Qualys.

Qualys Cloud Platform v2.x

Release Notes

Version 2.35
January 8, 2019

Here's what's new in Qualys Cloud Suite 2.35!

CA Cloud Agent

New columns in agents list

SAQ Security Assessment Questionnaire

Import Template in Excel Format

WAS Web Application Scanning

Custom Footer for Reports
Schedule Reactivation of Ignored Finding
Search Lists Simplified to Populate only WAS QIDs
Launch Now Option for Scheduled Reports
New Filters Added
Improved Notifications for Virtual Patch Installation
Latest Scan Data Now in Scan Reports

Qualys Cloud Platform

Dynamic tagging for AWS, AZURE, GCP

Qualys Cloud Platform 2.35 brings you many more Improvements and updates! Learn more

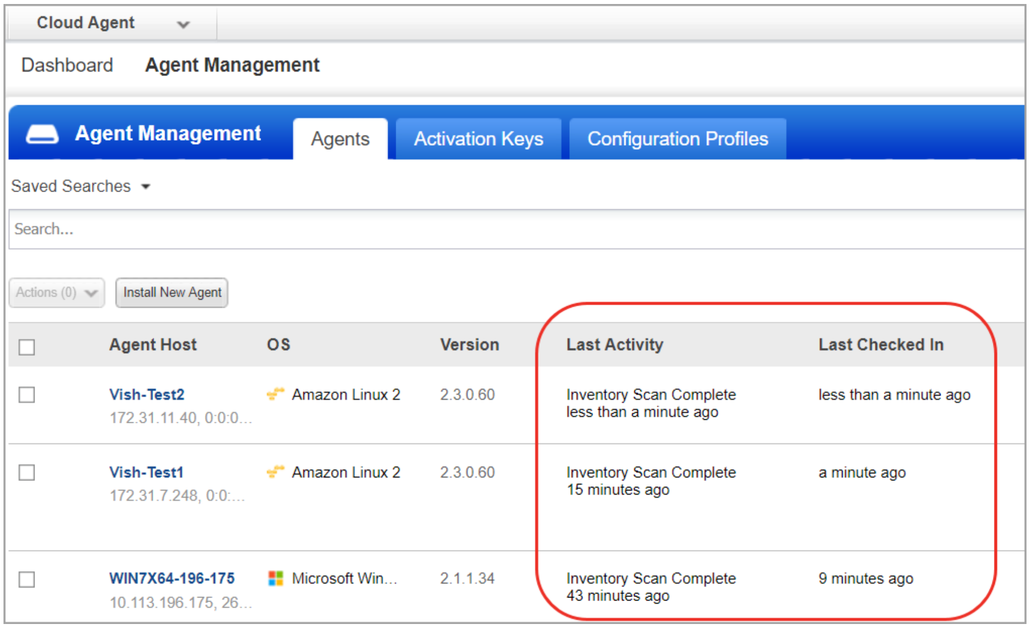
CA Cloud Agent

New columns in agents list

The agents list now contains new columns Last Activity and Last Checked In.

The Last Activity column shows when last activity on the agent occurred. Last activity could be when agent was last scanned, updated, activated, etc.

The Last Checked In column shows when the agent last checked in to the cloud platform. The agents list is sorted by this column by default.



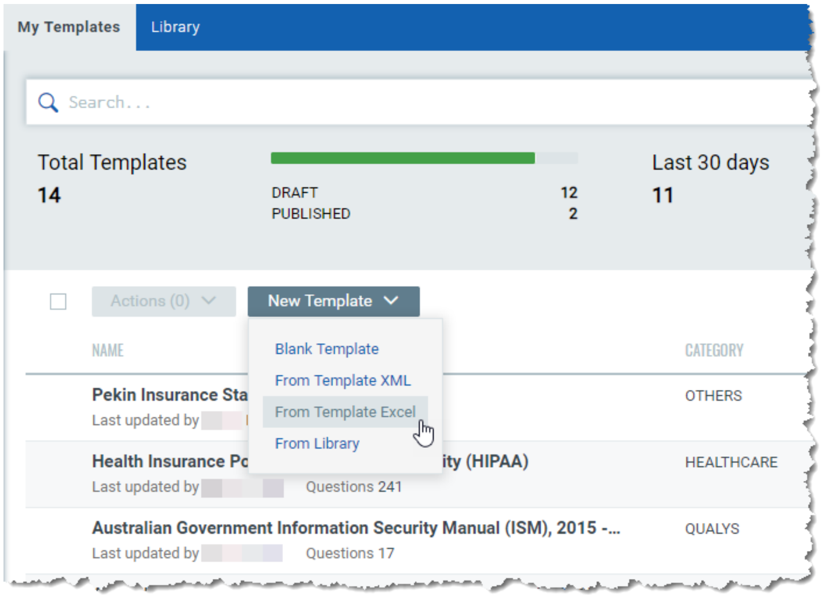
□	Agent Host	OS	Version	Last Activity	Last Checked In
□	Vish-Test2 172.31.11.40, 0:0:0...	Amazon Linux 2	2.3.0.60	Inventory Scan Complete less than a minute ago	less than a minute ago
□	Vish-Test1 172.31.7.248, 0:0:...	Amazon Linux 2	2.3.0.60	Inventory Scan Complete 15 minutes ago	a minute ago
□	WIN7X64-196-175 10.113.196.175, 26...	Microsoft Win...	2.1.1.34	Inventory Scan Complete 43 minutes ago	9 minutes ago

SAQ Security Assessment Questionnaire

Import Template in Excel Format

You can now import a template in your subscription even if it is in an Excel format.

Simply, navigate to Template > My Templates and from the New Templates drop down select From Template Excel option.



