

Qualys WAS 4.3 New Features

Being able to customize your web application scans just as much as your web applications are customized for your business is important. We get that. Qualys has always listened to our users' feedback and therefore made changes and developed cutting edge features to meet your needs. The release of WAS 4.3 is no different. With Qualys WAS 4.3, organizations now have the ability to easily further customize their scans based upon their web apps and specific properties thereof. Customers can also now receive clearer and enhanced feedback on the behavior and coverage of their scans. This will also allow customers to continue to deliver targeted web application security metrics to all the stakeholders while ensuring a successful web application security program meets the protection of all organizational demands.

Feature highlights include:

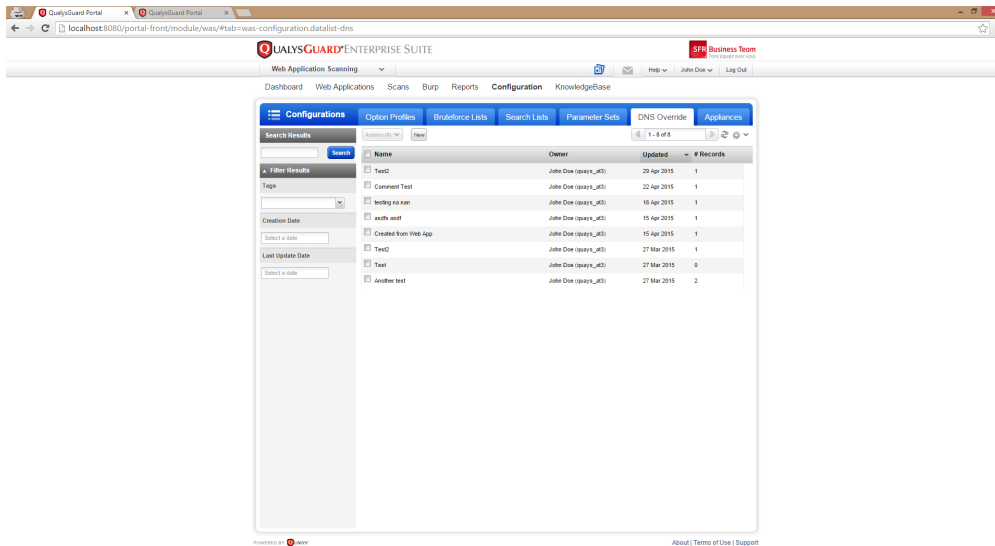
- **Override DNS for WAS Scans**
- **Enhanced Support for Sitemap for Scans**
- **Enhanced Patchable Detections Logic**
- **Clarify Time Limit Exceeded and Time Limit Reached and Scan Timeout**
- **Enhanced WAS Scan Reports**
- **Implement Web Application Custom Attributes**
- **User Customizable Mail Settings for When Scan is Launched**
- **Enhance Tag Selection Component in WAS Module**
- **WAS Search Lists - Deprecate Compliance Type options**

Override DNS for WAS Scans

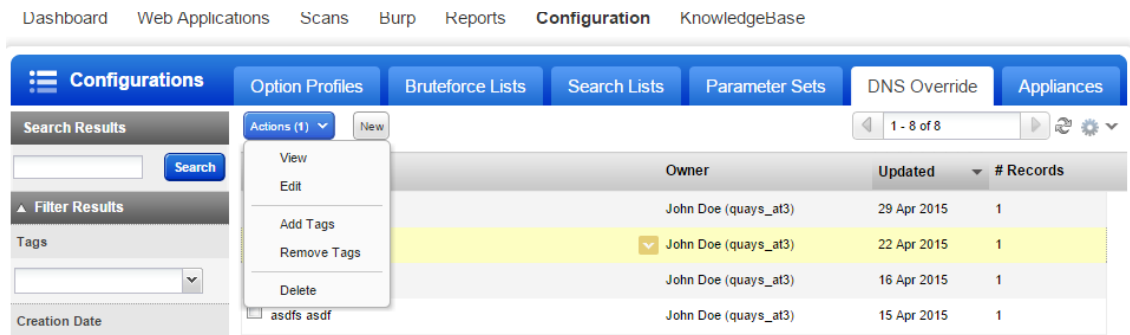
Our customers wanted to be able to override DNS for the FQDN included in the web application target specification. This would allow customers to scan web apps that may be in development and no DNS entry yet exists, or that there is a different IP address associated with the web application in the development or QA environment than what is available in DNS (typically the production IP). Previously customers would have had to stand up a special DNS server that the appliance uses to be able to manipulate the target IP for these situations, and many of our customers do not have this ability. Most customers can just update their own 'hosts' file on their local system to accomplish the DNS override for their system, but there is no way to do this for the Qualys appliance. Now, you can!

WAS UI > DNS Overrides Section

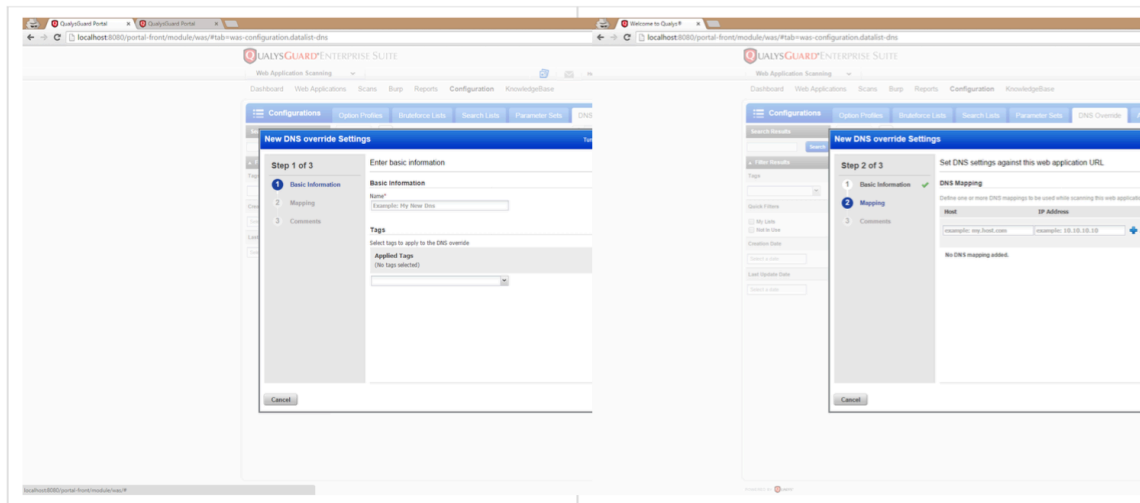
A new sub-tab under Configuration is added to display list of available DNS override records:



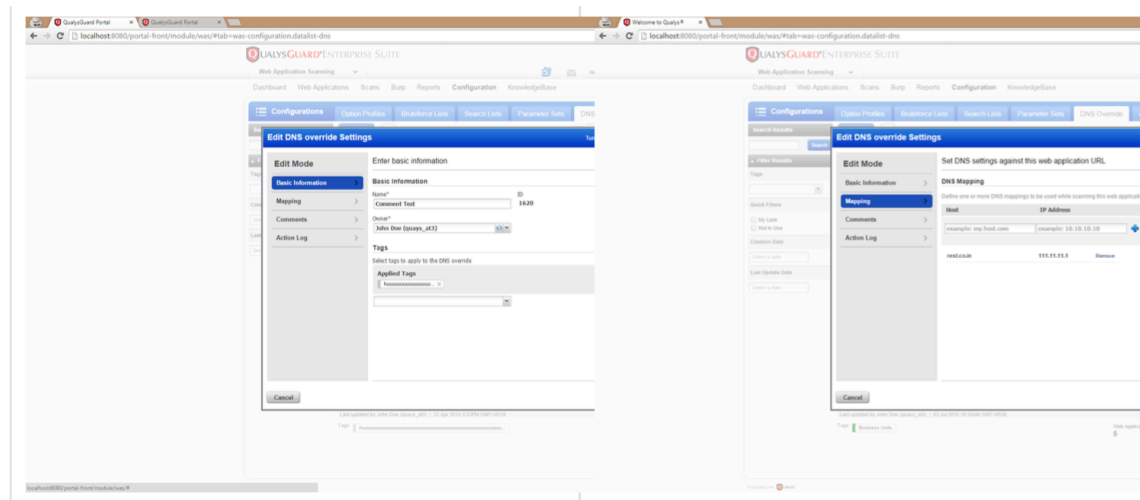
DNS override list has following Actions available:



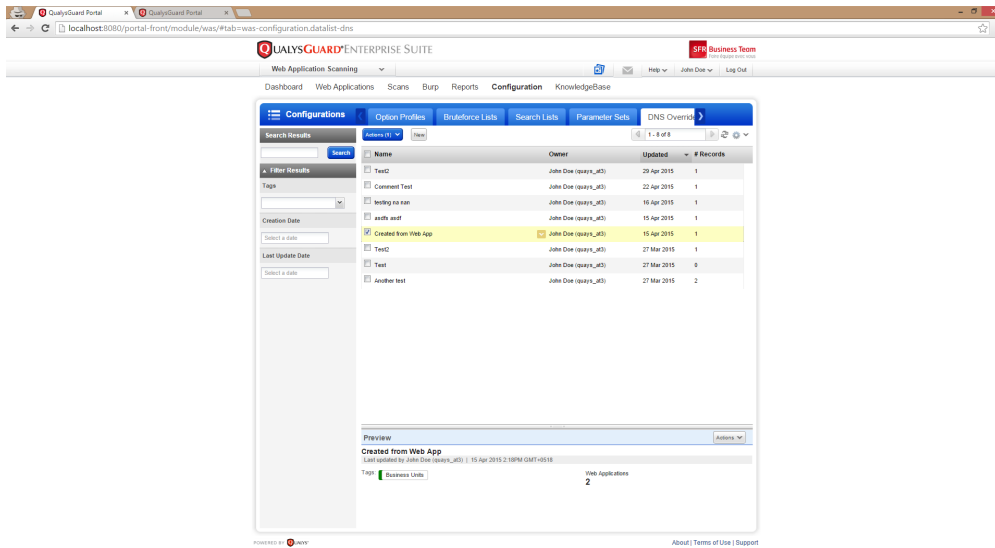
If user is having permission to create new DNS override record then this button will be enabled.



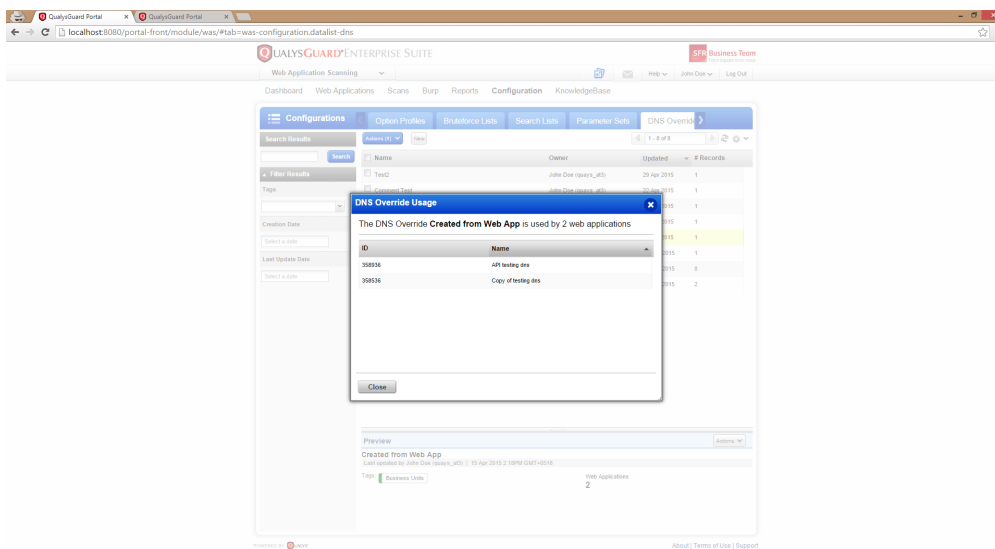
This will allow the user to edit the existing DNS override record.



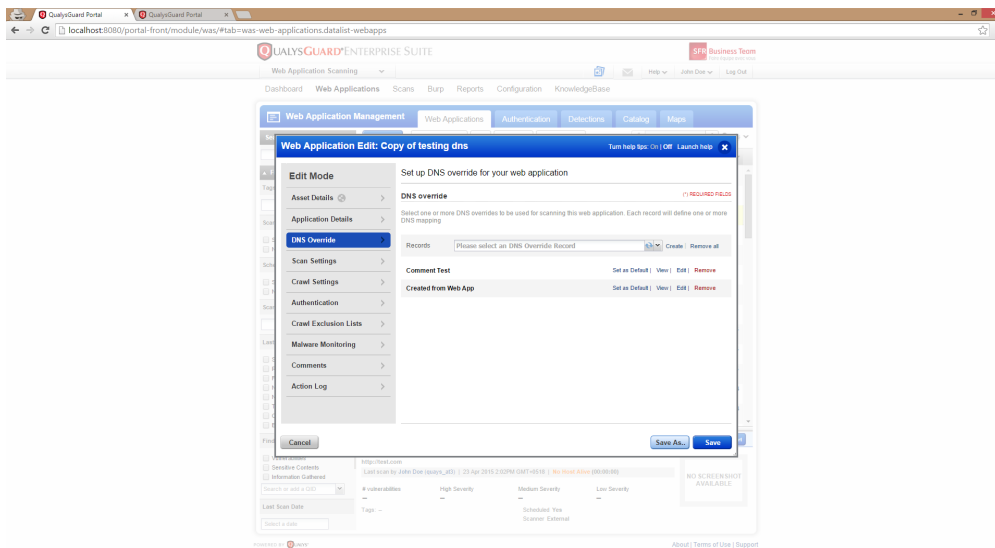
The Preview Panel has the name of the DNS override, last updated by, last updated date, tags, and number of web applications associated with the record.



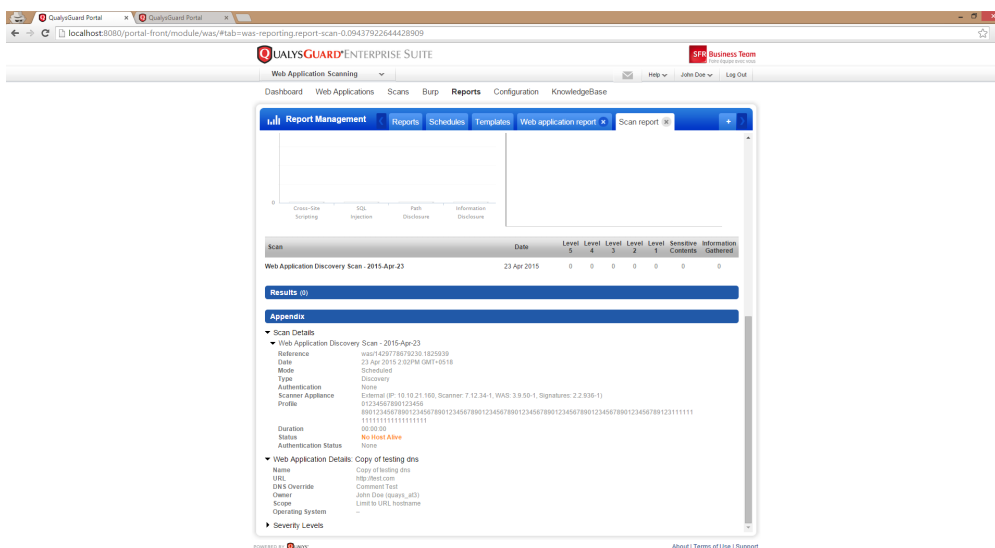
Upon clicking on the number of web applications, you will see a new dialog, which shows a list of web applications associated with it.



