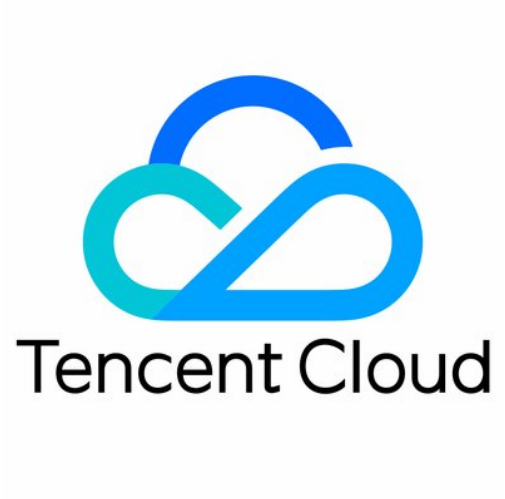
Vulnerability Scan Service

Operation Guide

Product Documentation



Contents

Operation Guide
Adding IP to Allowlist

Last updated：2024-12-30 16:47:49

This document describes how to add the monitoring IPs of VSS to the allowlist.

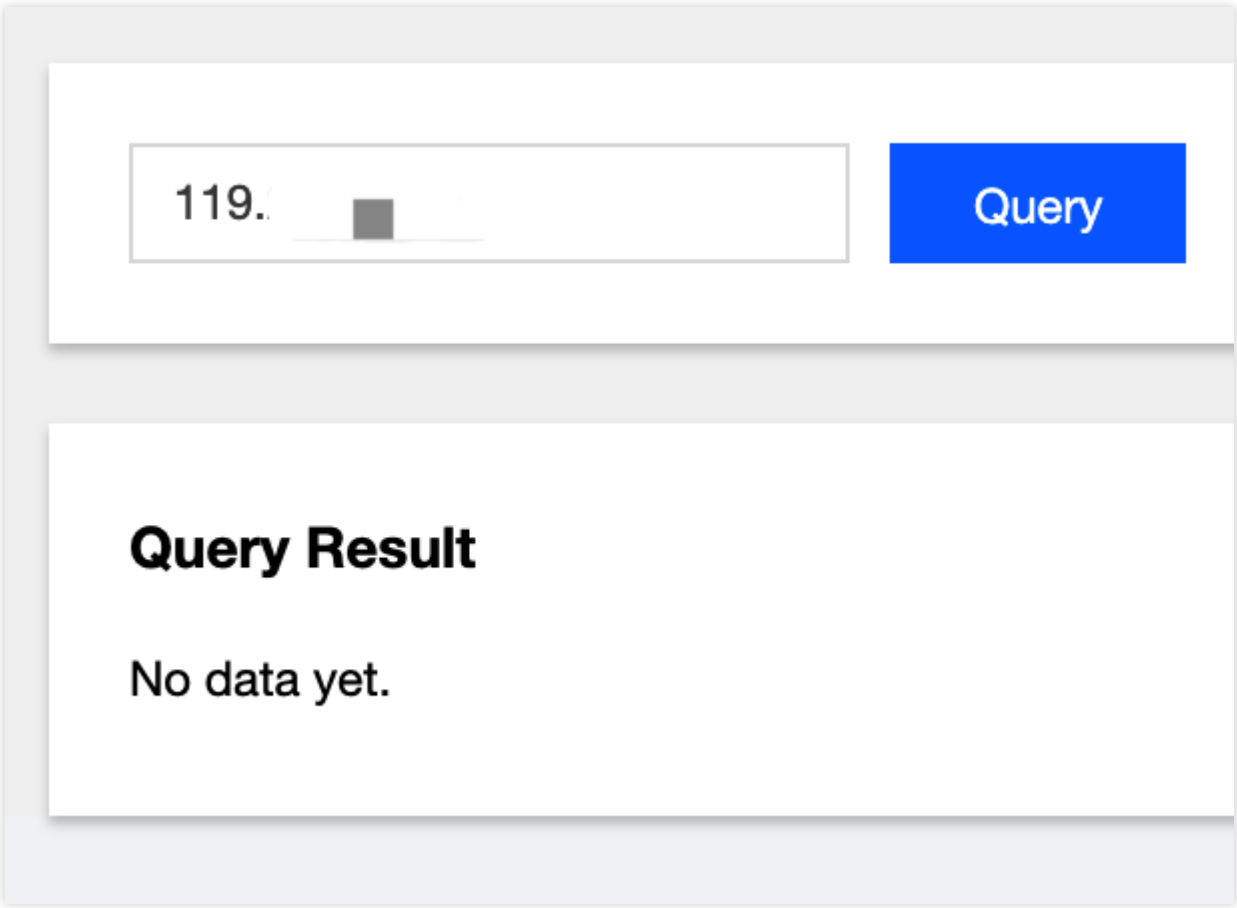
Overview

VSS simulates hacker intrusion attacks to conduct asset discovery and risk monitoring over the public network. If your server has security protection or monitoring services such as WAF and SOC deployed, we recommend you add the monitoring IPs of VSS to the allowlist and grant them scanning access, so that the monitoring service can work smoothly. Such service node scanning IPs include:
119.28.101.45
119.28.101.51
150.109.12.53
101.32.239.31
101.32.242.117
If your website can be accessed only after login, you need to suspend the security policy (to ensure that the website can be accessed from all IPs) and resume it after your cookie validity is verified.

