Overview

Vulnerabilities, or security risks, are weaknesses in websites and web applications. An insecure web application can provide hackers access to confidential corporate systems and user data and other malicious activities. Barracuda Vulnerability Manager scans your web applications based on your custom configuration settings, allowing you to automate the process to uncover and resolve weaknesses in your websites and web applications.

Barracuda Vulnerability Manager is a web application vulnerability management solution to help businesses automatically identify, assess, and mitigate web application security risks including those categorized by the Open Web Application Security Project (OWASP) including SQL Injection, Cross-Site Scripting (XSS), Cross-Site Request Forgery (CSRF), and others. Once vulnerabilities are identified, you can modify and update code, or select to integrate your systems with a Barracuda Web Application Firewall to modify applicable security policy settings or configure to mitigate the reported vulnerabilities. Together with Barracuda Web Application Firewall (WAF), Barracuda Vulnerability Manager provides a comprehensive solution to identify and secure against web application vulnerabilities.

Barracuda Vulnerability Manager scans web applications, targeting the web servers to which it is pointed; it does not scan your network or infrastructure.

You can scan any web application that is publicly accessible, regardless of where it is hosted, including on premises, co-located, or on a public cloud server. Web applications can be scanned regardless of whether they are behind a firewall or load balancer.

Vulnerability Manager does not collect any personally identifiable information (PII) or records from your application's database, regardless of whether this information is publicly accessible. It *does not* collect any data that could be compromised. It only alerts you to the problem.

Where to Start

- For detailed setup steps, refer to Initial Service Setup.
- To learn how to create and run scans, refer to How to Create a New Scan.

Key Features

- Scan URLs and URL Patterns
- Ability to Define Exclusions
- Vulnerability Reports
- Integrating with Barracuda Web Application Firewall

Initial Service Setup

To get started with Barracuda Vulnerability Manager, log in to your Barracuda Cloud Control account.

If you already have a Barracuda Cloud Control account, continue with **Connect to the Barracuda Vulnerability Manager** below.

If you do not have an account, use the following steps to create a new account:

1. If you do not have a Barracuda Cloud Control account, go to https://login.barracudanetworks.com/ and click **Create a user**.
2. Enter your name, email address, and company name, and specify whether this is a partner account. Click **Create User**.
3. Follow the instructions emailed to the entered email account to log in and create your Barracuda Cloud Control account.
4. After submitting your new account information, the **Account** page displays your account name, associated privileges, and username.

To log into the Barracuda Vulnerability Manager, continue with Step 2 below.

Connect to the Barracuda Vulnerability Manager

1. Log into https://login.barracudanetworks.com/.
2. Once you are logged in, click **Vulnerability Manager** in the left navigation pane.
3. Click **Sign Up For Free**.
4. Enter your **Phone Number**, select your **Country**, and then enter your **Postal Code**.
5. Read and accept the **terms of service**, and click **Sign Up**. The **Active Scans** page displays.

Click **New Scan** to start scanning your web applications.

In the future, when you log into your Barracuda Cloud Control Account, you will automatically be able to access the Barracuda Vulnerability Manager.

Dashboard

Use the **Dashboard** to view summary information on vulnerabilities found in scanned URLs 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 website 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".

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 **Active Scans** page for more details.

Recently Finished Scans

Displays a list of the most recent scans, the date they were run, and the number of vulnerabilities found. Click **Show All** to go to the **Finished Scans** page for more details.

Top Vulnerable Applications

Displays a pie chart and accompanying data for the web applications most at risk in your scanned site. If you have only scanned one site, the pie chart will be one solid color.

Vulnerability Severity Breakdown

Displays a pie chart and accompanying percentage data for the severity of vulnerabilities in all of your scanned sites.

Severity levels include:

- Critical
- High
- Medium
- Low

The **Dashboard** is an overview of all of your scans. To see severity details on a specific scan, go to the **Finished Scans** page and view the details or report for a specific scan.

Vulnerability Type Breakdown

Displays a pie chart and accompanying data for the top three types of vulnerabilities for your scanned sites. Other vulnerability types are grouped into "Others".

The **Dashboard** is an overview of all of your scans. To see vulnerability type details on a specific scan, go to the **Finished Scans** page and view report for a specific scan, along with descriptions and details for each type.

Understanding Verification

Important
It is unlawful to run a scan on a web application (web site) without express permission from its owner or operator. To prevent abuse of the system, you must first verify the domain you want to scan before you are able to run the scan.

How Verification Works

To verify a domain, you must have access to an email address at that domain. For example, if you want to scan **example.com**, you must have access to an email address ending in **@example.com**. You may also verify a domain using an email address at a subdomain or parent domain of the domain want to scan. For example, you may verify **example.com** with the address **user@*sub*.example.com**, and you may verify ***sub*.example.com** with the address **user@example.com**.

