



Qualys Cloud Platform v2.x

Release Notes

Version 2.41

September 18, 2019

Here's what's new in Qualys Cloud Suite 2.41!

AV

AssetView

Tag assets from [Global IT Asset Inventory](#)

WAF

Web Application Firewall

Configure to keep the Accept-Encoding Header in Request

WAS

Web Application Scanning

Support for Postman Collection File Upload

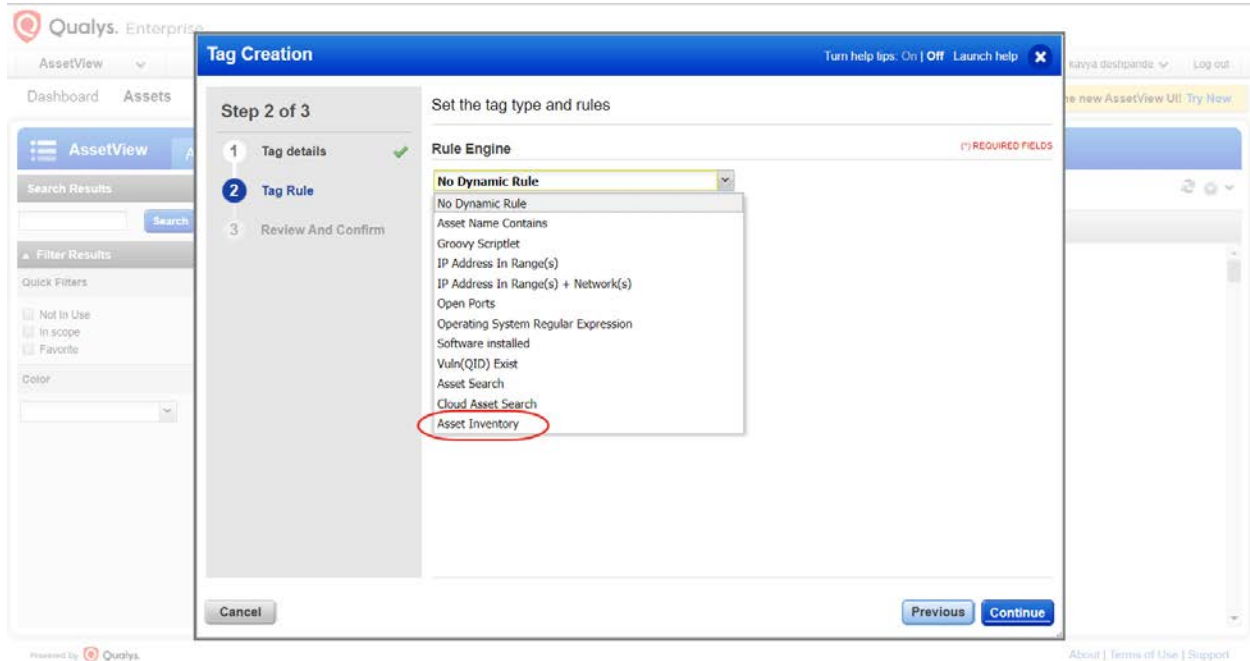
Full Path of Detections in Reports (PDF and HTML)

Qualys Cloud Platform 2.41 brings you many more Improvements and updates! [Learn more](#)

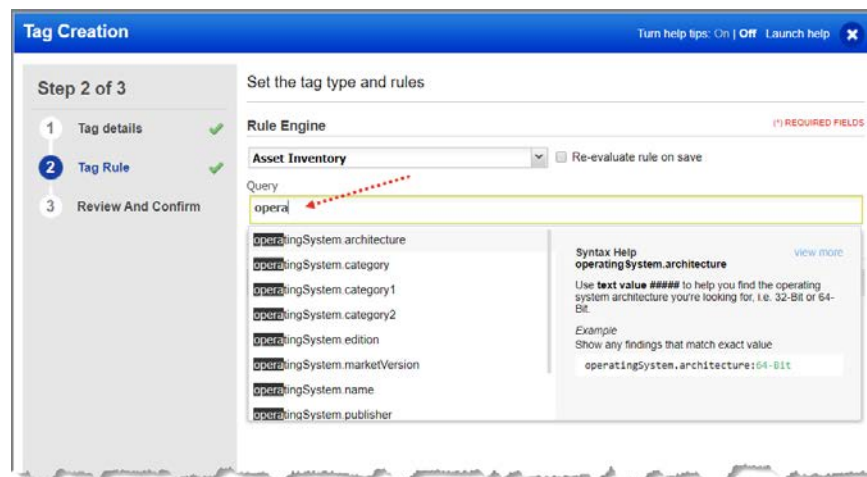
Tag assets from Global IT Asset Inventory

You can now apply tags to organize assets from Global IT Asset Inventory. Tagging assets provides a flexible and scalable way to automatically discover and organize the assets.