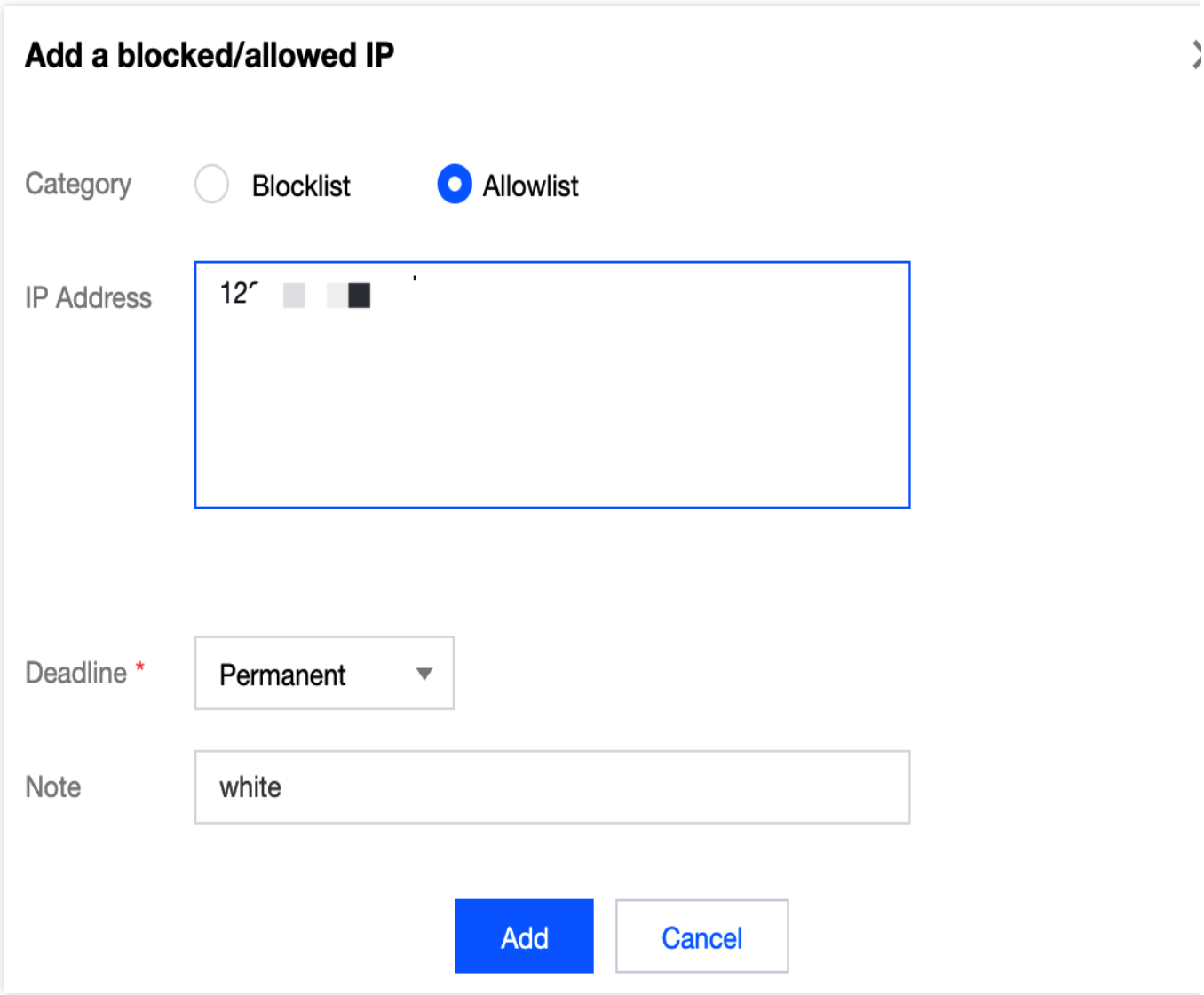
Directions

Method 1: allow IPs through IP query

1. Log in to the WAF console and select **IP Management** > **IP Query** on the left sidebar to enter the IP query page.
2. On the IP query page, enter the IP address to be queried, click **Query**, and the query result will be displayed.



3. Click **Add to Blocklist/Allowlist** to enter the **Add Blocked/Allowed IP** page, where you can manually