Scanner

https://campus.barracuda.com/doc/53676675/

To scan a web application, the Barracuda Vulnerability Remediation Server sends specially crafted requests to your web servers and analyzes the responses. When vulnerabilities are detected, a detailed report is automatically generated, allowing you to identify, assess, and mitigate the web application vulnerabilities. During the scan, information about your application is collected to increase accuracy and find vulnerabilities including data on technologies and components in use by your application, the structure of your application, as well as lists of pages, forms, fields, and cookies. No personally identifiable information (PII) or records from your application's database are collected. If a vulnerability is found that could compromise confidentiality of data on your web application, the Barracuda Vulnerability Remediation Service does not collect any of the data that could be compromised; instead, it alerts you to the problem, but does not collect application source code.

Scans are run at a reasonable speed, so as not to overload your web server or network infrastructure. During configuration, you can reduce the scan speed to further reduce the load on your network. If you are running a scan on a non-production server, it is recommended that you increase the speed in order to complete the scan faster.

Use the Barracuda Vulnerability Remediation Server to scan any of your publicly accessible web applications, regardless of where they are hosted (even if they are behind a load balancer or firewall).

Scans at a Glance

Navigate to the **SCANNER > Web Applications** page to see all of the web applications for which you have created scans, along with the associated scans.

Here, you can:

- Create and configure scans. Refer to How to Create a New Web Application Scan.
- Take actions on scans. Refer to Actions on Existing Scans and Web Applications.

Scan Status

To check the status of a scan, refer to Scan Status.