Understanding Barracuda Vulnerability Manager Reports

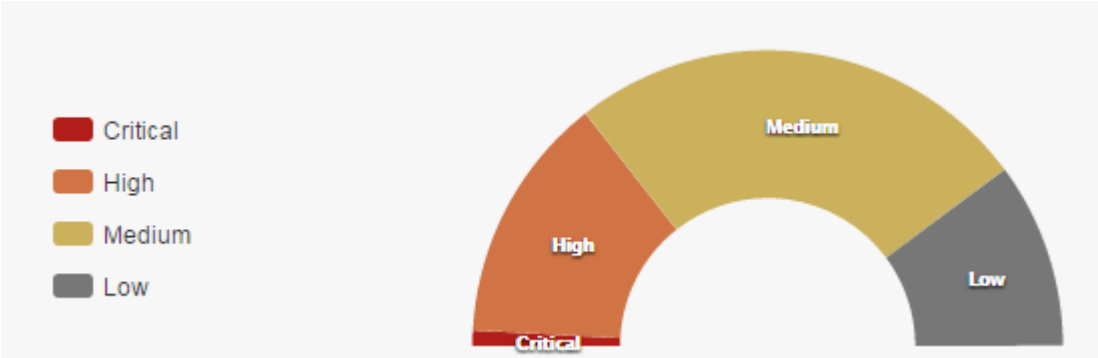
https://campus.barracuda.com/doc/45711678/

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

During the scan, Barracuda Vulnerability Manager collects information about your applications to increase accuracy and find vulnerabilities in the application. Barracuda Vulnerability Manager does not collect any personally identifiable information (PII), source code, or records from your application's database, whether or not it 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 scanner configuration details as well as server information and scan statistics.

Symbol	Description
	Server responsive
	Server not responsive

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/

Barracuda Vulnerability Manager 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 official name of each vulnerability is listed for each numbered section
- **CVSS** – The National Vulnerability Database's Common Vulnerability Scoring System score and vector.
- **Remediation Background** – Briefly describes methods by which you can mitigate this vulnerability in your system.

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 Interacting with the Barracuda Vulnerability Manager Reports for details 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 web site has this vulnerability.

Symbol	Description
Certain	Confidence is Certain
Likely	Confidence is Likely
Possible	Confidence is Possible

Status

Enables you to track your progress in solving issues. All issues start as New, but you can change the value as you progress through your work.

Refer to Interacting with the Barracuda Vulnerability Manager Reports for details on changing the **Status**.

Values include:

- **New**
- **Reviewed**
- **Fix in Progress**
- **Fixed**
- **Rejected**

Issue Detail

Describes how the scanner detected this vulnerability.

Notes

A location where you can create your own notes as you work on each vulnerability.

Refer to Interacting with the Barracuda Vulnerability Manager Reports for details on changing the **Notes**.

Exclusions

The **Exclusions** section lists all hostnames, IP addresses, URLs, URL patterns, and file extensions excluded based on the scanner configuration.

Crawler Database

This section lists the crawler configuration details based on your scanner configuration settings. For example, it lists the start page and maximum link depth. Additionally, the Crawler Database section lists all hostnames, IP addresses, URLs, URL patterns, and file extensions that were crawled.

Learn more about Interacting with the Barracuda Vulnerability Manager Reports.

Figures