add IPs to the allowlist. Select **Allowlist** as the category, enter the IP address to be allowed, select the expiration time of the allowlist, and click **Add**.



Method 2: add IPs directly to the allowlist

Log in to the WAF console and select **IP Management** > **IP Blocklist/Allowlist** on the left sidebar to enter the IP blocklist/allowlist page.

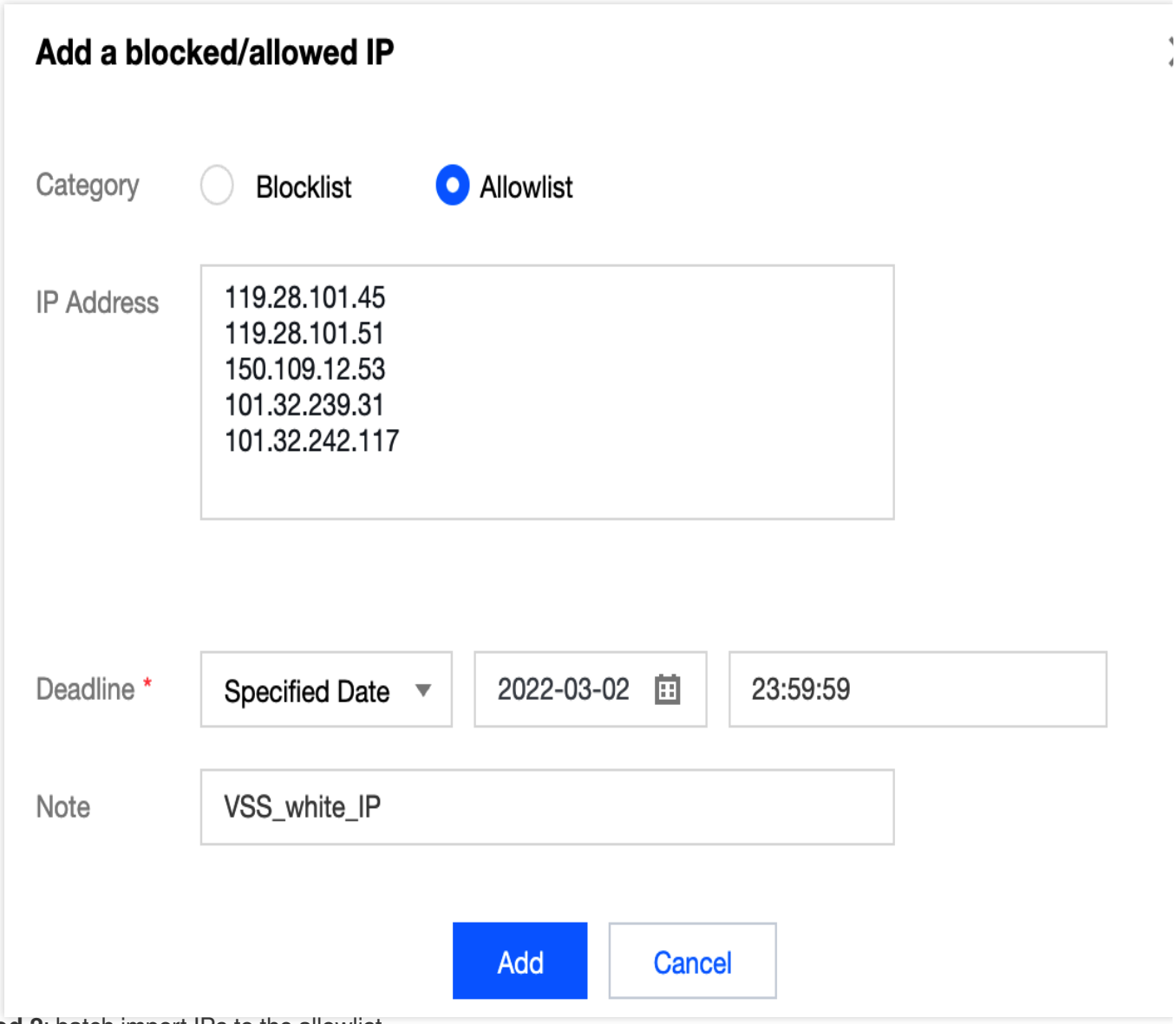
Method 1: manually add IPs to the allowlist.