NAME	CATEGORY
Pekin Insurance Sta Last updated by	OTHERS
Health Insurance Po ity (HIPAA) Last updated by Questions 241	HEALTHCARE
Australian Government Information Security Manual (ISM), 2015 -... Last updated by Questions 17	QUALYS

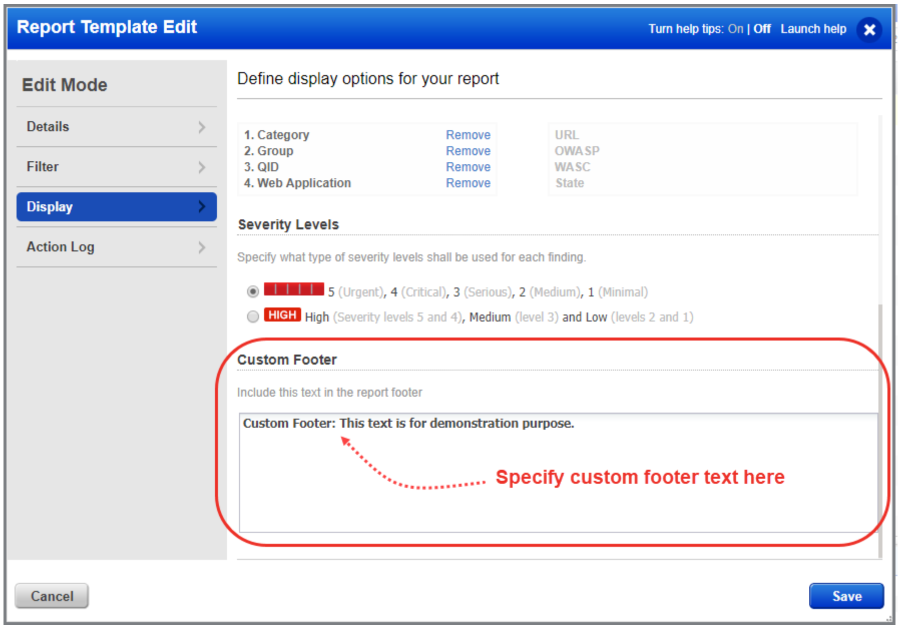
You can now edit your template and publish it to launch campaigns.

To successfully import a template, make sure you provide the template details in the same format as seen in the sample template file.

Custom Footer for Reports

You can now define a customized footer in all the WAS reports: Web application report and scan report (HTML and PDF formats). We have now added a new option in the report templates where you can specify the custom text to be displayed as footer in web application report and scan reports. You can use the report template when you generate the report and the custom footer is displayed in the reports.

Go to Reports > Templates and then edit an existing template or create a new template. In the Display section, you can define the custom footer text.



Define display options for your report

1. Category Remove
2. Group Remove
3. QID Remove
4. Web Application Remove

URL
OWASP
WASC
State

Severity Levels

Specify what type of severity levels shall be used for each finding.

● 5 (Urgent), 4 (Critical), 3 (Serious), 2 (Medium), 1 (Minimal)

○ HIGH High (Severity levels 5 and 4), Medium (level 3) and Low (levels 2 and 1)

Custom Footer

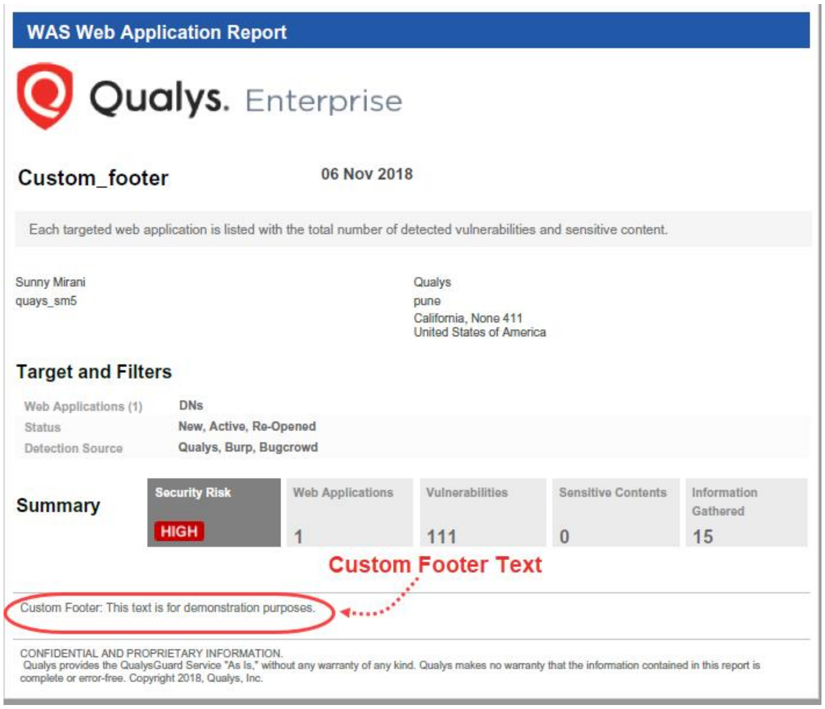
Include this text in the report footer

Custom Footer: This text is for demonstration purpose.

Specify custom footer text here

Now, go to reports and generate a web application report or scan report using the template with the custom footer text you defined.

PDF Report format



WAS Web Application Report

Qualys. Enterprise

Custom_footer 06 Nov 2018

Each targeted web application is listed with the total number of detected vulnerabilities and sensitive content.

Sunny Mirani
quays_sm5

Qualys
pune
California, None 411
United States of America

Target and Filters

Web Applications (1)	DNs
Status	New, Active, Re-Opened
Detection Source	Qualys, Burp, Bugcrowd

Summary

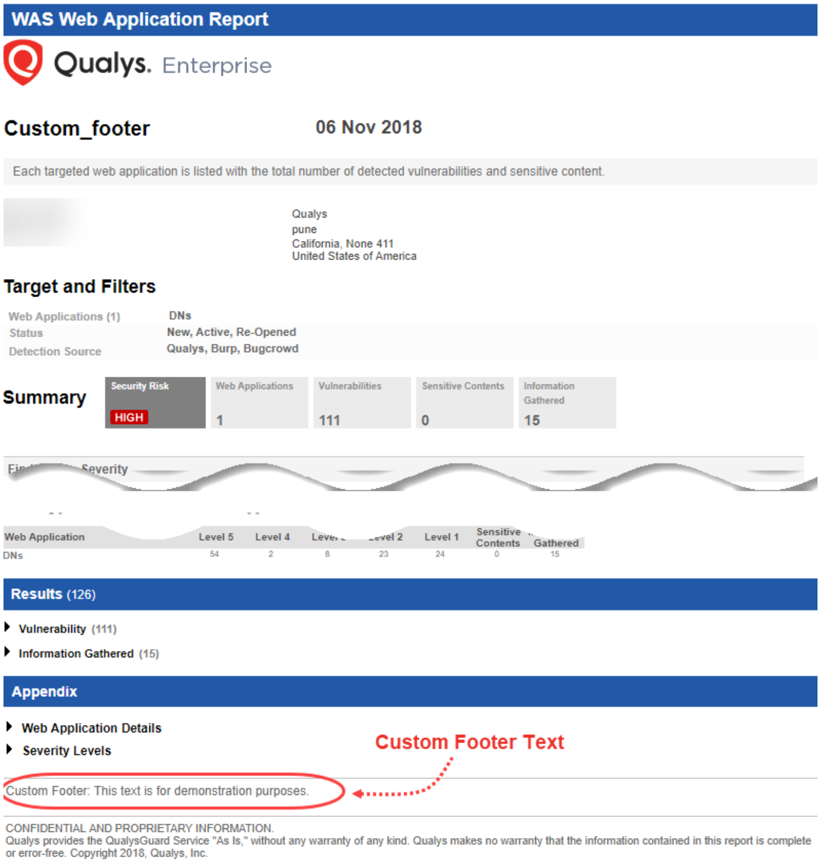
Security Risk	Web Applications	Vulnerabilities	Sensitive Contents	Information Gathered
HIGH	1	111	0	15

Custom Footer Text

Custom Footer: This text is for demonstration purposes.