A new step is added in web application create/edit/view dialog to bind DNS Override records with Web Application. Only these selected records will be available while launching scan/schedule for this web application



Scan report will show DNS override record name.



Enhanced Support for Sitemap for Scans

This feature is brought to you so you will now be able to display the sitemap results for a specific scan exactly as it is done already for WebApps. WebApplications blacklist and whitelist can now be created from the directory tree!

From the Scan List a new "View Sitemap" action can be launched if a scan is selected.

This Sitemap action is also accessible from the context menu.

Scan Management

[Scan List](#)
[Schedules](#)
[Option Profiles](#)

Search Results

Search

Filter Results

Quick Filters

☐ My Scans
 ☐ Multi Scans

Type

☐ Vulnerability Scan
 ☐ Discovery Scan

Mode

☐ Scheduled
 ☐ On-Demand
 ☐ API

Web Application

Tags

Scanner Appliance

Status

☐ Submitted
 ☐ Running
 ☐ Finished
 ☐ No Host Alive
 ☐ No Web Service
 ☐ Time Limit Exceeded
 ☐ ...

Actions (1)

New Scan

1 - 20 of 240

<input type="checkbox"/>	Name	Status	Links	Severity	Scan Date	
<input type="checkbox"/>	Relaunch Web Application Vulnerability Scan - WASUI-5401 - 2...	Error			22 Apr 2015	
	http://10.10.26.238					
<input type="checkbox"/>	Web Application Vulnerability Scan - WAVSEP - 2015-04-22	Error			22 Apr 2015	
	http://10.10.35.14:8080/wavsep/index-active.jsp					
<input type="checkbox"/>	Web Application Vulnerability Scan - 2015-04-15	Finished			15 Apr 2015	
	Total web applications: 2					
<input type="checkbox"/>	Web Application Discovery Scan - WASUI-5401 - 2015-04-15	Finished	242		15 Apr 2015	
	http://10.10.26.238					
<input checked="" type="checkbox"/>	Web Application Vulnerability Scan - WASUI-5401 - 2015-04-15		242	HIGH	15 Apr 2015	
	http://10.10.26.238					
<input type="checkbox"/>	Web Application Vulnerability Scan - WAVSEP - 2015-04-15		1		15 Apr 2015	
	http://10.10.35.14:8080/wavsep/					
<input type="checkbox"/>	Scan on WebApp with proxy as default		1		10 Apr 2015	
	http://10.10.26.238					
<input type="checkbox"/>	Scan on WebApp with proxy as default				10 Apr 2015	
	http://10.10.26.238					
<input type="checkbox"/>	Scan on WebApp with scanner as default				10 Apr 2015	
	http://10.10.26.238					
<input type="checkbox"/>	Web Application Discovery Scan - WASUI-5401 - 2015-04-09	Finished	1		09 Apr 2015	
	http://10.10.26.238					
<input type="checkbox"/>	Web Application Vulnerability Scan - WASUI-5401 - 2015-04-09	Error			09 Apr 2015	

Quick Actions

View Report

View Scans

View

View Sitemap

Download

Cancel

Scan Again

Schedule

Delete

Preview

Actions

View Report

Web Application Vulnerability Scan - WASUI-5401 - 2015-04-15

Web application: WASUI-5401

Scan Launched by John Doe (quays_at3) | 15 Apr 2015 10:59AM GMT+0200 | Finished (00:27:25)

Mode: On-Demand

vulnerabilities: 63

High Severity: 5

Medium Severity: 0

Low Severity: 58

Authentication: Test 1

Scanner: External

Or from the Preview panel.

Scan Management

[Scan List](#)
[Schedules](#)
[Option Profiles](#)

Search Results

Search

Filter Results

Quick Filters

☐ My Scans
 ☐ Multi Scans

Type

☐ Vulnerability Scan
 ☐ Discovery Scan

Mode

☐ Scheduled
 ☐ On-Demand
 ☐ API

Web Application

Tags

Scanner Appliance

Status

☐ Submitted
 ☐ Running
 ☐ Finished
 ☐ No Host Alive
 ☐ No Web Service
 ☐ Time Limit Exceeded
 ☐ Canceled

Actions (1)

New Scan

1 - 20 of 240

<input type="checkbox"/>	Name	Status	Links	Severity	Scan Date	
<input type="checkbox"/>	Relaunch Web Application Vulnerability Scan - WASUI-5401 - 2... http://10.10.26.238	Error		–	22 Apr 2015	
<input type="checkbox"/>	Web Application Vulnerability Scan - WAV/SEP - 2015-04-22 http://10.10.35.14:8080/wavsep/index-active.jsp	Error		–	22 Apr 2015	
<input type="checkbox"/>	Web Application Vulnerability Scan - 2015-04-15 Total web applications: 2	Finished		–	15 Apr 2015	
<input type="checkbox"/>	Web Application Discovery Scan - WASUI-5401 - 2015-04-15 http://10.10.26.238	Finished	242	–	15 Apr 2015	
<input checked="" type="checkbox"/>	Web Application Vulnerability Scan - WASUI-5401 - 2015-04-15 http://10.10.26.238	Finished	242	HIGH	15 Apr 2015	
<input type="checkbox"/>	Web Application Vulnerability Scan - WAV/SEP - 2015-04-15 http://10.10.35.14:8080/wavsep/	Finished	1	–	15 Apr 2015	
<input type="checkbox"/>	Scan on WebApp with proxy as default http://10.10.26.238	Finished	1	–	10 Apr 2015	
<input type="checkbox"/>	Scan on WebApp with proxy as default http://10.10.26.238	Submitted		–	10 Apr 2015	
<input type="checkbox"/>	Scan on WebApp with scanner as default http://10.10.26.238	Submitted		–	10 Apr 2015	
<input type="checkbox"/>	Web Application Discovery Scan - WASUI-5401 - 2015-04-09 http://10.10.26.238	Finished	1	–	09 Apr 2015	
<input type="checkbox"/>	Web Application Vulnerability Scan - WASUI-5401 - 2015-04-09	Error		–	09 Apr 2015	

Preview

Web Application Vulnerability Scan - WASUI-5401 - 2015-04-15

Web application: WASUI-5401

Scan Launched by John Doe (quays_at3) | 15 Apr 2015 10:59AM GMT+0200 | Finished (00:27:25)

