

# **Vulnerability Scan Service**

## **Operation Guide**

### **Product Documentation**



## Copyright Notice

©2013-2024 Tencent Cloud. All rights reserved.

Copyright in this document is exclusively owned by Tencent Cloud. You must not reproduce, modify, copy or distribute in any way, in whole or in part, the contents of this document without Tencent Cloud's the prior written consent.

## Trademark Notice



All trademarks associated with Tencent Cloud and its services are owned by Tencent Cloud Computing (Beijing) Company Limited and its affiliated companies. Trademarks of third parties referred to in this document are owned by their respective proprietors.

## Service Statement

This document is intended to provide users with general information about Tencent Cloud's products and services only and does not form part of Tencent Cloud's terms and conditions. Tencent Cloud's products or services are subject to change. Specific products and services and the standards applicable to them are exclusively provided for in Tencent Cloud's applicable terms and conditions.

# Contents

## Operation Guide

- Adding IP to Allowlist

- Adding Asset

- Simulating Login

# 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

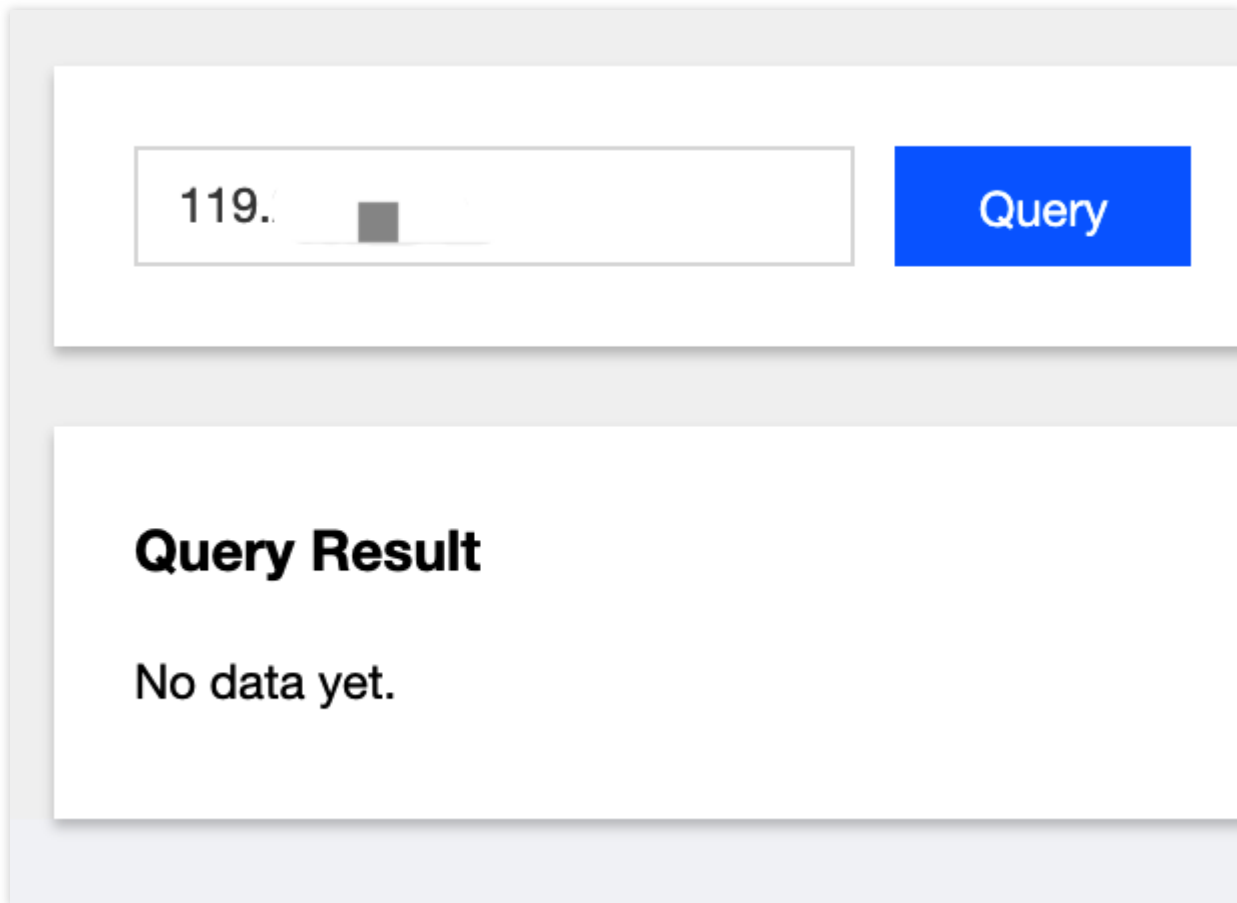
101.32.242.117

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.



