How to Create a New Scan

https://campus.barracuda.com/doc/46208077/

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

Once you are logged in and connected to the service, the **Active Scans** page displays. Complete the following steps to set up a website scan:

1. Click **New Scan**; the **Scanner Configuration** page 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`.

   For a sample scan and report, use the following URL: `test.blorpazort.com`

   If the URL cannot be verified, you are prompted to enter an email address to which you have access.
   If the domain is verified, the scan can be started immediately.
   For more information, refer to Understanding Verification.
4. Select each of the four tabs, described below, completing the necessary information.
5. When you are satisfied with your configuration, click **Start Scan**.

Select the General Tab

1. Specify when you want to scan the website:
   1. **Start scan immediately** – When selected, the scan begins once the scanner configuration is complete and you click **Start Scan**.
   2. **Start scan at this time** – When selected, you specify the date and time that the scan is to start.
      If the time zone shown is not correct, click its link. The Barracuda Cloud Control Profile page opens in a new browser tab. Set your time zone, then return to the Barracuda Vulnerability Manager tab of your browser. Note that time zone changes may take up to 60 minutes to take effect.
2. In the **Maximum Length of Scan (Hours)** field, you can specify a scan duration limit. For example, for a large site, limit the scan duration for faster results.
   The scanning process begins on the home page, then moves down to scan the next level, then once pages on that level are complete, moves to the following level, for a maximum of 3 levels deep. The home page is level zero. If you shorten the time of the scan, you will potentially not see results for the lower levels of your web site.
3. To receive a scan report via email once the scan is complete, select **Email me a report when the scan is completed**, and enter the email address in the associated field.
4. **Barracuda may contact me about the results of this scan** is selected by default. If you leave this option selected, Barracuda might contact you when the scan is complete to help you understand the report and mitigate any vulnerabilities found. If you do not want to be contacted, clear this check box.

Select the Crawling Tab

1. Select the type of scan you want:
    - **Scan Desktop Site –** Select **Firefox**, **Chrome**, **Safari**, or **Internet Explorer**.
    - **Scan Mobile Site –** Select **iPhone, iPad, or Android**.
    - **Scan using a custom browser** – To use a custom browser, specify the appropriate information in this field.
2. **Requests per second** – Specify the number of requests per second the scanner can make. Enter **0** (zero) to set the maximum requests your server can manage.

    > A value of **0** (zero) is not recommended if you are setting up a scan on a *production server*.
    > If you are running a scan on a *non-production server*, consider increasing the speed of the scan to as fast as the server can respond, so you will receive scan results more quickly.
    > If Barracuda Vulnerability Manager detects that it is starting to overwhelm your server, it will automatically throttle back on the number of requests per second.
3. **Maximum crawl depth** – Specify the maximum link depth from the start page. A value of zero means only the home page will be scanned.
4. Turn on **Enable evasion techniques** if you want the scan to attempt to "confuse" sanitizing or filtering code in your web application during the scan.

    > When **Enable evasion techniques** is activated, scanning takes approximately four times as long to complete as a normal scan.

Select the Authentication Tab

Specify whether to scan the parts of your site accessible only by a user who has logged in. Select from the following three options:

1. **No authentication** – Select if you do not want to scan these areas of your website.
2. **HTTP authentication –** Select to scan areas of your website requiring login credentials. Click the HTTP authentication type used by your website, and then enter the associated login credentials.

    > Do not enter administrator credentials when scanning a production site. See Avoiding Possible Scanning Side Effects for details.

    - **Basic** authentication uses static, standard HTTP headers and is the simplest technique for enforcing web resource access control. Basic sends plain text over the network.
    - **Digest** access authentication is a more complex technique to confirm user identity. Digest applies a hash function to a password before sending it over the network.
3. **HTML form-based authentication** – Select if your web application has a standard HTML login form that submits to the web server using HTTP POST.
    1. Enter the **Login form URL**, along with your associated user name and password. Then click **Autodetect** to automatically complete the rest of the fields in the section. Alternatively, you can enter the information manually.
    2. Click **Test Authentication** to verify the information you entered is correct and the test will run as expected.

Select the Exclusions Tab

Use the **Exclusions** tab to define hostnames, IP addresses, URL patterns, and file extensions that you do not want the scanner to test for vulnerabilities.

- **To exclude a hostname, IP address, URL pattern or file extension**:
  Enter the information into the correct segment of the page, then click **Add** in the **Actions** column.
- **To remove an exclusion**:
  In the row of the table with the exclusion you want to remove, click **Delete** in the **Actions** column.
- Click **Remove All** to remove all of the exclusions within a section of the page.
- By default, all images and videos are excluded.

> If you have unprotected forms that write data to a database or send emails based on form submissions, you might see a large number of database records or emails sent during the scan. You can safely ignore or delete these records and/or emails. They do not cause any damage.