Scanning Your Web Application Using the Barracuda Vulnerability Manager

https://campus.barracuda.com/doc/48660791/

Barracuda Vulnerability Manager is a web application scanner designed by Barracuda Networks to scan your web applications and uncover security vulnerabilities such as cross-site scripting, SQL injection, directory traversal, etc., in your web applications.

When you scan web applications protected by the Barracuda Web Application Firewall in active mode, the scan report generated may not find most of the vulnerabilities as they would be blocked by the Barracuda Web Application Firewall. To detect the security vulnerabilities more accurately in your web application, perform the following steps before scanning a service configured on the Barracuda Web Application Firewall:

Step 1 - Create a Trusted Hosts Group with the Barracuda Vulnerability Manager IP Addresses

1. Go to the **WEBSITES > Trusted Hosts** page.
2. In the **Add New Trusted Host** section, specify a name in **Trusted Host Group Name** and click **Add**. It is recommended to use "Barracuda-Vulnerability-Manager" as **Trusted Host Group Name**. Note: The name can include alphanumeric characters, periods (.), hyphens (-) and underscores (_). Any other special characters such as space, semicolon, asterisk, etc., are not allowed.
3. In the **Trusted Hosts** section, click **Add Host** next to the trusted host group created in Step **2**.
4. In the **Create Trusted Host** window, specify values for the following:
   - **Trusted Host Name** – Enter a name for the trusted host.
   - **Version** – Select IPv4.
   - **IP Address** – Enter 64.235.153.133
   - **Mask** – Enter 255.255.255.255
5. Click **Save**.
6. Repeat Step **3** and **4** for the following hosts:
   1. 64.235.153.134
   2. 64.235.153.135
   3. 64.235.153.136
   4. 64.235.150.121

For more information on trusted host group, see How to Configure Trusted Hosts.

Step 2 - Associate the Trusted Hosts Group with the Service

After creating the trusted hosts group and adding hosts, associate the trusted hosts group with the service that needs to be scanned by following the steps below:

1. Go to the **BASIC > Services** page.
2. In the **Services** section, identify the service you want to scan and click **Edit** next to it.
3. In the **Service** window, scroll down to the **Basic Security** section and do the following:
    1. Set **Trusted Hosts Action** to *Allow*.
    2. Select the trusted hosts group (i.e., *Barracuda-Vulnerability-Manager*) created in Step 1 - Create a Trusted Hosts Group with the Barracuda Vulnerability Manager IP Addresses from the **Trusted Hosts Group** drop-down list.
    3. Specify values for other parameters (if required).
    4. Click **Save**.

The web application is now ready to be scanned.

To scan the service by keeping the Barracuda Web Application Firewall security **ON**, perform the following steps:

1. Go to the **BASIC > Services** page.
2. In the **Services** section, identify the service you want to scan and click **Edit** next to it.
3. In the **Service** window, scroll down to the **Basic Security** section and do the following:
    1. Set the **Trusted Hosts Action** to *Default*.
    2. Specify values for other parameters (if required).
    3. Click **Save**.