Overview

The Barracuda Vulnerability Remediation Service, a free add-on to the Barracuda Web Application Firewall, 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) to protect new or existing applications. Deployment of the 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.

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.

What's New in Barracuda Vulnerability Manager Advanced

placeholder for release notes.

not yet published

Comparison with Barracuda Vulnerability Manager

Barracuda has two tools associated with web application vulnerabilities. The scanning engine in both tools is identical; the difference is in the additional capabilities provided beyond the scan.

This article helps you to distinguish between them and choose which one is right for you.

Barracuda Vulnerability Manager

The Barracuda Vulnerability Manager is a fast and easy way to assess the security of your web application. It is designed as an **informative** tool, determining and reporting your security status. It is free, easy-to-use, and requires no set-up.

If you ***do not have*** a Barracuda Web Application Firewall, use the Barracuda Vulnerability Manager to assess your security and help you understand how you can improve your web application security.

Barracuda Vulnerability Remediation Service

The Barracuda Vulnerability Remediation Service is a full-fledged tool that not only finds vulnerabilities, but remediates (fixes) them using the Barracuda Web Application Firewall. It also allows you to implement automated workflows to periodically scan your applications and mitigate newly-found vulnerabilities. It is included with your purchase of a Barracuda Web Application Firewall and requires use of the Barracuda Web Application Firewall.

If you ***have already purchased*** a Barracuda Web Application Firewall, use the Barracuda Vulnerability Remediation Service to simplify deployment and increase security.

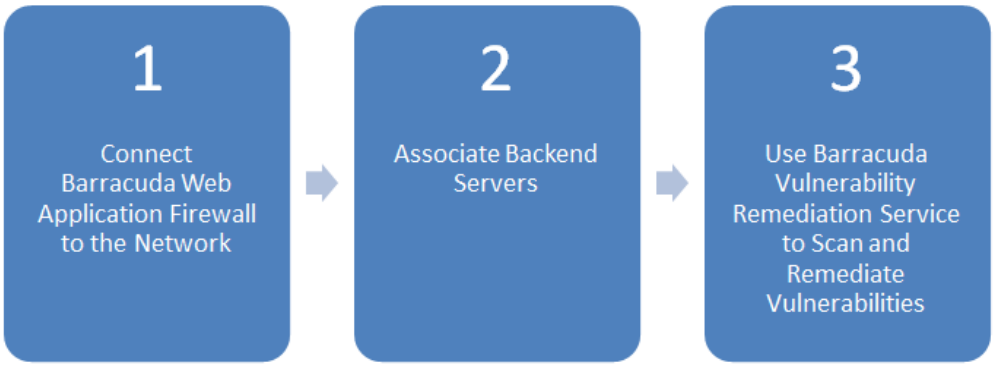
Feature Comparison

Feature	Barracuda Vulnerability Manager	Barracuda Vulnerability Remediation Service
Cost	Free	Currently available free of charge to customers who have purchased a Barracuda Web Application Firewall with an active Energize Update subscription.
Scan Scheduling	Users can schedule a single scan for a specified time.	Users can schedule any number of recurring scans (daily, weekly, monthly).
Vulnerability Reports	Users can view the report for a single scan.	Users can choose between two types of reports per scan: executive summary and technical detail report. Users can also view a consolidated Vulnerability view, which aggregates scan results across all scans of a single web application.
Mitigation Process	Manual: Users export the report from the scanner and import it into their WAF.	Automatic: Users can mitigate vulnerabilities on a Barracuda WAF with a single click from within the tool.
Mitigation Testing	None.	Users can apply a mitigation in “passive mode”, also known as “test mode.” In this mode, violations are logged, but not blocked. This allows the user to verify there are no false positives before enabling the mitigation in “active mode” or “block mode.” For more information, see Understanding Passive Mode and Active Mode .
Mitigation Automation	None.	Users can select one of three automation policies for new vulnerabilities: 1. **Manual**: Mitigations are not applied automatically. 2. **Passive Mode**: Mitigations are applied immediately in “passive mode,” so the user can confirm there are no false positives before applying them in “active mode.” 3. **Active Mode**: Mitigations are applied immediately in “active mode.”

Mitigation Monitoring	None.	Users can select a specific mitigation, and view Web Firewall logs from the Barracuda WAF that are related to that particular mitigation.
Email Notifications	Users can receive an email notification when a scan completes.	Users can receive an email notification either when a scan completes, or only when the scan detects new vulnerabilities. The email also contains a summary of the newly detected vulnerabilities.

Getting Started

There are three main steps to deploying the Barracuda Web Application Firewall and using it in conjunction with Barracuda Vulnerability Remediation Service to secure your web applications:

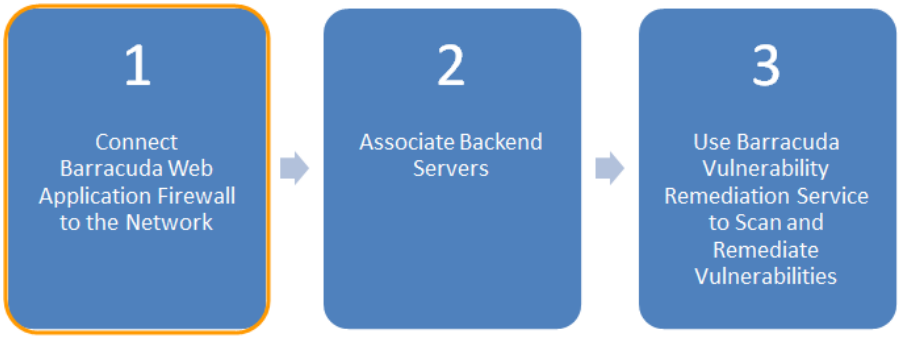


- Step 1: Connect the Barracuda Web Application Firewall to the Network
- Step 2: Associate Backend Servers
- Step 3: Scan and Remediate Vulnerabilities

Proceed to **Step 1:** Connect the Barracuda Web Application Firewall to the Network

Step 1: Connect the Barracuda Web Application Firewall to the Network

Step 1: Connect the Barracuda Web Application Firewall to the Network



In this step, assign the Barracuda Web Application Firewall an IP address for management, and verify it has access to the Internet as well as to the backend servers it protects.

Ensure it is running the latest firmware and has the latest security definition updates.

For detailed instructions on this step, consult the following Barracuda Campus articles:

Deployment	Barracuda Campus Article
Hardware Appliances	Step 1: Installing the Barracuda Web Application Firewall
Virtual Appliances	Barracuda Web Application Firewall Vx Quick Start Guide
Amazon Web Services (AWS) Instances	Barracuda Web Application Firewall Deployment and Quick Start Guide for Amazon Web Services
Microsoft Azure Instances	Deploying and Provisioning the Barracuda Web Application Firewall on Microsoft Azure
vCloud Air	VMware vCloud Air Deployment

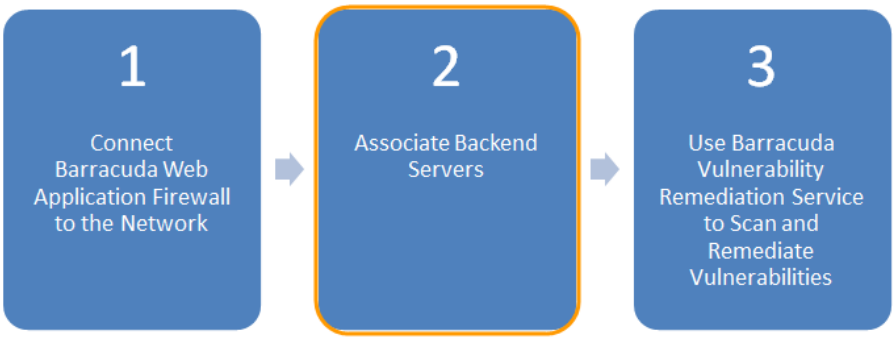
Connect the Barracuda Web Application Firewall to Barracuda Cloud Control

After you connect the Barracuda Web Application Firewall to the network, connect it to Barracuda Cloud Control as well. Connecting it to Barracuda Cloud Control allows you to control your Barracuda Web Application Firewall from the cloud, and also allows Barracuda Vulnerability Remediation Service to apply policy changes to secure your applications. For detailed instructions, refer to How to Set Up Barracuda Cloud Control in Barracuda Campus.

Continue to Step 2: Associate Backend Servers.

Step 2: Associate Backend Servers

Step 2: Associate Backend Servers



The Barracuda Web Application Firewall acts as a reverse proxy for your backend servers. That is, it listens for traffic on the (typically public) IPs that your users access, and forwards traffic to the application servers actually serving the requests. In this step, tell the Barracuda Web Application Firewall on which IPs to listen for traffic, and to which servers to forward legitimate traffic.

For detailed instructions on how to create services on your Web Application Firewall, refer to Step 2: Configuring a Service in the Barracuda Web Application Firewall section of Barracuda Campus.

