Web Application Security Made ~~Easy~~ Easier

Brian A. McHenry

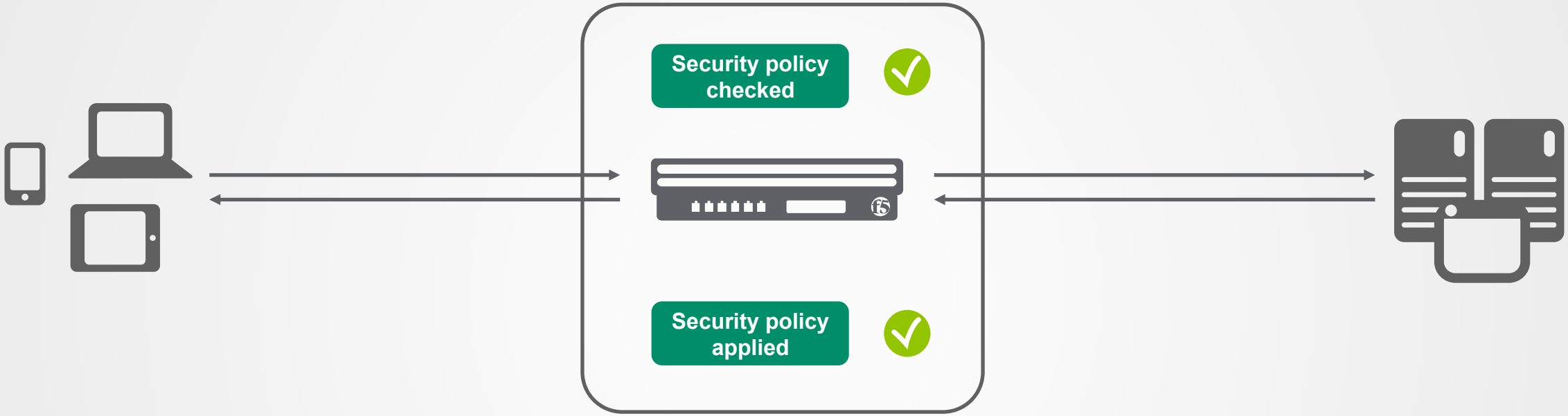
Security Solutions Architect

bam@f5.com

Practical Web Application Security Facts

- Remediation rates are low, especially for legacy or 3rd-party applications
- Building WAF policy is one tactic, but can also be challenging
- Applications are like snowflakes; no two alike
- WAF ownership varies, and AppSec expertise varies with it
- A WAF is only as effective as the integration with the SDLC process
- Management resources for WAF are often limited

Policy Deployment Options



DYNAMIC POLICY BUILDER

Automatic

- No knowledge of the app required
- Adjusts policies if app changes

Manual

- Advanced configuration for custom policies

INTEGRATION WITH APP SCANNERS

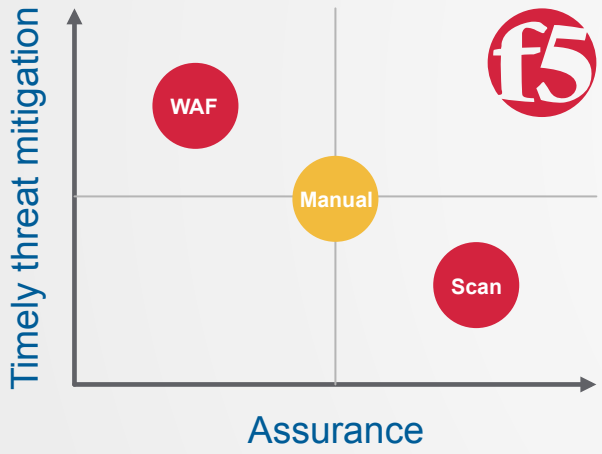
- Virtual patching with continuous application scanning

PRE-BUILT POLICIES

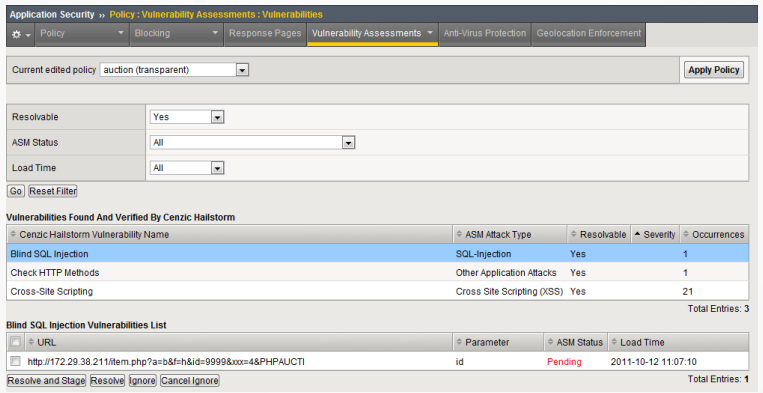
- Out-of-the-box
- Pre-configure and validated
- For mission-critical apps including: Microsoft, Oracle, PeopleSoft

