Qualys Cloud Platform v3.x
API Release Notes

Version 3.5

January 25, 2021

Qualys Cloud Suite API gives you many ways to integrate your programs and API calls with Qualys capabilities. You'll find all the details in our user guides, available at the time of release. Just log in to your Qualys account and go to Help > Resources.

What's New

WAS API: Added CVSS v3 scores in Findings Output

WAS API: Added New Input Parameters to Create and Delete Web Application API

Qualys API Server URL

The Qualys API URL you should use for API requests depends on the Qualys platform where your account is located.

Click here to identify your Qualys platform and get the API URL

This documentation uses the API gateway URL for Qualys US Platform 1 (https://gateway.qg1.apps.qualys.com) in sample API requests. If you're on another platform, please replace this URL with the appropriate gateway URL for your account.

WAS API: Added CVSS v3 scores in Findings Output

API affected	/qps/rest/3.0/get/was/finding/<id> /qps/rest/3.0/search/was/finding
New or Updated APIs	Updated
DTD or XSD changes	Yes

With this release, we will show CVSS v3 (Common Vulnerability Scoring System) information for the findings of types (Vulnerability and Sensitive Content) in the Search and Get Finding API outputs. Earlier, we were not showing the CVSS information in any of the WAS API outputs. The outputs will show cvssV3 <base>, cvssV3 <temporal> and cvssV3 <attackVector> information in the outputs.

You will see this information for Vulnerability and Sensitive Content QID types in the Scan and Web application reports. Reports in the XML, CSV, and CSV v2 formats show both CVSS v2 and CVSS v3 information. Reports in HTML and PDF formats show only CVSS v3 information.

Permissions

- You must have the WAS module enabled.

- You must have the "API access" and "Access WAS module" permissions.

Sample - Get details of a finding

The finding details show the CVSS v3 information.

API Request

```
curl -u "USERNAME:PASSWORD" -H "content-type: text/xml" -X "GET" --
"https://qualysapi.qualys.com/qps/rest/3.0/get/was/catalog/f717f2db-c6bb-
426f-ba80-f3617432317f"
```

XML Output

```
<?xml version="1.0" encoding="UTF-8"?>
<ServiceResponse xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="https://qualysapi.qualys.com/qps/xsd/3.0/w
as/finding.xsd">
    <responseCode>SUCCESS</responseCode>
    <count>1</count>
    <data>
        <Finding>
            <id>1995010</id>
            <uniqueId>8c9c933c-e5c5-f77e-e053-294f2c0ab892</uniqueId>
            <qid>150134</qid>
            <name>
```

```
                <![CDATA[Shellshock Apache Injection]]>
            </name>
            <type>VULNERABILITY</type>
            <potential>false</potential>
            <findingType>QUALYS</findingType>
            <group>INFO</group>
            <cwe>
                <count>1</count>
                <list>
                    <long>78</long>
                </list>
            </cwe>
            ...
            <webApp>
                <id>5250369</id>
                <name>
                    <![CDATA[1294]]>
                </name>
                <url>
                    <![CDATA[https://10.11.72.37]]>
                </url>
                <tags>
                    <count>15</count>
                    <list>
                        <Tag>
                            <id>110000818</id>
                            <name>
                                <![CDATA[499 webapps -VARUN]]>
                            </name>
                        </Tag>
                    </list>
                </tags>
            </webApp>
            <isIgnored>false</isIgnored>
            <cvssV3>
                <base>9.8</base>
                <temporal>8.8</temporal>
                <attackVector>Network</attackVector>
            </cvssV3>
        </Finding>
    </data>
</ServiceResponse>
```

Sample - Search for a finding to view the CVSS v3 information

Let us search for a finding of type vulnerability by its unique ID to view the CVSSv3 information of QIDs in the finding.

API Request

```
curl -u "USERNAME:PASSWORD" -H "content-type: text/xml" -X "POST" --
data-binary @-
"https://qualysapi.qualys.com/qps/rest/3.0/search/was/finding/" <
file.xml
Note: “file.xml” contains the request POST data.
```

Request POST data

```
<ServiceRequest>
    <preferences>
        <verbose>true</verbose>
    </preferences>
    <filters>
        <Criteria field="uniqueId" operator="EQUALS">8c9c933c-e5c5-f77e-
e053-294f2c0ab892</Criteria>
    </filters>
</ServiceRequest>
```

