Qualys Cloud Platform v2.x

Release Notes

Version 2.39

June 5, 2019

Here's what's new in Qualys Cloud Suite 2.39!

Qualys Cloud Platform 2.39 brings you many more Improvements and updates! Learn more

WAS Web Application Scanning

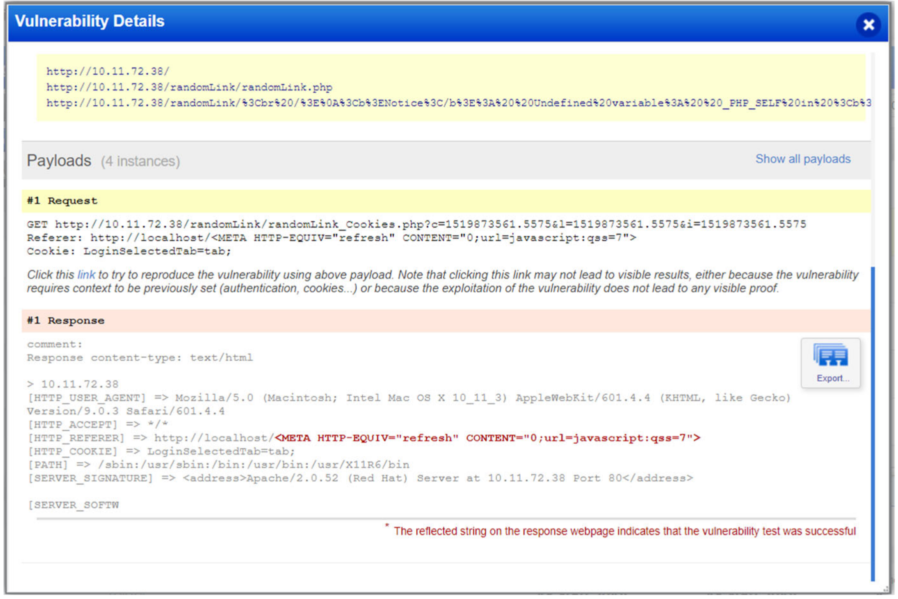
Full Path in Vulnerability Details for Detections

We now provide you with complete and raw HTTP request for detections (except for Information Gathered (IG) vulnerabilities).

Earlier, WAS displayed link, method, POST data, headers and snippets of the response body. Now, we will include full request headers and full request body for vulnerabilities. The complete requests and responses will help you to reproduce or validate the issue.

Examples:

Sample GET request



Vulnerability Details

```
http://10.11.72.38/
http://10.11.72.38/randomLink/randomLink.php
http://10.11.72.38/randomLink/%3Cbr%20/%3E%0A%3Cb%3ENotice%3C/b%3E%3A%20%20Undefined%20variable%3A%20%20_PHP_SELF%20in%20%3Cb%3
```

Payloads (4 instances)

#1 Request

```
GET http://10.11.72.38/randomLink/randomLink_Cookies.php?c=1519873561.5575&l=1519873561.5575&i=1519873561.5575
Referer: http://localhost/<META HTTP-EQUIV="refresh" CONTENT="0;url=javascript:qss=7">
Cookie: LoginSelectedTab=tab;
```

Click this link to try to reproduce the vulnerability using above payload. Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.