Identify, virtually patch, mitigate vulnerabilities

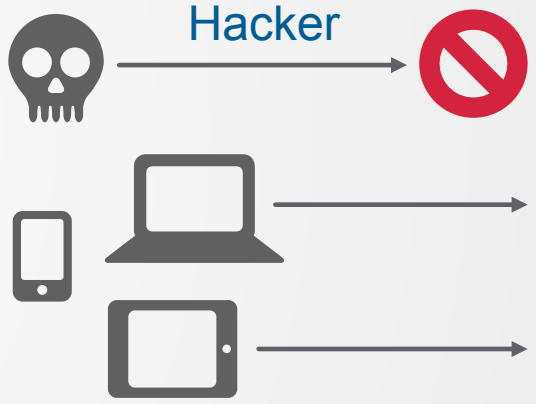
Scan application with:



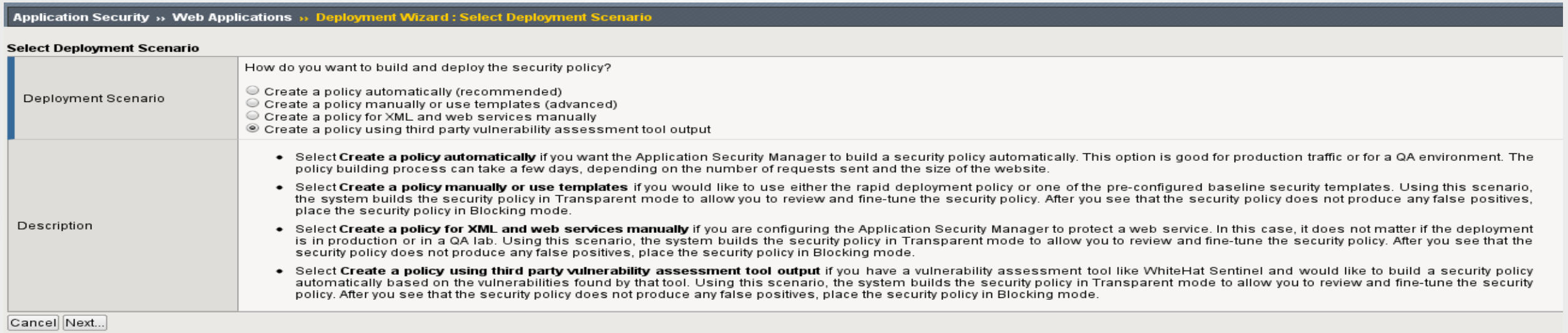
Configure vulnerability policy in BIG-IP ASM