XML Output

```
<?xml version="1.0" encoding="UTF-8"?>
<ServiceResponse xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="https://qualysapi.qualys.com/qps/xsd/3.0/w
as/finding.xsd">
    <responseCode>SUCCESS</responseCode>
    <count>1</count>
    <hasMoreRecords>false</hasMoreRecords>
    <data>
        <Finding>
            <id>1995010</id>
            <uniqueId>8c9c933c-e5c5-f77e-e053-294f2c0ab892</uniqueId>
            <qid>150134</qid>
            <name>
                <![CDATA[Shellshock Apache Injection]]>
            </name>
            <type>VULNERABILITY</type>
            <potential>false</potential>
            <findingType>QUALYS</findingType>
            <cwe>
                <count>1</count>
                <list>
                    <long>78</long>
                </list>
            </cwe>
           ...
            <webApp>
                <id>5250369</id>
                <name>
                    <![CDATA[1294]]>
                </name>
                <url>
                    <![CDATA[https://10.11.72.37]]>
                </url>
                <tags>
                    <count>15</count>
                    <list>
                        <Tag>
                            <id>8753812</id>
                            <name>
                                <![CDATA[Multiscan]]>
                            </name>
                        </Tag>
                    </list>
                </tags>
            </webApp>
            <isIgnored>false</isIgnored>
            <cvssV3>
                <base>9.8</base>
                <temporal>8.8</temporal>
                <attackVector>Network</attackVector>
            </cvssV3>
        </Finding>
    </data>
</ServiceResponse>
```

Sample - Web app report in the XML format showing the CVSS v3 information for the QIDs

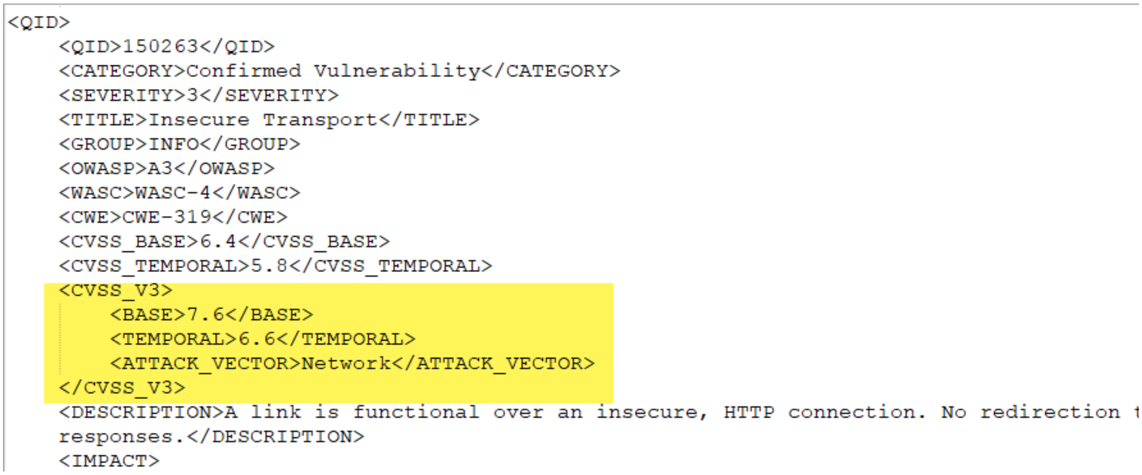
CVSS v3 information is shown in the Glossary section in the XML report.

API Request

```
curl -u "USERNAME:PASSWORD" -H "content-type: text/xml" -X "POST" --
data-binary @-
"https://qualysapi.qualys.com/qps/rest/3.0/create/was/report" <
file.xml
Note: “file.xml” contains the request POST data.
```

