ServiceNow Vulnerability Response Integration with Qualys WAS

User Guide
Version 1.2.0

June 15, 2022

Qualys, Inc.
919 E Hillsdale Blvd|
4th Floor
Foster City, CA 94404
1 (650) 801 6100

Table of Contents

About this Guide

Welcome to Qualys Cloud Platform! In this guide, we will show you how to integrate the Qualys WAS module with ServiceNow's Application Vulnerability Response app. On successful integration, you will be able to run web application scans on the Qualys WAS app and then sync the findings and vulnerabilities from the scan to the ServiceNow Application Vulnerability Response app.

About Qualys

Qualys, Inc. (NASDAQ: QLYS) is a pioneer and leading provider of cloud-based security and compliance solutions. The Qualys Cloud Platform and its integrated apps help businesses simplify security operations and lower the cost of compliance by delivering critical security intelligence on demand and automating the full spectrum of auditing, compliance and protection for IT systems and web applications.

Founded in 1999, Qualys has established strategic partnerships with leading managed service providers and consulting organizations including Accenture, BT, Cognizant Technology Solutions, Deutsche Telekom, Fujitsu, HCL, HP Enterprise, IBM, Infosys, NTT, Optiv, SecureWorks, Tata Communications, Verizon and Wipro. The company is also founding member of the Cloud Security Alliance (CSA). For more information, please visit www.qualys.com

Qualys Support

Qualys is committed to providing you with the most thorough support. Through online documentation, telephone help, and direct email support, Qualys ensures that your questions will be answered in the fastest time possible. We support you 7 days a week, 24 hours a day. Access support information at www.qualys.com/support/

Welcome to Vulnerability Response Integration with Qualys WAS

Qualys Web Application Scanning (WAS) provides organizations with the ease of use, centralized management and integration capabilities they need to keep the attackers at bay and their web applications secure. Qualys WAS enables organizations to assess, track and remediate web application vulnerabilities.

With Vulnerability Response Integration with Qualys WAS, Qualys leverages the WAS APIs to integrate with ServiceNow. Use this integration to get a single glass pane view of all your web application scans in ServiceNow.

Key Features

- View all WAS-related QIDs from within ServiceNow
- Run web application scans with Qualys WAS and view their results on ServiceNow
- View the list of all web applications scanned by Qualys in ServiceNow

Pre-requisites

You must have a valid Qualys account subscription with **API access** and access to the **Web Application Security (WAS) module.**

To use this integration with ServiceNow, also ensure that you have access to the **Vulnerability Response app** on ServiceNow.

Refer to the ServiceNow Documentation for information on installing and accessing this application in ServiceNow.

Get Started

Here we will help you with the initial configuration and setup needed to get started.

Quick Steps

- Install the Application
- Configure the Application- Provide the API source details and test the connection to ensure the connection between ServiceNow and the defined source is working fine.

Install the Application

Visit the ServiceNow Online Store.

Search for Qualys WAS App, and click Contact Seller. Your Technical Account Manager (TAM) will contact you, and then ServiceNow provisions the app into an instance of your choice. The app then appears in the “Downloads” list of your instance. Click “Install” to start using the app.

In the Search field, type Qualys WAS, and then select Qualys WAS App from the left pane. After you are done, new module appears in your ServiceNow instance.

Configure the Application

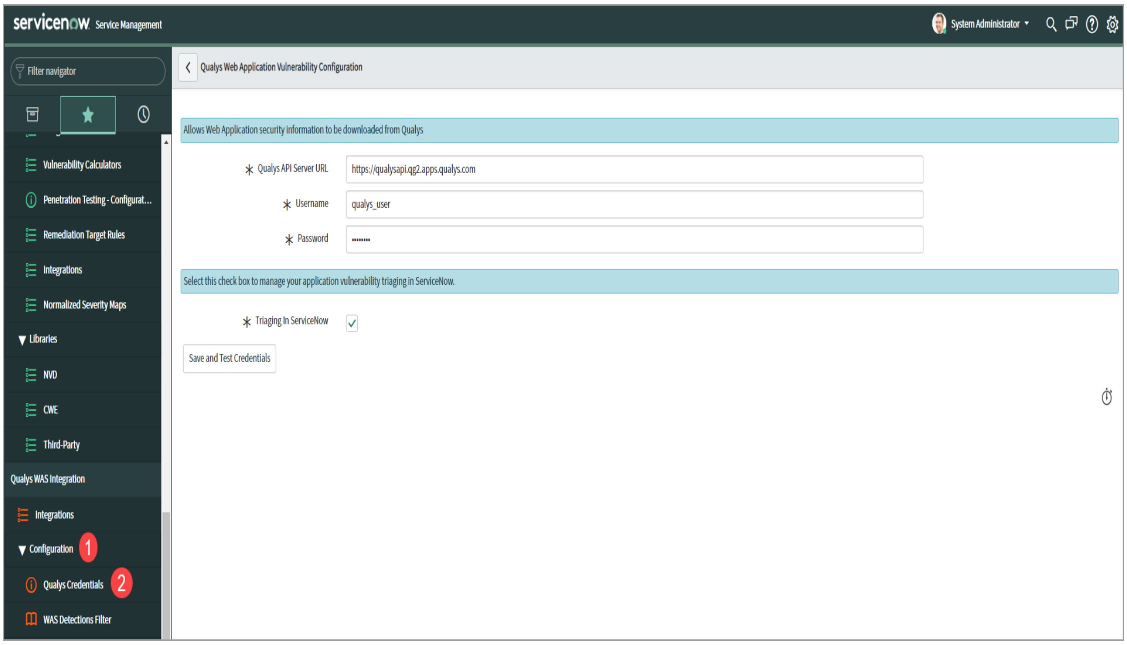
Once you install the Vulnerability Response Integration with Qualys WAS app, you will need to configure it. Go to **Qualys WAS Integration** > **Configuration** to begin configuring the app.