CONFIDENTIAL AND PROPRIETARY INFORMATION.
Qualys provides the QualysGuard Service "As Is," without any warranty of any kind. Qualys makes no warranty that the information contained in this report is complete or error-free. Copyright 2018, Qualys, Inc.

HTML Report format



WAS Web Application Report

Qualys. Enterprise

Custom_footer 06 Nov 2018

Each targeted web application is listed with the total number of detected vulnerabilities and sensitive content.

Qualys
pune
California, None 411
United States of America

Target and Filters

Web Applications (1)	DNs
Status	New, Active, Re-Opened
Detection Source	Qualys, Burp, Bugcrowd

Summary

Security Risk	Web Applications	Vulnerabilities	Sensitive Contents	Information Gathered
HIGH	1	111	0	15

Fi[illegible] Severity

Web Application	Level 5	Level 4	Leve[illegible]	[illegible]evel 2	Level 1	Sensitive Contents	[illegible] Gathered
DNs	54	2	8	23	24	0	15

Results (126)

- **Vulnerability** (111)
- **Information Gathered** (15)

Appendix

- **Web Application Details**
- **Severity Levels**

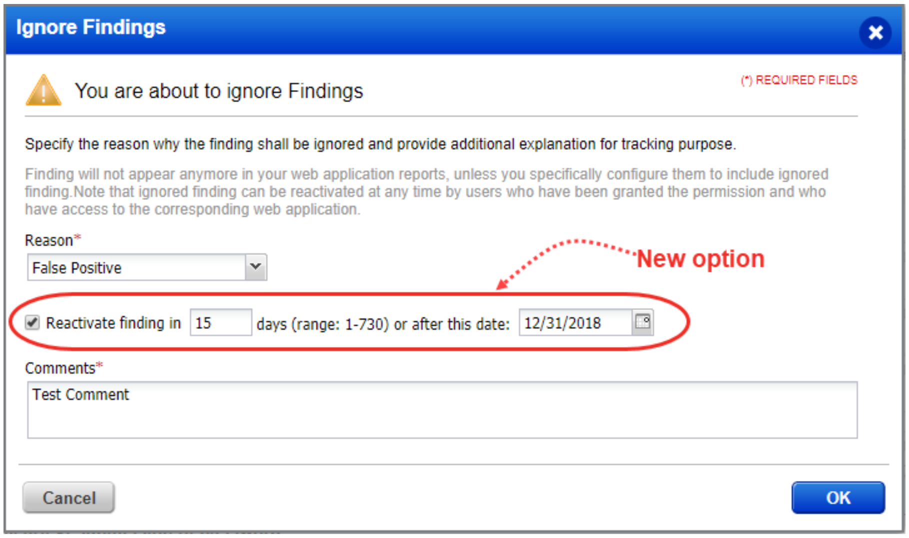
Custom Footer Text

Custom Footer: This text is for demonstration purposes.

CONFIDENTIAL AND PROPRIETARY INFORMATION.
Qualys provides the QualysGuard Service "As Is," without any warranty of any kind. Qualys makes no warranty that the information contained in this report is complete or error-free. Copyright 2018, Qualys, Inc.

Schedule Reactivation of Ignored Finding

We have introduced a new checkbox that allows you to reactivate an ignored finding. You can now schedule when to reactivate an ignored finding by specifying a date or number of days after which the currently ignored finding can be re-activated again.



Ignore Findings

You are about to ignore Findings

(*) REQUIRED FIELDS

Specify the reason why the finding shall be ignored and provide additional explanation for tracking purpose.

Finding will not appear anymore in your web application reports, unless you specifically configure them to include ignored finding.Note that ignored finding can be reactivated at any time by users who have been granted the permission and who have access to the corresponding web application.

Reason*: False Positive

New option

☑ Reactivate finding in 15 days (range: 1-730) or after this date: 12/31/2018

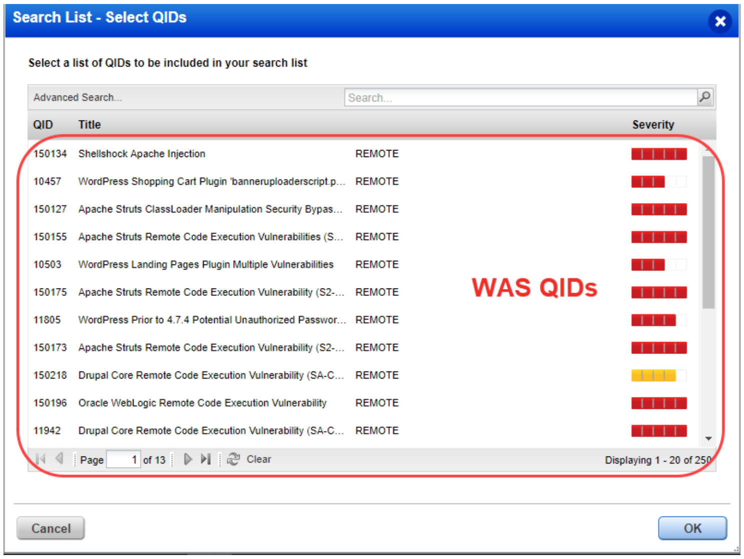
Comments*: Test Comment

Go to Detections > Detections List and select the detection to be ignored and select Ignore from the quick action menu (for multiple detections, select Ignore from the Actions menu).

Once you select the reason for ignoring the finding, you can then select the Reactivate finding checkbox and then specify the number of days or a date after which the detection should reactivated again. Click OK.

Search Lists Simplified to Populate only WAS QIDs

The process to create search lists (static and dynamic) is now simplified so that only WAS QIDs are included in the lists. Defining WAS scan detection scope is now easier with Option Profile using search lists that will contain only WAS QIDs.