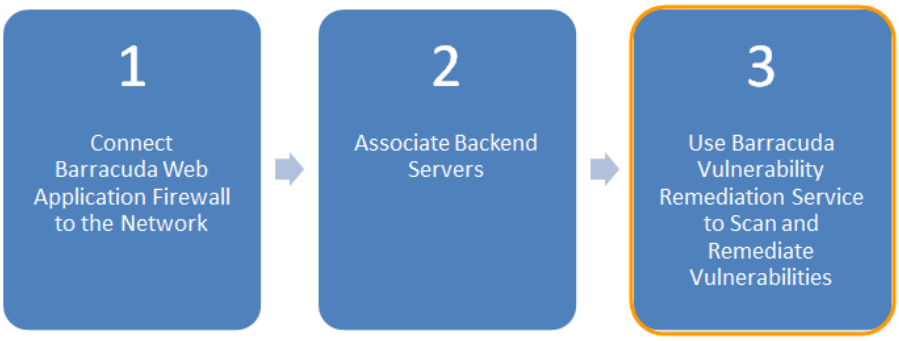
You may *initially* configure the service you created in Passive Mode, but you **must** switch it to Active Mode after verifying that the application runs properly. Passive Mode is intended for testing only; in Passive Mode, the Web Application Firewall *does not* secure your application.

Continue to Step 3: Scan and Remediate Vulnerabilities.

Step 3: Scan and Remediate Vulnerabilities

This article outlines the basic workflow for using the Barracuda Vulnerability Remediation Service. It is not just Step 3 in the setup process; it is a handy guide to the basic workflow you can use for reference.

Step 3: Use Barracuda Vulnerability Remediation Service to Scan and Remediate Vulnerabilities



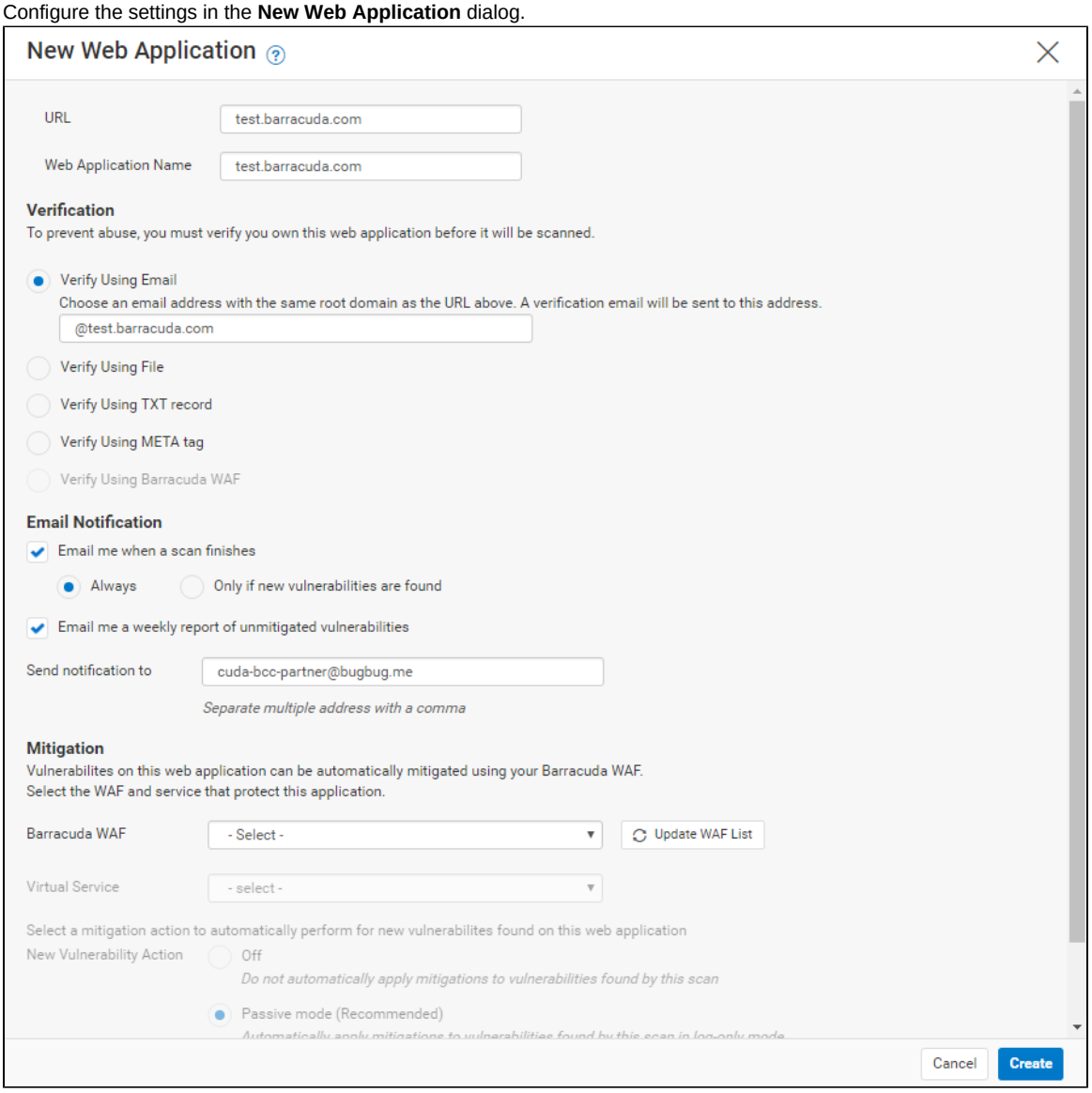
Configure the Barracuda Vulnerability Remediation Service to scan the application, and use the scan results to apply security policy changes on the Barracuda Web Application Firewall to secure your applications.

Log into the Barracuda Vulnerability Remediation Service

Log into the Barracuda Vulnerability Remediation Service at https://vrs.barracuda.com/, using the same email and password you used to connect your Barracuda Web Application Firewall to Barracuda Cloud Control in Step 1 above.

Run a Scan of the Application

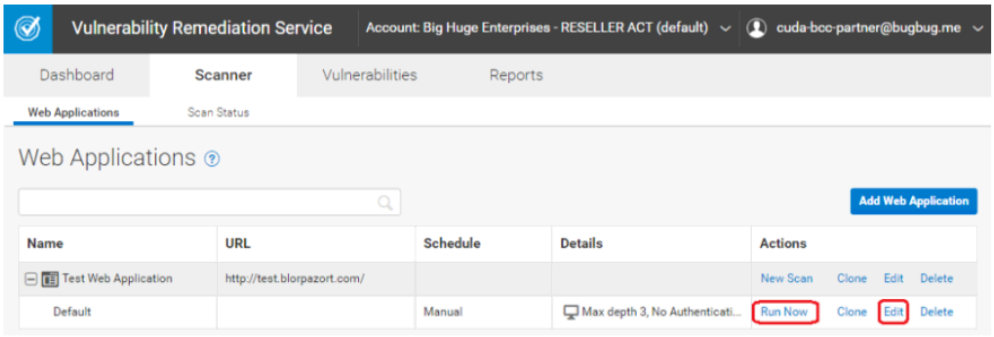
1. Navigate to the **Scanner > Web Applications** page. Click **Add Web Application**.
2. Configure the settings in the **New Web Application** dialog.



For more detailed information, refer to How to Create a New Web Application Scan.

a. Enter the publicly-accessible **URL** of your web application.
b. Enter a **Name** for the application.
c. Under **Verification**, select a method to verify that you are authorized to scan the application.
   - If you already have your Web Application Firewall set up correctly, select **Verify using Barracuda WAF**.
   - Otherwise, the easiest method is to specify an email address at the same domain. You will receive a verification email to this address with a link you must click to start the scan. If you do not have email set up, use a different verification method.
d. Under **Email Notification**, select your email notification preferences.
e. Under **Mitigation**, select the Web Application Firewall and Virtual Service that you created in Step 2: Associate Backend Servers .
f. Click **Create** to create the web application.

3. The **Web Applications** page refreshes to show the newly created application, along with a **Default** scan.
   - To edit scan settings, or schedule the scan for a particular time, click **Edit** on the scan.
   - To run the scan immediately, click **Run Now**.

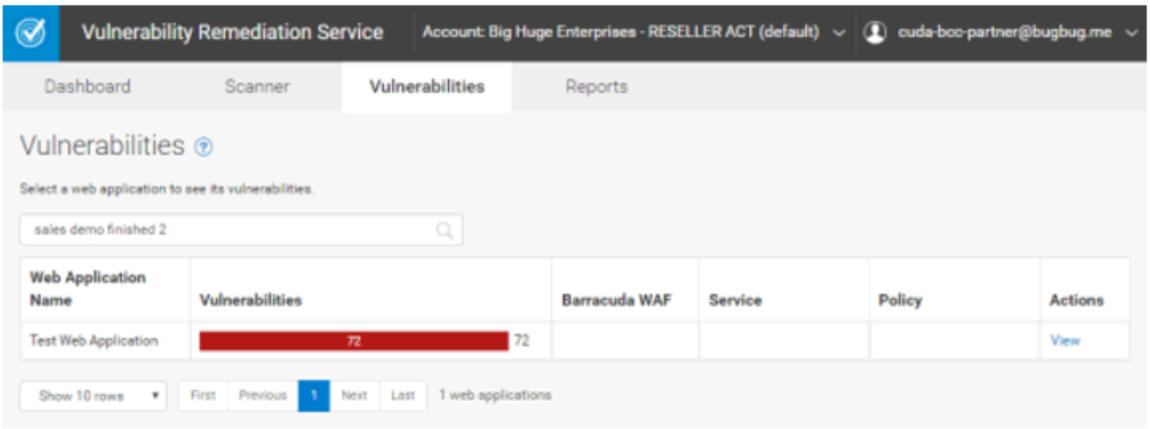


4. To track the progress of the scan, navigate to the **Scanner > Scan Status** page.
   If you enabled email notifications when creating the application, you will receive an email when the scan is complete.