On the Qualys Web Application Vulnerability Configuration page, enter the following details:

Step 1

Qualys API Server URL: Enter the API Server URL as per your subscription. For information on your API Server URL, refer the Identify your Qualys Platform page.

Username and Password: Enter valid Qualys Cloud Platform credentials for an account on the selected POD. Ensure that the credentials you use has API access enabled.



Qualys Web Application Vulnerability Configuration

Allows Web Application security information to be downloaded from Qualys

* Qualys API Server URL: https://qualysapi.qg2.apps.qualys.com

* Username: qualys_user

* Password: ••••••••

Select this check box to manage your application vulnerability triaging in ServiceNow.

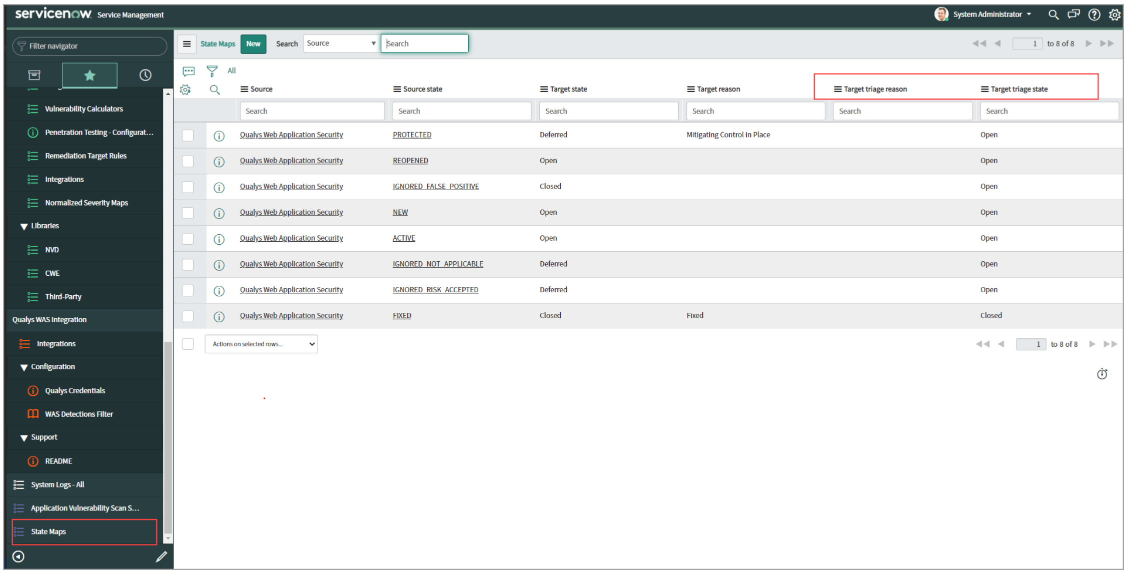
* Triaging In ServiceNow ☑

Save and Test Credentials

Triaging in ServiceNow: This checkbox enables the support for the “Automatic Triage of Vulnerabilities” feature in the Vulnerability Response remediation workflow of the ServiceNow Vulnerability Response application.

Select this check-box to map the vulnerability (detection) state in the Vulnerable Items table, that is, AVIT table (sn_vul_app_vulnerable_item) as per the Triage map maintained in the sn_vul_app_state_map table. The detection state is mapped based on its source state and respective mapping to the Target Triage state. Refer to the screenshot for the default mapping configuration.

The Target Triage state is the configurable; hence you can make changes in the sn_vul_app_state_map table as per your triaging criteria.

