Cloud Web Scanner

Operation Guide

Product Documentation

Contents

Operation Guide
Adding a Website

Last updated：2018-11-21 15:31:02

Adding a Website

Website is the smallest unit of vulnerability scanning, which can be scanned individually or added to a detection task for scheduled scan. You can add websites on the website management page. Currently, CWS support adding websites accessed through domain names and IPs, including HTTP and HTTPS, multi-level sub-domain name, ported and multi-level sub-directory websites.

Steps

1.Go to the website management console and click **Add a website**.

2.Complete the fields and click **OK** to go to the next step to verify the website.

- Choose the type of website to be added based on how your website is accessed.
- Enter the website URL in the website input box, one per line.
- Select your website type. CWS will set User-Agent access according to the type you choose:

  a. PC website: A website accessible through a PC browser.

  b. Mobile website: A website accessible through a mobile browser.

  c. WeChat website: A website accessible through WeChat.

3.Select DNS verification or file verification in the website verification pop-up.

i. If you choose DNS verification, please copy the host records and record values.

Enter the domain name resolution service console of your website (all domain name resolution service providers are supported, including Tencent Cloud DNS, DNSPod, Alibaba Cloud DNS, Net.cn DNS) and add TXT resolution.

Go back to the Tencent Cloud Console and click **Verify now** to complete the verification.

ii. If you choose file verification, please download the verification file (in HTML format).

Upload it to the corresponding directory on your website.

Confirm that the file is successfully uploaded.

Click **Verify now** to complete the verification.

4.The website is added and verified now.

Simulated Login

Last updated：2018-11-21 15:31:06

Stimulated Login

If some or all pages or features of your website require login to access, it is recommended to set a cookie to simulate login for a complete and comprehensive vulnerability scan. Currently, you can simulate the login by setting a cookie after successful login, and the system will use the cookie to visit the website regularly to ensure that it never expires.

Steps

1.Go to the website management console, hover your mouse over the simulated login column and click **Settings**.

2.Indicate whether your website needs to be set to scanning after login in the simulated login pop-up.
i. If your website does not require login to access all pages or features, please select "Login not required", and you can modify this setting later.
ii. If some or all pages of your website require login to access, select "Login required".

3.After selecting "Login required", fill in the following fields.

Please use Chrome to log in to your website, visit a page that requires login to access and hit F12 or right click on the page and select "Inspect".

Select "Network > All" in the developer tool that appears and refresh the page.

Click the first network request.

Find the "Cookie" item in "Headers", copy its value and paste into "Cookie after successful login" in the simulated login pop-up.

Copy the URL of the page that requires login to access and paste into the "Verify login URL" in the simulated login pop-up.

Copy the string (such as username or nickname) that only appears after login on the page that requires login to access and paste into the "Verify login keywords" in the simulated login pop-up.

The "Keywords for forbidding path scan" in the simulated login pop-up indicates that if the page address contains these keywords, the scanner is prohibited from accessing the page so as to prevent logging out

or accessing the admin backend.

After completing the fields, click **OK** to save. You can check whether the cookie works in the website list. If it does not work, you can click **Modify** to modify it.

4.The simulated login is successfully set up.