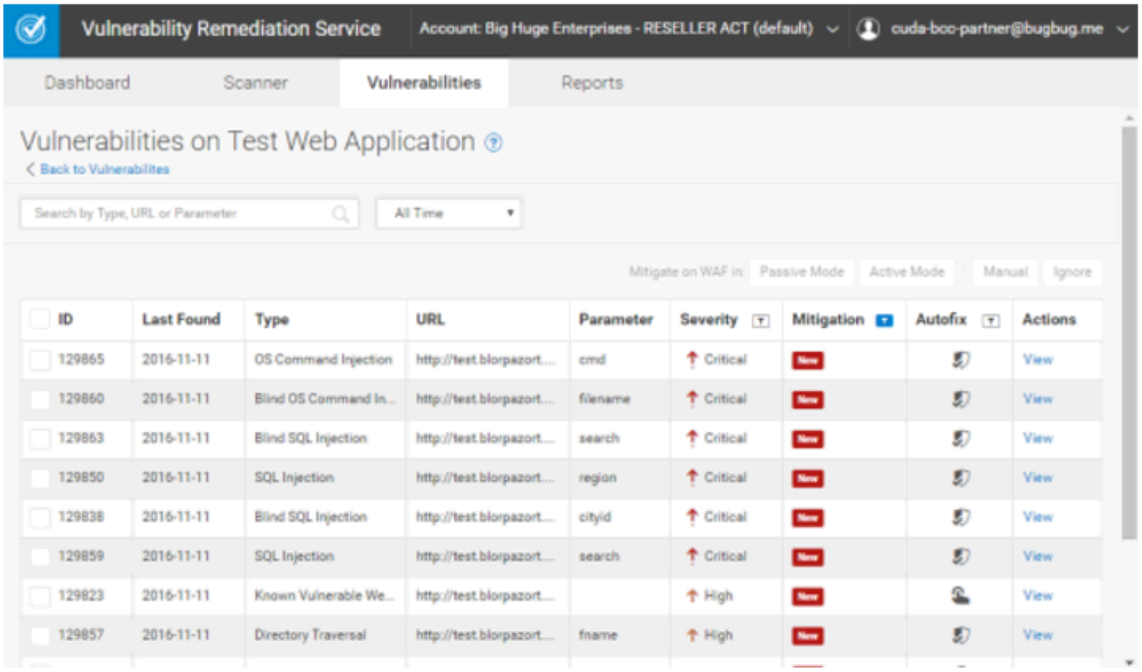
   For additional details, refer to Scan Status.

Review Vulnerabilities on the Application

1. When the scan is complete, navigate to the **Vulnerabilities** tab.
2. Click the name of the web application for which you want to view vulnerabilities.



3. Click on a vulnerability to view detailed information, including technical information on how the vulnerability was detected.



For additional details, refer to Vulnerabilities and How to Work with Vulnerabilities in the Vulnerability Details Page.

Fix Vulnerabilities

After you have reviewed the vulnerabilities, select the check box to the left of the vulnerabilities you want to fix and, next to **Mitigate on WAF in**, select **Active Mode**. Security policy changes will be applied to your Web Application Firewall to mitigate these vulnerabilities.

For additional details, refer to Vulnerabilities and How to Work with Vulnerabilities in the Vulnerability Details Page.

Video - Scan Your Web Application and Remediate Vulnerabilities

This video describes how to scan your web application and remediate vulnerabilities that are found in the scan.

Best Practices: Keeping Your Web Application Secure

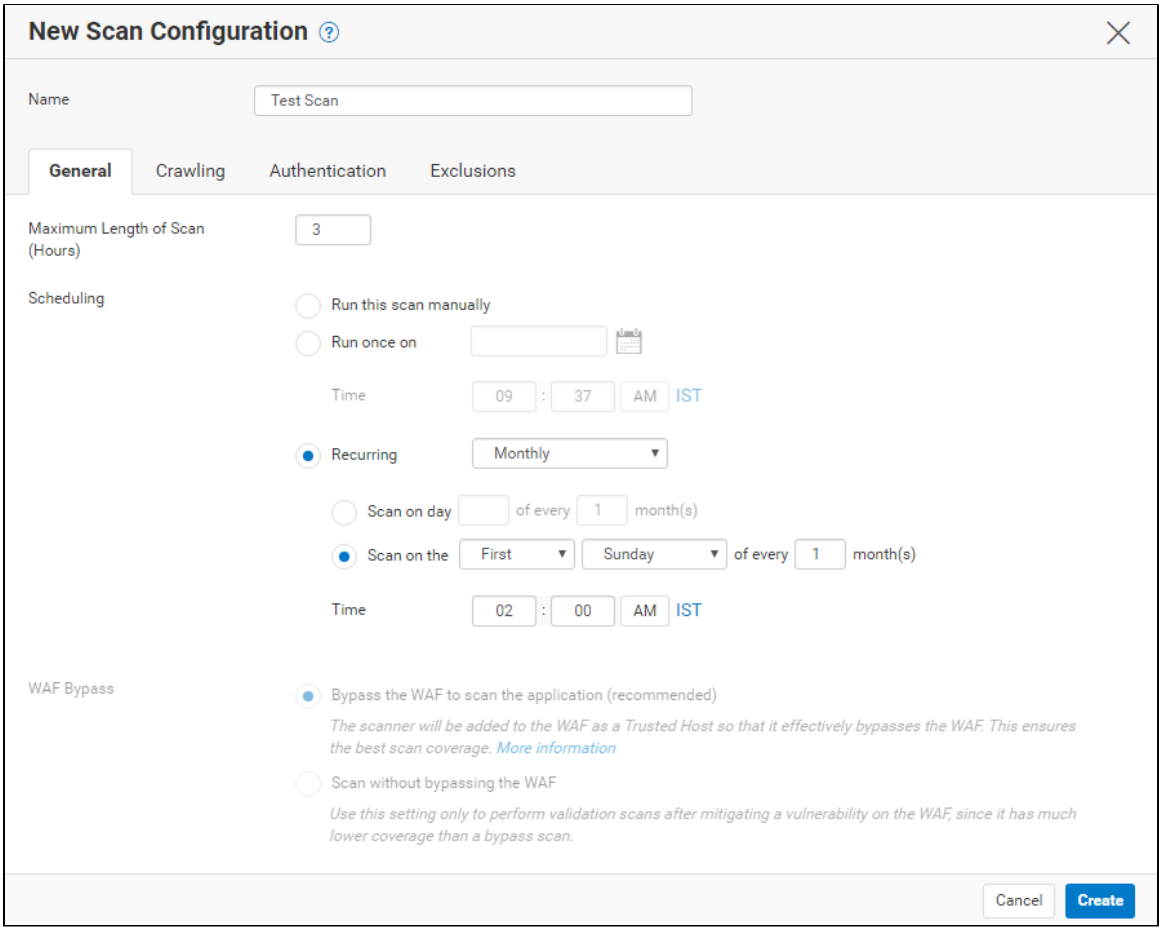
This article explains how to use the Barracuda Vulnerability Remediation Service to keep your application secure after deployment.

Scan Applications Periodically

The web application threat landscape is constantly evolving. New threats are constantly being discovered. To keep your application secure, scan your applications periodically to search for new threats.

> Barracuda recommends scanning your applications monthly.

You can use the Barracuda Vulnerability Remediation Service to scan your applications on a set schedule. For example, in the **New Scan Configuration** dialog below, we have configured the scan to run on the first Sunday of each month at 2:00 AM.



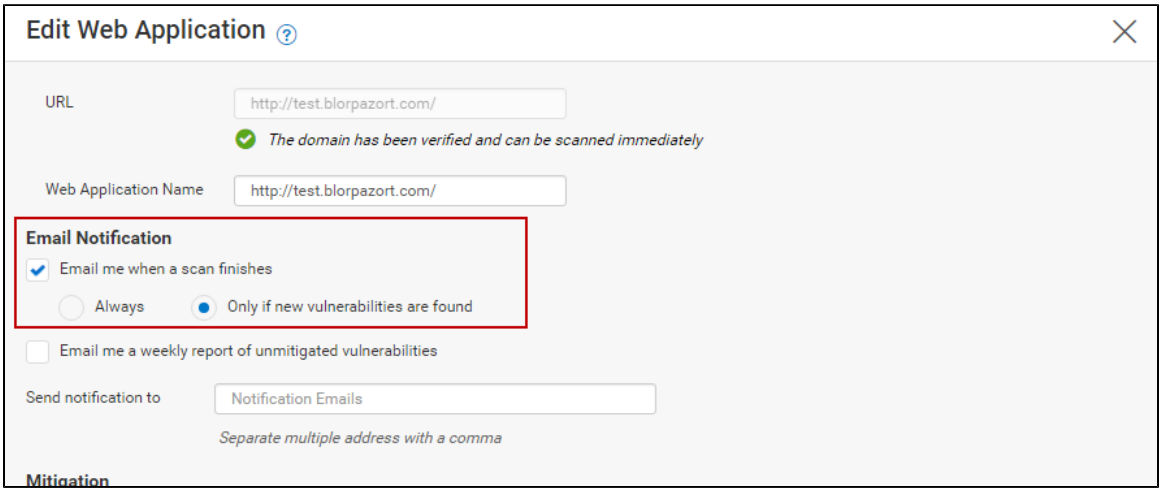
For additional information, refer to Actions on Existing Scans and Web Applications.