Search List - Select QIDs

Select a list of QIDs to be included in your search list

QID	Title		Severity
150134	Shellshock Apache Injection	REMOTE	🟥🟥🟥🟥🟥
10457	WordPress Shopping Cart Plugin 'banneruploaderscript.p...	REMOTE	🟥🟥🟥
150127	Apache Struts ClassLoader Manipulation Security Bypas...	REMOTE	🟥🟥🟥🟥🟥
150155	Apache Struts Remote Code Execution Vulnerabilities (S...	REMOTE	🟥🟥🟥🟥🟥
10503	WordPress Landing Pages Plugin Multiple Vulnerabilities	REMOTE	🟥🟥🟥
150175	Apache Struts Remote Code Execution Vulnerability (S2-...	REMOTE	🟥🟥🟥🟥🟥
11805	WordPress Prior to 4.7.4 Potential Unauthorized Passwor...	REMOTE	🟥🟥🟥🟥
150173	Apache Struts Remote Code Execution Vulnerability (S2-...	REMOTE	🟥🟥🟥🟥🟥
150218	Drupal Core Remote Code Execution Vulnerability (SA-C...	REMOTE	🟨🟨🟨🟨
150196	Oracle WebLogic Remote Code Execution Vulnerability	REMOTE	🟥🟥🟥🟥🟥
11942	Drupal Core Remote Code Execution Vulnerability (SA-C...	REMOTE	🟥🟥🟥🟥🟥

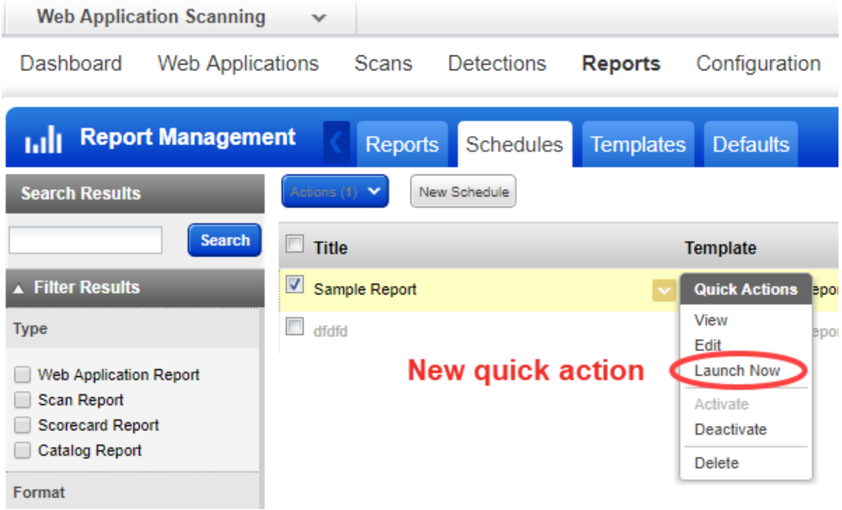
Page 1 of 13 Clear Displaying 1 - 20 of 250

Static List: Simply add WAS QIDs or select from the list of WAS QIDs that are automatically populated and click OK.

Dynamic List: You can choose criteria for the dynamic list and automatically only WAS QIDs that match the criteria are added to the list.

Launch Now Option for Scheduled Reports

The scheduled reports can now be instantly generated using the new quick action option Launch Now. You need not wait for the schedule to be executed.



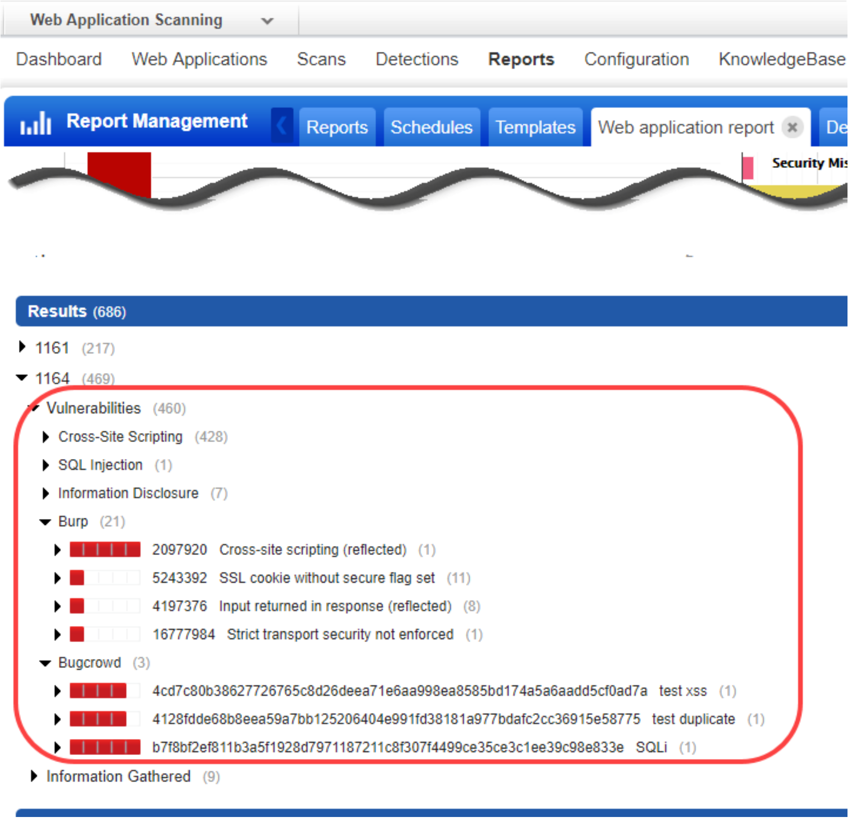
Go to Reports > Schedules and select the report you want to generate. Click the quick action menu and then click Launch Now. The report is immediately generated.

New Filters Added

We have simplified search in WAS with addition of various new filters. Check them out.
- Detection Type Filter in Report Template
- Web application ID Filter in Detections
- OWASP, WASC, CWE ID, CVE ID filters in Knowledgebase

Detection Type Filter in Report Template

We have now enhanced the reports so that you can now view all detection types: Qualys, Burp and Bugcrowd in a single report. You could select either Qualys, Burp, or Bugcrowd or all the detection types in the report template and configure the detection type to be displayed in a report.