1.1 On the IP blocklist/allowlist page, click **Add to Blocklist/Allowlist**, and the **Add Blocked/Allowed IP** window will pop up.

1.2 In the **Add Blocked/Allowed IP** window, select **Allowlist** as the category, copy the scanning node IPs of VSS into the IP address input box, select the expiration time of the allowlist, and click **Add**.

Note:

Up to 100 IP addresses can be entered and separated by line break.



Method 2: batch import IPs to the allowlist.

1.1 On the IP blocklist/allowlist page, click **Import Data**, and the **Import IP List** window will pop up.

1.2 In the **Import IP List** window, click **Import**, select the allowlist file to be imported, and click **Confirm Import** after successful upload.

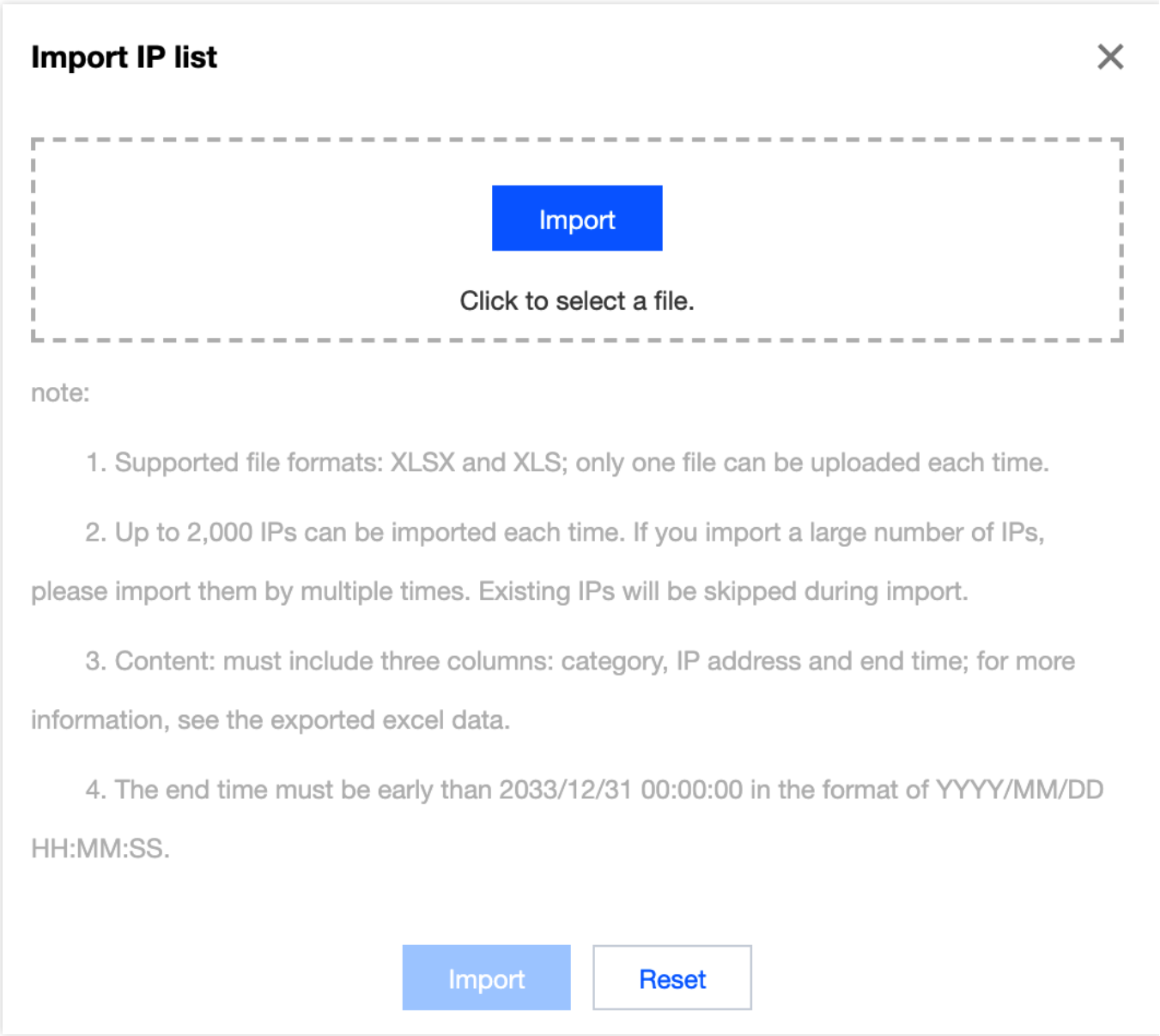
Note:

Import file format: only .xlsx and .xls files are supported.

Quantity: currently, only one single file can be uploaded.

Content: the file must include three columns: category, IP address, and end time. For more information on the format, see the exported Excel file.

The end time must be before 2033/12/30 23:59:59 in the format of `YYYY/MM/DD HH:MM:SS` .



Method 3: add blocked IPs to the allowlist.

1. Log in to the WAF console and select **IP Management** > **IP Blocking Status** on the left sidebar to enter the IP blocking status page.
2. On the IP blocking status page, enter the relevant information, click **Query** to query the relevant IPs of VSS, and then add them to the allowlist.

Adding Asset

Last updated：2024-12-30 16:48:28

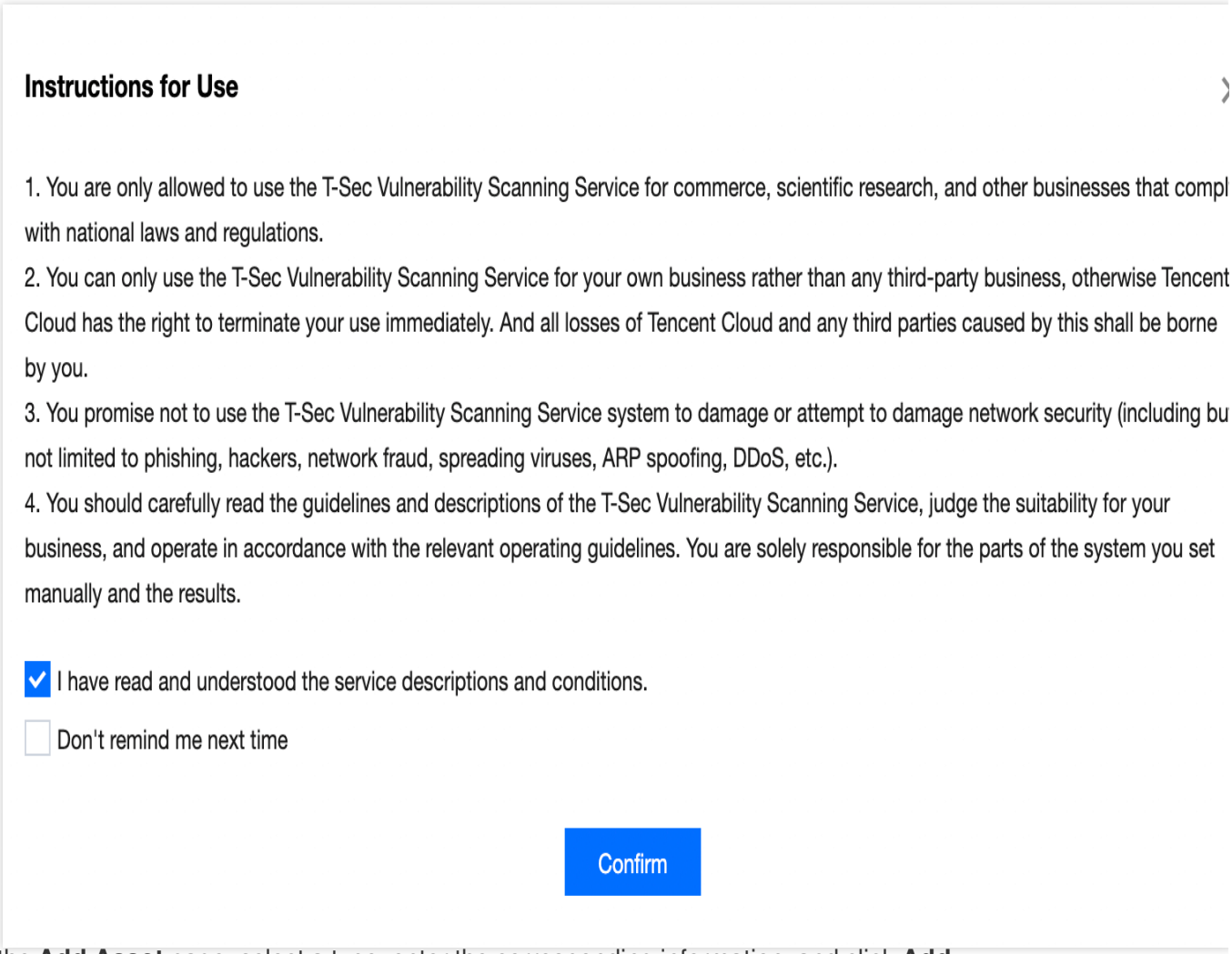
This document describes how to add an asset in the VSS console.

Overview

You can add assets on the asset management page to scan them for vulnerabilities. Currently, all websites accessed through domain name, IP, or WeChat Official Account, servers, and APIs can be added as assets.

Directions

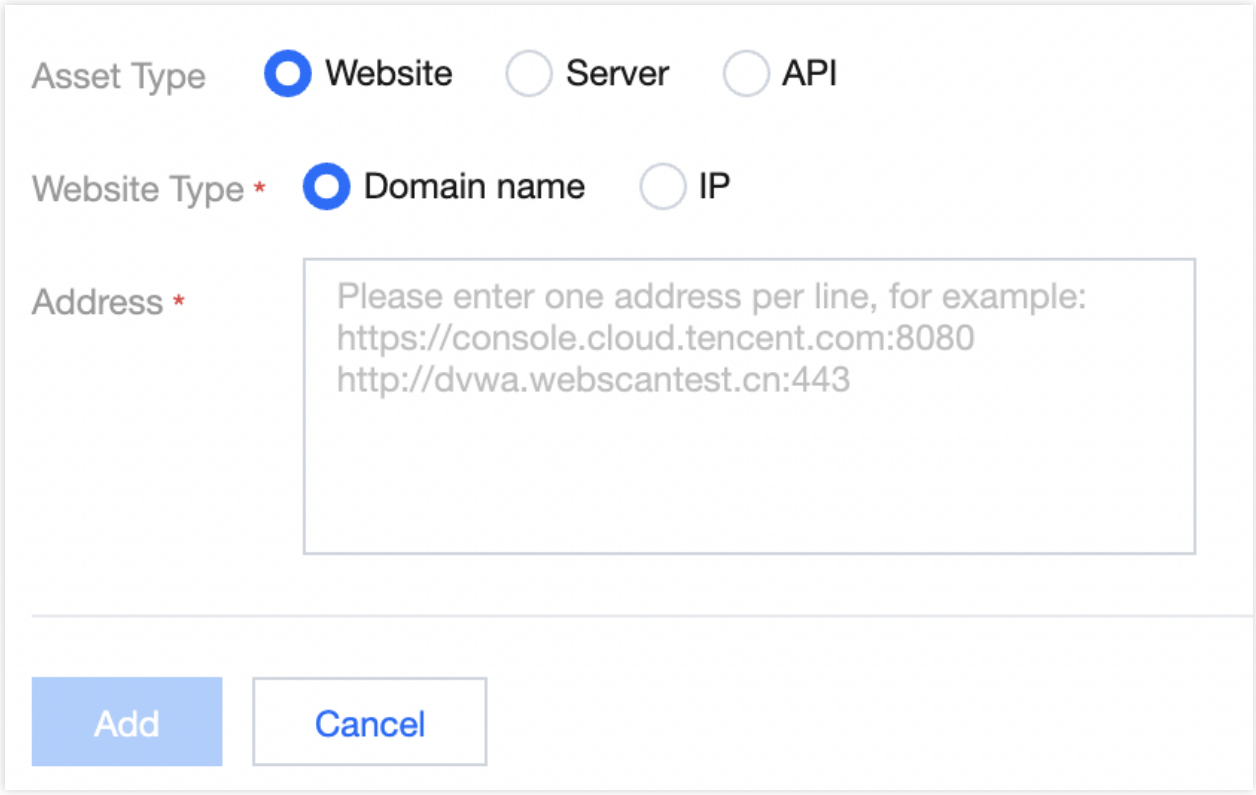
1. Log in to the VSS console and click **Asset Management** on the left sidebar to enter the asset management page.
2. On the asset management page, click **Add Asset**, and the **Use Instructions** window will pop up.
3. In the **Use Instructions** pop-up window, read the use instructions, select **I have read and understood the product's service descriptions, conditions, and restrictions**, and click **OK** to enter the **Add Asset** page.