Scan Applications After Updates

In addition to scheduled periodic scans, it is important to scan your applications whenever you deploy new versions or make changes to the configuration. To quickly run a scan, navigate to the **Scanner > Web Applications** page, locate the scan you want to run, and click **Run Now**.

Enable Email Notifications

You can configure the Barracuda Vulnerability Remediation Service to send a notification to your email address whenever a new vulnerability is found during web application scans. This automatic email serves as an alert that the scanner found something new, so you do not have to check each scan. When you add or edit a web application on the **Scanner > Web Applications** page, select that you want to be notified when a scan finishes only if new vulnerabilities are found, as shown here:



For additional information, refer to How to Create a New Web Application Scan.

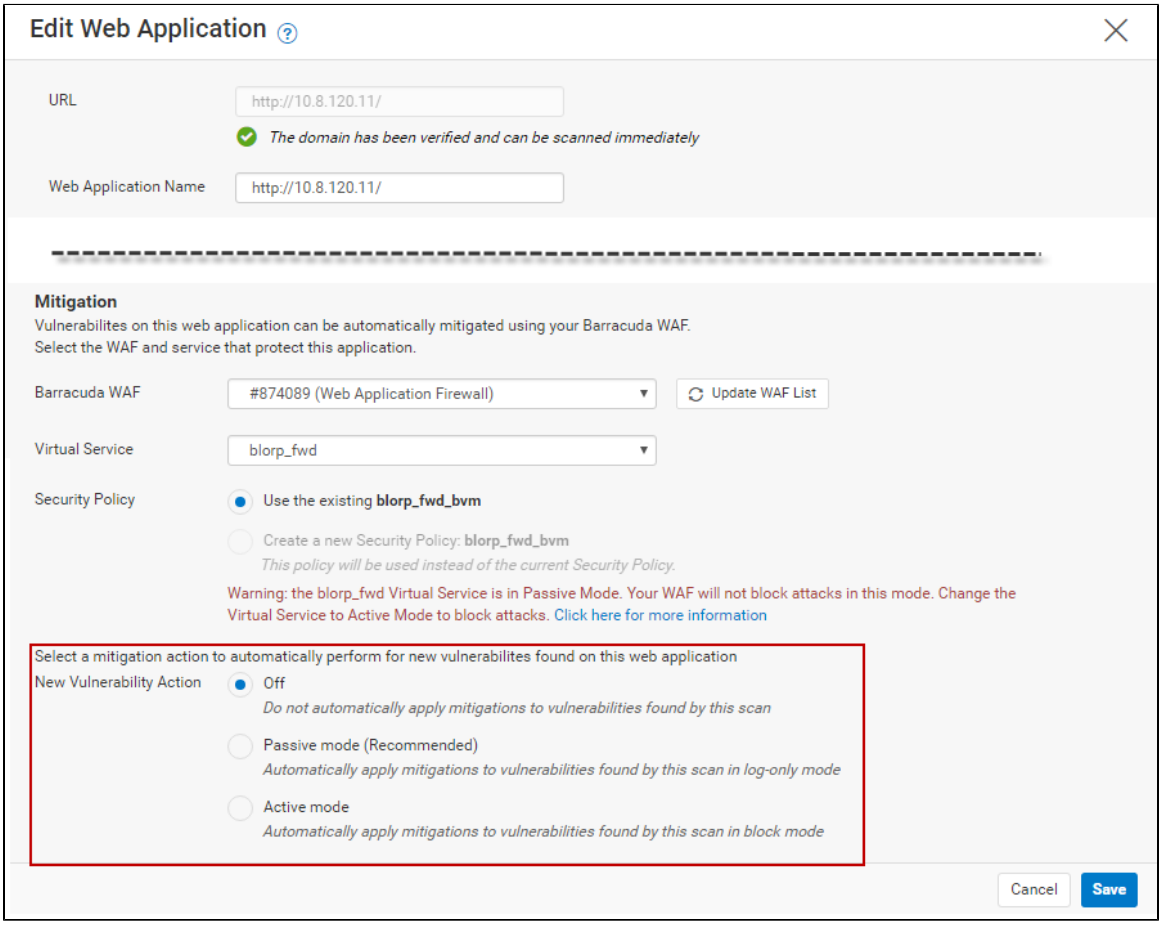
Automatic Remediation Policy

The Barracuda Vulnerability Remediation Service works in tandem with the Barracuda Web Application Firewall to automatically take action when a new vulnerability is discovered during a scan of your web application.

You can configure three possible actions when you add or edit the web application from the **Scanner > Web Applications** page:

- **Off** – Vulnerability Remediation Service notifies you if you have enabled email notifications, but takes no further action.
- **Passive Mode** – (Recommended) Vulnerability Remediation Service automatically applies security policy changes to your Web Application Firewall in passive mode. This logs violations, but does not block them, so no behavior changes on your site.
- **Active Mode –** Vulnerability Remediation Service automatically applies security policy changes to your Web Application Firewall in active mode. This blocks violations immediately.

> **Recommendation**
> Barracuda strongly recommends that you select automatic remediation in **Passive Mode**. Passive Mode allows you to manually audit the policy changes and verify no false positives are logged. After verifying, you can deploy the fix in Active Mode.



For additional information, refer to How to Create a New Web Application Scan and Vulnerabilities.

Recommended Workflow

Integrating the recommendations made earlier, Barracuda recommends the following workflow to keep your web applications secure:

1. When you configure your web applications:
    a. **Enable email notifications** to be sent when new vulnerabilities are discovered.
    b. Configure them to **scan automatically every month**.
    c. Select **Passive Mode** for your automatic remediation policy.
2. Run a **manual scan** every time you make significant changes to your application.

3. When a new vulnerability is discovered and you receive an email, wait 1-2 business days, then log in and look at the logs for that particular vulnerability, since it was fixed in Passive Mode. If you do not see any false positives or other issues, **fix the vulnerability in Active Mode**.

Understanding Passive Mode and Active Mode

The differences between these two modes, and where they are used, can be confusing. This article aims to clarify the differences between the two modes.

Where you can make the settings:

- In the **Barracuda Web Application Firewall**, you can **configure** a service (site) in two modes: *Passive Mode* and *Active Mode*.
- In the **Barracuda Vulnerability Remediation Service**, you can also **mitigate** a single vulnerability in either *Passive Mode* or *Active Mode*.

What the settings mean:

- **In Passive Mode**, the Barracuda Web Application Firewall monitors for security violations and logs them, but does not block them.

> **Important**
> In Passive Mode, the Barracuda Web Application Firewall **does not secure your application**. This mode is intended for temporary testing only.

- **In Active Mode**, the Barracuda Web Application Firewall monitors for security violations and blocks them, thereby ensuring they do not reach your server.

Barracuda recommends:

Mitigate vulnerabilities temporarily in *Passive Mode*, monitor the logs to ensure no issues arise, and then switch them to *Active Mode*.

For more information on the recommended workflow for the Barracuda Vulnerability Remediation Service, see Step 3: Scan and Remediate Vulnerabilities.

Note that **both** the service (site) and a particular vulnerability mitigation must be in *Active Mode* to block violations, as shown here:

Setting of Service (on Barracuda WAF)	Setting for Mitigating Vulnerability (on Barracuda Vulnerability Mitigation Service)	Effect
Passive Mode	Passive Mode	Passive Mode
Passive Mode	Active Mode	Passive Mode
Active Mode	Passive Mode	Passive Mode
Active Mode	Active Mode	**Active Mode**

Dashboard

Use the **Dashboard** to view summary information on vulnerabilities found in scanned web applications as well as to view scans in progress and those that have recently finished.

Vulnerabilities Over Time

Displays a bar chart of the number of vulnerabilities for each web application scanned over a period of time. If you are working on improving your website, these numbers should trend downward.

If you have been scanning several sites, the top three sites will be displayed, with other sites grouped together as "Others."

Click the name of a web application at the top of the chart to remove it from the chart, so you can focus on the other web applications. Click the name again to restore the web application data to the chart.

Scans In Progress

Displays a list of scans that are currently running or are pending, along with the percentage complete for each scan. Click **Show All** to go to the **Scan Status** page for more details.

Recently Finished Scans

Displays a list of the most recently completed scans, the date they were run, and the number of vulnerabilities found. Click a **URL** to go directly to the Report for the scan of that web application.

Scanner

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.

How to Create a New Web Application Scan

Use the steps in the article to define a scanner configuration in order to discover security risks in your website or website application.

Creating a Web Application

After you have completed the steps in Getting Started, navigate to the **Scanner > Web Applications** page. Complete the following steps to set up a website scan:

1. Click **Add Web Application**. The **New Web Application** dialog displays.
2. Enter a name to represent the scan. For example, `test site scan 1`.
3. Enter the URL you want to scan. For example, `test.MyCompany.com`.

   > For a sample scan and report, use the following URL: `test.blorpazort.com`

4. **Verification** – Verify that you own the domain of this web application in one of the following ways. Note that the scan cannot be

performed until the web application is verified.

- **Email** – The most common method of verification. Enter an email with the same root domain as the URL you want to scan. An email is sent to this address. You musts clink a link in the email to verify you are the owner of the domain.

  For the following options, make a specific, small addition to your DNS or site so the scanner can verify you are the owner. These changes will not be noticeable or affect your site.
- **File** – Add a text file with the specified name and content under the site to be scanned.
- **TXT Record** – Add a TXT record with the specified content to the domain DNS.
- **META Tag** – Add a META tag with the specified content within the <HEAD> tag of the site's home page.
- **Barracuda WAF** – This option is available if you are using a Barracuda Web Application Firewall. Select the option and the name of the Barracuda Web Application Firewall. The scanner uses the Barracuda Web Application Firewall to determine you own the URL to be scanned.

