Mitigating Website Vulnerabilities Using Vulnerability Scanners

https://campus.barracuda.com/doc/4259943/

Overview

The Barracuda Web Application Firewall integrates with web application vulnerability scanners to make it easier to address web application vulnerabilities detected by these scanning tools. The vulnerabilities can be mitigated quickly and easily using the Barracuda Web Application Firewall, allowing an optimal engineering solution to be designed and incorporated through the regular code release cycle without incurring continued risk.

Administrators use vulnerability scanners to detect and report website vulnerabilities in a variety of report formats. Vulnerability reports can be imported using the **ADVANCED > Vulnerability Reports > Import Vulnerability Report** section. The Barracuda Web Application Firewall uses imported reports to provide security policy recommendation(s), which, if applied by the administrator, modify applicable security policy settings or configurations to mitigate the reported vulnerabilities.

Currently, the Barracuda Web Application Firewall supports the following scanners:

- Barracuda Vulnerability Manager
- Cenzic Hailstorm v6.6
- HPE Security WebInspect
- HPE Security Fortify On Demand
- IBM AppScan v7.9
- IBM AppScan v9.0
- ImmuniWeb
- ThreadFix

The assessment report exported should be in XML format.

To configure the Barracuda Web Application Firewall to connect to the Barracuda Vulnerability Manager, contact Barracuda Networks Technical Support.

Importing Vulnerability Report

Perform the following steps to import a vulnerability assessment report:

1. Go to the **ADVANCED > Vulnerability Reports** page.

2. Specify a name for the assessment report in the **Assessment Name** field.
3. Select the scanner used to detect vulnerabilities in the web application from the **Scanner Used** list.
4. Click **Browse** next to **Vulnerability Report** to locate and select the scanned file. The report should be in XML format.
5. Click **Import Vulnerability Report**.

Viewing and Applying Recommendations to a Service

Summaries of imported vulnerability assessment reports are visible, along with corresponding configuration update recommendations, using the **Manage Vulnerability Assessments** section. To view the summary of an assessment report and apply recommendations, perform the following steps:

1. Go to the **ADVANCED > Vulnerability Reports** page.
2. In the **Manage Vulnerability Assessments** section:
    1. Select the assessment report from the **Assessment Name** list.
    2. Select the service for which you want to apply the recommendations from the **Apply To Service** drop-down list.
3. The **Scanner Information** panel provides the following details:
    - **Scanner Type** – The name of the scanner tool used to detect vulnerabilities.
    - **Scanner Version** – The version of the scanner tool.
    - **Import Date** – The date and time at which the vulnerability assessment report was imported to the Barracuda Web Application Firewall.
    - **Vulnerabilities Detected** – The number of vulnerabilities detected in the website.
4. Recommendations for vulnerabilities detected by the scanner get displayed in the **Security Policy Recommendation(s)** section. For information on how to choose recommendations before applying, see Choosing the Recommendations .
5. In the **Security Policy Recommendation(s)** section, select the check box(es) to apply the recommended fixes for website vulnerabilities identified by the scanner.
6. Click **Apply** to apply the fixes.
7. The **Recommendation Summary** panel displays the following details: (Click on the number to display the recommendations for the selected status in the **Security Policy Recommendation(s)** section.)
    - **Total Recommendations** – Number of recommendations generated by the Barracuda Web Application Firewall for vulnerabilities detected.
    - **Pending Recommendations** – Number of recommendations pending, not yet applied to the service.
    - **Applied Recommendations** – Number of recommendations applied to the service to mitigate threats.
    - **Rejected Recommendations** – Number of recommendations viewed and rejected by the administrator.

Choosing the Recommendations

The **Security Policy Recommendation(s)** section displays the recommendations for the selected assessment report. Before applying the recommended fixes, the administrator must review the recommendations and choose one or more entries by selecting the check box(es).

Steps to View Recommendations

1. From the **ADVANCED > Vulnerability Reports** page, select an assessment report in the **Manage Vulnerability Assessments** section from the **Assessment Name** list.
2. Recommendations for the selected assessment report get populated in the **Security Policy Recommendation(s)** section.
3. Select an entry in the Recommendation List to view detailed information about the vulnerability detected and security policy recommended by the Barracuda Web Application Firewall in the **Preview Pane**. By default, **Preview Pane** is turned *Off*. Use the **Settings** option on the tool bar to turn on the **Preview Pane** at Right, Bottom or Left. The following information is displayed in the **Preview Pane**:
    - **Attack** – Name of the attack detected in the web application.
    - **Attack Group** – Name of the attack group of this attack. Example: *constTransient* is an attack in the *Session Identifier Not Updated* Attack Group.
    - **Severity** – Vulnerabilities are categorized as HIGH, MEDIUM, or LOW severity.
        - **HIGH** – Indicates a critical security threat that can potentially affect the web application. This should be fixed immediately.
        - **MEDIUM** – Indicates that these vulnerabilities are not harmful by themselves but combined with other vulnerabilities may cause a potential threat to the web application. The administrator needs to review the recommendation before applying the fix.
        - **LOW** – Vulnerabilities that have little impact on the web application, so the fix has a lower priority.
    - **URL** – The URL in the web application where vulnerability was detected.
    - **Parameter** – The parameter(s) in which vulnerability was detected.
    - **Status** – The recommendation status: **New** if not yet applied by administrator or **Applied**.
    - **Attack Information** – Click to see detailed information about the attack detected in the web application.
    - **Recommendations** – Click to see the security policy recommended by the scanner and Barracuda Web Application Firewall to mitigate the identified vulnerability.
4. Select the service from the **Apply To Service** list using the **Manage Vulnerability Assessments** section.
5. Select one or more check box(es) next to the recommendations and use one of the action controls on the tool bar:
    - **Apply** – Applies the recommended fixes for selected vulnerabilities**.**
    - **Reject** – Rejects the recommendations for selected vulnerabilities. If you want to apply

rejected recommendations, you need to **Un-Reject** first and then **Apply**.
- **Un-Reject** – Un-rejects the rejected recommendations.

Once the recommendations are applied to a service, they cannot be re-applied or rejected.

Steps to Mitigate Website Vulnerabilities

1. Scan web application(s) using third party vulnerability scanning software.
2. Choose *.xml (the only supported format) for the exported vulnerability output file format.
3. Navigate to the **ADVANCED > Vulnerability Reports > Import Vulnerability** section, and import the scanned file. For information on how to import, see Importing Vulnerability Report.
4. Select the assessment report from the **Assessment Name** list, select the service from the **Apply To Service** list in the **Manage Vulnerability Assessments** section.
5. In the **Security Policy Recommendation(s)** section, select the check box(es) to apply the recommended fixes.
6. Click **Apply** to mitigate corresponding vulnerabilities.