Mode: On-Demand

vulnerabilities: 63

Authentication: Test 1

Scanner: External

High Severity: 5

Medium Severity: 0

Low Severity: 58

Actions

View Report

View

View Sitemap

Download

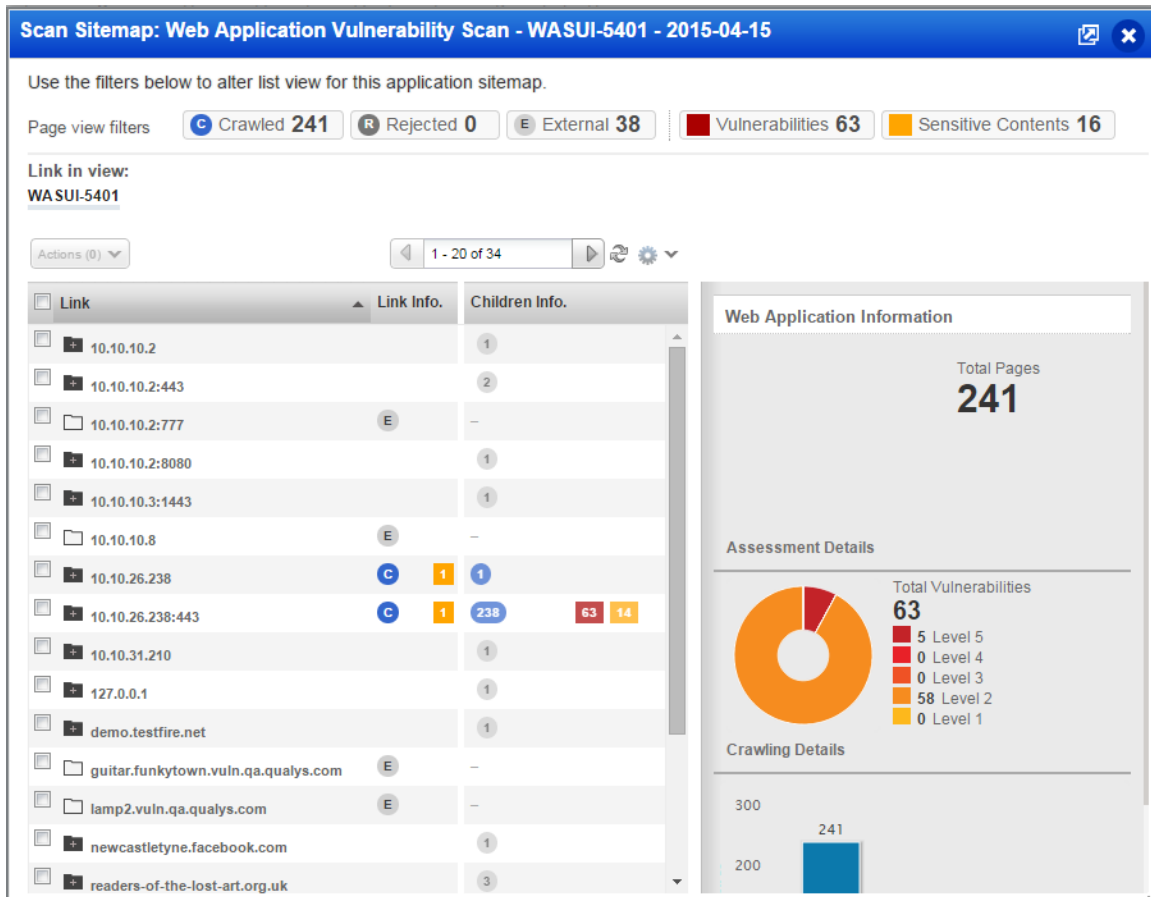
Cancel

Scan Again

Schedule

Delete

This action opens a Sitemap window the same way as it is in the WebApp section except that data are taken from a scan result.



Enhanced Patchable Detections Logic

1.) Enable Add Patch action even when patch cannot be added

The WAS > Web Applications > Detections section allows users to add a virtual patch to a vulnerability. The contextual action "Install Patch" is however only enabled when WAF module is enabled in subscription and that the web application has WAF module provisioned. This will lead this action for most users disabled, without them the possibility to understand why the feature is disabled.

We now allow for enabling the Install Patch action in Detections datalist in all cases and explain to the user why the action cannot be performed. This will allow user to understand the need of activating WAF module to enhance their security.

When clicking the action, we would display a dialog explaining that user cannot add a patch because <the correct reason> and we explain steps to enable the feature.

QUALYS GUARD ENTERPRISE SUITE

Web Application Scanning

Dashboard Web Applications Scans Burp Reports Configuration KnowledgeBase

Web Application Management Web Applications Authentication Detections Catalog Maps

Search Results

Filter Results

Target

Web Application

Tags

Last Scan Date

Finding

Confirmed Vulnerability Level

Potential Vulnerability Level

Sensitive Content Level

Information Gathered Level

Status

150124 Framable Page

150108 Secure attribute set to false in crossd...

150084 Unencoded characters

150081 X-Frame-Options header is not set

150012 Blind SQL Injection

150003 SQL Injection

150001 Reflected Cross-Site Scripting (XSS) ...

150084 Unencoded characters

150081 X-Frame-Options header is not set

150081 X-Frame-Options header is not set

Quick Actions

View

Ignore

Activate

Install Patch

Remove Patch

External References

Preview

150012 Blind SQL Injection

http://10.10.25.116/phpBB/1.4.4_basic/viewforum.php?forum=1&start=1%2DOR%2D%2DLIKE%2D&start=50

Web Application: Form Auth+ Basic Auth for 10.10.25.116/phpBB + WAS Options - G&P, Vulnerable Parameter: forum, Status: Fixed

Finding #: 295804

Patch #: -

CWE: CWE-49

OWASP: A1 Injection

WASC: WASC-19 SQL Injection

External Reference: -

First Detected: 09 Sep 2011

Last Detected: 09 Sep 2011

Times Detected: 1

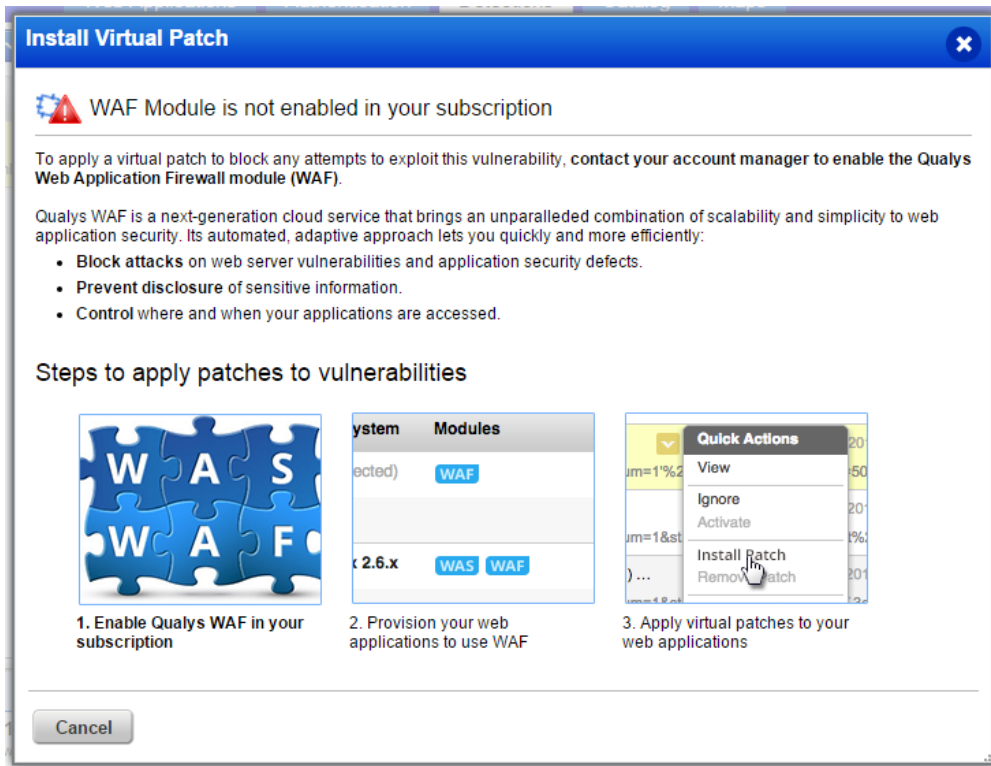
WHETHER USER HAS WAS/WAF provisioned or not, we should show "Install Patch" action active at all times. This will trigger messages.

