Understanding Barracuda Vulnerability Remediation Service Reports

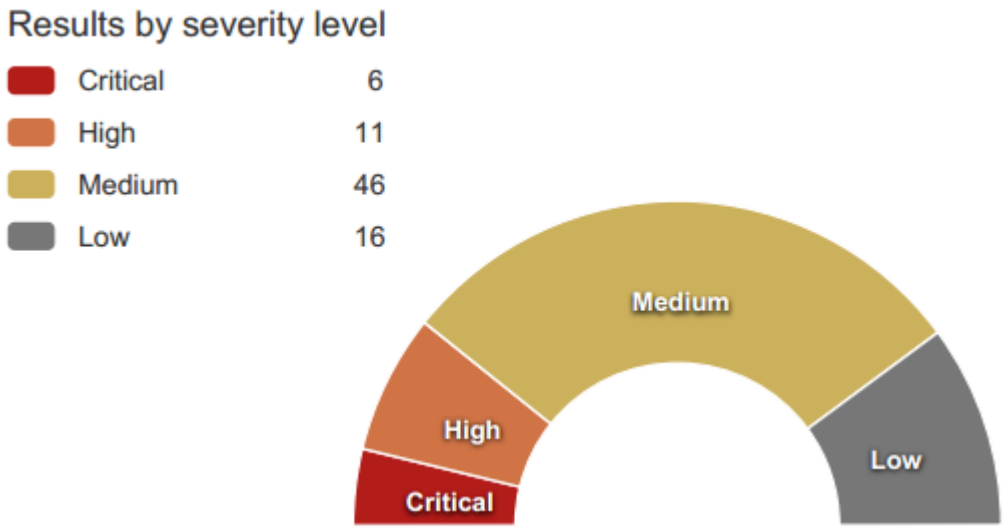
https://campus.barracuda.com/doc/53676680/

The Barracuda Vulnerability Remediation Service Report contains a comprehensive set of details to help you determine how to resolve existing vulnerabilities.

During the scan, the Barracuda Vulnerability Remediation Service collects information about your applications to increase accuracy and find vulnerabilities in the application. The Barracuda Vulnerability Remediation Service does not collect any personally identifiable information (PII), source code, or records from your application's database, regardless of whether the information is publicly accessible.

Executive Summary

The **Executive Summary** section is a quick glance at your risk level based on the vulnerabilities discovered on your application website, including a breakdown by severity level.



Scan Information

The **Scan Information** section lists the basic information about the scan, including domain verification and the authentication username, if authentication was used.

Server Information

The **Server Information** section lists basic information about the server that was scanned.

Standard Compliance

This section shows whether you qualify for compliance with several different industry-standard compliance measures, including:

- **OWASP Top 10** – Open Web Application Security Project https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project
- **PCI DSS** – Payment Card Industry Data Security Standard https://www.pcisecuritystandards.org/security_standards/
- **HIPAA** – The Health Insurance Portability and Accountability Act of 1996 http://www.hhs.gov/ocr/privacy/hipaa/understanding/

The Barracuda Vulnerability Remediation Service cannot guarantee that you comply with these measures, but can determine if you are not compliant. Links in this section direct you to compliance information direct from the respective sources.

Table of Contents

This section lists web application vulnerabilities found in the scan, ordered by severity level. Click a link to view the detailed results for each issue.

> This is *not a guarantee* that there are not additional vulnerabilities that were undiscovered.

Each section within the detailed results includes:

Name of the Vulnerability

The title of each section is the official name of each vulnerability.

CVSS

The National Vulnerability Database's Common Vulnerability Scoring System score and vector.

List of Pages

The pages in your web application on which this vulnerability was found.

Path

The path in your web server where the vulnerability was located.

Severity

The severity of the vulnerability. You can change this value, based on your organization's perception of the **Severity**. Refer to Vulnerabilities or click the Help icon on the **Vulnerabilities on** page for information on changing the Severity.

Symbol	Description
Critical	Attack severity is Critical
High	Attack severity is High
Medium	Attack severity level is Medium
Low	Attack severity level is Low
False Positive	Attack severity level is False Positive

Confidence

How likely it is that your website has this vulnerability. Confidence levels include:

- Certain
- Likely
- Possible

Status

Shows the current status of this vulnerability. All vulnerabilities start as **New** when they are first detected. You can use the **Vulnerability Details** page to mitigate or otherwise change the status of vulnerabilities. For more information, see How to Work with Vulnerabilities in the Vulnerability Details Page.

- New
- Passive Mode
- Active Mode
- Manual
- Ignored

Details

Describes how the scanner detected this vulnerability.

Recent Scans Table

This table lists recent scans on this application and shows in which of them this vulnerability was found. The table includes:

- **Scan Date** – The date the scan was run.
- **Configuration** – The name of the scan.
- **Type** – The description of the scan.
- **Status** – Whether the vulnerability was found in that specific scan.

Refer to Vulnerabilities and How to Work with Vulnerabilities in the Vulnerability Details Page to learn more about changing certain vulnerability-related values.

Figures