How to Create a New Web Application Scan

https://campus.barracuda.com/doc/53676676/

Use the steps in the article to define a scanner configuration in order to discover security risks in your website or website application.

Creating a Web Application

After you have completed the steps in Getting Started, navigate to the **Scanner > Web Applications** page. Complete the following steps to set up a website scan:

1. Click **Add Web Application**. The **New Web Application** dialog displays.
2. Enter a name to represent the scan. For example, `test site scan 1`.
3. Enter the URL you want to scan. For example, `test.MyCompany.com`.
   For a sample scan and report, use the following URL: `test.blorpazort.com`
4. **Verification** – Verify that you own the domain of this web application in one of the following ways. Note that the scan cannot be performed until the web application is verified.
   - **Email** – The most common method of verification. Enter an email with the same root domain as the URL you want to scan. An email is sent to this address. You musts clink a link in the email to verify you are the owner of the domain.

     For the following options, make a specific, small addition to your DNS or site so the scanner can verify you are the owner. These changes will not be noticeable or affect your site.
   - **File** – Add a text file with the specified name and content under the site to be scanned.
   - **TXT Record** – Add a TXT record with the specified content to the domain DNS.
   - **META Tag** – Add a META tag with the specified content within the tag of the site's home page.
   - **Barracuda WAF** – This option is available if you are using a Barracuda Web Application Firewall. Select the option and the name of the Barracuda Web Application Firewall. The scanner uses the Barracuda Web Application Firewall to determine you own the URL to be scanned.

     In some rare situations, you might not be able to verify that you own the web application. Refer to How to Request a Manual Domain Verification for details.
5. **Email Notification** – Specify if and how you want to be contacted by email after scans.
   - **Email me when a scan finishes** – Select this check box to be notified when scans complete.
     - Select **Always** to be notified after every scan.
     - Select **Only if new vulnerabilities are found** if you want to be notified only when new vulnerabilities are detected in a scan.

- **Email me a weekly report of unmitigated vulnerabilities** – Select this check box to receive weekly reports of unmitigated vulnerabilities.
- **Send Notification to** – Enter one or more email addresses, separated by commas.

6. **Mitigation** – If you are using a Barracuda Web Application Firewall, complete this section. Refer to documentation for details.
   - **Barracuda WAF** – Select the Barracuda Web Application Firewall you want to use. If you have recently added or changed a Web Application Firewall, click **Update WAF List** to ensure that your changes are reflected in the list.
   - **Virtual Service** – Select the service on the Barracuda Web Application Firewall you want to use to protect this application. A Virtual Service is a combination of a Virtual IP (VIP) address and a TCP port, which listens and directs the traffic to the intended Service.
   - **Security Policy** – Select whether to use the existing Security Policy within the Barracuda Web Application Firewall, or whether you want to create a new one. A Security Policy determines what action to take when one or more of the rules match the request.
   - **Mitigation** – Select if and how to mitigate the vulnerabilities found by the scan.
     - **Off** – No action will be taken automatically. You will manually mitigate any vulnerabilities found.
     - **Passive Mode** – (Recommended) Vulnerability Remediation Service automatically applies security policy changes to your Web Application Firewall in Passive Mode. This logs violations, but does not block them, so no behavior changes on your site.
     - **Active Mode** – Vulnerability Remediation Service automatically applies security policy changes to your Web Application Firewall in Active Mode. This blocks violations immediately.

       Barracuda Networks strongly recommends that you select automatic remediation in **Passive Mode**. Passive Mode allows you to manually audit the policy changes and verify no false positives are logged. After verifying, you can deploy the fix in Active Mode.
7. Click **Create**.
   The new Web Application you created appears in the **Web Applications** table.
   By default, Web Applications appear in this table in order of creation date, with the Applications most recently added to the end of the list.
8. Repeat steps 1-7 to set up additional Web Applications.
   Continue with the steps below to set up scans for this Web Application.

Creating a Scan for this Web Application

After you have specified the Web Application you want to test for vulnerabilities, you must create specific scans to perform.
By default, a basic scan is configured for you. It is named ***Default*** and appears below the Web Application in the Web Application table.

For this Web Application, you can:

- **Edit the default scan**: In the table row for the default scan, click **Edit**.

- **Create a new scan**: In the table row for the Web Application, click **New Scan**.

Refer to Actions on Existing Scans and Web Applications for details.

.