1) Click New Tag, 2) choose the Asset Inventory rule, and 3) enter your query.



Just start typing in the Query field and we'll show you the Asset Inventory attributes you can search.



Configure to keep the Accept-Encoding Header in Request

You can now create an HTTP profile for your web application to specify the WAF application to either retain or remove the Accept-Encoding header field in requests. If you choose to retain the header field then WAF will keep the header field in requests that contain this header field while forwarding the requests to your web application. By default, WAF will remove this header field.

The screenshot shows the 'Profile Creation' wizard in the AWS WAF console, specifically 'Step 2 of 6: HTTP Protocol'. The left sidebar lists the steps: 1. Profile Details (checked), 2. HTTP Protocol (active), 3. Web Services, 4. Information Leakage, 5. Declarative Security, and 6. Review And Confirm. The main content area is titled 'Configure HTTP Protocol analysis for your HTTP profile'. It contains three sections: 'Request Method' with options 'Allow All, Detect Violations' (selected), 'Detect Invalid Methods', and 'Detect TRACE, TRACK'; 'Accept-Encoding' with the 'Keep Accept-Encoding' checkbox checked (highlighted by a red box); and 'Request Headers' with the 'Detect Invalid Headers' checkbox. At the bottom are 'Cancel', 'Previous', and 'Continue' buttons.

To configure accept encoding, go to Security > HTTP Profiles > Create or Edit an HTTP Profile.

Support for Postman Collection File Upload

We now support security test of REST APIs exported using Postman tool.

Postman tool, used to test the REST APIs, has the facility to export and share the REST APIs. Postman Collection file is the group of REST APIs. Just upload the Postman Collection exported file in JSON format and we will then scan for vulnerabilities.

Web Application Creation Turn help tips: On | Off Launch help

Step 2 of 10

1 Asset Details ✓
2 **Application Details** ✓
3 Scan Settings
4 Crawl Settings
5 Redundant Links
6 Authentication
7 Exclusions
8 Advanced Options
9 Comments
10 Review And Confirm

Tell us about the web application you want to scan

API Endpoint Definition (non-Swagger based APIs)

☐ None
☒ **Postman Collection**
Upload a valid Postman Collection file for your API. We currently only support v2.0.0 and v2.1.0. for Postman Collection. Once uploaded, we will parse the file to create requests and then crawl and test those request

+ **Upload Postman Collection File (Mandatory)**
Sample_PostmanCollection.json Download Remove
+ **Upload Postman Environment Variables File (Optional)**
+ **Upload Postman Global Variables File (Optional)**

☐ **Burp Proxy Capture**
You have the option to upload a Burp Log File with your scan tests. Once uploaded we will parse it to create requests and then crawl and test those requests.

+ **Upload Burp Log File**

Cancel Previous Continue

Go to Web Applications > New Web Application. After you define the mandatory parameters in Asset Details, go to Application Details and select Postman Collection in API Endpoint Definition (non-Swagger based APIs).

Upload the Postman Collection File (mandatory) and click Continue. We also support upload of Postman Environmental Variables and Postman Global Variables file.

Note: We currently only support v2.0.0 and v2.1.0. for Postman Collection. The size of the file you upload should not exceed 5 MB.

We provided you with complete and raw HTTP request for detections. Now, the reports downloaded in PDF and HTML format also display complete and raw HTTP request for detections (except for Information Gathered (IG) vulnerabilities).

Examples:

Bookmarks

- Target and Filters
- Summary
- Detailed Results
- Vulnerability
 - Cross-Site Scripting
 - 150001 Reflected Cross-Site Scripting (XSS) Vulnerabilities
 - https://10.11.2.37/?account=personal%20%3Cscript%3E_q_%3Drandom()%3C%2Fscript%3EReferer: http://10.11.72.37/Cookie: cookie3=cookiethree; cookie2=cookietwo; cookie1=cookieone; PHPSESSID=34c2ee00ee4fa73f0c862aa94a2c4fd; Host: 10.11.72.37 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 Accept: */*

WAS Web Application Report

#1 Request

```
GET http://10.11.72.37/?account=personal%20%3Cscript%3E_q_%3Drandom()%3C%2Fscript%3EReferer: http://10.11.72.37/Cookie: cookie3=cookiethree; cookie2=cookietwo; cookie1=cookieone; PHPSESSID=34c2ee00ee4fa73f0c862aa94a2c4fd; Host: 10.11.72.37 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 Accept: */*
```