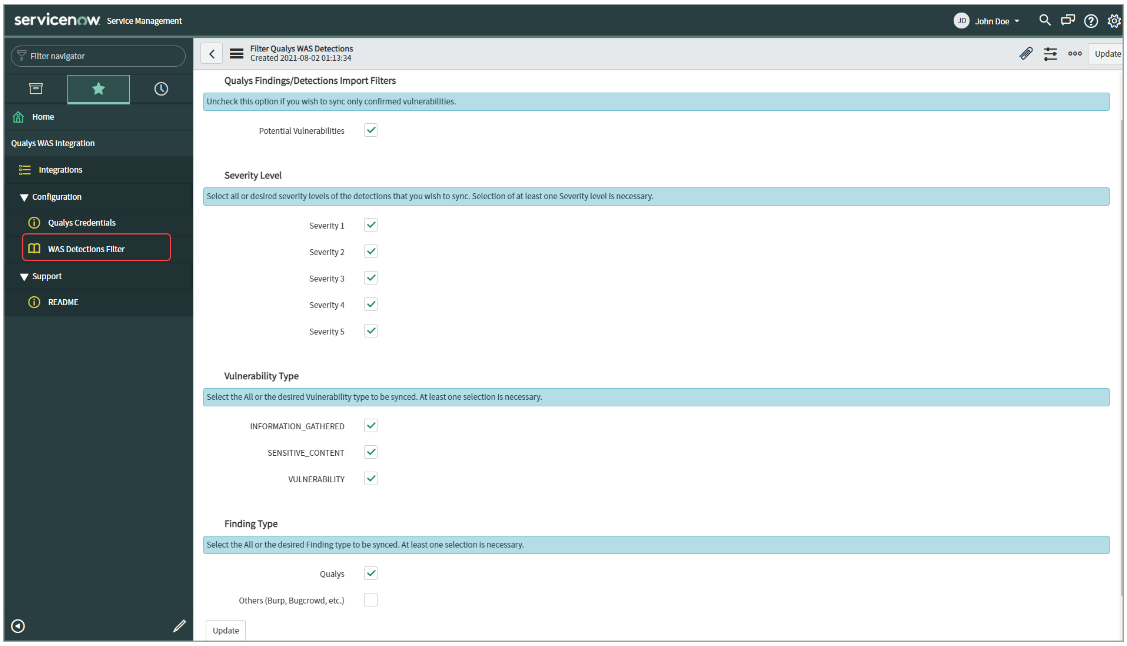


Source	Source state	Target state	Target reason	Target triage reason	Target triage state
Qualys Web Application Security	PROTECTED	Deferred	Mitigating Control in Place		Open
Qualys Web Application Security	REOPENED	Open			Open
Qualys Web Application Security	IGNORED_FALSE_POSITIVE	Closed			Open
Qualys Web Application Security	NEW	Open			Open
Qualys Web Application Security	ACTIVE	Open			Open
Qualys Web Application Security	IGNORED_NOT_APPLICABLE	Deferred			Open
Qualys Web Application Security	IGNORED_RISK_ACCEPTED	Deferred			Open
Qualys Web Application Security	FIXED	Closed	Fixed		Closed

Use the **Save and Test Credentials** button to test the connection between ServiceNow and Qualys WAS. A success message is displayed when the connection is tested successfully.

Step 2

Select the required filters from WAS Detection Filter. These filters are only applicable to Qualys Web Application Vulnerable Item Integration.



Filter Qualys WAS Detections
Created 2021-08-02 01:13:34

Qualys Findings/Detections Import Filters

Uncheck this option if you wish to sync only confirmed vulnerabilities.

Potential Vulnerabilities ☑

Severity Level

Select all or desired severity levels of the detections that you wish to sync. Selection of at least one Severity level is necessary.

Severity 1 ☑
Severity 2 ☑
Severity 3 ☑
Severity 4 ☑
Severity 5 ☑

Vulnerability Type

Select the All or the desired Vulnerability type to be synced. At least one selection is necessary.

INFORMATION_GATHERED ☑
SENSITIVE_CONTENT ☑
VULNERABILITY ☑

Finding Type

Select the All or the desired Finding type to be synced. At least one selection is necessary.

Qualys ☑
Others (Burp, Bugcrowd, etc.) ☐

Select the required filters to sync WAS detections based on **Severity level, Vulnerability** and **Finding type**. Configured filters will be applicable to both Confirmed and Potential detections or, just Confirmed detection, based on selection of the **Potential Vulnerabilities** check-box.

By default, all the check-boxes are selected and hence 'Qualys Web Application Vulnerable Item Integration' run will sync all the detections available in Qualys WAS module.

Qualys WAS Integrations

The Vulnerability Response Integration with Qualys WAS app offers four integrations. Access **Qualys WAS Integration** from the left panel and then click **Integrations** to view these integrations.

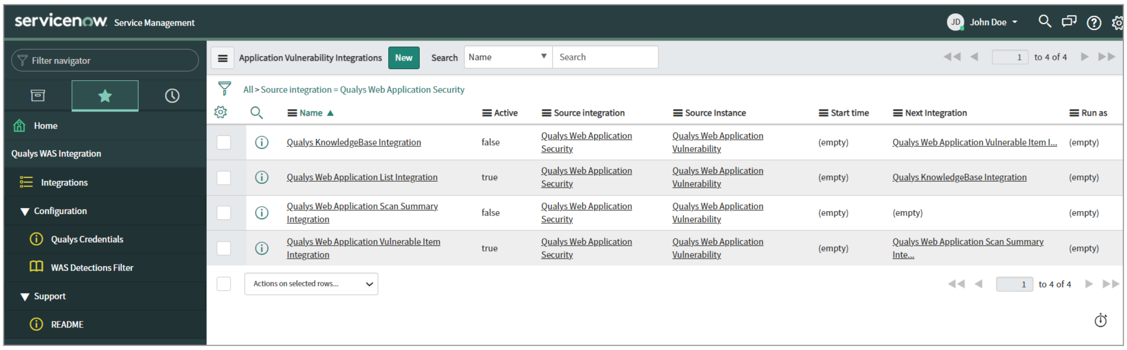
1. **Qualys KnowledgeBase Integration** – Syncs the WAS-related KnowledgeBase entries from the Qualys KnowledgeBase with ServiceNow.

Note: While the Qualys KnowledgeBase has several thousand QIDs, this integration syncs only those QIDs that are related to WAS.

2. **Qualys Web Application Vulnerable Item Integration** – Fetches all the WAS detections related to the configured account from the Qualys platform.

3. **Qualys Web Application List Integration** – Fetches all the Web applications associated with the configured account from the Qualys platform.

4. **Qualys Web Application Scan Summary Integration** – Syncs all the scans-related data associated with the configured account from the Qualys platform.