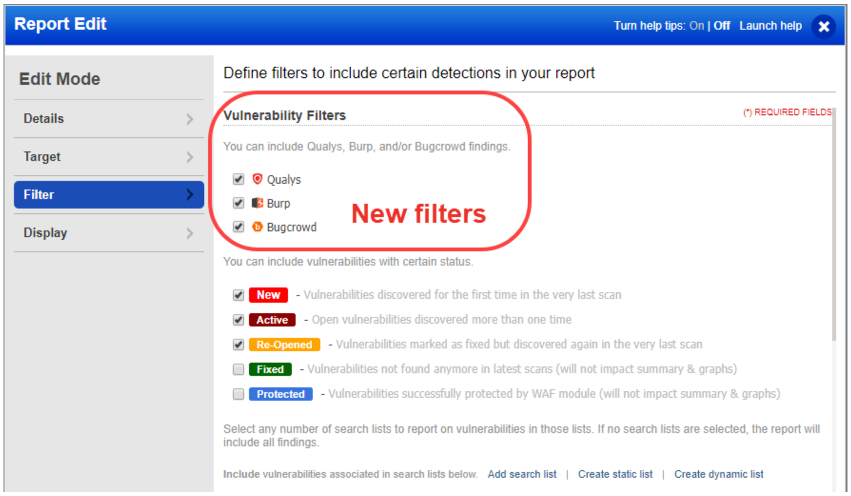


Results (686)
- 1161 (217)
- 1164 (469)
  - Vulnerabilities (460)
    - Cross-Site Scripting (428)
    - SQL Injection (1)
    - Information Disclosure (7)
  - Burp (21)
    - 2097920 Cross-site scripting (reflected) (1)
    - 5243392 SSL cookie without secure flag set (11)
    - 4197376 Input returned in response (reflected) (8)
    - 16777984 Strict transport security not enforced (1)
  - Bugcrowd (3)
    - 4cd7c80b38627726765c8d26deea71e6aa998ea8585bd174a5a6aadd5cf0ad7a test xss (1)
    - 4128fdde68b8eea59a7bb125206404e991fd38181a977bdafc2cc36915e58775 test duplicate (1)
    - b7f8bf2ef811b3a5f1928d7971187211c8f307f4499ce35ce3c1ee39c98e833e SQLi (1)
  - Information Gathered (9)

Go to Reports > Reports > New Report and select report type, report template, web application or tags and click Finish. The Web application report that you view will now display all detection types in Results section. By default, all the detection types are displayed in a report.

You can configure the report template to decide which detection types should be displayed in a report.

If you want to update the current report, simply click Edit Report and select Filter tab. You can now choose which detection type should be displayed in your report.



Define filters to include certain detections in your report

Vulnerability Filters

(*) REQUIRED FIELDS

You can include Qualys, Burp, and/or Bugcrowd findings.

☑ Qualys
☑ Burp
☑ Bugcrowd

You can include vulnerabilities with certain status.

☑ 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)
☐ Protected - Vulnerabilities successfully protected by WAF module (will not impact summary & graphs)

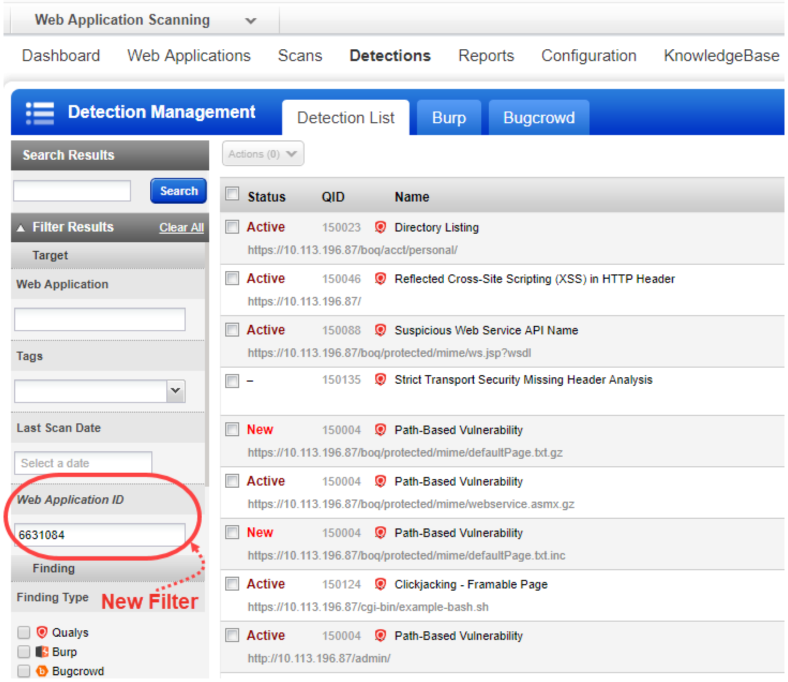
Select any number of search lists to report on vulnerabilities in those lists. If no search lists are selected, the report will include all findings.

Include vulnerabilities associated in search lists below. Add search list | Create static list | Create dynamic list

Web application ID Filter in Detections

Searching detections associated for a particular web application is now easier and simpler with our new filter: web application ID. The web application ID is unique and hence the search results using a web application ID are more precise and accurate.

Go to Detections > Detection List and then type the web application ID. All detections associated with the web application are displayed.



Web Application ID: 6631084

Status	QID	Name
Active	150023	Directory Listing https://10.113.196.87/boq/acct/personal/
Active	150046	Reflected Cross-Site Scripting (XSS) in HTTP Header https://10.113.196.87/
Active	150088	Suspicious Web Service API Name https://10.113.196.87/boq/protected/mime/ws.jsp?wsdl
–	150135	Strict Transport Security Missing Header Analysis
New	150004	Path-Based Vulnerability https://10.113.196.87/boq/protected/mime/defaultPage.txt.gz
Active	150004	Path-Based Vulnerability https://10.113.196.87/boq/protected/mime/webservice.asmx.gz
New	150004	Path-Based Vulnerability https://10.113.196.87/boq/protected/mime/defaultPage.txt.inc
Active	150124	Clickjacking - Framable Page https://10.113.196.87/cgi-bin/example-bash.sh
Active	150004	Path-Based Vulnerability http://10.113.196.87/admin/

OWASP, WASC, CWE ID, CVE ID filters in Knowledgebase

Search capability in the Knowledgebase is now simplified and easier with the addition of four new filters.