https://qualysguard.plata.eng.qualys.com/portal-front/module/was/#

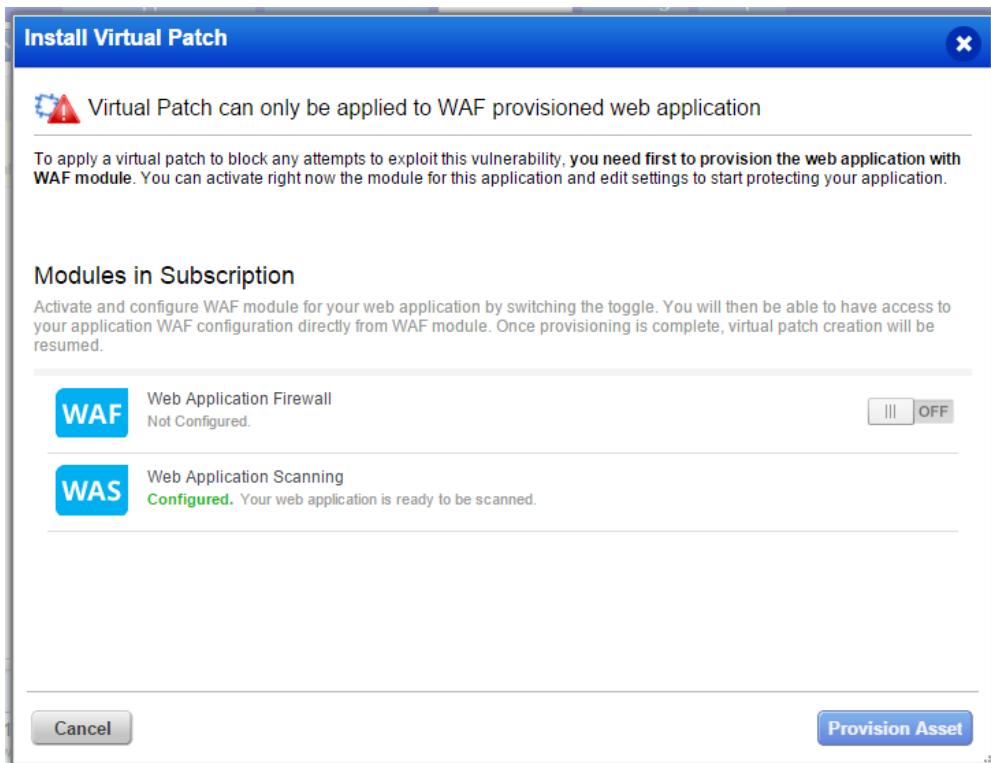
About | Terms of Use | Support

When WAF module is not enabled at all in subscription, we will display a dialog explaining that WAF module needs first to be added to the subscription to have virtual patches installed.

A description of the WAF module will help user understand the goal of WAF, and a list of steps will be added to make it clear to the users what needs to be done to have virtual patches feature available.



When WAF module is enabled in subscription, but the web application on which the vulnerability is not yet provisioned on WAF side, we will explain to user that the application needs now to be added to this module in order to apply the patch.

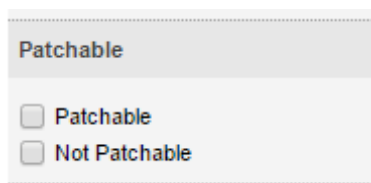


2.) Add Patchable Filter for WAS Detections

This feature provides customers a detection filter that allows them to see only patchable/not patchable detections. Doing so will make it very easy to apply virtual patches and not cause customer to try each one and get confused on why the option is not available for many in the list.

The datalist will provide a new filter Patchable Status with following options:

- a. Patchable - Show all detections for which WAF module would be able to create a patch for.
- b. Not Patchable - Show all detections that cannot be patched by Qualys WAF



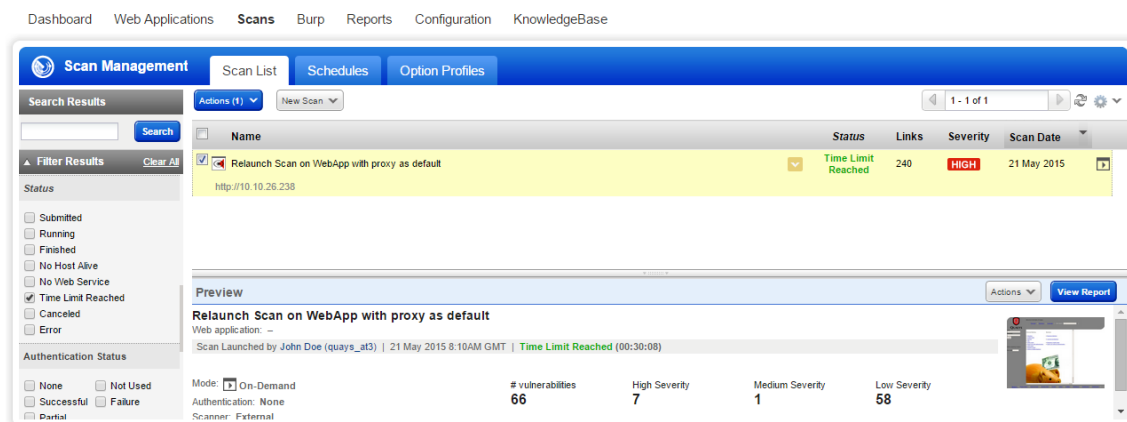
A screenshot of a filter panel titled "Patchable". It contains two radio button options: "Patchable" and "Not Patchable". The "Patchable" option is selected.

Clarify Time Limit Exceeded and Time Limit Reached and Scan Timeout

The "Time Limit Exceeded" status indicates that the scan went beyond the time limit when in fact the scan was actually stopped at the time limit. This change will provide clarification that the scan did not go beyond the time limit set by the user.

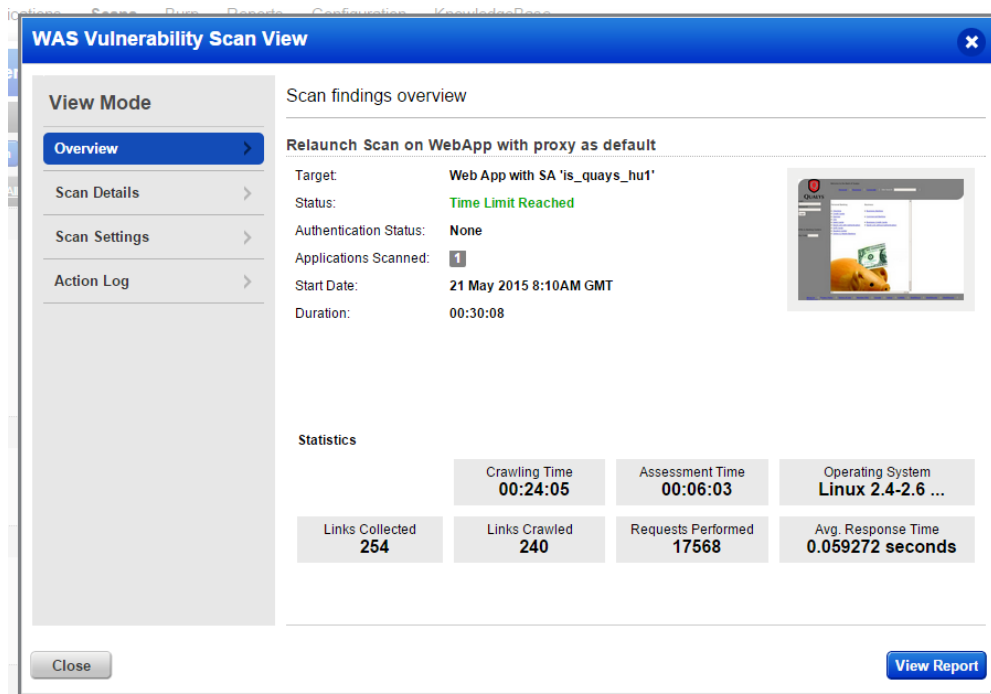
We now display Time Limit Reached instead of Time Limit Exceeded for following components:

- a. Status column
- b. Last Scan Status filter
- c. Preview Panel



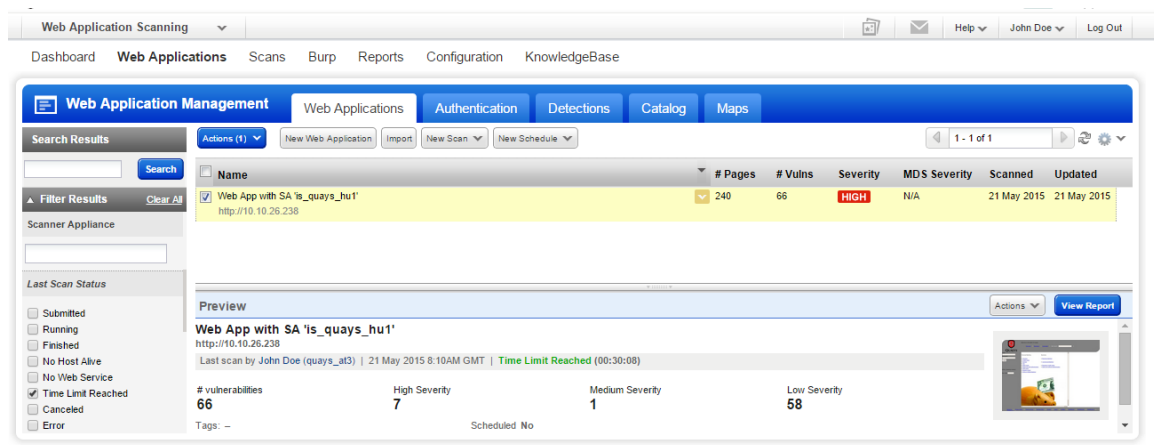
The screenshot shows the Qualys Scan Management interface. The top navigation bar includes links for Dashboard, Web Applications, Scans, Burp, Reports, Configuration, and KnowledgeBase. The main section is titled "Scan Management" and has tabs for Scan List, Schedules, and Option Profiles. The "Scan List" tab is active, showing a table of scan results. The table has columns for Name, Status, Links, Severity, and Scan Date. A single scan is listed: "Relaunch Scan on WebApp with proxy as default" with a status of "Time Limit Reached", 240 links, HIGH severity, and a scan date of 21 May 2015. Below the table, there is a "Preview" section for the selected scan. It shows the scan was launched by John Doe on 21 May 2015 at 8:10AM GMT, with a time limit reached of 00:30:08. The preview also displays a summary of vulnerabilities: 66 total, 7 High Severity, 1 Medium Severity, and 58 Low Severity.

The view dialog will also display the new Time Limit Reached value in its Overview panel.



We now display Time Limit Reached instead of Time Limit Exceeded for following components:

- a. Last Scan Status
- b. Filter Preview Panel



Another issue that has been raised is the problem of scans stopping before the end of the scan, because they reached an internal threshold of target connection / timeout errors.

However the UI reports the scan status as Finished, leading the user to think that the scan thoroughly assessed the web application, which can lead to confusion/frustration. This has been fixed. To help with this feature, the WAS scan

engine team has fixed the Critical error conditions for WAS scans, listing the different error cases that we have to support when monitoring scan or processing scan results.

The screenshot displays the 'WAS Vulnerability Scan View' window. On the left is a 'View Mode' sidebar with options: Overview (selected), Scan Details, Scan Settings, and Action Log. The main area is titled 'Scan findings overview' and shows details for a scan titled 'Schedule proxy Internal - Proxy out of scope to subuser'. The target is 'Test Proxy - External', status is 'Service Errors Detected' (in orange), authentication status is 'None', one application was scanned, the start date is '11 Oct 2015 3:07PM GMT-0400', and the duration is '00:21:05'. A yellow box explains the 'Service Errors Detected' status, stating that the scan encountered too many connection or timeout errors and provides instructions on how to collect problematic URLs and adjust scan settings. Below this, a table of performance metrics is shown: Crawling Time (00:20:55), Assessment Time (00:00:10), Operating System (Linux 2.4-2.6 ...), Links Collected (418), Links Crawled (300), Requests Performed (832), and Avg. Response Time (0.154295 seconds). At the bottom, there are 'Close' and 'View Report' buttons.

Performance Metrics	
Crawling Time	00:20:55
Assessment Time	00:00:10
Operating System	Linux 2.4-2.6 ...
Links Collected	418
Links Crawled	300
Requests Performed	832
Avg. Response Time	0.154295 seconds

Enhanced WAS Scan Reports

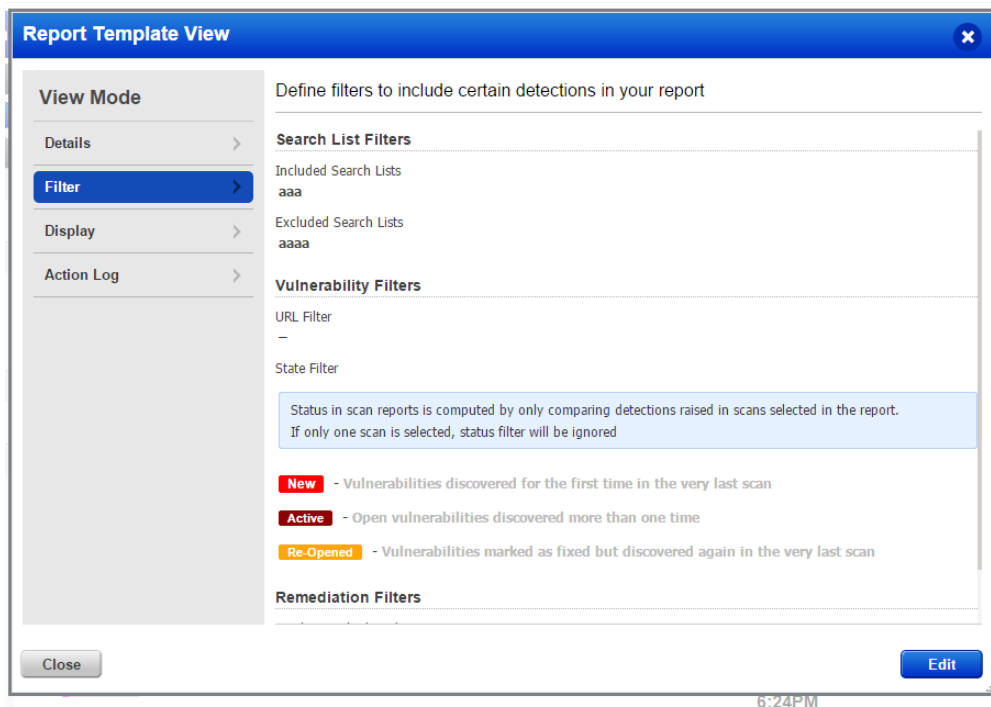
Current scan reports display a status along each detection, which corresponds to the status when comparing vulnerability detection among all scans selected.