  In some rare situations, you might not be able to verify that you own the web application. Refer to How to Request a Manual Domain Verification for details.

5. **Email Notification** – Specify if and how you want to be contacted by email after scans.
   - **Email me when a scan finishes** – Select this check box to be notified when scans complete.
     - Select **Always** to be notified after every scan.
     - Select **Only if new vulnerabilities are found** if you want to be notified only when new vulnerabilities are detected in a scan.
   - **Email me a weekly report of unmitigated vulnerabilities** – Select this check box to receive weekly reports of unmitigated vulnerabilities.
   - **Send Notification to** – Enter one or more email addresses, separated by commas.
6. **Mitigation** – If you are using a Barracuda Web Application Firewall, complete this section. Refer to Barracuda Web Application Firewall d ocumentation for details.
   - **Barracuda WAF** – Select the Barracuda Web Application Firewall you want to use. If you have recently added or changed a Web Application Firewall, click **Update WAF List** to ensure that your changes are reflected in the list.
   - **Virtual Service** – Select the service on the Barracuda Web Application Firewall you want to use to protect this application. A Virtual Service is a combination of a Virtual IP (VIP) address and a TCP port, which listens and directs the traffic to the intended Service.
   - **Security Policy** – Select whether to use the existing Security Policy within the Barracuda Web Application Firewall, or whether you want to create a new one. A Security Policy determines what action to take when one or more of the rules match the request.
   - **Mitigation** – Select if and how to mitigate the vulnerabilities found by the scan.
     - **Off** – No action will be taken automatically. You will manually mitigate any vulnerabilities found.
     - **Passive Mode** – (Recommended) Vulnerability Remediation Service automatically applies security policy changes to your Web Application Firewall in Passive Mode. This logs violations, but does not block them, so no behavior changes on your site.
     - **Active Mode** – Vulnerability Remediation Service automatically applies security policy changes to your Web Application Firewall in Active Mode. This blocks violations immediately.

     > **Recommendation**
     > Barracuda strongly recommends that you select automatic remediation in **Passive Mode**. Passive Mode allows you to manually audit the policy changes and verify no false positives are logged. After verifying, you can deploy the fix in Active Mode.
7. Click **Create**.
   The new Web Application you created appears in the **Web Applications** table.
   By default, Web Applications appear in this table in order of creation date, with the Applications most recently added to the end of the list.
8. Repeat steps 1-7 to set up additional Web Applications.
   Continue with the steps below to set up scans for this Web Application.

Creating a Scan for this Web Application

After you have specified the Web Application you want to test for vulnerabilities, you must create specific scans to perform.
By default, a basic scan is configured for you. It is named ***Default*** and appears below the Web Application in the Web Application table.

For this Web Application, you can:

- **Edit the default scan**: In the table row for the default scan, click **Edit**.

- **Create a new scan**: In the table row for the Web Application, click **New Scan**.

Refer to Actions on Existing Scans and Web Applications for details.

How to Request a Manual Domain Verification

In some cases, you might need to request a manual domain verification from Barracuda.

To request a manual domain verification, email VRS_Support@barracuda.com.

In your message, include the following information:

- your Barracuda Cloud Control email address
- the domain(s) you want to scan
- an explanation of the ownership of the domain
  Barracuda will usually verify a domain manually in these cases:
  - The domain is very similar to another domain that does have email set up. For example, your email address is example.com, but you are scanning example.co.uk.
  - The domain's whois record refers to a different domain that you can verify using an email address.
  - The Contact page of the site refers to a different domain that you can verify using an email address.

Verifying an IP Address or Range of IP Addresses

You may request manual verification of an IP address or range of IP addresses. In this case, you or your organization must be listed as owning this IP range in ARIN.

Actions on Existing Scans and Web Applications

After you have created one or more web applications and/or scans, there are additional actions you can take with them. For example, after you have set up the original scan, you can create other related scans while impersonating different devices or different schedules.

Working with Scans

All of these actions are performed from the **Scanner > Web Applications** page.

Run an Existing Scan

You can manually start a scan from this screen.

Locate the desired scan in the **Web Applications** table. In the **Actions** column, click **Run Now**. The scan begins immediately.

Cancel a Scan in Progress

If a scan is currently running, a **Cancel** link displays first in the **Actions** column.

For the target scan, click **Cancel**. The scan will stop when it finishes the operation currently in progress.

Create a New Scan; Clone or Edit an Existing Scan

- **To create a new scan**, locate the desired web application to scan in the **Web Applications** table. In the **Actions** column, click **New Scan**.
- **To Edit an existing scan**, locate the desired scan in the **Web Applications** table. In the **Actions** column, click **Edit**.
- **To Clone an existing scan**, locate the desired scan in the **Web Applications** table. In the **Actions** column, click **Clone**.
  - Be sure to enter a new **Name** for this scan to distinguish it from the original scan.
  - Cloning a scan is faster than creating a new scan if you are making only minor changes. For example, you might choose to clone a scan to:
    - change the crawling method, to scan the same web application on the same schedule, for both the desktop and mobile sites.
    - change the schedule, to perform identical scans on both the 1st and 15th of each month.

In the **New/Edit/Clone Scan Configuration** window, select each tab, in turn, and complete the information. When you have finished, click **Save**.

Select the General Tab

1. Type, or edit, the **Name** of the scan.
2. In the **Maximum Length of Scan (Hours)** field, you can specify a scan duration limit. For example, for a large site, limit the scan duration for faster results. If you shorten the time of the scan, you might not see results for the deeper levels of your web application.
3. Specify the **Scheduling** for this scan:
    a. **Run this scan manually** – When selected, you must manually start this scan. For configured scans, locate the desired scan on the **Scanner > Web Applications** page, and click **Run Now**.
    b. **Once** or **Recurring** – When selected, you specify the date and time that the scan is to start. Options for **Recurring** include **Daily** , **Weekly**, and **Monthly**.
    If the time zone shown is not correct, click its link. The **Barracuda Cloud Control Profile** page opens in a new browser tab. Set your time zone, then return to the **Barracuda Vulnerability Remediation Service** tab of your browser. Although the time zone update might not immediately display on the **Scanner Configuration** page, the correct time zone information will be used for the scan.
4. In the **WAF Bypass** section, specify whether to bypass the Web Application Firewall 's security policies to perform the scan. If you do not have a Web Application Firewall associated with the application, this option is disabled.
    - Select **Bypass the WAF to scan the application (recommended)** to enable the bypass. This increases the accuracy of your scan results.
    - Select **Scan without bypassing the WAF** to disable the bypass. Use this option only if you are running a compliance scan for audit purposes, because it might not find vulnerabilities that exist on your application.

Select the Crawling Tab

1. Select the type of scan you want:
    - **Scan Desktop Site –** Select **Firefox**, **Chrome**, **Safari**, or **Internet Explorer**.
    - **Scan Mobile Site –** Select **iPhone, iPad, or Android**.
    - **Scan using a custom browser** – To use a custom browser, specify the appropriate information in this field.
2. **Requests per second** – Specify the number of requests per second the scanner can make. Enter **0** (zero) to send the maximum requests your server can manage.

    > A value of **0** (zero) is not recommended if you are setting up a scan on a *production server*.
    >
    > If you are running a scan on a *non-production server*, consider increasing the speed of the scan to as fast as the server can respond, so you will receive scan results more quickly.
    >
    > If Barracuda Vulnerability Remediation Service detects that it is starting to overwhelm your server, it will automatically throttle the number of requests per second. You cannot disable this feature.

3. **Maximum crawl depth** – Specify the maximum link depth from the start page. A value of zero means only the home page will be scanned; the first layer of links is a value of 1, and so on.
4. Select the **Enable evasion techniques** check box if you want the scan to attempt to "confuse" sanitizing or filtering code in your web application during the scan.

    > When **Enable evasion techniques** is activated, scanning takes approximately four times as long to complete as a normal scan.

Select the Scan Elements Tab

Select specific scan elements you want to include or exclude from the scan. Each scan element finds a certain set of vulnerabilities. For your first scans, select all of the elements for a thorough check of your web application. If there are certain vulnerabilities you are investigating, select only those elements.

Note: For the most thorough scans, select all scan elements.

Select the Authentication Tab

> Do not enter administrator credentials when scanning a production site. See Avoiding Possible Scanning Side Effects for details.

Specify whether to scan the parts of your site accessible only by a user who has logged in. Select from the following three options:

1. **No authentication** – Select if you do not want to scan these areas of your website.
2. **HTTP authentication –** Select to scan areas of your website requiring login credentials. Click the HTTP authentication type used by your website, and then enter the associated **Username** and **Password**.
   Use this option for HTTP Basic authentication, HTTP Digest authentication, and NTLM authentication.
3. **HTML form-based authentication** – Select if your web application has a standard HTML login form that submits to the web server using HTTP POST.
   a. Enter the **Username** and **Password** for the site.
   b. Enter the **Login form URL**, along with your associated username and password. Then, click **Autodetect** to automatically complete the rest of the fields in the section. Alternatively, you can enter the information manually.
   c. Click **Test Authentication** to verify the information you entered is correct and the test will run as expected.

Select the Exclusions Tab

Use the **Exclusions** tab to define hostnames, IP addresses, URL patterns, and file extensions that you do not want the scanner to test for vulnerabilities.