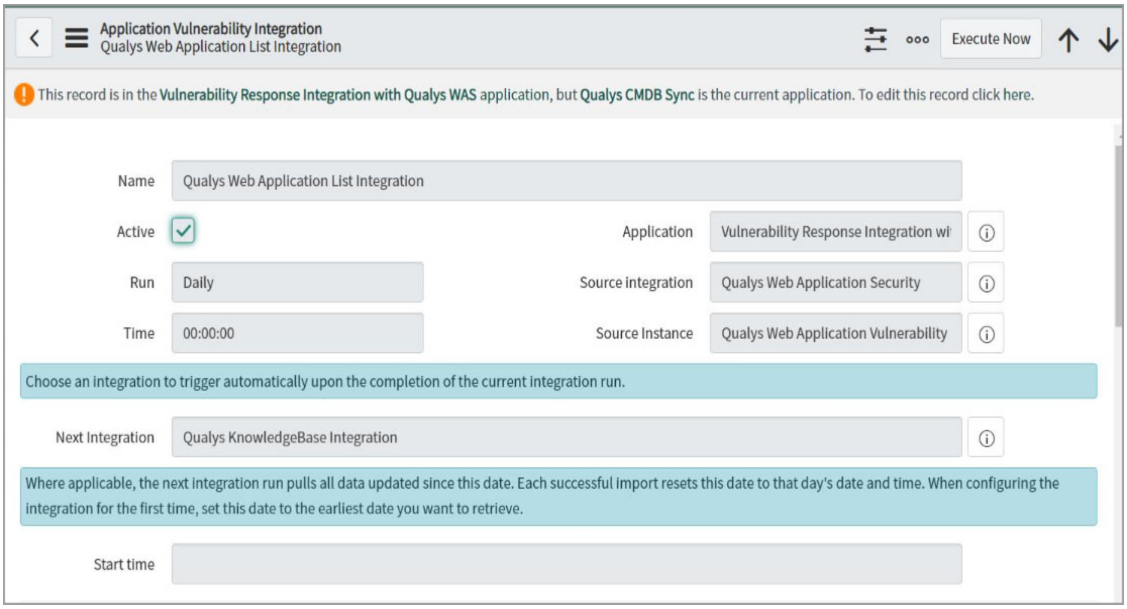
All > Source integration = Qualys Web Application Security

Name ▲	Active	Source integration	Source Instance	Start time	Next Integration	Run as
Qualys KnowledgeBase Integration	false	Qualys Web Application Security	Qualys Web Application Vulnerability	(empty)	Qualys Web Application Vulnerable Item I...	(empty)
Qualys Web Application List Integration	true	Qualys Web Application Security	Qualys Web Application Vulnerability	(empty)	Qualys KnowledgeBase Integration	(empty)
Qualys Web Application Scan Summary Integration	false	Qualys Web Application Security	Qualys Web Application Vulnerability	(empty)	(empty)	(empty)
Qualys Web Application Vulnerable Item Integration	true	Qualys Web Application Security	Qualys Web Application Vulnerability	(empty)	Qualys Web Application Scan Summary Inte...	(empty)

Use these integrations to sync data from the Qualys platform to ServiceNow. Refer to the sections below for details on using these integrations.

Using the Qualys WAS Integrations

Access the Qualys Integrations page by navigating to the **Qualys WAS Integration** in the left panel and then clicking **Integrations**. To configure/run an integration, select the integration from the right pane.



Application Vulnerability Integration
Qualys Web Application List Integration

This record is in the Vulnerability Response Integration with Qualys WAS application, but Qualys CMDB Sync is the current application. To edit this record click here.

Name: Qualys Web Application List Integration
Active: ☑
Application: Vulnerability Response Integration wi
Run: Daily
Source integration: Qualys Web Application Security
Time: 00:00:00
Source Instance: Qualys Web Application Vulnerability

Choose an integration to trigger automatically upon the completion of the current integration run.

Next Integration: Qualys KnowledgeBase Integration

Where applicable, the next integration run pulls all data updated since this date. Each successful import resets this date to that day's date and time. When configuring the integration for the first time, set this date to the earliest date you want to retrieve.

Start time:

Note: The default Run for List Integration is set as **Daily** and default Time as 00:00:00. For the other three integrations the Run is set as **On Demand**.

You can choose to run the integration using one of the following options:

- **Daily**: Runs the integration daily at the configured time
- **Weekly**: Runs the integration weekly at the configured time of the configured day
- **Monthly**: Runs the integration monthly at the configured time of the configured month day
- **Periodically**: Runs the integration at the configured interval
- **Once**: Runs the integration only once at the configured date and time
- **On-Demand**: Runs the integration only when the "Execute Now" button is hit
- **Business Calendar: Entry Start:** Refer to the ServiceNow documentation for information on Business calendar.
- **Business Calendar: Entry End**: Refer to the ServiceNow documentation for information on Business calendar.

Sequence	Integration Name	Active	Default Run type	Default Time (if applicable)	Next Integration
1	Qualys Web Application List Integration	true	Daily	00:00:00	Qualys Knowledge Base Integration
2	Qualys Knowledge Base Integration	false	On-Demand	NA	Qualys Web Application Vulnerable Item Integration
3	Qualys Web Application Vulnerable Item Integration	false	On-Demand	NA	Qualys Web Application Scan Summary Integration
4	Qualys Web Application Scan Summary Integration	false	On-Demand	NA	NA

Note: As recommended by ServiceNow only 'Qualys Web Application List Integration' is kept active and other integrations are inactive, to let the customer add remediation rules, assignment rules etc for AVR. Customers can enable the inactive integrations once they have added desired rules.

The **Start Time** field defines the time after which the data needs to be synced from the Qualys platform. The blank field during the first run indicates that the integration would sync all data from the platform during the first run. All subsequent runs of the integration will only sync data post this start time.

Note: It is recommended to keep the **Start Time** field empty for the very first integration run of Qualys Web Application Vulnerable Item Integration, so that the application can sync all the vulnerabilities appropriately.

Note: Qualys recommends not making changes to the Integration Details section.

Click the **Execute Now** button when you are ready to run the integration or click **Update** to run the integration as per the defined schedule.