Request POST data

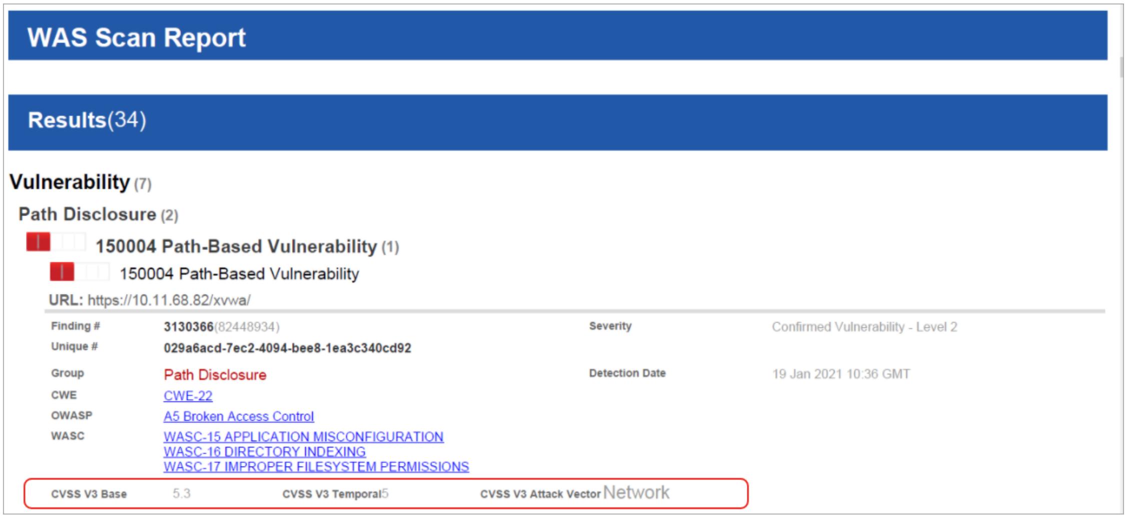
```
<ServiceRequest>
 <data>
 <Report>
 <name><![CDATA[WebApp rport with CVSS v3 information]]></name>
 <description><![CDATA[WebApp report]]></description>
 <format>XML</format>
 <type>WAS_WEBAPP_REPORT</type>
 <template> <id>694840</id> </template>
 <config>
 <webAppReport>
 <target>
 <webapps>
 <WebApp><id>6304279</id></WebApp>
</webapps>
</target>
</webAppReport>
</config>
</Report>
 </data>
</ServiceRequest>
```



```
<QID>
    <QID>150263</QID>
    <CATEGORY>Confirmed Vulnerability</CATEGORY>
    <SEVERITY>3</SEVERITY>
    <TITLE>Insecure Transport</TITLE>
    <GROUP>INFO</GROUP>
    <OWASP>A3</OWASP>
    <WASC>WASC-4</WASC>
    <CWE>CWE-319</CWE>
    <CVSS_BASE>6.4</CVSS_BASE>
    <CVSS_TEMPORAL>5.8</CVSS_TEMPORAL>
    <CVSS_V3>
        <BASE>7.6</BASE>
        <TEMPORAL>6.6</TEMPORAL>
        <ATTACK_VECTOR>Network</ATTACK_VECTOR>
    </CVSS_V3>
    <DESCRIPTION>A link is functional over an insecure, HTTP connection. No redirection t
    responses.</DESCRIPTION>
    <IMPACT>
```

Sample - Scan report in the PDF format showing the CVSS v3 information for a finding

CVSS v3 information is shown in the Scan report for a finding having QID 15004.



WAS Scan Report

Results(34)

Vulnerability (7)

Path Disclosure (2)

150004 Path-Based Vulnerability (1)

150004 Path-Based Vulnerability

URL: https://10.11.68.82/xvwa/

Finding #	3130366(82448934)	Severity	Confirmed Vulnerability - Level 2
Unique #	029a6acd-7ec2-4094-bee8-1ea3c340cd92		
Group	Path Disclosure	Detection Date	19 Jan 2021 10:36 GMT
CWE	CWE-22		
OWASP	A5 Broken Access Control		
WASC	WASC-15 APPLICATION MISCONFIGURATION WASC-16 DIRECTORY INDEXING WASC-17 IMPROPER FILESYSTEM PERMISSIONS		

CVSS V3 Base 5.3 CVSS V3 Temporal5 CVSS V3 Attack Vector Network

Updated XSD

<platform API server>/qps/xsd/3.0/was/finding.xsd

We added three new elements: base, temporal, and attackVector under the CvssV3 element in finding.xsd.

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema
    xmlns:xs="http://www.w3.org/2001/XMLSchema"
    elementFormDefault="qualified">

    <!-- REQUEST -->
    <xs:element name="ServiceRequest">
        ...
            <xs:element name="cvssV3" type="CvssV3" minOccurs="0"/>
      </xs:all>
   </xs:complexType>

   <xs:complexType name="CvssV3">
       <xs:all>
           <xs:element name="base" type="xs:float"/>
           <xs:element name="temporal" type="xs:float"/>
           <xs:element name="attackVector" type="xs:string"/>
       </xs:all>
   </xs:complexType>
...
```

WAS API: Added New Input Parameters to Create and Delete Web Application API

API affected	/qps/rest/3.0/create/was/webapp /qps/rest/3.0/delete/was/webapp/<id> /qps/rest/3.0/delete/was/webapp/<filters>
New or Updated APIs	Updated
DTD or XSD changes	Yes

Now, while deleting a web application, you can specify in the request if you want to remove the web application asset from your subscription also. Earlier, the Delete Web application API when used to delete web applications would delete the web application from WAS but never removed the web application asset from your subscription.

We added a new input parameter “removeFromSubscription” that when set to true deletes the web application asset from your subscription if the web application is not shared with other modules such as WAF.

If the “removeFromSubscription” parameter is set in the delete web application request, but the web application is shared with other modules, then the Delete Web application API will show you a message that web application is deleted from WAS but can not be deleted from your subscription because it is shared with other modules.

Earlier, while creating a web application using Create Web application API, we were not checking whether the web application with the same name and URL already exist in the subscription. As Delete Web application API would only delete the application from WAS and not from subscription and no checks are made to see if the web application exists in a subscription while creating a new application, the user was able to create a web application with the same name and URL. This behavior leads to the creation of multiple web application assets in subscription with the same name and URL

From this release, we added a new input parameter "reactivateIfExists" in the Create Web application API that when set to true will allow you to create a web application with the same name and URL. In such a case, all the data of the old web application such as findings, detections, scans will be deleted. The new web application will have the same web application asset ID as the old web application.

But if you try to create a web application with a different URL but with a name that already exists in your subscription, then API will return an error “Webapp with the same name exists” in the response. The flag "reactivateIfExists" will be ignored even if it is set to true.

If this flag is not set to true and if you try to create a web application with the same name and URL, then the Create web application API returns an error response informing the user that a web application with the same name and URL exist in the subscription.

Permissions

- You must have the WAS module enabled.

- You must have the "API access", and WAS Asset Permissions 1) “Create Web Asset” and 2) “Delete Web Asset”.

Create Web Application

We added a new input parameter reactivateIfExists.

Input Parameter

Parameter	Description
reactivateIfExists	(Boolean) Set this parameter to “true” to create a web application with the same name and URL. In such a case, all the data of the old web application such as findings, detections, scans will be deleted. The new web application will have the same web application asset ID as the old web application. But if you try to create a web application with different URL but with a name that already exists in your subscription , then API will return an error “Webapp with same name exists” in the response. The flag "reactivateIfExists" will be ignored even if it is set to true. If this flag is not set to true and if you try to create a web application with the same name and URL, then we show this error message in the response: “We found in your subscription an existing asset that already uses the same name and URL. The asset is currently being used by the modules: Was, Waf. Please set flag reactivateIfExists to true to use that existing asset. If not, you will need to change the name of the one you are trying to create.”

Sample - Create a web app with the reactivateIfExists flag set to true

API Request

```
curl -u "USERNAME:PASSWORD" -H "content-type: text/xml" -X "POST" --
"https://qualysapi.qualys.com/qps/rest/3.0/create/was/webapp/"<
file.xml
```

Note: “file.xml” contains the request POST data.

Request POST data

```
<ServiceRequest>
```

```
    <data>
        <WebApp>
            <reactivateIfExists>true</reactivateIfExists>
            <name><![CDATA[My Web application]]></name>
            <url><![CDATA[http://test.com]]></url>
            <config>
                <defaultDnsOverride>
                    <id>68820</id>
                </defaultDnsOverride>
            </config>
        </WebApp>
    </data>
</ServiceRequest>
```

Delete Web Application

We added a new input parameter removeFromSubscription.

Input Parameter

Parameter	Description
removeFromSubscription	(Boolean) When set to true, deletes the web application asset from your subscription if the web application is not shared with other modules such as WAF.

Sample - Delete web app with removeFromSubscription set to true

API Request

```
curl -u "USERNAME:PASSWORD" -X "GET"
""https://qualysapi.qualys.com/qps/rest/3.0/delete/was/webapp/"<
file.xml
```

Note: “file.xml” contains the request POST data.

Request POST data

```
<ServiceRequest>
    <data>
        <WebApp>
            <removeFromSubscription>true</removeFromSubscription>
        </WebApp>
    </data>
</ServiceRequest>
```

Updated XSD

<platform API server>/qps/xsd/3.0/was/webapp.xsd

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema
    xmlns:xs="http://www.w3.org/2001/XMLSchema"
    elementFormDefault="qualified">
    <!-- REQUEST -->
    ...
    <!-- RESPONSE -->
   ...
           <xs:element name="screenshot" type="Cdata" minOccurs="0"/>
           <xs:element name="proxy" type="HttpProxy" minOccurs="0"/>
           <xs:element name="config" type="WebAppConfig" minOccurs="0"/>
           <xs:element name="crawlingScripts" type="CrawlingScriptList"
minOccurs="0"/>
           <xs:element name="lastScanStatus" type="WasLastScanStatus"
minOccurs="0"/>
           <xs:element name="removeFromSubscription" type="xs:boolean"
minOccurs="0"/>
           <xs:element name="reactivateIfExists" type="xs:boolean"
minOccurs="0"/>
       </xs:all>
    </xs:complexType
...
```