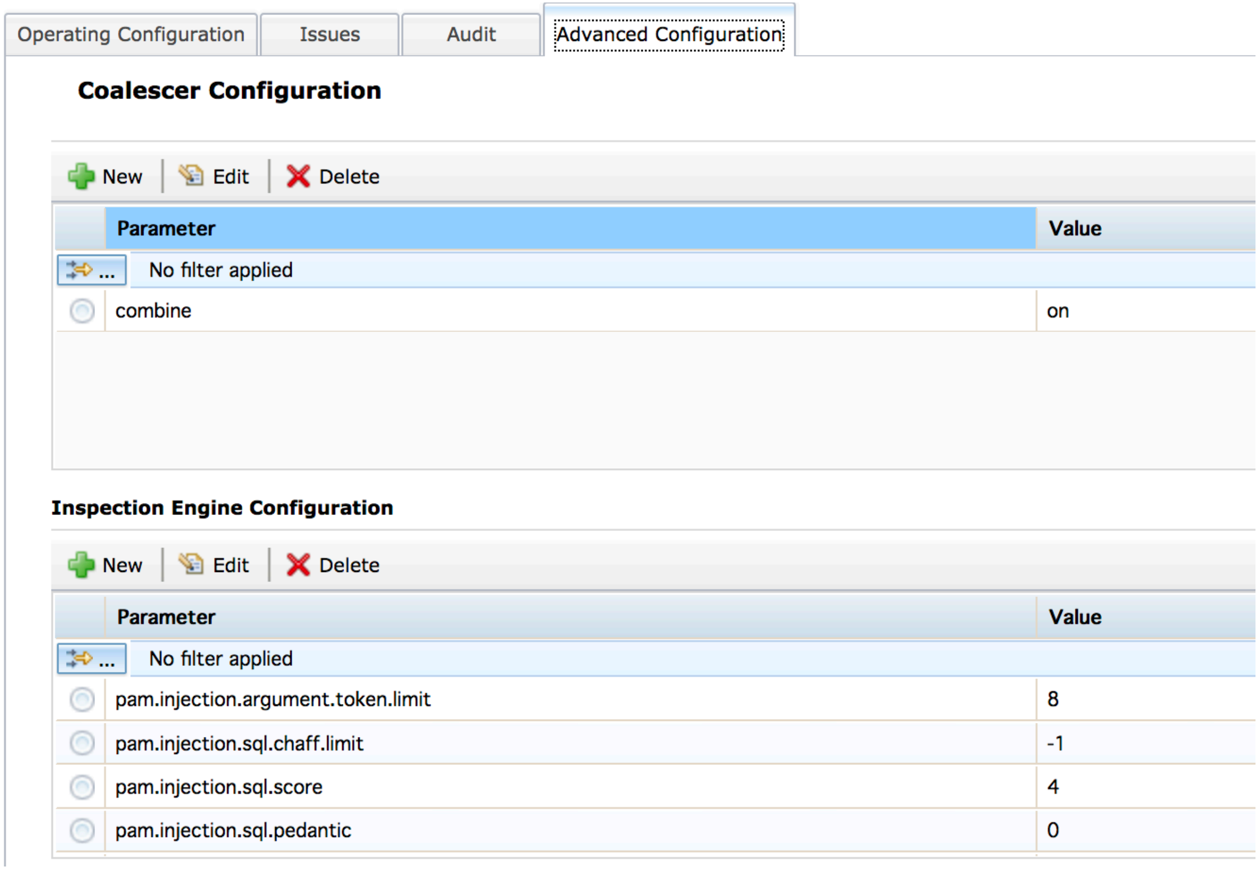
○ Log to Remote Authorization Server

○ Log to Remote Syslog Server

Log Audit Config

File Name: pam.log	Queue Size: 0
Rollover Size: 2000000	High Water Mark: 100
Buffer Size: 0	Flush Interval: 20

Advanced Configuration



Coalescer Configuration

Parameter	Value
combine	on

Inspection Engine Configuration

Parameter	Value
pam.injection.argument.token.limit	8
pam.injection.sql.chaff.limit	-1
pam.injection.sql.score	4
pam.injection.sql.pedantic	0

Questions for the panel

Now is your opportunity to ask questions of our panelists.

To ask a question now:

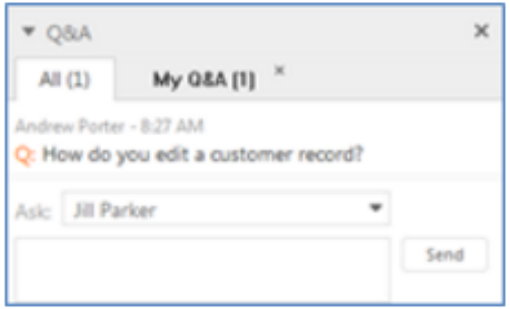
Raise your hand by clicking Raise Hand. The Raise Hand icon appears next to your name in the Attendees panel on the right in the WebEx Event. The host will announce your name and unmute your line.

or

Type a question in the box below the Ask drop-down menu in the Q&A panel.

Select *All Panelists* from the Ask drop-down-menu.

Click Send. Your message is sent and appears in the Q&A panel.



Andrew Porter - 8:27 AM

Q: How do you edit a customer record?

Ask: Jill Parker

To ask a question after this presentation:

You are encouraged to participate in the new IBM Support Forums:

https://www.ibm.com/mysupport/s/forumshome

Where do you get more information?

Questions on this or other topics can be directed to the ISAM forum:
http://ibm.biz/ISAM-support-forum

More information:

- **Security Learning Academy for Identity and Access Management: https://ibm.biz/IAM-SecLearnAcademy**
- **ISAM documentation:**
  https://www.ibm.com/support/knowledgecenter/SSPREK_9.0.6/com.ibm.isam.doc/welcome.html

Useful links:

Get started with IBM Security Support

IBM My Support | Sign up for “My Notifications”

FREE learning resources on the Security Learning Academy

ibm.com/security/community

Follow us:

www.youtube.com/user/IBMSecuritySupport twitter.com/askibmsecurity http://ibm.biz/ISCS-LinkedIn

IBM Security

THANK YOU

FOLLOW US ON:

youtube/user/IBMSecuritySupport

@askibmsecurity

IBM Security Client Success

SecurityLearningAcademy.com

securityintelligence.com

xforce.ibmcloud.com

ibm.com/security/community

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM does not warrant that any systems, products or services are immune from, or will make your enterprise immune from, the malicious or illegal conduct of any party.

IBM