This means that when only one scan is selected, the status always displays NEW, which is misinterpreted by users as being a vulnerability newly discovered for the web application in that scan. This is now corrected!

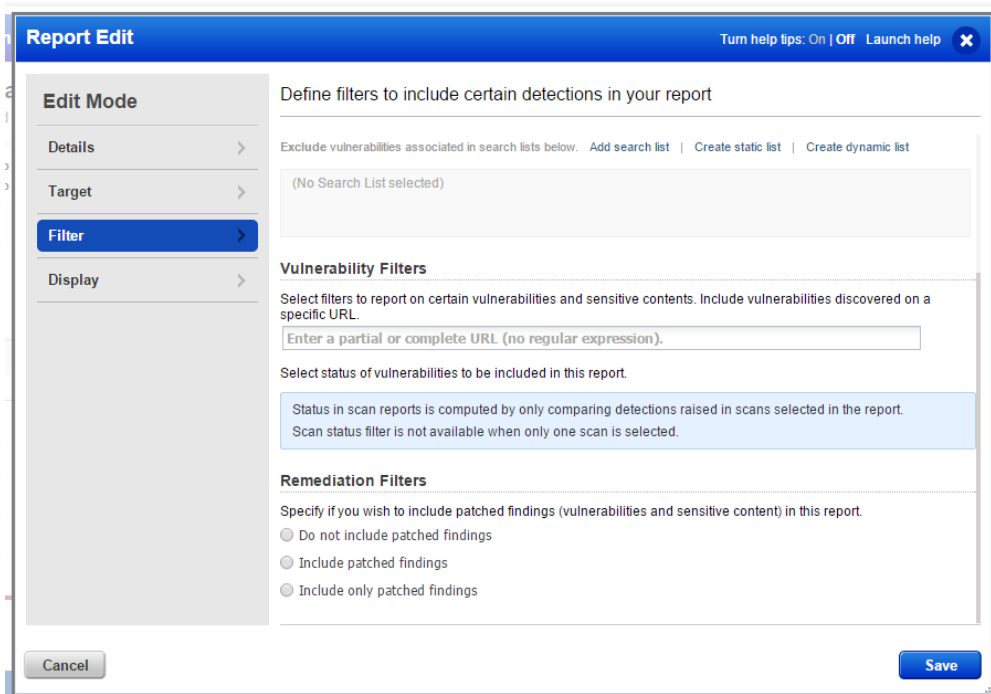
The main changes are:

- For scan reports, we will add a mention for the Status filter to explain when this filter is effectively used
- Whenever it is possible we will not show the Status filter options when only one scan is selected
- For any scan report generated with only one scan, we will not add anymore the finding status

The Scan Report view dialog will add in the Filter step, Vulnerability Filters > State Filter section a notification block explaining to users its application context:



If only one scan is selected, the status options in Filter step will be replaced by notification block explaining that the status filter has no meaning in this context:



When more than one scan is selected, we will display the usual notification block explaining how status is computed in scan reports:

Report Edit Turn help tips: On | Off Launch help X

Edit Mode

- Details >
- Target >
- Filter >**
- Display >

Define filters to include certain detections in your report

Vulnerability Filters

Select filters to report on certain vulnerabilities and sensitive contents. Include vulnerabilities discovered on a specific URL.

Enter a partial or complete URL (no regular expression).

Select status of vulnerabilities to be included in this report.

Status in scan reports is computed by only comparing detections raised in scans selected in the report. Note that if only one scan is selected, status filter will be ignored.

- ☒ **New** - Vulnerabilities discovered for the first time in the very last scan
- ☒ **Active** - Open vulnerabilities discovered more than one time
- ☒ **Re-Opened** - Vulnerabilities marked as fixed but discovered again in the very last scan
- ☐ **Fixed** - Vulnerabilities not found anymore in latest scans (will not impact summary & graphs)

Remediation Filters

Specify if you wish to include patched findings (vulnerabilities and sensitive content) in this report.

- ☐ Do not include patched findings
- ☐ Include patched findings
- ☐ Include only patched findings

Cancel Save

Implement Web Application Custom Attributes

Users requested that they would like to associate to each asset, different information, like their internal host ID. This feature changes the details of a web application, in order to support custom attributes for them.

We removed Information data section on "Application details" of web application dialog.

Web Application View: Test Schedule (multi - 2)

View Mode

Asset Details

Application Details

Scan Settings

Crawl Settings

Authentication

Crawl Exclusion Lists

Malware Monitoring

Comments

Action Log

Tell us about the web application you want to scan

Target Details

Crawl Scope

Limit to URL hostname (10.10.26.238)

Explicit URLs to Crawl

Information

Operating System

Linux 2.4-2.6 / Embedded Device / F5 Networks Big-IP

Business Function

Business Location

Business Description

Close

Edit

Save As..

Scan

View Report

Asset details additions.

Web Application View: "Test XXE from Create webapp - API #2"



View Mode

Asset Details



Application Details



Scan Settings



Crawl Settings



Authentication



Crawl Exclusion Lists



Malware Monitoring



Comments



Action Log



Tell us about the asset you want to scan

Asset Details

Name	ID
"Test XXE from Create webapp - API #2"	358136
Owner	Active Modules
John Doe (quays_at3)	WAS

Target Details

Asset URL
http://10.10.26.238

Information

Operating System
Linux 2.4-2.6 / Embedded Device / F5 Networks Big-IP

Custom Attributes

power	rangers
salut	ghihi

Tags

Close

Edit

Save As..

Scan

View Report

Web Application Edit: "Test XXE from Create webapp - API #2"

Turn help tips: On | Off Launch help

Edit Mode

Asset Details

Application Details

Scan Settings

Crawl Settings

Authentication

Crawl Exclusion Lists

Malware Monitoring

Comments

Action Log

Tell us about the asset you want to scan

Web Application URL*

http:// 10.10.26.238

Custom Attributes

Provide attribute information that will help you categorize this web application within your subscription.

Name

Value

Add

Enter one or many lines

power

rangers

Remove

salut

ghihi

Remove

Tags

Select tags to apply to the web application

Applied Tags

(No tags selected)

Cancel

Save As..

Save

When you edit a web application on which has previous business information data, these old fields data are always displayed. In order to remove them, click on remove link. The save process will delete these old information and won't be displayed the next edit time.

Web Application Edit: Test 1829 V7

Turn help tips: On | Off Launch help

Edit Mode

Asset Details

Application Details

Scan Settings

Crawl Settings

Authentication

Crawl Exclusion Lists

Malware Monitoring

Comments

Action Log

Tell us about the asset you want to scan

Web Application URL*
http:// google.fr

Custom Attributes

Provide attribute information that will help you categorize this web application within your subscription.

NameValueAdd

Enter one or many lines

Business Description3333333Remove

Business Function11111Remove

Business Location22222Remove

Tags

Select tags to apply to the web application

Applied Tags

(No tags selected)

Cancel

Save As..Save

Custom attributes filter results.

For this, we added a combobox on the filter results left panel for "Custom Name Attribute." Below, we have a search field used to find the associated "Custom Value Attribute." These two fields allow values which are not present in the datalist.