4. On the **Add Asset** page, select a type, enter the corresponding information, and click **Add**.

Note:

You can enter multiple website addresses and separate them with line break.



Simulating Login

Last updated：2024-12-30 16:52:05

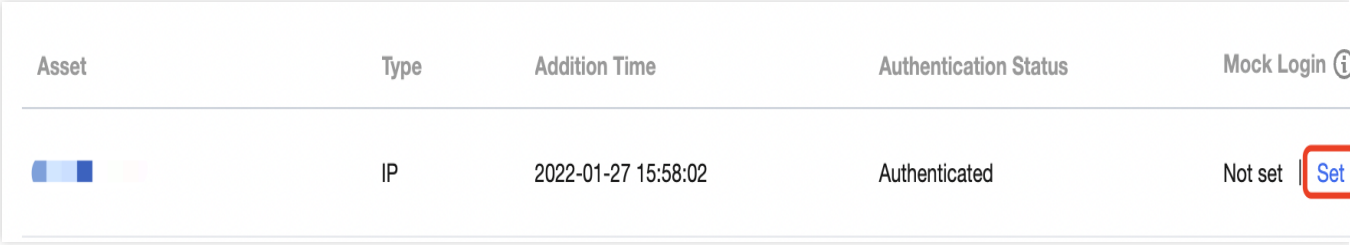
Overview

If some or all pages or features of your website can be accessed only after login, we recommend you set a cookie to simulate website login for comprehensive vulnerability scan. Currently, VSS can simulate login by setting a cookie with the value of successful login, and the backend will periodically bring the set cookie to access the website, so as to ensure that the cookie won't expire.