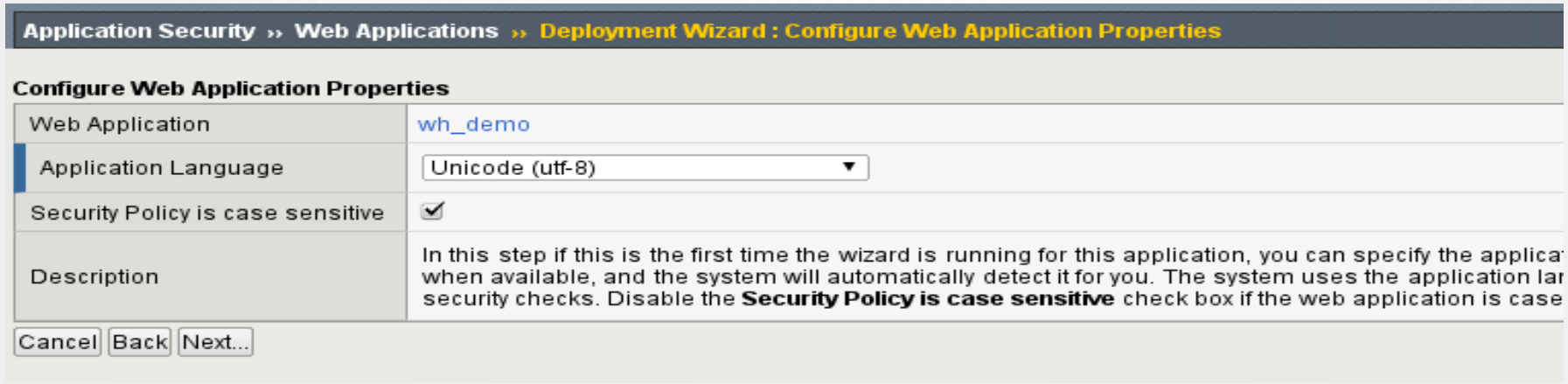


Mitigate web app attacks



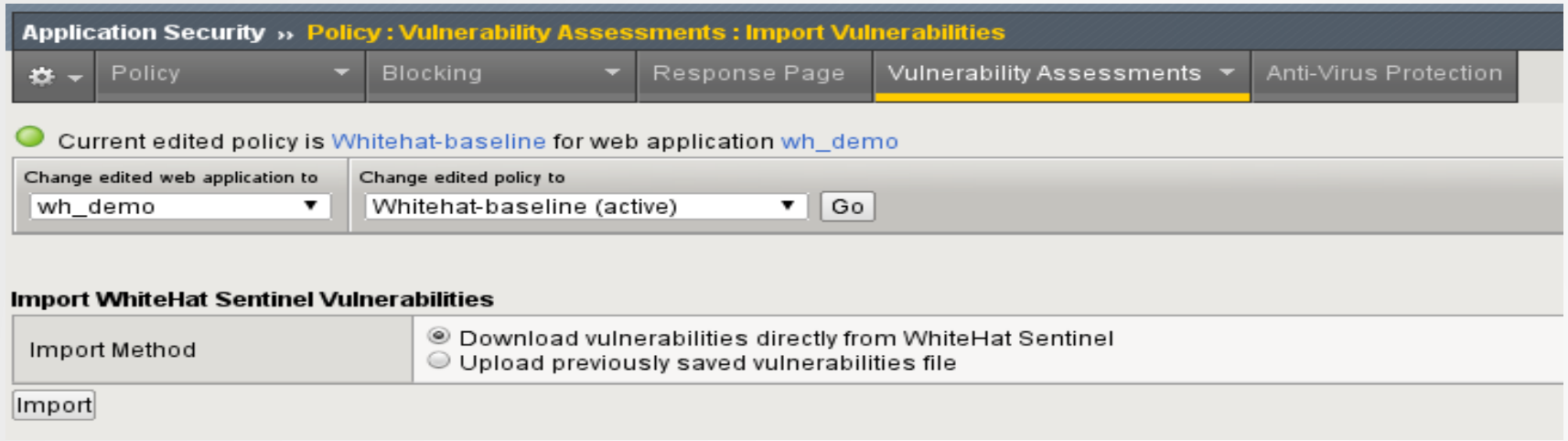
Configuration

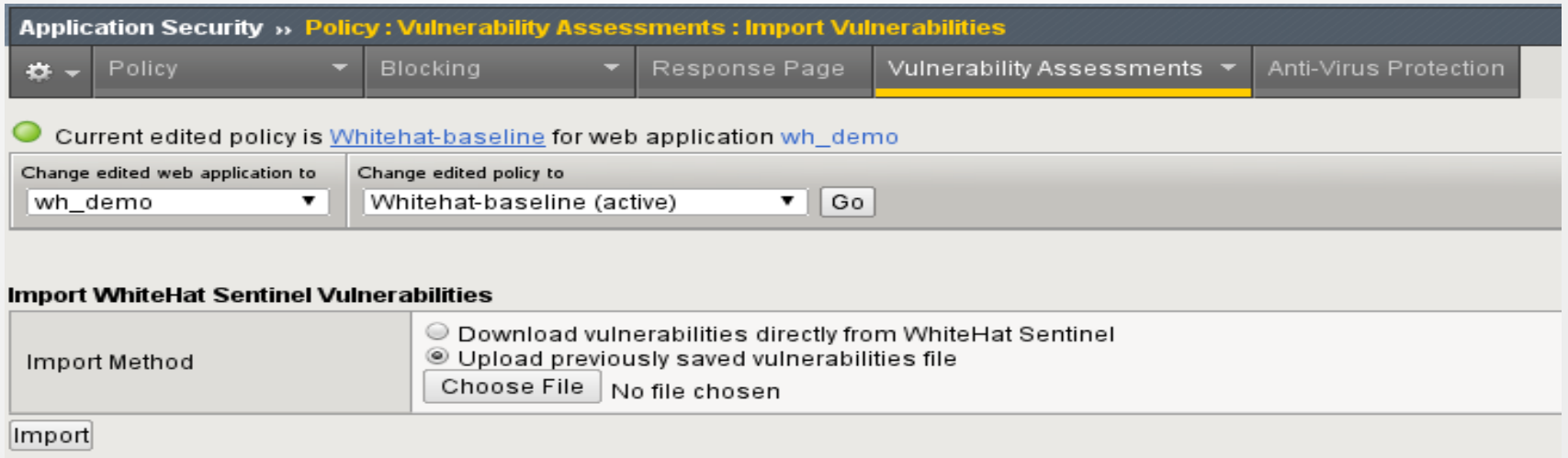




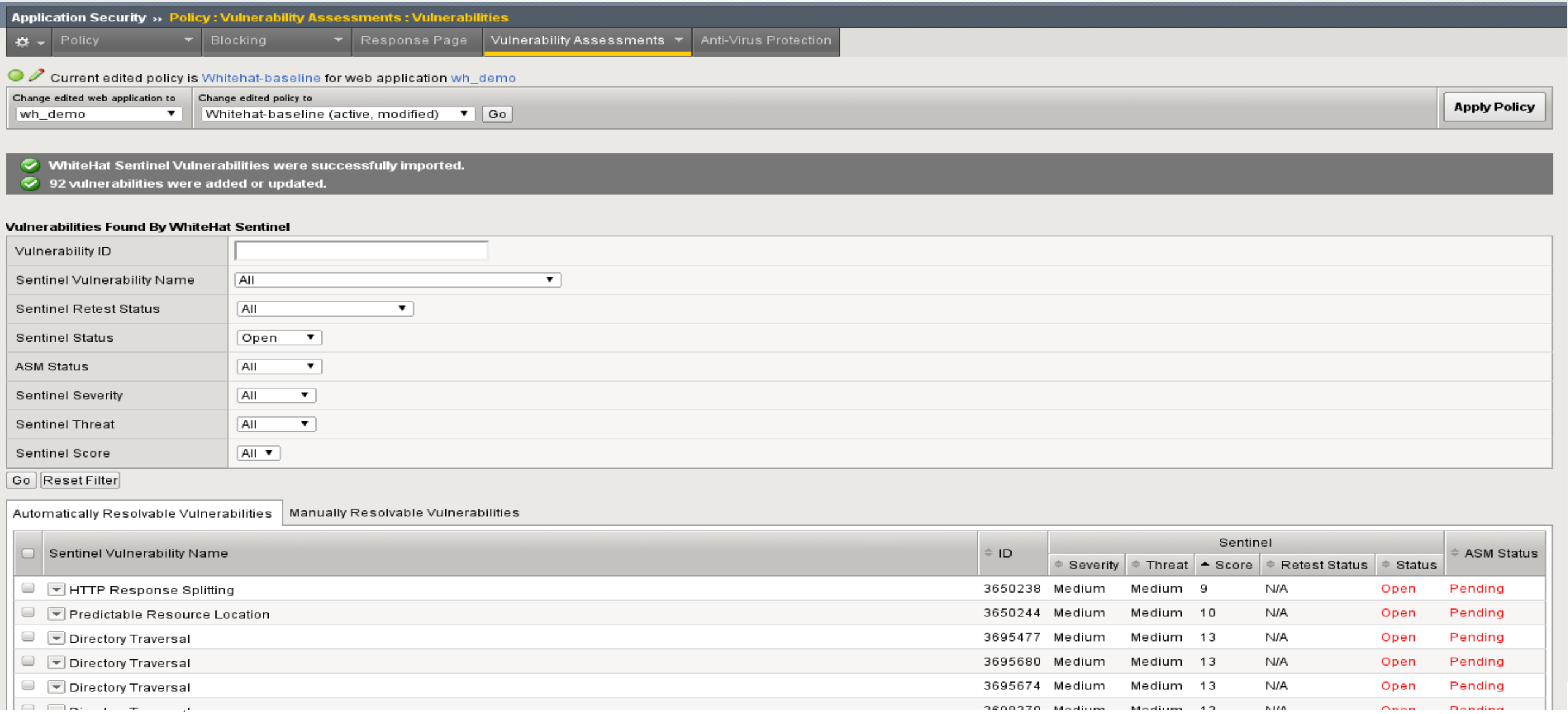
Configuration

Importing Vulnerabilities





Importing Vulnerabilities



A Deeper Look

Automatically Resolvable Vulnerabilities | Manually Resolvable Vulnerabilities

Sentinel Vulnerability Name	ID	Sentinel					ASM Status
		Severity	Threat	Score	Retest Status	Status	
HTTP Response Splitting	3650238	Medium	Medium	9	N/A	Open	Pending
ASM Attack Type: HTTP Response Splitting							
URL: http://71.141.64.43/w3af/audit/response_splitting/response_splitting_err.php?header=None							