Note that, by default, all images and videos are excluded.

- **To exclude a hostname, IP address, URL pattern, or file extension**:
  Enter the information into the correct segment of the page, then click **Add**.
- **To remove an exclusion**:
  - Click the X next to the exclusion you want to remove.
  - Click **Remove All** to remove all of the exclusions within a section of the page.

> If you have unprotected forms that write data to a database or send emails based on form submissions, you might 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.

Delete an Existing Scan

This action permanently deletes a scan from the Barracuda Vulnerability Remediation Server.

1. Locate the desired scan in the **Web Applications** table. In the **Actions** column, click **Delete**.
2. Confirm that you want to delete the selected scan. This will permanently delete the scan.

Note: If you think you might use a scan again in the future, you can keep it as a manually scheduled scan and run it when you need it.

Verify an Existing Scan

You must verify that you are the owner of the web application before you can scan it. If you created a scan, but it has not yet been verified, an orange triangle  and **Verify** link display in the **URL** column.

1. Click the **Verify** link.
2. In the **Verify** window, choose a method of verification, as described in How to Create a New Web Application Scan.
   - If you specified email, double-check the email address you entered, correct it if needed, then click **Resend Email**.
   - For other methods, select the appropriate method and take the appropriate action on your web application. Then click **OK**.

Working with Web Applications

All of these actions are performed from the **Scanner > Web Applications** page.

Create a New Web Application

See How to Create a New Web Application Scan.

Clone or Edit an Existing Web Application

Goal	Steps

Edit an existing web application	1. Navigate to the **Scanner > Web Applications** page. 2. In the **Web Applications** table, locate the Web Application you want to edit. 3. In the **Actions** column, click **Edit**.

Clone an existing scan	1. Navigate to the **Scanner > Web Applications** page.
	2. In the **Web Applications** table, locate the Web Application you want to clone.
	3. In the **Actions** column, click **Clone**.
	• Be sure to enter a new **Name** for this Web Application to distinguish it from the original scan.
	• Cloning a Web Application is faster than creating a new scan, if you are making only minor changes. For example, you might choose to clone a Web Application to:
	  ◦ use the same configuration to scan a different Web Application that you own.
	  ◦ maintain all configured scans in a second copy of a site, for example, a staging copy.

In the **Edit/Clone Web Application** window, complete the required information. When you have finished, click **Save**.

Scan Status

The **SCANNER > Scan Status** page lists each scan that is currently running or is scheduled to run in the future. From this page, you can view the scheduled scan date and current status and take action with the scans.

Viewing Scheduled Scans

Click the plus sign to the left of the web application name to display its associated scans.

The **Schedule** and **Details** columns display basic information about the scan. To edit the scans, go to the **SCANNER > Web Applications** page and follow the directions in Actions on Existing Scans and Web Applications.

Scan Status

For scans scheduled to run in the future, the **Status** column displays the date and time of the next scan.

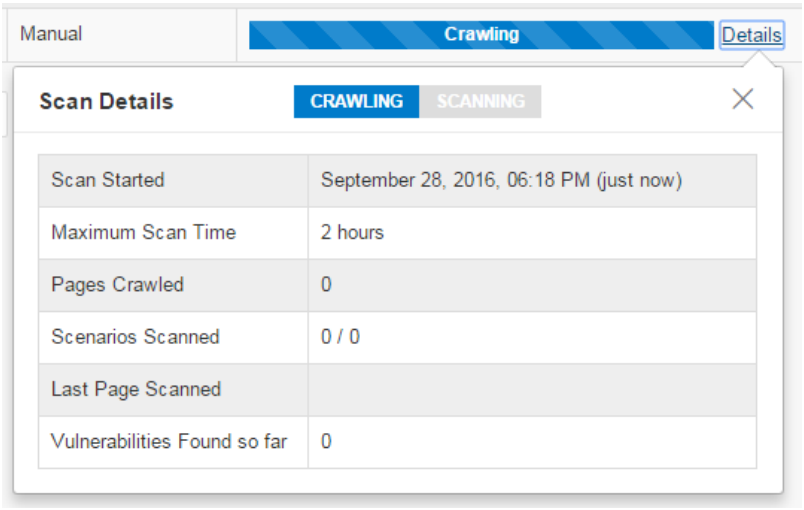
For scans that are currently running, the **Status** column displays the Scan Stage and an animated bar showing the scan progress.

Scan Stages

There are two stages to a scan, *Crawling* and *Scanning.*

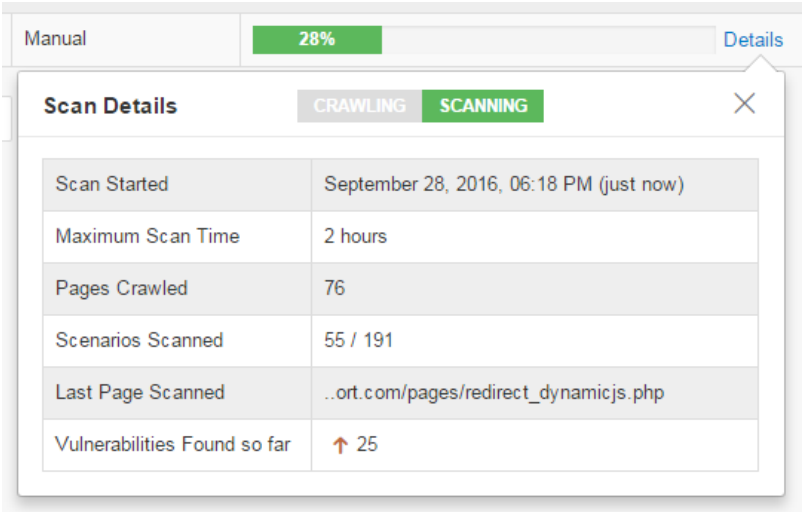
Crawling Stage

The Crawling stage is the discovery mode. During this stage, the scan examines the entire site map, cataloging all pages, forms, and files on the site. During this phase, the scan time duration bar in the **Status** field on the **Active Scans** page displays as indeterminate:



Scanning Stage

After the discovery is complete, the scan begins, and the scan progress indicates the percentage of the scan that has completed:



Completed and Cancelled Scans

The **Status** column displays **Finished** or **Canceled**, depending on how the scan ended. Links are available:

- **See finished scan** – Opens the **Reports** page for that web application. Locate the desired scan, then click **View** or **Download** to see the results.
- **Details** – Opens the details window, showing basic information about the scan.

Taking Actions with Scans

Run Now

To start a scan immediately, click **Run Now**.

This action does not affect future scans that are already scheduled. It only adds the scan you just requested.

Skip Occurrence

Click **Skip Occurrence** to skip a single occurrence of a scheduled scan. The scan time will change to the next scheduled occurrence. For example, if you skip a weekly scan, it will run the following week.

Cancel a Scan

Click **Cancel** to stop the scan. You can cancel a scan that is scheduled, but is not running yet, or a scan that is actively running. When you cancel a running scan, the scanner finishes its current scenario and aborts. Note that this might take a few minutes, depending on the length of the current scenario.

Refer to Actions on Existing Scans and Web Applications for additional actions you can take.

Vulnerabilities

The **Vulnerabilities** page is an overview, showing the number and type of vulnerabilities found on each web application.

Searching for Web Applications

To refine the list of web applications, begin typing in the **Search** field, or use the navigation tools to move through the list. You can search by Web Application Name, associated Barracuda Web Application Firewall (WAF), or Service.

Web Application Table

The Web Application table includes:

- **Web Application Name** – The name of your Web Application that is being scanned.
- **Vulnerabilities** – A graphical representation of the number of vulnerabilities found in the web application. The total number of vulnerabilities is shown to the right of the bar in the **Vulnerabilities** column. For example:

  Within the bar, colors represent how the vulnerability is currently mitigated:

  - New **Red / New** – All vulnerabilities start as **New**. After you change a **New** vulnerability to a different category, you cannot change it back to **New**.
  - Active Mode **Green / Active Mode** – Active Mode. Performs the action configured in association with the perceived threat.
  - Passive Mode **Yellow / Passive Mode** – Passive Mode. Logs violating events and allows the request to pass through.
  - Manual **Blue / Manual** – Enables you to mitigate the vulnerability manually.
  - Ignored **Grey / Ignored** – Does not take any action with this vulnerability, and marks it to be ignored.

  For details on using Active and Passive Mode, refer to Understanding Passive Mode and Active Mode.
- **Barracuda WAF** – The name of the Barracuda Web Application Firewall associated with this scan, if any.
- **Service** – The service on the Barracuda Web Application Firewall associated with this scan, if any.
- **Policy** – The security policy on the Barracuda Web Application Firewall associated with this scan, if any.

Click **View**, or anywhere in the row, to open the **Vulnerabilities on <Web Application>** page for vulnerabilities found on a specific web application, described in the next section.

Vulnerabilities on <Web Application> Page

This page displays all vulnerabilities for a specific web application.

The Vulnerabilities table displays the following information about each vulnerability:

- **ID** – A unique identifier for each specific vulnerability in a specific web application.
- **Last Found** – Date the vulnerability was last found on this web application. This can be the date of the last scan or earlier. If the date is earlier, then the vulnerability was not found in this latest scan and was likely mitigated.
- **Type** – The category of this vulnerability.
- **URL** – The specific URL within the web application that is affected by this vulnerability.
- **Parameter** – The specific parameter that is affected by this vulnerability, if any.
- **Severity** – How serious the threat is to your web application. Levels include Critical, High, Medium, Low, and False Positive.
- **Mitigation** – How this vulnerability is currently mitigated. Refer to the color chart description above.
- **Autofix** – Whether the vulnerability can be fixed automatically by the Barracuda Web Application Firewall. Some vulnerabilities cannot be

mitigated automatically and require manual user input to fix. Click a vulnerability for more specific details.

