# Overview

https://campus.barracuda.com/doc/53676690/

The Barracuda Vulnerability Remediation Service, a free add-on to the Barracuda Web Application Firewall and Barracuda WAF-as-a-Service, enables automatic scanning, remediation, and maintenance of web application policies. The Barracuda Vulnerability Remediation Service makes it easy for organizations of any size to deploy comprehensive web application security with minimal administrative overhead. There is no need to hire security experts or spend time coding, testing, and deploying fixes. This eliminates the cost and complexity traditionally associated with securing web applications.

The Barracuda Vulnerability Remediation Service finds and mitigates vulnerabilities such as those on the OWASP Top 10, including SQL Injection, Cross-Site Scripting, and others, to help your organization stay safe in a changing technological landscape.

The service can be used through the entire application security workflow:

1. Scanning applications to find vulnerabilities
2. Learning about the threats posed by those vulnerabilities
3. Deploying fixes
4. Monitoring fix performance

All of these steps can be performed either automatically on a recurring schedule or manually.

Use the Barracuda Vulnerability Remediation Service in conjunction with Barracuda Web Application Firewalls (WAFs) or the Barracuda WAF-as-a-Service to protect new or existing applications.

#### Deploying with Barracuda Web Application Firewalls

Deployment with Barracuda Web Application Firewalls is a three-step process:

1. Deploy the Barracuda Web Application Firewalls in the network.
2. Associate them with the web servers that you want to secure.
3. Use the Barracuda Vulnerability Remediation Service to automatically create security configurations customized for your web application.

This automatic configuration, based on the specific vulnerabilities in an application, eliminates errors in manual configuration, maximizes security, and greatly reduces false positives. It also reduces deployment overhead by providing true “plug-and-play” web application security.

In addition to automatically configuring security policies through the Barracuda Vulnerability Remediation Service, as an administrator, you can also access the granular policy management framework provided through the Barracuda Web Application Firewall administrative interface to

further tune and customize your security posture.

The service can be used across all deployment surfaces – virtually, in the public cloud, and in on-premises environments.

#### Deploying with Barracuda WAF-as-a-Service

Deployment with Barracuda WAF-as-a-Service involves these steps:

1. Deploy the Barracuda WAF-as-a-Service.
2. Associate with the applications that you want to secure.
3. Add the Vulnerability Scanning component to automatically create security configurations customized for your web application.

## Where to Start

- To learn about the differences between this product and Barracuda Vulnerability Manager, refer to Comparison with Barracuda Vulnerability Manager.
- For detailed setup steps, refer to Getting Started.
- For best practices in using this tool to protect your web applications, refer to Best Practices: Keeping Your Web Application Secure.
- To learn how to create and run scans, refer to How to Create a New Web Application Scan.
- For information on Barracuda Web Application Firewalls, refer to Overview - Barracuda Web Application Firewalls.
- For information on Barracuda WAF-as-a-Service, refer to Overview - Barracuda WAF-as-a-Service.