Predictable Resource Location	3650244	Medium	Medium	10	N/A	Open	Pending
ASM Attack Type: Predictable Resource Location							
URL: http://71.141.64.43/http://71.141.64.43/mod_security/w3af/audit/xss/stored/data							
Directory Traversal	3695477	Medium	Medium	13	N/A	Open	Pending
ASM Attack Type: Path Traversal							
URL: http://qatest4.qa.wh/w3af/audit/remoteFileInclusion/vulnerable.php?file=/../../../../../../../../../../../../etc/hosts%00							
Parameter: file							
Directory Traversal	3695680	Medium	Medium	13	N/A	Open	Pending
Directory Traversal	3695674	Medium	Medium	13	N/A	Open	Pending
Directory Traversal	3698370	Medium	Medium	13	N/A	Open	Pending

A Deeper Look

Cross Site Scripting	2152264	Medium	Medium	14	N/A	Open	Pending
OS Command Injection	3695424	Medium	Medium	14	N/A	Open	Pending
Cross Site Scripting	2152664	Medium	Medium	14	N/A	Open	Pending

ASM Attack Type	Cross Site Scripting (XSS)		
URLs	Total: 1	In policy: 0	In staging: 0
Parameters	Total: 11	In policy: 0	In staging: 0

URL	http://71.141.64.43/wh/xss.php?var_xss1=1&var_xss2=2&var_xss3=3&var_xss4=4&var_xss5=5&var_↵ xss6=6&var_xss7=7&var_xss8=8&var_xss9=%3Cwhscheck%3E&var_xss10=10
Parameter	var_xss9

URL	http://71.141.64.43/wh/xss.php?var_xss1=1&var_xss2=%3Cwhscheck%3E&var_xss3=3&v↵ ar_xss4=4&var_xss5=5&var_xss6=6&var_xss7=7&var_xss8=8&var_xss9=9&var_xss10=10
Parameter	var_xss2