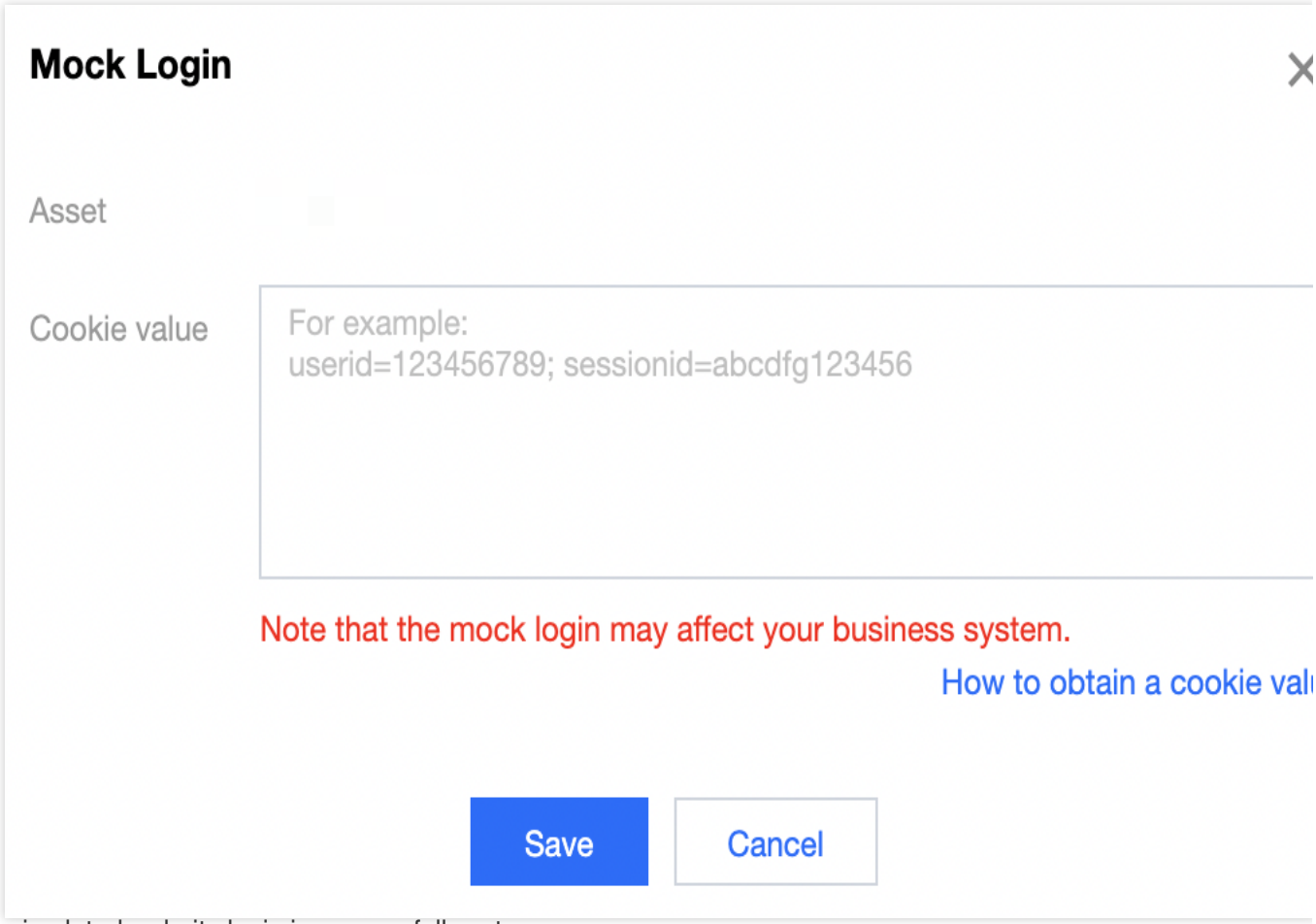
Directions

Settings of simulated website login

1. Log in to the VSS console and click **Asset Management** on the left sidebar to enter the asset management page.
2. On the asset management page, click **Website** and find the asset for which to simulate a login.
3. Click **Set** in the **Simulated Login** column of the target asset, and the **Simulated Login** window will pop up.



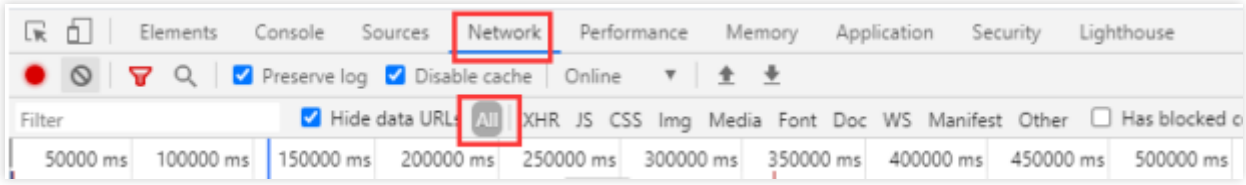
4. In the **Simulated Login** window, enter the correct cookie value (see How to get cookie value) and click **Save**.



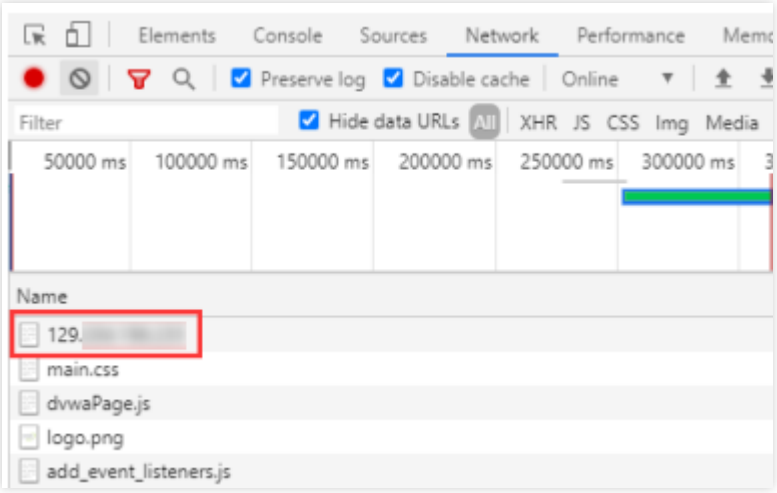
5. The simulated website login is successfully set.

How to get cookie value

1. Log in to your website in Chrome, access a page that requires login, and press F12 or right-click on the page and select **Inspect**.
2. Select **Network** > **All** in DevTools that appears and refresh the page.



3. Click the first network request.



4. Find the **Cookie** item in **Headers** and copy the cookie value.