- **Actions** – Click **View**, or anywhere in the row, to learn more about a specific vulnerability and edit certain attributes. Refer to How to Work with Vulnerabilities in the Vulnerability Details Page.

Filtering Vulnerabilities

Control which vulnerabilities are displayed in the Vulnerabilities table by searching and filtering.

- **Search field** – Use the **Search** field to search for Type, URL, or Parameter for the vulnerability.
- **Time frame** – Specify the time frame of when the vulnerability was last found.
- **Filtering by Severity** – Click the arrow at the top of the **Severity** column to select which **Severity** levels to display. Select any or all check boxes to choose which Severity levels to display.
- **Filtering by Mitigation**– Click the arrow at the top of the **Mitigation** column to select which **Mitigation** types to display. Select any or all check boxes to choose which Mitigation types to display.

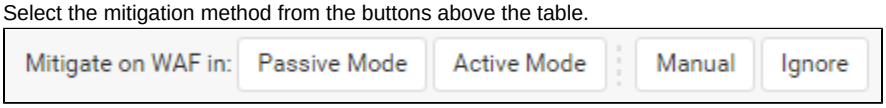
Note that if you are too restrictive with your searching and/or filtering, there might not be any results to display. Broaden your search and/or filtering criteria to display some results.

Click **View**, or anywhere in the row, to open the page for a specific vulnerability found on this specific web application.

Updating Mitigation Method for Multiple Vulnerabilities

You can mitigate multiple vulnerabilities on the Barracuda WAF in bulk without having to open the **Vulnerability Detail** window for each one. You can also remove mitigations for multiple vulnerabilities.

1. Select the check box to the left of the **ID** for one or more vulnerabilities. To select all vulnerabilities, select the check box next to the **ID** in the heading row.
2. Select the mitigation method from the buttons above the table.



   Note that if you are selecting multiple vulnerabilities at once, the same selection will apply to all of the selected vulnerabilities.
3. A dialog appears, explaining what your proposed change entails. Click **Confirm** to assert that you understand the implications of the change. The change is then made on the Barracuda Web Application Firewall.

How to Work with Vulnerabilities in the Vulnerability Details Page

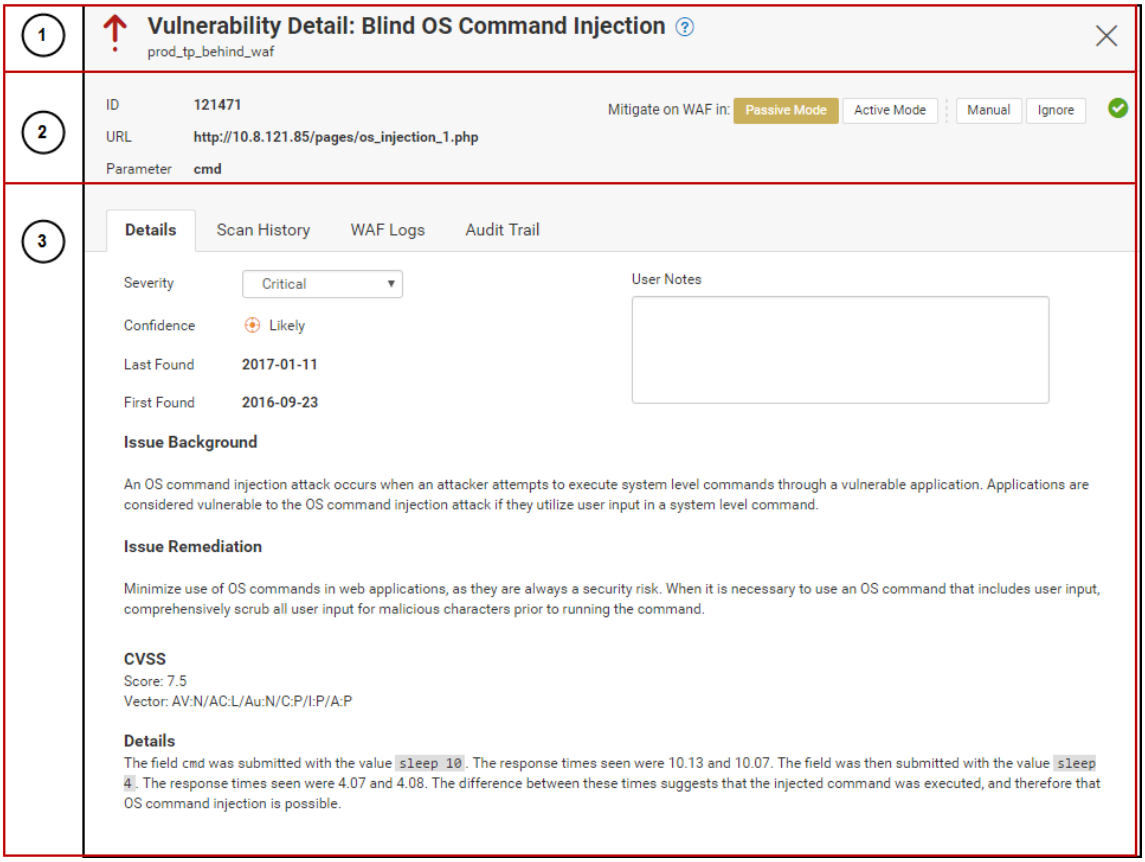
You can work with some attributes of a vulnerability in the **Vulnerability Detail** window.

To navigate to the **Vulnerability Detail** window:

1. Click the **Vulnerabilities** tab.
2. On the **Vulnerabilities** page, locate the web application you want to work with. Click **View** or anywhere in the associated table row.
3. On the **Vulnerabilities on <web application name> page**, locate the vulnerability you want to work with. Click **View** or anywhere in the associated table row.
   The **Vulnerability Detail** window for that specific vulnerability appears.

The **Vulnerability Detail** window displays details about one specific vulnerability found within the scan.

This window includes the following information. Numbered regions correspond to numbered sections in the article below.



1. Title Section

The title section of the page includes:

- The name of the vulnerability.
- The web application on which it was found.
- An icon indicating the severity of the vulnerability.

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	You have marked this vulnerability as a False Positive

2. Basic Information

The main section of the page includes information from the overview page:

- **ID** – A unique identifier for each specific vulnerability in this specific web application.
- **URL** – The specific URL within the web application that is affected by this vulnerability.
- **Parameter** – The specific component of the web application that is affected by this vulnerability.
- ***Mitigate on WAF in** – How this vulnerability is mitigated. You can change the selection here, if you choose.
  All vulnerabilities start as New, without a category. After you change a new vulnerability to a different category, you cannot change it back

to **New**.

- 

Green / Active Mode – Performs the action configured in association with the perceived threat.
- 

Yellow / Passive Mode – Logs violating events and allows the request to pass through.
- 

Blue / Manual – Enables you to mitigate the vulnerability manually.
- 

Grey / Ignore – Does not take any action with this vulnerability, and marks it to be ignored.

For details on using Active and Passive Mode, refer to Understanding Passive Mode and Active Mode.

*Editable fields. Your changes are saved in the system so they appear wherever these fields appear.

3. Tabs

Details Tab

The **Details** tab includes detailed information about the vulnerability and includes editable fields.

Information on the **Details** tab:

- ***Severity** – How serious the threat is to your web application. Levels include **Critical**, **High**, **Medium**, **Low**, and **False Positive**. You can change this value based on your assessment of the severity level.
- **Confidence** – How likely it is that your website has this vulnerability. Confidence levels include **Certain**, **Likely**, and **Possible**.
- **Last Found** – The date of the most recent scan in which this vulnerability was found.
- **First Found** – The date of the first scan in which this vulnerability was found.
- ***User Notes** – A free-form field where you can add your own notes about the vulnerability.
- **CVSS** – The National Vulnerability Database's Common Vulnerability Scoring System score and vector. Refer to https://nvd.nist.gov/cvss.cfm for details.
- **Details** – Describes, in detail, how the scanner detected this vulnerability.

*Editable fields. Your changes are saved in the system, so they appear wherever these fields appear.

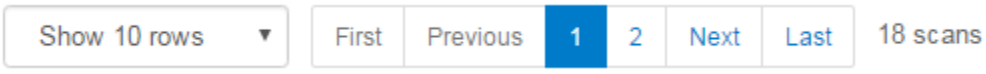
Scan History Tab

The **Scan History** tab shows the status of this vulnerability in scans of this web application, from the scan with the **First Found** date to the scan with the **Last Found** date.

Information on the **Scan History** tab:

- **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.

Below the table, you can see the total number of scans between the **First Found** and **Last Found** dates. You can choose how many rows of the table you want to show and navigate through the list with the navigation buttons.



WAF Logs Tab

The **WAF Logs** tab shows log information from the Barracuda Web Application Firewall associated with this scan.

Information on the **WAF Logs** tab:

- **Date** – Date the scan was run, in the form Year-Month-Day.
- **Time** – Time the scan was run, in the form Hours:Minutes:Seconds:Milliseconds.
- **User Agent** – The name and version of the browser or other client software making the request.
- **Client IP** – The IP address of the client that originated the request.
- **Method** – The HTTP method used by the request.
- **Action** – The action to be taken for a particular type of web attack.
- **Query String** – The query part of the request.