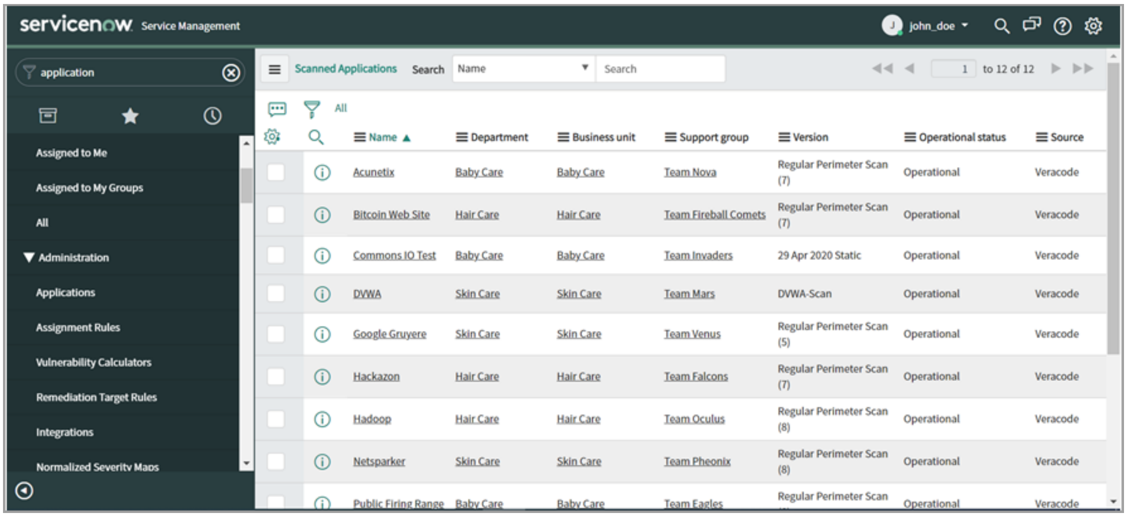
The Vulnerability Integration Runs tab at the bottom summarizes each integration run. This section displays the status of the integration runs and also informs the number of records synced between the Qualys Platform and ServiceNow.

Viewing Qualys WAS Data in ServiceNow

The ServiceNow Application Vulnerability Response (AVR) app helps you view all your application vulnerability on a single page. With the Vulnerability Response Integration for Qualys WAS app, you can view all your Qualys WAS data from the Qualys platform on the ServiceNow Application Vulnerability Response page.

Viewing Web Application List Data in ServiceNow

To view a list of Web Applications in ServiceNow, navigate to **Application Vulnerability Response** > **Administration** > **Applications**.



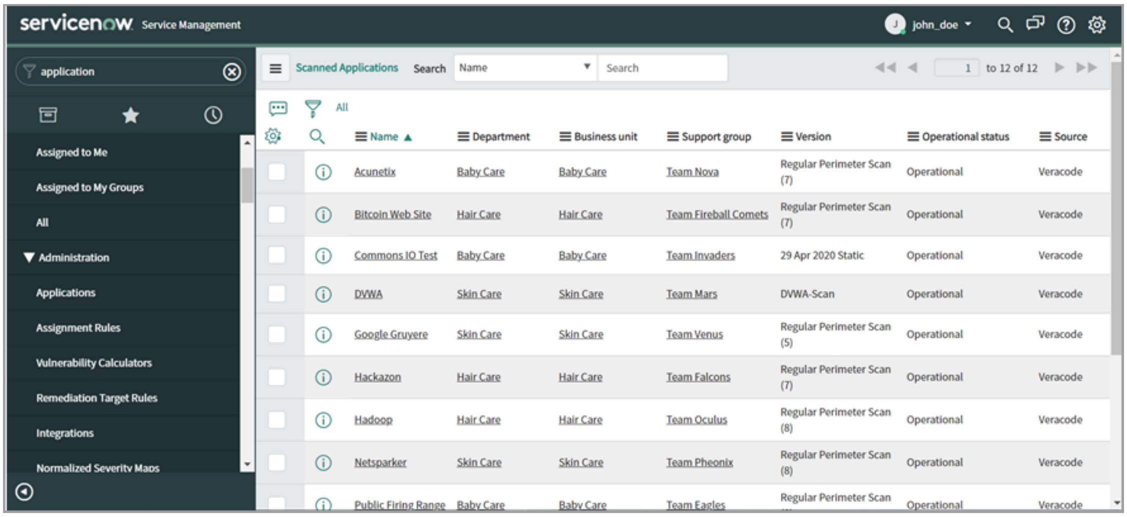
Name ▲	Department	Business unit	Support group	Version	Operational status	Source
Acunetix	Baby Care	Baby Care	Team Nova	Regular Perimeter Scan (7)	Operational	Veracode
Bitcoin Web Site	Hair Care	Hair Care	Team Fireball Comets	Regular Perimeter Scan (7)	Operational	Veracode
Commons IO Test	Baby Care	Baby Care	Team Invaders	29 Apr 2020 Static	Operational	Veracode
DVWA	Skin Care	Skin Care	Team Mars	DVWA-Scan	Operational	Veracode
Google Gruyere	Skin Care	Skin Care	Team Venus	Regular Perimeter Scan (5)	Operational	Veracode
Hackazon	Hair Care	Hair Care	Team Falcons	Regular Perimeter Scan (7)	Operational	Veracode
Hadoop	Hair Care	Hair Care	Team Oculus	Regular Perimeter Scan (8)	Operational	Veracode
Netsparker	Skin Care	Skin Care	Team Pheonix	Regular Perimeter Scan (8)	Operational	Veracode
Public Firing Range	Baby Care	Baby Care	Team Eagles	Regular Perimeter Scan	Operational	Veracode

Filter by “Qualys” on the Source column to view applications scanned by Qualys.

