Barracuda Vulnerability Manager

Frequently Asked Questions

Barracuda Vulnerability Manager is a web application vulnerability management solution to help businesses automatically identify, assess and mitigate web application vulnerabilities. It finds vulnerabilities such as those on the OWASP Top 10, including SQL Injection, Cross-Site Scripting, and others. Together with Barracuda's Web Application Firewall (WAF), the Barracuda Vulnerability Manager provides a comprehensive solution to identify and secure against web application vulnerabilities.

What does Vulnerability Manager scan?

Vulnerability Manager scans web applications only, so it will only target the web server it is pointed at. It does not scan your network or infrastructure. For example, Vulnerability Manager will not target or scan layer 3 firewalls, VPN devices, email servers or devices, FTP servers, phone systems, or any other network devices.

What types of vulnerabilities does Vulnerability Manager detect?

Vulnerability Manager detects many common web application vulnerabilities, including SQL Injection, Cross-Site Scripting (XSS), Cross-Site Request Forgery (CSRF), and others. For a more detailed list, see the "Barracuda Vulnerability Manager Vulnerability Type Reference."

Where are the scans performed from?

Vulnerability Manager scans are performed from Barracuda's data center in Southfield, Michigan. The IP range is 64.235.153.0/24.

How is the scan performed?

In order to scan the web application, Vulnerability Manager will send specially crafted requests to your web server and analyze the responses. Vulnerable servers will respond in ways that the scanner can detect, and we will report this to you. The requests Vulnerability Manager sends are specially designed not to cause any damage to your servers—they will only detect vulnerabilities, not exploit them in any way.

What data does Vulnerability Manager collect during the scan?

During the scan, Vulnerability Manager collects various information about your application; this information is used to increase accuracy and find vulnerabilities in the application. This information may include data on the technologies and components in use by your application, the structure of your application, as well as lists of pages, forms, fields, and cookies.

Vulnerability Manager does not collect any personally identifiable information (PII) or records from your application's database, whether this information is publicly accessible or not. If Vulnerability Manager finds a vulnerability that could compromise confidentiality of data on your web application, it does not collect any of the data that could be compromised; instead, it only alerts you to the problem.

Vulnerability Manager also does not collect the source code (whether client-side or server-side) of your application.

How long does a scan take?

The length of the scan varies widely with the size of your application—from a few minutes up to multiple days. You can monitor the progress of the scan from Vulnerability Manager's Active Scans screen. If you like, you can also limit the length of the scan; in this case, you will only see the vulnerabilities that were found within this period of time. You can always cancel a currently running scan; again, you will only see the vulnerabilities found until it was canceled.

What are the risks of running the scan?

The scan is specially engineered not to cause damage to your web application, web server, database, or network infrastructure.

During the scan process, the scanner submits all web forms found on your application a large number of times in order to test for vulnerabilities. If you have unprotected forms that write data to a database or send emails based on form submissions, you may see a large number of database records or emails sent during the scan. You can safely ignore or delete these records and/or emails; they do not cause any damage.

Will the scan overload my web server?

Vulnerability Manager has an automatic overload protection feature: If it detects high load on your web server, it will automatically reduce the scan speed until high load is no longer detected. Regardless of overload protection, Vulnerability Manager sends a maximum of 15 requests per second to your server. If you wish, you may adjust this number on the Crawling tab of the scan configuration dialog. For example, you may want to increase this number if you are scanning a non-production server and want the scan to complete faster.

Can I scan applications hosted on public cloud servers, on-premises, collocated, etc.?

Vulnerability Manager can scan any web application that is publicly accessible, regardless of where it is hosted. If any user on the internet can enter your application's URL and access it, it can be scanned.

Can I scan applications that are behind a load balancer or firewall?

Yes. Vulnerability Manager can scan regardless of any load balancers or firewalls in front of the application, as long as the application is publicly accessible.

Will Vulnerability Manager "hack" my application in order to detect vulnerabilities?

No. Vulnerability Manager will determine if your application could be hacked by a malicious attacker, but it will not hack your application. In particular, Vulnerability Manager will not cause your application to execute any harmful code, steal data from your application, or cause it to crash.

Will Barracuda employees have access to my application's data?

No. While Vulnerability Manager may store request and response data to help you locate vulnerabilities, your application's data will not be stored on Barracuda servers or accessible to Barracuda employees.

Are scan reports stored in Barracuda's cloud? How can you ensure the reports remain confidential?

Scan reports are stored on specially designated servers in Barracuda's dedicated data center. Only you can access your reports using your Barracuda Cloud Control credentials. If you have regulatory requirements that your data be kept on physically separate servers, or on-premises, please contact us to discuss on-premises options.

Can anyone with access to Vulnerability Manager scan my application?

No. For security reasons and to prevent abuse, users must verify every domain they intend to scan, either through the Cloud Control domain verification process or through Vulnerability Manager itself. Users will be prompted to perform this verification process, which is easy and just requires clicking a link in an email.

Vulnerability Manager found a vulnerability on my application. What should I do?

You should take immediate action to remediate vulnerabilities found by Vulnerability Manager, especially those with High or Critical severity levels.

The easiest way to remediate web application vulnerabilities is to use a Barracuda Web Application Firewall (WAF). Barracuda's WAF can import the results of a Vulnerability Manager scan and automatically remediate all the vulnerabilities found by the scan. For more information, see the Solution Brief, "Web Application Vulnerabilities: from Detection to Remediation."

The information provided in Vulnerability Manager's report can also be used by your web application's developers to find and fix the problem manually in the application's source code.

How do I contact support?

Please email BVM_Support@barracuda.com for support.