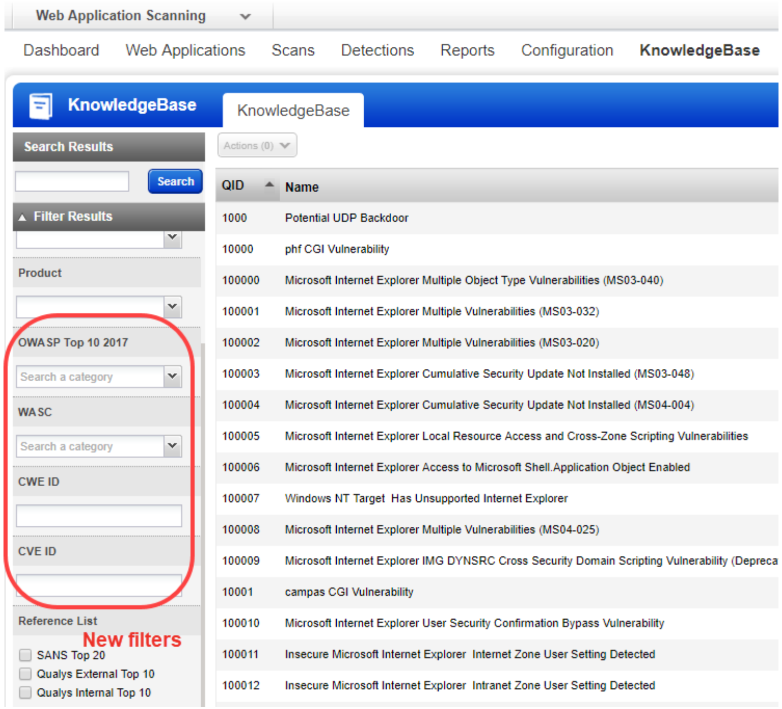
Go to Knowledgebase and expand Identification category in the Filter Results search pane. You will notice the new filters.

-OWASP Top 10 2017: Select the required OWASP category to view the associated QIDs.

-WASC: Select the required WASC category search to view the associated QIDs.

-CWE ID: Type the CWE ID and view the associated QIDs

-CVE ID: Type the CVE ID and view the associated QIDs

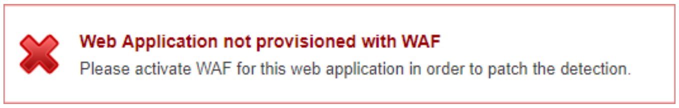
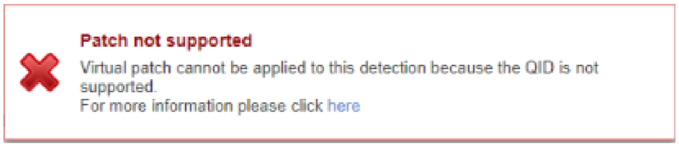
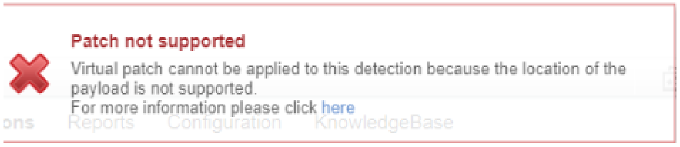
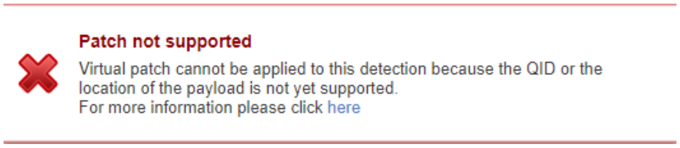


QID	Name
1000	Potential UDP Backdoor
10000	phf CGI Vulnerability
100000	Microsoft Internet Explorer Multiple Object Type Vulnerabilities (MS03-040)
100001	Microsoft Internet Explorer Multiple Vulnerabilities (MS03-032)
100002	Microsoft Internet Explorer Multiple Vulnerabilities (MS03-020)
100003	Microsoft Internet Explorer Cumulative Security Update Not Installed (MS03-048)
100004	Microsoft Internet Explorer Cumulative Security Update Not Installed (MS04-004)
100005	Microsoft Internet Explorer Local Resource Access and Cross-Zone Scripting Vulnerabilities
100006	Microsoft Internet Explorer Access to Microsoft Shell.Application Object Enabled
100007	Windows NT Target Has Unsupported Internet Explorer
100008	Microsoft Internet Explorer Multiple Vulnerabilities (MS04-025)
100009	Microsoft Internet Explorer IMG DYNSRC Cross Security Domain Scripting Vulnerability (Depreca
10001	campas CGI Vulnerability
100010	Microsoft Internet Explorer User Security Confirmation Bypass Vulnerability
100011	Insecure Microsoft Internet Explorer Internet Zone User Setting Detected
100012	Insecure Microsoft Internet Explorer Intranet Zone User Setting Detected

Improved Notifications for Virtual Patch Installation

We have now added improved notifications when you patch findings/detections.

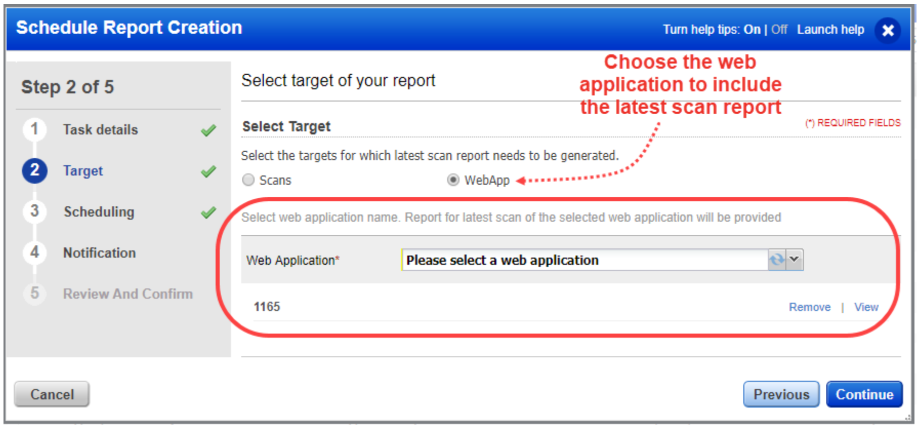
Let us see the various scenarios and the corresponding new notifications that are displayed when you patch the detections.

Scenario	Notification
The web application for which the detection is being patched is not activated in Web Application Firewall (WAF).	 **Web Application not provisioned with WAF** Please activate WAF for this web application in order to patch the detection.
QID not supported by WAF.	 **Patch not supported** Virtual patch cannot be applied to this detection because the QID is not supported. For more information please click here
Location of the payload not supported by WAF.	 **Patch not supported** Virtual patch cannot be applied to this detection because the location of the payload is not supported. For more information please click here
Either QID or location of the payload is not supported by WAF	 **Patch not supported** Virtual patch cannot be applied to this detection because the QID or the location of the payload is not yet supported. For more information please click here

Latest Scan Data Now in Scan Reports

You can now configure the scan (as well as scheduled) report to fetch latest scan data for the web application. When you configure the target for the scan report, choose the web application and we will include the latest scan conducted on the web application in the scan report.