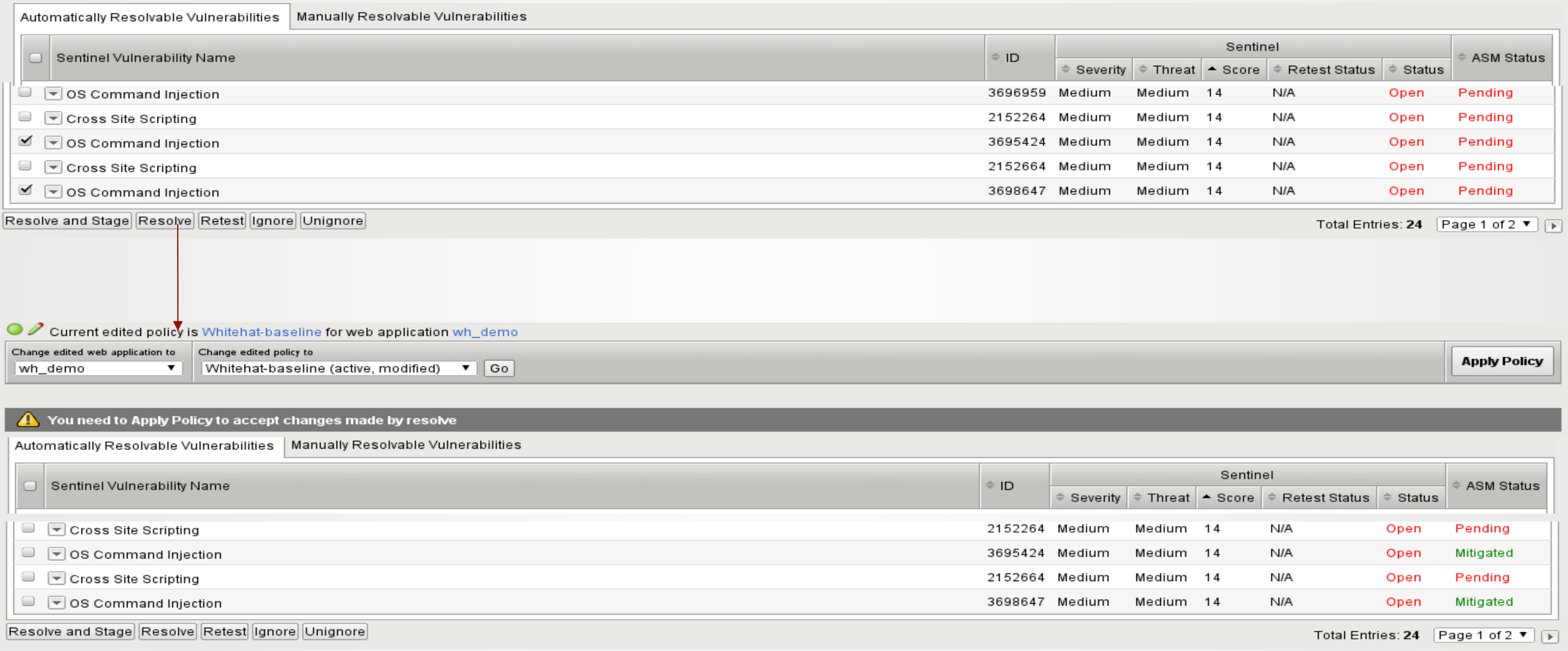
URL	http://71.141.64.43/wh/xss.php?var_xss1=1&var_xss2=2&var_xss3=3&var_xss4=4&var_xss5=5&var_xss6=<w↵ hscheck>&var_xss7=7&var_xss8=8&var_xss9=9&var_xss10=10
Parameter	var_xss6

URL	http://71.141.64.43/wh/xss.php?var_xss1=1&var_xss2=2&var_xss3=3&var_xss4=%00%3↵ Cwhscheck%3E&var_xss5=5&var_xss6=6&var_xss7=7&var_xss8=8&var_xss9=9&var_xss10=10
Parameter	var_xss4

URL	http://71.141.64.43/wh/xss.php?var_xss1=1&var_xss2=<whscheck>&var_xss3=3&var_xss4=4&var_xss5=5&var_↵ xss6=6&var_xss7=7&var_xss8=8&var_xss9=9&var_xss10=10
Parameter	var_xss2

URL	http://71.141.64.43/wh/xss.php?var_xss1=1&var_xss2=2&var_xss3=3&var_xss4=4&var_xss5=5&var_↵ xss6=6&var_xss7=7&var_xss8=8&var_xss9=9&var_xss10=%3Cwhscheck%3E
Parameter	var_xss10

Resolve, Resolve and Stage



Resolve, Resolve and Stage

OS Command Injection	3696959	Medium	Medium	14	N/A	Open	Pending
Cross Site Scripting	2152264	Medium	Medium	14	N/A	Open	Mitigated

ASM Attack Type	Cross Site Scripting (XSS)		
URLs	Total: 1	In policy: 1	In staging: 0
Parameters	Total: 11	In policy: 11	In staging: 0