The image shows a user interface for a query function. At the top, there is a text input field containing the value "119." followed by a small grey square icon. To the right of the input field is a blue button labeled "Query". Below this is a section titled "Query Result" in bold black text. Underneath the title, the text "No data yet." is 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**.

### Add a blocked/allowed IP ›

Category  Blocklist  Allowlist

IP Address

Deadline \*

Note

#### 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.

## Add a blocked/allowed IP

Category  Blocklist  Allowlist

IP Address  
119.28.101.45  
119.28.101.51  
150.109.12.53  
101.32.239.31  
101.32.242.117

Deadline \* Specified Date ▼ 2022-03-02 📅 23:59:59

Note VSS\_white\_IP

Add

Cancel

**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` .

## Import IP list



Import

Click to select a file.

note:

1. Supported file formats: XLSX and XLS; only one file can be uploaded each time.
2. Up to 2,000 IPs can be imported each time. If you import a large number of IPs, please import them by multiple times. Existing IPs will be skipped during import.
3. Content: must include three columns: category, IP address and end time; for more information, see the exported excel data.
4. The end time must be early than 2033/12/31 00:00:00 in the format of YYYY/MM/DD HH:MM:SS.

Import

Reset

### 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.

## Instructions for Use



1. You are only allowed to use the T-Sec Vulnerability Scanning Service for commerce, scientific research, and other businesses that comply with national laws and regulations.
2. You can only use the T-Sec Vulnerability Scanning Service for your own business rather than any third-party business, otherwise Tencent Cloud has the right to terminate your use immediately. And all losses of Tencent Cloud and any third parties caused by this shall be borne by you.
3. You promise not to use the T-Sec Vulnerability Scanning Service system to damage or attempt to damage network security (including but not limited to phishing, hackers, network fraud, spreading viruses, ARP spoofing, DDoS, etc.).
4. You should carefully read the guidelines and descriptions of the T-Sec Vulnerability Scanning Service, judge the suitability for your business, and operate in accordance with the relevant operating guidelines. You are solely responsible for the parts of the system you set manually and the results.

I have read and understood the service descriptions and conditions.

Don't remind me next time

Confirm

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.

Asset Type  Website  Server  API

Website Type \*  Domain name  IP

Address \*

Please enter one address per line, for example:  
https://console.cloud.tencent.com:8080  
http://dvwa.webscantest.cn:443

Add

Cancel

# 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.

| Asset   | Type | Addition Time       | Authentication Status | Mock Login ⓘ  |
|---|------|---------------------|-----------------------|---|
|  | IP   | 2022-01-27 15:58:02 | Authenticated         | Not set  |

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

## Mock Login ✕

Asset

Cookie value

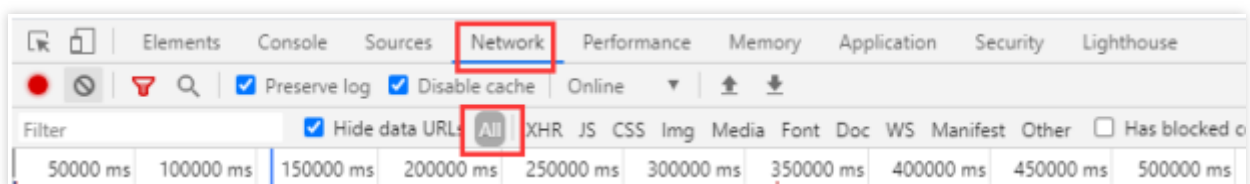
Note that the mock login may affect your business system.

[How to obtain a cookie value](#)

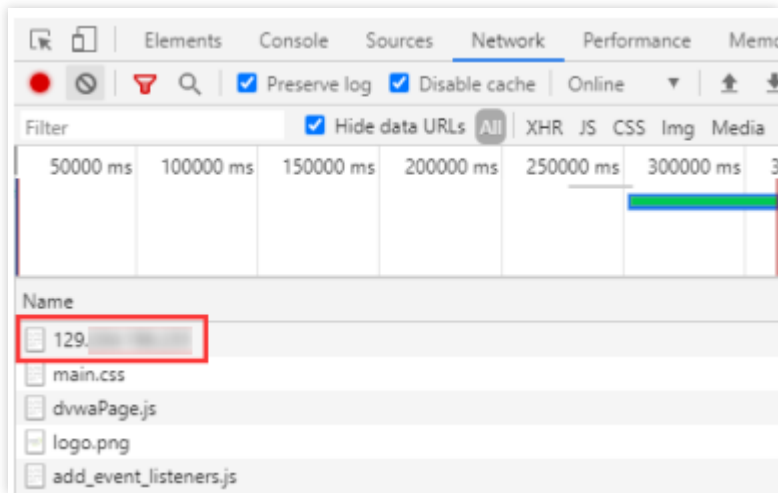
5. The simulated website login is successfully set.

### 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.