Scheduled Scan Report



Schedule Report Creation

Step 2 of 5

1 Task details ✓
2 Target ✓
3 Scheduling ✓
4 Notification
5 Review And Confirm

Select target of your report

Choose the web application to include the latest scan report

Select Target

(*) REQUIRED FIELDS

Select the targets for which latest scan report needs to be generated.

○ Scans ● WebApp

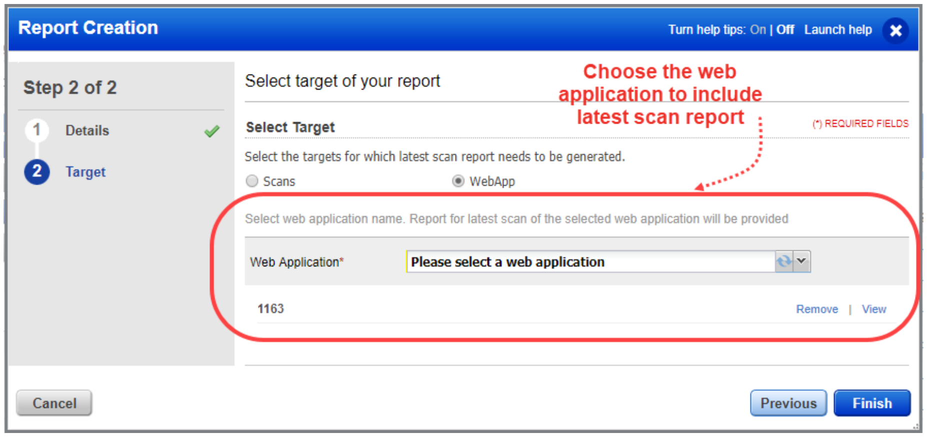
Select web application name. Report for latest scan of the selected web application will be provided

Web Application* Please select a web application

1165 Remove | View

Go to Reports > Schedules and then click New Schedule or edit an existing schedule. In the target section, select the web application.

Scan Report



Report Creation

Step 2 of 2

1 Details ✓
2 Target

Select target of your report

Choose the web application to include latest scan report

Select Target

(*) REQUIRED FIELDS

Select the targets for which latest scan report needs to be generated.

○ Scans ● WebApp

Select web application name. Report for latest scan of the selected web application will be provided

Web Application* Please select a web application

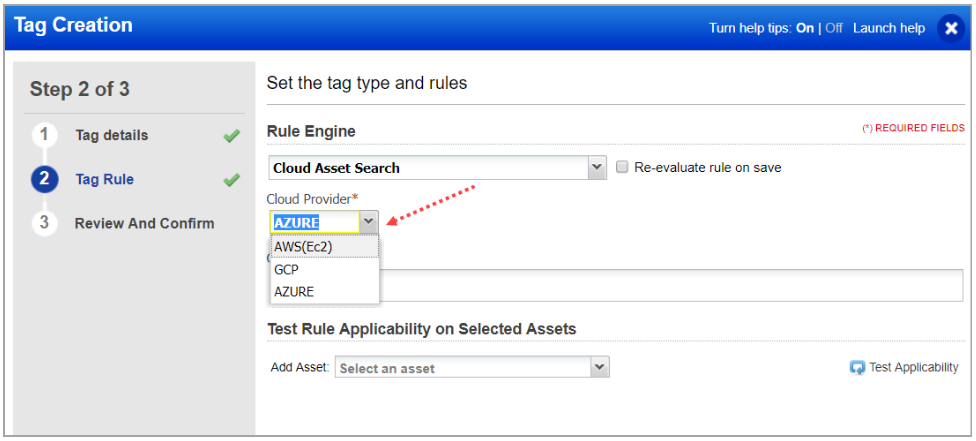
1163 Remove | View

Go to Reports > New Report > Scan Report. In the target section, select the web application.

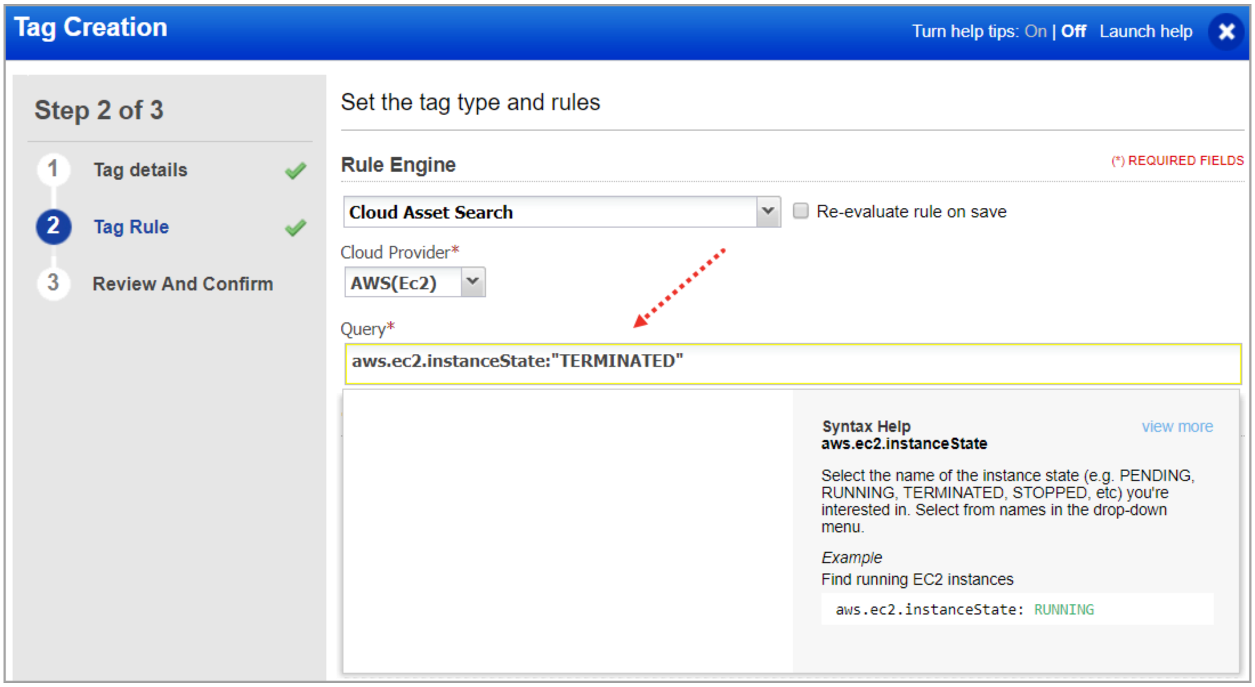
The scan report then populates the latest scan data in the report.