Audit Trail Tab

The **Audit Trail** tab shows all activity associated with this vulnerability, including when it was created and any changes to the mitigation method.

Information on the **Audit Trail** tab:

- **Time** – Date and time the action was performed. Most recent events are listed at the top of the table.
- **User** – The username responsible for the action.
- **Action** – A brief description of the action taken and whether it was successful.

Reports

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. Barracuda Vulnerability Remediation Server reports contain a comprehensive set of details to help your web application developers determine how to resolve existing vulnerabilities.

Here is a sample report PDF to give you an idea of the information provided by a scan. This report was generated using the **Include technical vulnerability details** option. Selecting this option provides additional details that are suitable for engineers working on the application code; without technical detail, the report is more suitable to IT professionals and those who are not working on code.

In this section

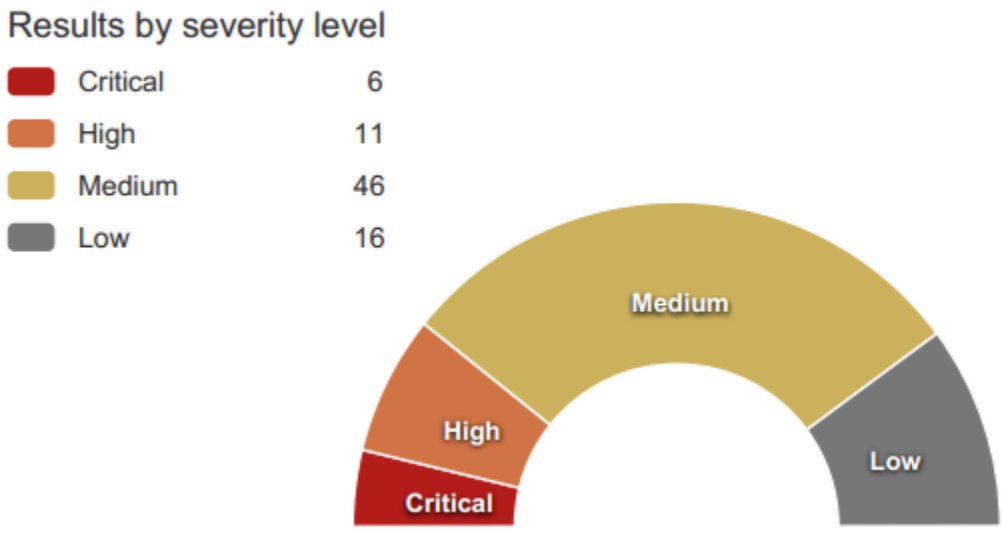
Understanding Barracuda Vulnerability Remediation Service Reports

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.

> **Important**
> 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 <Web Application>** 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.

How to Customize Reports

Customizing the Report Header

You can customize the top of the first report page with your logo or other image and your name.

1. Click **Customize Web Application Reports** to display the customization window.
2. Click **Browse** to upload an image. Note that image must be a PNG, GIF, or JPG that is less than 50kB in size.
3. In the **Tagline** field, add a tagline for your organization.
4. Click **Save**. Then click **Hide Customize Options**.

Your custom header displays at the top of the report.

Tips and Troubleshooting

These articles contain information on common problems and how to fix them.

In This Section

In Other Sections

Allowing Barracuda Vulnerability Remediation Service IP Addresses

If you have any protection elements on your network, like a firewall, they might mistakenly block the Barracuda Vulnerability Remediation Service, thinking it is creating malicious traffic.

Before running any scans, Barracuda Networks recommends that you add the IP addresses used by the Barracuda Vulnerability Remediation Service to your allow list, or whitelist.

Note: If you are using a Barracuda Web Application Firewall, this step is performed automatically by default. See the **WAF Bypass** section of Actions on Existing Scans and Web Applications for more information.

How to Allow Barracuda Vulnerability Remediation Service IP Addresses

Consult the technical documentation associated with your protection element for instructions on allowing an IP address.

Allow the following IP addresses:

- 64.235.153.133
- 64.235.153.134
- 64.235.153.135
- 64.235.153.136
- 64.235.150.121

Why Allow Barracuda Vulnerability Remediation Service IP Addresses

A network protection element, like a firewall, web application firewall (WAF), or intrusion detection/prevention system (IDS/IPS), typically cannot distinguish between an actual malicious user and a non-malicious scan, since the two look alike. Based on this potential confusion, a protection element on your network might block Barracuda Vulnerability Remediation Service by mistake, prohibiting it from accessing your web application.

Most protection elements have rules that block IP addresses based on rate limit violations (e.g., protecting against denial of service and brute force attacks). During a scan, these protection rules are likely to trigger, causing the protection element to entirely block the Barracuda Vulnerability Remediation Service. When blocked, the Barracuda Vulnerability Remediation Service cannot access your application, typically causing the scan abort with an error.

Some protection elements might also block IP addresses after a set number of failures (known as “fail2ban”). This also causes the scan to abort with an error.

Allowing IP addresses is not specific to the Barracuda Vulnerability Remediation Service; all web application vulnerability scanners require the same procedure. In fact, to be compliant with the PCI Security Standard, you *must* allow these IP addresses when running your scan. The following is a quote from the *PCI Security Scanning Procedures document*, where *ASV* is the Approved Security Vendor, in this case Barracuda Networks:

> *13. Arrangements must be made to configure the intrusion detection system/intrusion prevention system (IDS/IPS) to accept the originating IP address of the ASV. If this is not possible, the scan should be originated in a location that prevents IDS/IPS interference*

Not allowing IP addresses might cause your protection element to generate false logs and/or alerts, which can be a nuisance and add extra work to the administration team. Allowing the IP addresses of the Barracuda Vulnerability Remediation Service will ensure that your protection

elements will not generate logs due to scans.

Failed Login Mid-Scan

When running a scan using HTML form-based authentication, you might receive the following message in your scan report and on the Vulnerabilities page:

> *The scan was not able to complete because the login information you provided stopped working mid-scan. You may need to exclude any "change password" or similar forms to verify the scan cannot alter its own login credentials.*

Why This Happens

As part of the comprehensive web application vulnerability scan, the Barracuda Vulnerability Remediation Service will identify all of the forms in your application, and will submit those forms to test for vulnerabilities. A common pitfall is when the scanner identifies and submits the "change password" form. This might cause it to change the password to the account it is using to log in. When this happens, the scanner sees that it can no longer log in using the credentials you provided, and, therefore, aborts the scan.

How to Fix It

Find any forms on your application that might change or invalidate the credentials the scanner is using to log in. These forms could be:

- Change Password
- Change Username (less common)
- Delete Account

To ensure the scan can complete successfully, you must exclude the URLs of these forms.

1. On the **Scanner > Web Applications** page, find the failed scan configuration.
2. In the same row of the table, click the **Edit** link for that scan to edit the scan configuration.
3. Select the **Exclusions** tab.
4. Under **Exclude URL patterns**, enter the URLs of each of the above forms and click **Add**.
5. Click **OK** to save your new scan.
6. Click **Run Now** to run the scan again.
   The exclusions you specified will appear in the completed report.

What is this IP Address?

Traffic from this IP address might appear to be malicious, but it is not.

You are seeing this message because you entered the IP address of a Barracuda Vulnerability Remediation Service scan node into your browser. The Barracuda Vulnerability Remediation Service is a web application vulnerability management tool used by authorized individuals to scan sites they control. It finds vulnerabilities such as SQL Injection, Cross-Site Scripting, and others.

Although traffic generated by a web application vulnerability scan might look malicious, it is not. Traffic generated by the Barracuda Vulnerability R emediation Service is specially engineered to determine if a vulnerability exists while causing no damage to the application being scanned. Although certain firewalls might flag the traffic as malicious due to its nature, rest assured that this traffic will not harm your application.

If you ran a scan using the Barracuda Vulnerability Remediation Service yourself, you can cancel the scan at any time by clicking **Cancel** on your the **Scanner > Scan Status** page. This is described in the Actions on Existing Scans and Web Applications article. If you did not run the scan yourself, another authorized person (such as your IT provider) might be running the scan. Ask your IT personnel. If you need help, contact VRS_S upport@barracuda.com.

Avoiding Possible Scanning Side Effects

During the scan process, the Barracuda Vulnerability Remediation Service tests all of the functionality of your web application, including pushing buttons and entering text. This might lead to unintended results, depending on the configuration of your web application and the scan.

Consider the following suggestions to stave off potential side effects:

- **Scan using non-administrative credentials.** Scans run with full administrative credentials will have privileges to access all areas of

your web application. This could result in changing settings or states.

    - If you want to scan using administrative credentials, scan a staging or test environment. In this way, the scanner has full access to all features, but you eliminate any risk of side effects on your production environment.

- **Exclude sensitive areas** if there are areas of your application that you do not want tested. When creating a new scan, use the **Exclusions** tab to exclude IP addresses, URL patterns, and file extensions. Refer to How to Create a New Web Application Scan for details.
- **Back up your data first.** If you are concerned about your data, back it up before starting a scan.

Note: The Barracuda Vulnerability Remediation Service includes built-in overload protection. If, during the scan, your server exhibits signs of overloading, such as slow response time, the Barracuda Vulnerability Remediation Service will automatically reduce scan speed. For your protection, this feature cannot be turned off.