#1 Response

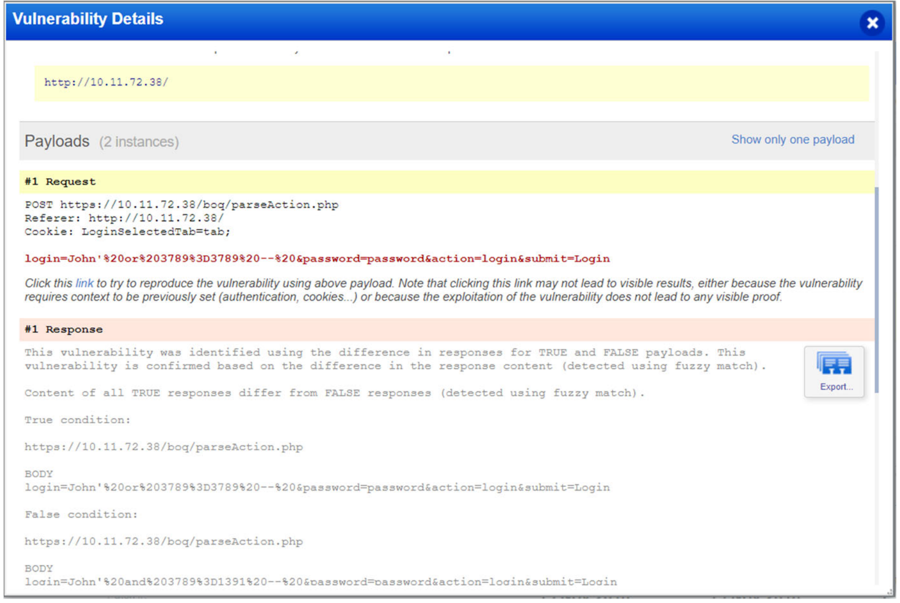
```
comment:
Response content-type: text/html

> 10.11.72.38
[HTTP_USER_AGENT] => Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_3) AppleWebKit/601.4.4 (KHTML, like Gecko)
Version/9.0.3 Safari/601.4.4
[HTTP_ACCEPT] => */*
[HTTP_REFERER] => http://localhost/<META HTTP-EQUIV="refresh" CONTENT="0;url=javascript:qss=7">
[HTTP_COOKIE] => LoginSelectedTab=tab;
[PATH] => /sbin:/usr/sbin:/bin:/usr/bin:/usr/X11R6/bin
[SERVER_SIGNATURE] => <address>Apache/2.0.52 (Red Hat) Server at 10.11.72.38 Port 80</address>

[SERVER_SOFTW
```

* The reflected string on the response webpage indicates that the vulnerability test was successful

Sample POST request



Vulnerability Details

```
http://10.11.72.38/
```

Payloads (2 instances)

#1 Request

```
POST https://10.11.72.38/boq/parseAction.php
Referer: http://10.11.72.38/
Cookie: LoginSelectedTab=tab;

login=John'%20or%203789%3D3789%20--%20&password=password&action=login&submit=Login
```

Click this link to try to reproduce the vulnerability using above payload. Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.

#1 Response

```
This vulnerability was identified using the difference in responses for TRUE and FALSE payloads. This
vulnerability is confirmed based on the difference in the response content (detected using fuzzy match).

Content of all TRUE responses differ from FALSE responses (detected using fuzzy match).

True condition:

https://10.11.72.38/boq/parseAction.php

BODY
login=John'%20or%203789%3D3789%20--%20&password=password&action=login&submit=Login

False condition:

https://10.11.72.38/boq/parseAction.php

BODY
login=John'%20and%203789%3D1391%20--%20&password=password&action=login&submit=Login
```

Enhanced Crawling for Web Application Scans

We have now introduced enhanced crawling in your option profile for your scans to improve scan coverage for your web application. With the enhanced crawling enabled, more links can be crawled and it will improve scan coverage. We will re-crawl individual directories present in the links which are found during crawling.

For example, if the following link is found during crawling:
https://www.example.com/foo/abc/xyz/register.php

If the enhanced crawling is enabled, it will first make a request to
https://www.example.com/foo/abc/xyz

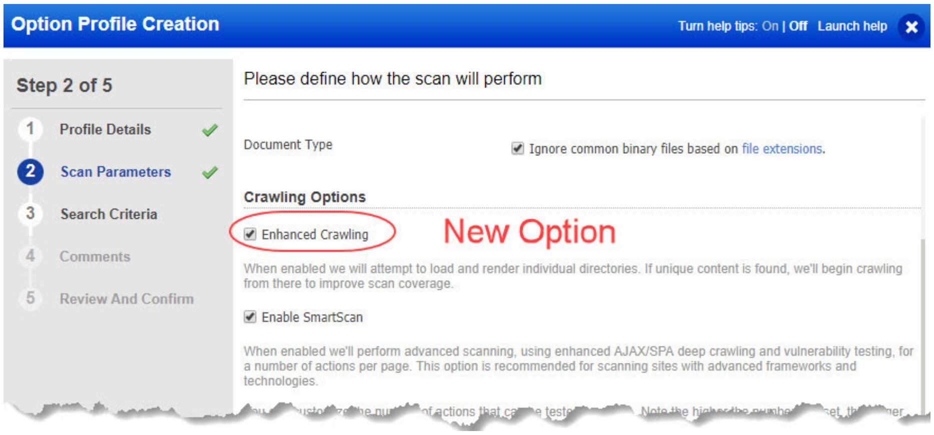
and will then remove the directory "xyz/" from the URL and crawl,
https://www.example.com/foo/abc/

and later it will further remove "abc/" and will crawl https://www.example.com/foo/.