Refer to the Field Mappings Table section for information on how Qualys WAS fields are mapped to fields in ServiceNow.

Viewing Web Application Vulnerable Item in ServiceNow

To view a list of web application detections in ServiceNow, navigate to **Application Vulnerability Response** > **Vulnerable** Items. Here you can use any of the pages that show the vulnerabilities based on assignee filters.

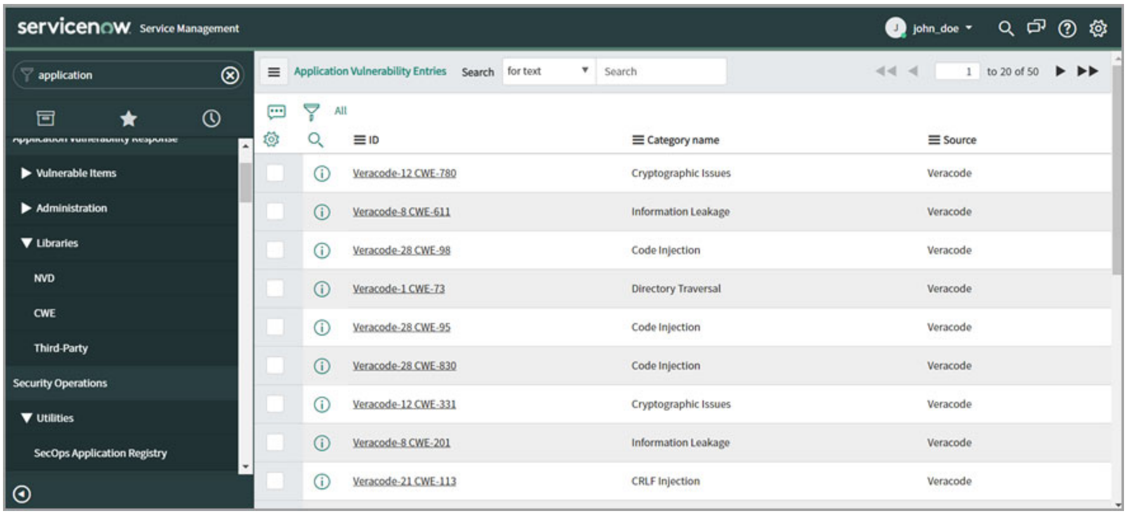


Name ▲	Department	Business unit	Support group	Version	Operational status	Source
Acunetix	Baby Care	Baby Care	Team Nova	Regular Perimeter Scan (7)	Operational	Veracode
Bitcoin Web Site	Hair Care	Hair Care	Team Fireball Comets	Regular Perimeter Scan (7)	Operational	Veracode
Commons IO Test	Baby Care	Baby Care	Team Invaders	29 Apr 2020 Static	Operational	Veracode
DVWA	Skin Care	Skin Care	Team Mars	DVWA-Scan	Operational	Veracode
Google Gruyere	Skin Care	Skin Care	Team Venus	Regular Perimeter Scan (5)	Operational	Veracode
Hackazon	Hair Care	Hair Care	Team Falcons	Regular Perimeter Scan (7)	Operational	Veracode
Hadoop	Hair Care	Hair Care	Team Oculus	Regular Perimeter Scan (8)	Operational	Veracode
Netsparker	Skin Care	Skin Care	Team Pheonix	Regular Perimeter Scan (8)	Operational	Veracode
Public Firing Range	Baby Care	Baby Care	Team Eagles	Regular Perimeter Scan	Operational	Veracode

Filter by “Qualys” on the Source column to view detections identified by Qualys. Refer to the Field Mappings Table section for information on how Qualys WAS fields are mapped to fields in ServiceNow.

Viewing Qualys KnowledgeBase Data in ServiceNow

To view Qualys KnowledgeBase data in ServiceNow, navigate to **Application Vulnerability Response** > **Libraries** > **Third-Party**.



ID	Category name	Source
Veracode-12 CWE-780	Cryptographic Issues	Veracode
Veracode-8 CWE-611	Information Leakage	Veracode
Veracode-28 CWE-98	Code Injection	Veracode
Veracode-1 CWE-73	Directory Traversal	Veracode
Veracode-28 CWE-95	Code Injection	Veracode
Veracode-28 CWE-830	Code Injection	Veracode
Veracode-12 CWE-331	Cryptographic Issues	Veracode
Veracode-8 CWE-201	Information Leakage	Veracode
Veracode-21 CWE-113	CRLF Injection	Veracode

Filter by “Qualys” on the Source column to view the Qualys KnowledgeBase records.

Refer to the Field Mappings Table section for information on how Qualys WAS fields are mapped to fields in ServiceNow.

Viewing Web Application Scan Summary data in ServiceNow

ServiceNow Application Vulnerability Response app currently does not offer a screen to view Qualys web application scan summary data. The Qualys web application scan summary data is currently stored in the *sn_vul_app_vul_scan_summary* table of ServiceNow.

Refer to the Field Mappings Table section for information on how Qualys WAS fields are mapped to fields in ServiceNow.

Field Mappings Table

The Vulnerability Response Integration with Qualys WAS app maps fields from the Qualys WAS APIs to the fields on the ServiceNow AVR app. This section details how the fields from the WAS API are mapped to corresponding fields on the ServiceNow AVR UI.