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

=255>
<input name="ui_mode" type="hidden" value="atm_lookup">
<form>
<p> <p> <p> <p> <p> <p>
<div id=gc;
<div id="content">
<center><h3>Products - personal<script>_q_q=random()%3C%2Fscript></h3></center>
<ul class="vertical_list">
<li><a href=boq/acc/personal/checking.html>Checking</a></li>
<li><a href=boq/acc/personal/savings.html>Savings</a></li>
<li><a href=boq/acc/personal/creditcard.html>Credit Cards</a></li>
```

```
Payloads
```

#1 Request

```
GET https://10.11.72.37/?account=business%22%3E%3CDIV%20STYLE%3D%22width%3Eexpression(qs=%3D7)%22%3E
Referer: http://10.11.72.37/
Cookie: cookie3=cookiethree; cookie2=cookietwo; cookie1=cookieone; PHPSESSID=34c2ee00e4a0a73f0c862aa94a2c4fd;
Host: 10.11.72.37
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
Accept: */*
```

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.

Issues addressed in this release

Qualys Cloud Platform 2.41 brings you many more improvements and updates.

AV

AssetView

- Fixed an issue in AssetView where incorrect OS icon was shown for Cisco assets.

CA

Cloud Agent

- Fixed an issue in Cloud Agent where incorrect messages were shown while activating agents for modules when module licenses are expired.
- You can now assign the UDC manifest to all agents at once.
- Cloud Agent action logs will now show actions performed on Activation Keys.
- Fixed an issue in Cloud Agent where the MAC VERSION DISTRIBUTION widget on the dashboard was not showing any data.

VM

VM Dashboard

- Fixed an issue in VM Dashboard where upon applying the tag filter, trending data was getting displayed with vulnerability count instead of displaying only the vulnerability count.

SAQ

Security Assessment Questionnaire

- Fixed the error message shown while updating a campaign for which the template is deleted or is in draft mode.
- Security Assessment Questionnaire now supports sending email to email addresses with top level domain length up to 8 characters.

WAS

Web Application Scanning

- We have now fixed an issue so that the downloaded reports in PDF and HTML format now display correct data and the data is in sync with the online report.
- Creating schedules and reports using API with ALL option for tags reflected ANY on UI. This is now fixed to correctly reflect ALL option in tags during schedule and report creation from API.
- We have now fixed the broken link in Vulnerability details for QID 150085 so that the link now opens the correct web page.
- We have updated the WAS online help to reflect correct information related to scan results storage settings.

- We have now fixed an issue so that error is not displayed during retest of a finding due to long scanner name. We have resolved the issue as we are able to retest findings on scanners with long size name.
- Clicking Save during update of Global Settings temporarily disables all the options to avoid duplicate entries caused by multiple clicks in single attempt. Once the update is complete, all options are available for editing again.
- The error message during catalog and maps update was displayed inconsistently. We have now fixed the issue by increasing the character length for error message to 1000 characters. The error message if displayed is consistent across various users.
- We have now resolved an exception so that the finding could be retested correctly without the exception 'Vulnerable URL cannot be found anymore'. For example, QID 150001.
- The cookie related vulnerability details for QIDs 150103, 150120, 150121, 150122, 150123, 150159, 150160, and 150161 for existing scans and web applications is now shown correctly.
- The preview of schedules with authentication records now display correct details. Earlier, the preview displayed "None" despite the schedule having authentication records.
- We have now extended our support so that the Detection Datalist report download successfully works for up to 10000 records.
- We have now fixed data inconsistency for "Function" and "AJAX request" column in downloaded reports with CSV format.
- We have fixed the font anomalies for Web Application Details section of the appendix in the scan report (both PDF and HTML format).
- We have fixed an issue where updating web applications that contain attributes is done successfully. Earlier, web applications with attributes were not updated correctly.

Qualys Cloud Platform

- Fixed an issue is Asset Details > Asset Summary where Last System Boot was showing incorrect date-time.
- Fixed an issue where the Host Asset update API (/qps/rest/2.0/update/am/hostasset) was throwing an error if the POST request contained a large number of Asset IDs.
- Users will now be able to run Azure connectors successfully through the Run Connector API (/qps/rest/2.0/run/am/assetdataconnector).
- Fixed an issue where AWS connectors were getting stuck in the "Synchronizing" state and as a result stale assets were seen in the Assets list.