All the links found during this process of removal and re-crawling will get added to the crawl queue thus improving the scan coverage.

Tell me the steps

Go to Configuration > Option Profiles and either create a new option profile or edit an existing option profile. Enable the Enhanced Scanning checkbox in Scan Parameters tab under Crawling Options section and save the settings.



Please define how the scan will perform

Document Type ☑ Ignore common binary files based on file extensions.

Crawling Options

☑ Enhanced Crawling

When enabled we will attempt to load and render individual directories. If unique content is found, we'll begin crawling from there to improve scan coverage.

☑ Enable SmartScan

When enabled we'll perform advanced scanning, using enhanced AJAX/SPA deep crawling and vulnerability testing, for a number of actions per page. This option is recommended for scanning sites with advanced frameworks and technologies.

Issues addressed in this release

Qualys Cloud Platform 2.39 brings you many more improvements and updates.

AV AssetView

TP ThreatPROTECT

- Asset details now show EC2/Azure information for cloud assets discovered via AWS/Azure connector, even though the Cloud Agent module is not enabled for the user.
- Fixed an issue where Asset Details did not show network information for EC2 assets in classic zone.

CA Cloud Agent

- Fixed an issue in Cloud Agent where the Activation Key window took a lot of time to load, while editing an existing activation key.
- Fixed an issue in Cloud Agent API where the "asset" and "hostasset" APIs took a long time to fetch data resulting in timeouts.

SAQ Security Assessment Questionnaire

- Users with appropriate permissions can now successfully edit comments.
- Users can now view all SAQ templates appropriately while creating Campaigns.

VM Vulnerability Management

- We have fixed an issue and users can now create and view Vulnerability Management dashboard widgets properly.
- Accurate count of assets is now displayed on the Vulnerability page in Asset Details.

WAF Web Application Firewall

- Now when you create an HTTP profile, the Review and Confirm tab will show the Web Services Protection details section after Protocol Anomalies details.
- The exception icon tooltip for events will show message according to the action chosen for the exception by the user.
- On the Events tab, we have added a navigation button on the right side of the search bar to allow the user to navigate the search filters from the right side of the bar.

WAS Web Application Scanning

- We fixed an issue that caused the scan to fail during normalization phase (for few scans). As a result, all the scans are running successfully now.
- We have rectified the help tip for the Make this the default report template option. The new text states: Select "Make this the default report template..." and we'll select this template type by default in a new report - a report run by you or another user in your subscription. You can define only one default template for each template type in your subscription.
- We have updated WAS API User Guide to include example related to latest version of burp (2.0.0) and removed outdated example in Burp Import Issue topic (page 445 to 456).
- Users can now retest all AJAX vulnerabilities which was earlier being forbidden.
- We now allow using same scan name for different scan type. However using same scan name for same scan type is forbidden.
- We now display the correct count of total vulnerabilities on dashboard in case of multiple tags associated with a single web application. Earlier, the count of vulnerabilities was incorrectly displayed.
- We have updated the status of finding from 'under-retest' to "NO_RETEST" as it provides a better visibility for the status to the user and allows to perform retest for findings that could not be retested due to scan failure.
- If a web site is down, the email notification now correctly displays the website name. Previously, it incorrectly stated domain title instead of website name.
- The count of vulnerabilities for CMS identification (type, version, and plugins) type during definition of option profile search criteria is now correctly displayed. Earlier the number of QIDs in some cases did not match with the count of vulnerabilities being displayed.
- We have fixed the font anomalies for Web Application Details section of the appendix in the scan report (both PDF and HTML format).
- The result of QIDs 150103, 150120, 150121, 150122, 150123, 150159, 150160, and 150161 are now consolidated on only one vulnerability instance (displaying all the vulnerable cookies on same vulnerability instance).

Qualys Cloud Platform

- Qualys Cloud Platform UI now shows a single PC-SCA module if both PC and SCA are enabled for the user.
- Fixed an issue where the number of users shown in VM and Admin apps were different. Now VM and Admin apps both show the same number of users.
- A new Azure dashboard template is available to configure an Azure dashboard in CloudView.