Qualys KnowledgeBase Integration

The Qualys KnowledgeBase Integration syncs data from the Qualys platform to the sn_vul_app_vul_entry table of ServiceNow. The following table shows the mapping between Qualys and the ServiceNow UI:

Field in Qualys WAS API Response XML	Corresponding Field on ServiceNow UI	Expected Values
<QID>	ID	vuln qid
<SEVERITY_LEVEL>	Source Severity	vuln severity level
<VECTOR_STRING>CVSS:2.0/AV:N/**AC:L**/Au:N/C:P/I:N/A:N/E:U/RL:W/RC:C</VECTOR_STRING>	Access complexity (v2)	AC: High (H), Medium (M), Low (L)
<VECTOR_STRING>CVSS:2.0/**AV:N**/AC:L/Au:N/C:P/I:N/A:N/E:U/RL:W/RC:C</VECTOR_STRING>	Access vector (v2)	AV: Local (L), Adjacent Network (A), Network (N)
<VECTOR_STRING>CVSS:2.0/AV:N/AC:L/**Au:N**/C:P/I:N/A:N/E:U/RL:W/RC:C</VECTOR_STRING>	Authentication (v2)	Au: M (multiple), Single (S), None (N)
<VECTOR_STRING>CVSS:2.0/AV:N/AC:L/Au:N/**C:P**/I:N/A:N/E:U/RL:W/RC:C</VECTOR_STRING>	Confidentiality impact (v2)	C: None (N), Partial (P), Complete - C
<VECTOR_STRING>CVSS:2.0/AV:N/AC:L/Au:N/C:P/**I:N**/A:N/E:U/RL:W/RC:C</VECTOR_STRING>	Integrity impact (v2)	C: None (N), Partial (P), Complete - C
<VECTOR_STRING>CVSS:2.0/AV:N/AC:L/Au:N/C:P/I:N/**A:N**/E:U/RL:W/RC:C</VECTOR_STRING>	Availability impact (v2)	A: None (N), Partial (P), Complete - C
<VECTOR_STRING>CVSS:2.0/AV:N/AC:L/Au:N/C:P/I:N/A:N/E:U/**RL:W**/RC:C</VECTOR_STRING>	Remediation level (v2)	RL: Official Fix (OF), Temporary Fix (TF), Workaround (W), Unavailable (U)
<VECTOR_STRING>CVSS:2.0/AV:N/AC:L/Au:N/C:P/I:N/A:N/E:U/RL:W/**RC:C**</VECTOR_STRING>	Report confidence (v2)	RC: Confirmed - C, Uncorroborated (UR), Unconfirmed (UC)
<CVSS> .. <EXPLOITABILITY>1</EXPLOITABILITY> .. </CVSS>	Exploitability subscore (v2)	

Field in Qualys WAS API Response XML	**Corresponding Field on ServiceNow UI**	**Expected Values**
<PUBLISHED_DATETIME>	Date published	Date on which the vuln published
<SOLUTION>	Mitigation description	Description of the steps to address the vuln
<TITLE>	Name	
<DIAGNOSIS>	Short description	
<SOLUTION>	Remediation notes	
<DIAGNOSIS>	Threat	
<CVSS> .. <TEMPORAL> .. </CVSS>	Temporal score (v2)	CVSS v2 temporal score
<CVSS_V3> .. <TEMPORAL>4.7</TEMPORAL> .. </CVSS>	Temporal score (v3)	CVSS v3 temporal score
<CVSS_V3> .. <BASE>5.3</BASE> .. </CVSS>	Vulnerability score (v3)	
<CVSS> .. <VECTOR_STRING> </VECTOR_STRING> .. </CVSS>	Vector string (v2)	CVSS v2 vesctor string
<CVSS_V3> .. <VECTOR_STRING></VECTOR_STRING> .. </CVSS>	Vector string (v3)	CVSS v3 vesctor string
<VECTOR_STRING>CVSS:3.0/AV:N/**AC:L**/PR:N/UI:N/S:U/C:L/I:N/A:N/E:U/RL:W/RC:C</VECTOR_STRING>	Attack complexity (v3)	AC: High (H), Low (L)
<VECTOR_STRING>CVSS:3.0/**AV:N**/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N/E:U/RL:W/RC:C</VECTOR_STRING>	Attack vector (v3)	AV: Network (N), Adjacent (A), Local (L), Physical (P)
<VECTOR_STRING>CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/**A:N**/E:U/RL:W/RC:C</VECTOR_STRING>	Availability impact (v3)	A: None (N), High (H), Low (L)

Field in Qualys WAS API Response XML	Corresponding Field on ServiceNow UI	Expected Values
<VECTOR_STRING>CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/**C:L**/I:N/A:N/E:U/RL:W/RC:C</VECTOR_STRING>	Confidentiality impact (v3)	C: None (N), High (H), Low (L)
<VECTOR_STRING>CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N/**E:U**/RL:W/RC:C</VECTOR_STRING>	Exploit code maturity (v3)	E: Not Defined (X), Unproven (U), Proof-of-Concept (P), Functional (F), High (H)
<VECTOR_STRING>CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/**I:N**/A:N/E:U/RL:W/RC:C</VECTOR_STRING>	Integrity impact (v3)	I: None (N), High (H), Low (L)
<VECTOR_STRING>CVSS:3.0/AV:N/AC:L/**PR:N**/UI:N/S:U/C:L/I:N/A:N/E:U/RL:W/RC:C</VECTOR_STRING>	Privileges required (v3)	PR: None (N), High (H), Low(L)
<VECTOR_STRING>CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N/E:U/**RL:W**/RC:C</VECTOR_STRING>	Remediation level (v3)	RL: Not Defined (X), Official Fix (O), Temporary Fix (T), Workaround (W), Unavailable (U)
<VECTOR_STRING>CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N/E:U/RL:W/**RC:C**</VECTOR_STRING>	Report confidence (v3)	RC: Not Defined (X), Unknown (U), Reasonable (R), Confirmed (C)
<VECTOR_STRING>CVSS:3.0/AV:N/AC:L/PR:N/UI:N/**S:U**/C:L/I:N/A:N/E:U/RL:W/RC:C</VECTOR_STRING>	Scope change (v3)	S: Unchanged (U), Changed (C)
<VECTOR_STRING>CVSS:3.0/AV:N/AC:L/PR:N/**UI:N**/S:U/C:L/I:N/A:N/E:U/RL:W/RC:C</VECTOR_STRING>	User interaction (v3)	UI: None(N), Required (R)