Web Application Management

Web Applications

Authentication

Detections

Search Results

Search

▲ Filter Results

☐ Information Gathered

Search or add a QID

▼

Last Scan Date

Select a date

Creation Date

Select a date

Last Update Date

Select a date

Authentication Record

All records

↻ ▼

Custom Attribute

Search attribute name

↻ ▼

Search attribute value

Actions (0) ▼

New Web Application

Import

New Scan ▼

New Schedule ▼

☐ Name

☐ Test 1829 V5
http://google233.fr

☐ Test 1829 V7
http://google.fr

☐ Test 1829 V6
http://google.fr

☐ WAFUI-796
https://www.qa.qualys.com

☐ http://1111.11.com
http://1111.11.com

☐ Funkytown
http://funktown.vuln.qa.qualys.com/cassium/regression/sensitive_content/

☐ Web App with SA 'is_quays_hu1'
http://10.10.26.238

☐ WASUI-5401
http://10.10.26.238

☐ "Test XXE from Create webapp - API #2"
http://10.10.26.238

☐ 2
http://2.com

☐ 143112
http://143112.143112

☐ www.bryan-talbot.com
http://www.bryan-talbot.com/

User Customizable Mail Settings for When Scan is Launched

After successful completion or cancellation of scan, an email notification is sent to an email address or set of email addresses. Now you have the ability to disable this for automation testing purpose for example.

Scan settings edition step on scan dialog

Launch New WAS Discovery Scan

Turn help tips: On | OffLaunch help

Step 2 of 3

1Scan Details

2Scan Settings

3Review And Confirm

Configure settings for your scan

Scanner Appliance*External

Proxy Support

Add ability for WAS scan through proxy

ProxyNoneViewCreate

Cancel Scan

Cancel the scan after N hours or at a certain time. By default the scan will run until it completes, or the maximum scan time is reached.

Cancel OptionDo not Cancel Scan

Mail notification

When a scan is completed, failed or canceled, you will receive email notification. You can disable this behavior using the option below.

☒ Send mail at scan completion

Cancel

PreviousContinue

Scan review step on scan dialog

Launch New WAS Discovery Scan

Turn help tips: On | Off Launch help

Step 3 of 3

1 Scan Details

2 Scan Settings

3 Review And Confirm

Review and confirm scan settings

Name

Web Application Discovery Scan - 2015-07-07

Target Information

Web Applications

1 web application

Settings

Authentication Record

None

Option Profile

<script>alert("y")</script>

Scanner Appliance

External

Duration

This task will run till completion.

Mail notification

Send mail at scan completion

Cancel

Previous

Finish

Enhance Tag Selection Component in WAS Module

This feature enhances the current tags selection component used in the WAS Webapp/Scorecard reports to look and work the same as the one implemented in VM and other modules, for consistency.

Examples are as follows:

Associate Authentication Records with the selected Web Applications ✕

Select tags and/or web applications to add selected record(s) to.

Tags

Applied Tags
(No tags selected)

2222

Asset Groups

Bug #130334

Changed for Nico's Test

Common

funkytown

Malware Domain Assets

OS

Close

Cancel Save

Before

Associate Authentication Records with the selected Web Applications ✕

Select tags and/or web applications to add selected record(s) to.

Tags

Include hosts that have any of the tags below. Add Tag

Recent Tags

2222

Malware - Habi

Business Units

2 more tags

Web Applications

Web Applications Please select a web application

No web applications selected.

Favorite Tags

Common

funkytown

222.3

2 more tags

Cancel Save

After

Web Application Authentication Record View: 129513_2 ✕

View Mode

Basic Information

Form Record

Server Records

Comments

Action Log

Give a name to authentication record

Basic Information

Name 129513_2 ID 1915

Owner John Doe (quays_at3)

Updated 16 Apr 2015 5:25PM GMT+0200 By John Doe (quays_at3)

Tags

Assigned tags

2222 Malware - Habi

Usage

Last Status Not Used Last Time Tested -

Web apps 5 application(s) using this authentication record Scans 0 scan(s) using this authentication record Scheduled scans 0 task(s) using this authentication record

Close Save As... Edit

BEFORE

Web Application Authentication Record View: 129513_2 ✕

View Mode

Basic Information

Form Record

Server Records

Comments

Action Log

Give a name to authentication record

Basic Information

Name 129513_2 ID 1915

Owner John Doe (quays_at3)

Updated 16 Apr 2015 5:25PM GMT+0200 By John Doe (quays_at3)

Tags

Assigned tags

Malware - Habi 2222

Usage

Last Status Not Used Last Time Tested -

Web apps 5 application(s) using this authentication record Scans 0 scan(s) using this authentication record Scheduled scans 0 task(s) using this authentication record

Close Save As... Edit

AFTER

Web Application Authentication Record Creation

Turn help tips On | Off Launch help

Step 1 of 5

1 Basic Information
2 Form Record
3 Server Records
4 Comments
5 Review And Confirm

Give a name to authentication record

Basic Information (*) REQUIRED FIELDS

Name*

Tags

Select tags to apply to the authentication record

Applied Tags (No tags selected)

Cancel Continue

BEFORE

Web Application Authentication Record Creation

Turn help tips On | Off Launch help

Step 1 of 5

1 Basic Information
2 Form Record
3 Server Records
4 Comments
5 Review And Confirm

Give a name to authentication record

Basic Information (*) REQUIRED FIELDS

Name* 15 Avril Test

Tags

Select tags to apply to the authentication record Add Tag

2222 x

2222

Malware - Nabl

Business Units

2 more tags

Favorite Tags

Common

Funlytown

222.3

2 more tags

Cancel Continue

AFTER

CREATION

Web Application Authentication Record Edit: 129513_2

Turn help tips On | Off Launch help

Edit Mode

Basic Information
Form Record
Server Records
Comments
Action Log

Give a name to authentication record

Basic Information (*) REQUIRED FIELDS

Name* 129513_2 ID 1915

Owner* John Doe (quays_at3)

Updated 14 Apr 2015 5:01PM GMT+0200 By John Doe (quays_at3)

Tags

Select tags to apply to the authentication record

Applied Tags 2222 x

Cancel Save As... Save

Web Application Authentication Record Edit: / AUTH /

Turn help tips On | Off Launch help

Edit Mode

Basic Information
Form Record
Server Records
Comments
Action Log

Give a name to authentication record

Basic Information (*) REQUIRED FIELDS

Name* / AUTH / ID 1906

Owner* John Doe (quays_at3)

Updated 15 Apr 2015 2:41PM GMT+0200 By John Doe (quays_at3)

Tags

Select tags to apply to the authentication record Add Tag

2222 x

Cancel Save As... Save

EDITION

Save report

Turn help tips On | Off Launch help

Save a report for the web applications you are deleting

Name Web Application Security Status Report

Description This report shows you the security status for web applications selected for deletion.

Report Format (*) REQUIRED FIELDS

Select a format* Comma-Separated Value (CSV)

Timezone used for dates in report* (GMT 02:00) Central African Time (CAT Africa/Blantyre)

Add tags to the report

Select one or more tags to apply to this report

Suggested Tags

This tag is associated with the selected web applications. Apply all suggested

2222

Cancel Save

BEFORE

Save report

Turn help tips On | Off Launch help

Save a report for the web applications you are deleting

Name Web Application Security Status Report

Description This report shows you the security status for web applications selected for deletion.

Report Format (*) REQUIRED FIELDS

Select a format* Comma-Separated Value (CSV)

Timezone used for dates in report* (GMT 02:00) Central African Time (CAT Africa/Blantyre)

Add tags to the report

Select one or more tags to apply to this report Add Tag

2222

Malware - Nabl

Business Units

2 more tags

Favorite Tags

Common

Funlytown

222.3

2 more tags

Cancel Save

AFTER

WAS Search Lists - Deprecate Compliance Type Options

Compliance Type - PCI has been removed from Create/Edit Dynamic Search List dialog.

To open the advanced search panel:

1. Launch Create Dynamic Searchlist>Go to Criteria tab>Set Criteria
2. Click Test button>Click Advanced Search button

Please see attached screenshot:

