Vulnerabilities

https://campus.barracuda.com/doc/53676683/

The **Vulnerabilities** page is an overview, showing the number and type of vulnerabilities found on each web application.

Searching for Web Applications

To refine the list of web applications, begin typing in the **Search** field, or use the navigation tools to move through the list. You can search by Web Application Name, associated Barracuda Web Application Firewall (WAF), or Service.

Web Application Table

The Web Application table includes:

- **Web Application Name** – The name of your Web Application that is being scanned.
- **Vulnerabilities** – A graphical representation of the number of vulnerabilities found in the web application. The total number of vulnerabilities is shown to the right of the bar in the **Vulnerabilities** column. For example:

  Within the bar, colors represent how the vulnerability is currently mitigated:
  - New **Red / New** – All vulnerabilities start as **New**. After you change a **New** vulnerability to a different category, you cannot change it back to **New**.
  - Active Mode **Green / Active Mode** – Active Mode. Performs the action configured in association with the perceived threat.
  - Passive Mode **Yellow / Passive Mode** – Passive Mode. Logs violating events and allows the request to pass through.
  - Manual **Blue / Manual** – Enables you to mitigate the vulnerability manually.
  - Ignored **Grey / Ignored** – Does not take any action with this vulnerability, and marks it to be ignored.

  For details on using Active and Passive Mode, refer to Understanding Passive Mode and Active Mode.
- **Barracuda WAF** – The name of the Barracuda Web Application Firewall associated with this scan, if any.
- **Service** – The service on the Barracuda Web Application Firewall associated with this scan, if any.
- **Policy** – The security policy on the Barracuda Web Application Firewall associated with this

scan, if any.

Click **View**, or anywhere in the row, to open the **Vulnerabilities on** page for vulnerabilities found on a specific web application, described in the next section.

Vulnerabilities on Page

This page displays all vulnerabilities for a specific web application.

The Vulnerabilities table displays the following information about each vulnerability:

- **ID** – A unique identifier for each specific vulnerability in a specific web application.
- **Last Found** – Date the vulnerability was last found on this web application. This can be the date of the last scan or earlier. If the date is earlier, then the vulnerability was not found in this latest scan and was likely mitigated.
- **Type** – The category of this vulnerability.
- **URL** – The specific URL within the web application that is affected by this vulnerability.
- **Parameter** – The specific parameter that is affected by this vulnerability, if any.
- **Severity** – How serious the threat is to your web application. Levels include Critical, High, Medium, Low, and False Positive.
- **Mitigation** – How this vulnerability is currently mitigated. Refer to the color chart description above.
- **Autofix** – Whether the vulnerability can be fixed automatically by the Barracuda Web Application Firewall. Some vulnerabilities cannot be mitigated automatically and require manual user input to fix. Click a vulnerability for more specific details.
- **Actions** – Click **View**, or anywhere in the row, to learn more about a specific vulnerability and edit certain attributes. Refer to How to Work with Vulnerabilities in the Vulnerability Details Page.

Filtering Vulnerabilities

Control which vulnerabilities are displayed in the Vulnerabilities table by searching and filtering.

- **Search field** – Use the **Search** field to search for Type, URL, or Parameter for the vulnerability.
- **Time frame** – Specify the time frame of when the vulnerability was last found.
- **Filtering by Severity** – Click the arrow at the top of the **Severity** column to select which **Severity** levels to display. Select any or all check boxes to choose which Severity levels to display.
- **Filtering by Mitigation**– Click the arrow at the top of the **Mitigation** column to select which **Mitigation** types to display. Select any or all check boxes to choose which Mitigation types to display.

Note that if you are too restrictive with your searching and/or filtering, there might not be any results

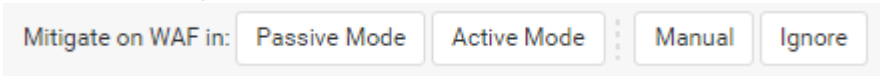
to display. Broaden your search and/or filtering criteria to display some results.

Click **View**, or anywhere in the row, to open the page for a specific vulnerability found on this specific web application.

Updating Mitigation Method for Multiple Vulnerabilities

You can mitigate multiple vulnerabilities on the Barracuda WAF in bulk without having to open the **Vulnerability Detail** window for each one. You can also remove mitigations for multiple vulnerabilities.

1. Select the check box to the left of the **ID** for one or more vulnerabilities. To select all vulnerabilities, select the check box next to the **ID** in the heading row.
2. Select the mitigation method from the buttons above the table.

   Note that if you are selecting multiple vulnerabilities at once, the same selection will apply to all of the selected vulnerabilities.
3. A dialog appears, explaining what your proposed change entails. Click **Confirm** to assert that you understand the implications of the change. The change is then made on the Barracuda Web Application Firewall.

Figures