Dynamic tagging for AWS, AZURE, GCP

AssetView tag creation wizard now supports dynamic tagging for AWS (EC2), AZURE, and GCP assets. You can now group your cloud assets according to the cloud provider they belong to. Tags are applied to assets found by cloud agents (AWS, AZURE, GCP) and EC2 connectors (AWS).



Once you select the cloud provider you can use the predefined tokens to form a search query to create the tag rule.



aws.ec2.instanceState:"TERMINATED"

Syntax Help
aws.ec2.instanceState

Select the name of the instance state (e.g. PENDING, RUNNING, TERMINATED, STOPPED, etc) you're interested in. Select from names in the drop-down menu.

Example
Find running EC2 instances

```
aws.ec2.instanceState: RUNNING
```

Issues addressed in this release

Qualys Cloud Platform 2.35 brings you many more improvements and updates.

AV AssetView

TP ThreatPROTECT

- The issue is now resolved and asset count in displayed accurately in the appropriate widgets on the dashboard.
- Asset search query now returns correct results after drill down.
- Fixed an issue with Asset Search tag defined with "not scanned in <n> days" not re-evaluating assets automatically.
- We've added these Query Limits which are now implemented for these apps - AV, TP, VM dashboard, CA
    - Maximum field value length: 256 characters
    - Maximum query length: 4096 characters

  If your query exceeds a limit, an error message is shown and you won't get search results.
- Fixed an issue where Internet Explorer displayed an error while launching asset details in AssetView.

CA Cloud Agent

- Fixed an issue where an incorrect number was shown for total count of agents activated by an activation key.
- Fixed an issue where the Agent Summary did not show Manifest/VulnSign information.
- You can now click the "activation in progress" message for FIM/IOC/PM on the Agents tab to view the assets on which activation is pending.
- FIM profile status (green dot and tool tip) are no longer available in the Cloud Agent UI. This status will now be visible in the FIM module.
- Fixed an issue where the Linux Version Distribution widget on Cloud Agent dashboard did not show Ubuntu and Debian information.
- Fixed an issue where bulk agent activation through API failed due to duplicate host assets.

SAQ Security Assessment Questionnaire

- The User Action Log is now sorted accurately and is working as expected.

WAS Web Application Scanning

- The issue is fixed and you can now delete WAS controlled MDS schedule scan.
- The UI-based reports in WAS are now updated to not show "Authentication Not Used" for information gathered type of vulnerabilities.
- We have now fixed the issue to display the correct count of the assets selected during removal of web assets (WAS --> Web Applications -->> Actions -->> Remove Web Assets).
- The API now returns result in JSON format, if acceptable type is JSON, as it was not previously provisioned.
- When a user is deleted from the report distribution group, the user gets now successfully deleted from the distribution group.
- When user removes only the child tag from the Web Application, despite Parent tag being associated with the Web Application, it now displays correct message: "0 Tags have been successfully removed from the selected record(s).
- We have now improved the text displayed in error messages when the web applications to be scanned during a scan exceed 2500 or if the target to concurrency ratio exceeds 25.
- A web application now correctly displays scheduled status as "Yes" when the Web App is scheduled for a scan using tags.
- The Null Pointer Exception error is prevented from being displayed to not block the user while downloading the CSV web app report.
- WAS schedules now do not switch from Single to Daily occurrences without making specific changes related to occurrences.
- Scheduled scans now point to correct error message when the mandatory parameters needed for the scan are not specified.
- The export link at following locations now exports correctly:
  - Scans > Scan List > View Report > Vulnerabilites > Export
  - Web applications > View Report > Vulnerabilities > Export
  - Detections > Detection List > Vulnerabilities > Export
- We have fixed Web App Report Generation API Error for big size report.
- The user will now be able to successfully use "Scan Again" from the WAS dashboard.
- Authentication scan now can be successfully launched for the subuser with WAS manager, WAS Scanner and WAS User access roles.
- We now display an error message when the user exceeds total records against Text and Graphical Threshold.
- The retest API functionality now functions as expected.
- Online and downloaded WebApp reports now display correct data (count of records) and the data is in sync as well.
- We now display '-' under report Downloads in case of null value.
- Logos for Qualys, Burp and Bugcrowd (in SVG format) are now correctly displayed.

WAF Web Application Firewall

- WAF UI for Event section is revamped. Important improvements include new search with wide-range of event filters and support highlighting of events when moving the mouse over one or more valid QID rows in the Event Details section.
- We have updated our Event Inspection and Event Details sections to display contextual events along with their respective confidence and threat level scores for a detection event.
- We have fixed an issue where very long profile names were moving out of the "Add to Sites" window.
- We have fixed an issue where end date under Freeze Period in the Automatic Updates tab getting changed in view/edit mode of WAF clusters. The issue is resolved by fixing the code for saving the end date.
- The WAF appliance list page now displays a new Platform column to display the icons of platforms on which the WAF appliances are deployed.
- We have updated the text on Quick Start Guide page for Configure WAF appliances.
- You will now see an in-process notification for an event for which updating a flag is in progress.
- Now you can click on a custom rule displayed in the Security tab in the Web Application Create/Edit mode to view or edit that rule.
- We have updated the label for Server Timeout to HTTP Response Timeout. You will find the label when you go to the Application tab while creating or editing a web application.
- We have increased the display size of the Response Page Body frame, which you can see when you click the Configuration tab while creating or editing a Custom Response Page.
- You will now see a warning message when you delete a cluster that is linked to an appliance.
- We have added a "Status" filter in the Rules Section to let you search rules by their status.
- We have added a new graph filter "By Platform" on the appliances overview panel to show you the count of appliances running on each platform.

Qualys Cloud Platform

- Granted modules are now visible under view mode of subuser when the user clicks View Role, using the Administration utility.
- Fixed some discrepancies between asset data returned by the Search Host Asset API (/qps/rest/2.0/search/am/hostasset)
- Fixed an issue with ServiceNow CMDB connector not getting enabled.
- Fixed an issue where incorrect Spot Instance information was displayed for EC2 assets.
- You can now specify the default date filter to be set on the IOC UI (for example, last month, yesterday, etc). You can get this configured by contacting Qualys Support.
- Fixed an issue where the rogue container widget on Container Security dashboard displayed an incorrect number for total count of rogue containers.
- Fixed an issue where AWS connectors were stuck in synchronization state and errored out.