Qualys Web Application Vulnerable Item Integration

The Qualys Web Application Vulnerable Item Integration syncs data from the Qualys platform to the sn_vul_app_vulnerable_item table of ServiceNow. The following table shows the mapping between Qualys and the ServiceNow UI:

Field in Qualys WAS API Response XML	Corresponding Field on ServiceNow UI	Expected Values
<webApp> .. <id>web_app_id</id> .. </webApp>	Source Application ID	Web app ID
<uniqueId>	Source AVIT ID	unique Id from API response
<qid>	Vulnerability	
source_scan_id	Source Scan ID	

Field in Qualys WAS API Response XML	Corresponding Field on ServiceNow UI	Expected Values
<severity>	Source Severity	Severity of the vuln detection (1 to 5)
<webApp> .. <name>web_app_name</name> .. </webApp>	Application Release	Web app name
<firstDetectedDate>	First Found	
<lastDetectedDate>	Last Found	
Deferral date	ignore_date	
Deferral notes	ignore_reason	
<lastTestedDate>	Last Scan Date	Note: Qualys WAS stores this time in the UTC format. The integration converts this UTC time into the time zone configured for this ServiceNow instance.
	Last Opened	Note: This field is populated based on when the record was synced from the Qualys platform to ServiceNow. This field is populated by ServiceNow and does not correspond to a field in Qualys.
	Scan summary name	Scan summary name from sn_vul_app_vul_scan_summary table
Name	Short Description	Combination of QID and Web App name
	Source	Qualys (Hardcoded)
<PayloadInstance> <payload> + <request> </PayloadInstance>	Source Request	
<response>	Source Response	
	Source link	Link to finding on Qualys UI. This field is generated by ServiceNow AVR.
<PayloadInstance> <request> <link> </link> </PayloadInstance>	Location	

Field in Qualys WAS API Response XML	Corresponding Field on ServiceNow UI	Expected Values
<Finding> <name> qid_title </name> </Finding>	Summary	QID title
from KB to AVIT table	Vulnerability Summary	QID title (from KB)
from KB to AVIT table	Vulnerability explanation	DIAGNOSIS from QID (KB)
from KB to AVIT table	Recommendation	SOLUTION from QID (KB)
<status>	Source Remediation Status	Status of the respective detections

Note: STATE and REASON fields are mapped based on 'Source Remediation Status' field and sn_vul_app_state_map table.

Qualys Web Application List Integration

The Qualys Web Application List Integration syncs data from the Qualys platform to the sn_vul_app_scanned_application table of ServiceNow. The following table shows the mapping between Qualys and the ServiceNow UI:

Field in Qualys WAS API Response XML	Corresponding Field on ServiceNow UI	Expected Values
<WebApp> .. <name>web_app_name</name> .. </WebApp>	Name	Web app name
<WebApp> .. <id>web_app_id</id> .. </WebApp>	Source Application ID	Web app ID
	Source	Qualys (Hardcoded)
<url>	Description	Web app URL

Qualys Web Application Scan Summary Integration

The Qualys Web Application Scan Summary Integration syncs data from the Qualys platform to the sn_vul_app_vul_scan_summary table of ServiceNow. The following table shows the mapping between Qualys and the ServiceNow table:

Field in Qualys WAS API Response XML	Corresponding Field on ServiceNow UI	Expected Values
<WasScan>.. <id></id>.. </WasScan>	Source Scan ID	WAS Scan ID
<WasScan>.. <id></id> <name> </name>.. </WasScan>	Scan Summary Name	WAS Scan Name
<webApp>.. <name></name>.. </webApp>	Application Release	Web app name
launchedDate	Last Scan date	Note: Qualys WAS stores this time in the UTC format. The integration converts this UTC time into the time zone configured for this ServiceNow instance.
launchedDate	Last Dynamic Scan Date	Note: Qualys WAS stores this time in the UTC format. The integration converts this UTC time into the time zone configured for this ServiceNow instance.

Known Issues/Limitations

- Qualys WAS module does not support 'Sensitive Content' and 'Potential' as a vulnerability type for non-qualys (eg. Burp, Bugcrowd) detections.
- Qualys WAS API returns 0 detections for 'Information_Gathered' vulnerability type for non-qualys (eg. Burp, Bugcrowd) detections.
- ServiceNow Vulnerability Response Integration with Qualys WAS app might face issues with connectivity to Qualys platform if the ServiceNow instance is missing Key Management Framework plugin on Quebec version. Make sure your ServiceNow instance has the latest patch installed on it.
- If you try to pull the already existing detections having a Deferred state or a False Positive state when the Triaging is enabled, the whole batch of the API responses will fail to update in the table (sn_vul_app_vulnerable_item), resulting in the loss of data. This is a known issue for ServiceNow Vulnerability Response Application. Ref. ticket PRB - PRB1564344 [support.servicenow.com].
- As per the design of the ServiceNow Vulnerability Response application, Web application name records in the table (sn_vul_app_scanned_application) will not be updated even if the fields (such as application name and URL) are updated from the Qualys UI.