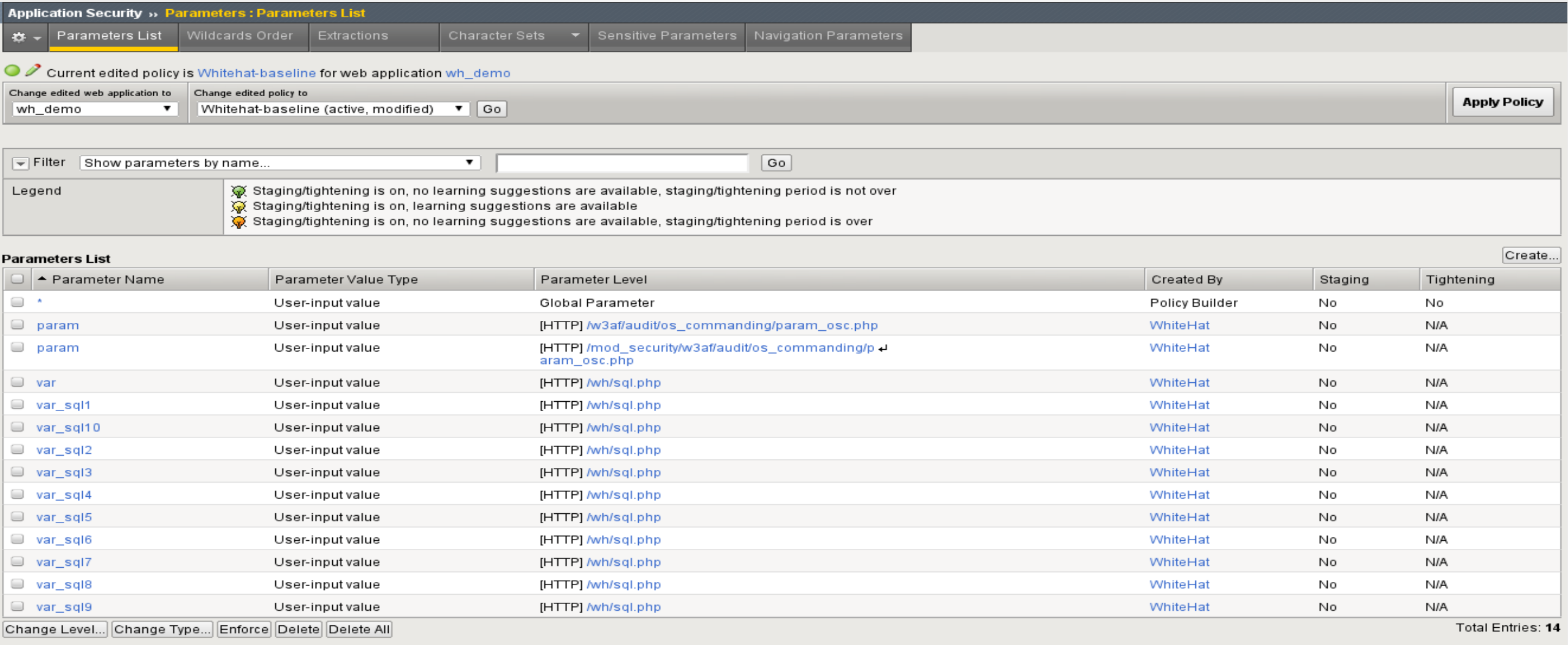
URL	http://71.141.64.43/wh/sql.php?var_sql1=1&var_sql2=%3Cwhscheck%3E&var_sql3=3&var_sql4=4&var_sql5=5&var_sql6=6&var_sql7=7&var_sql8=8&var_sql9=9&var_sql10=10
Parameter	var_sql2

URL	http://71.141.64.43/wh/sql.php?var_sql1=1&var_sql2=%00%3Cwhscheck%3E&var_sql3=3&var_sql4=4&var_sql5=5&var_sql6=6&var_sql7=7&var_sql8=8&var_sql9=9&var_sql10=10
Parameter	var_sql2

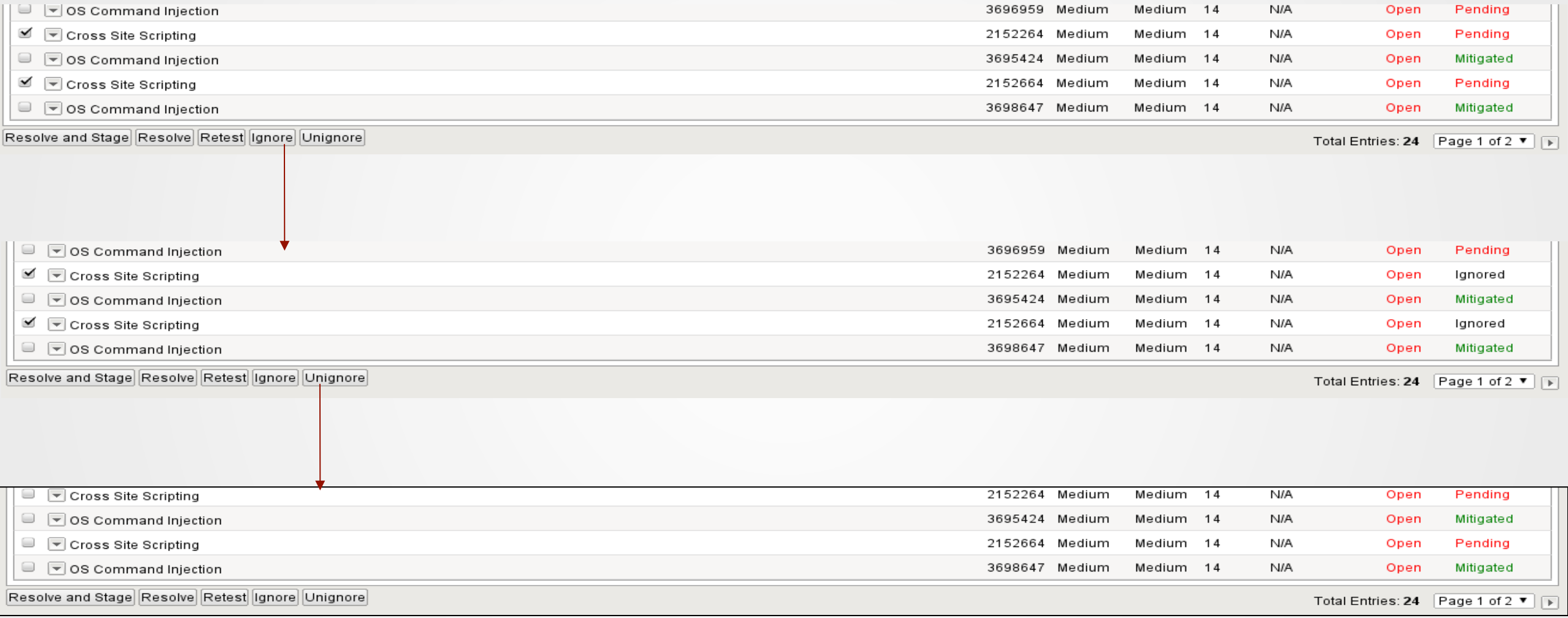
URL	http://71.141.64.43/wh/sql.php?var_sql1=1&var_sql2=2&var_sql3=3&var_sql4=4&var_sql5=5&var_sql6=6&var_sql7=7&var_sql8=8&var_sql9=<whscheck>&var_sql10=10
Parameter	var_sql9

URL	http://71.141.64.43/wh/sql.php?var_sql1=1&var_sql2=2&var_sql3=3&var_sql4=4&var_sql5=5&var_sql6=6&var_sql7=<whscheck>&var_sql8=8&var_sql9=9&var_sql10=10
Parameter	var_sql7

Resolve, Resolve and Stage



Ignore, Unignore



Retest

- The same attack vectors will be re-sent during a retest.
- Asynchronous

Automatically Resolvable Vulnerabilities | Manually Resolvable Vulnerabilities

Sentinel Vulnerability Name	ID	Sentinel					ASM Status
		Severity	Threat	Score	Retest Status	Status	
Cross Site Scripting	2152264	Medium	Medium	14	N/A	Open	Pending
OS Command Injection	3695424	Medium	Medium	14	N/A	Open	Mitigated
Cross Site Scripting	2152664	Medium	Medium	14	N/A	Open	Pending
OS Command Injection	3698647	Medium	Medium	14	Retest Requested	Open	Mitigated

Resolve and Stage | Resolve | Retest | Ignore | Unignore

Total Entries: **24** Page 1 of 2

- ... after a couple of minutes ...

Automatically Resolvable Vulnerabilities | Manually Resolvable Vulnerabilities

Sentinel Vulnerability Name	ID	Sentinel					ASM Status
		Severity	Threat	Score	Retest Status	Status	
Cross Site Scripting	3632944	Medium	Medium	14	N/A	Closed	Pending
OS Command Injection	3698647	Medium	Medium	14	N/A	Closed	Mitigated
Cross Site Scripting	3632925	Medium	Medium	14	N/A	Closed	Pending

Retest

- ASM polls the status of the 'Retest Requested' vulnerabilities each 2 minutes.
- Vulnerabilities are to be retested are queued in the Sentinel. Generally they process in some minutes.
- Can end up with:
  - Opened (vulnerability was not mitigated)
  - Closed (vulnerability was solved)
  - Mitigated (vulnerability was mitigated by ASM)

We couldn’t have provided safe remote access to SharePoint without the security F5 offers through BIG-IP ASM. And we don’t have to spend hours reviewing thousands of vulnerability log entries in order to configure ASM effectively.

- IT Director, Large US Community College

“By deploying F5’s comprehensive Application Security Manager (ASM) solution, Aura is now enabling customers to fix its security issues within a reasonable timeframe, and subsequently shield and prevent reoccurrences.