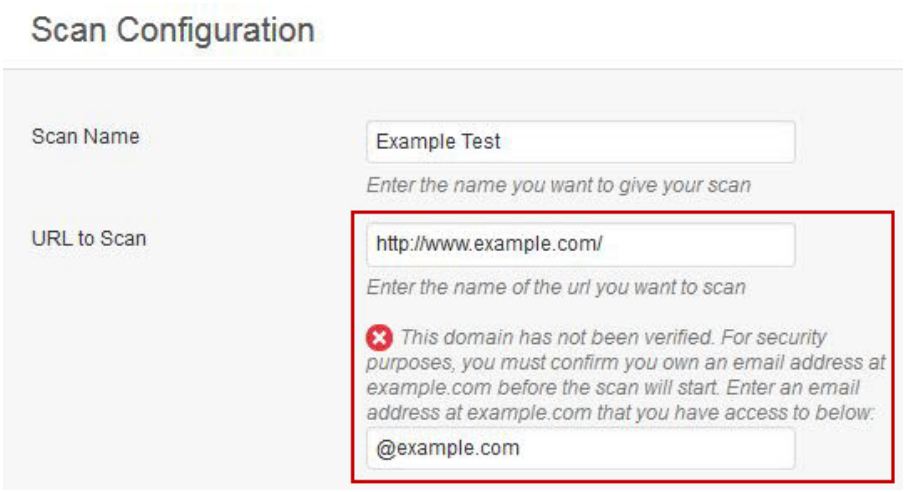
Barracuda Vulnerability Manager will send a verification link within an email to the verification address you provide. To verify the domain, click the link in the email.

> **Note:** If you are having an authorized user perform the verification for you, instruct them to click the link in the email they receive from Barracuda Vulnerability Manager. The user performing verification does **not necessarily** need to log in to Barracuda Vulnerability Manager. If they are not logged in, they will **not** have access to any Barracuda Vulnerability Manager data.

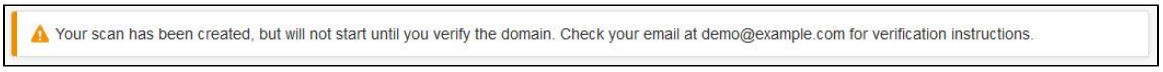
Once you have verified a domain, you are not required to verify it again to run subsequent scans on that domain.

How to Verify a Domain

1. On the **Active Scans** page, click **New Scan** to create a new scan.
2. In the **Scan Configuration** window, enter the domain you want to scan in the **URL to Scan** field. A message appears, indicating the domain must be verified and that you must provide a verification email.



3. Enter the verification email you want to use to verify the domain (e.g., **demo@example.com**).
4. Configure the parameters of the scan in the Scan Configuration window. Click **Help** for details on the configuration parameters.
5. Click **Start Scan**. You will receive a message that the scan will start as soon as the domain is verified:



6. Open the email that was sent to your verification address. Click the link in that email.
   The scan will start as soon as the link is clicked.
   If you have set the scan to run at a future time, it will run automatically at that time. You will not need to verify the domain again.

Scans

To scan a web application, Barracuda Vulnerability Manager 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 is collected. If a vulnerability is found that could compromise confidentiality of data on your web application, Barracuda Vulnerability Manager does not collect any of the data that could be compromised, instead it alerts you to the problem, and 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 Barracuda Vulnerability Manager to scan any publicly accessible web application, regardless of where it is hosted, even if it is behind a load balancer or firewall.

Be sure to read the following articles about Scans:

- How to Create a New Scan
- How to Copy Scan Configurations
- Active Scans
- Finished Scans

How to Create a New Scan

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

Once you are logged in and connected to the service, the **Active Scans** page displays. Complete the following steps to set up a website scan:

1. Click **New Scan**; the **Scanner Configuration** page 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`.

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

   If the URL cannot be verified, you are prompted to enter an email address to which you have access.
   If the domain is verified, the scan can be started immediately.
   For more information, refer to Understanding Verification.
4. Select each of the four tabs, described below, completing the necessary information.
5. When you are satisfied with your configuration, click **Start Scan**.

Select the General Tab

1. Specify when you want to scan the website:
   a. **Start scan immediately** – When selected, the scan begins once the scanner configuration is complete and you click **Start Scan**.
   b. **Start scan at this time** – When selected, you specify the date and time that the scan is to start.
      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 Manager tab of your browser.
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.
   The scanning process begins on the home page, then moves down to scan the next level, then once pages on that level are complete, moves to the following level, for a maximum of 3 levels deep. The home page is level zero. If you shorten the time of the scan, you will potentially not see results for the lower levels of your web site.
3. To receive a scan report via email once the scan is complete, select **Email me a report when the scan is completed**, and enter the email address in the associated field.
4. **Barracuda may contact me about the results of this scan** is selected by default. If you leave this option selected, Barracuda might contact you when the scan is complete to help you understand the report and mitigate any vulnerabilities found. If you do not want to be contacted, clear this check box.

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 set 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 Manager detects that it is starting to overwhelm your server, it will automatically throttle back on the number of requests per second.

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.
4. Turn on **Enable evasion techniques** 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 Authentication Tab

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 login credentials.

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

   - **Basic** authentication uses static, standard HTTP headers and is the simplest technique for enforcing web resource access control. Basic sends plain text over the network.
   - **Digest** access authentication is a more complex technique to confirm user identity. Digest applies a hash function to a password before sending it over the network.

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 **Login form URL**, along with your associated user name and password. Then click **Autodetect** to automatically complete the rest of the fields in the section. Alternatively, you can enter the information manually.
   b. 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.

- **To exclude a hostname, IP address, URL pattern or file extension**:
  Enter the information into the correct segment of the page, then click **Add** in the **Actions** column.
- **To remove an exclusion**:
  In the row of the table with the exclusion you want to remove, click **Delete** in the **Actions** column.
- Click **Remove All** to remove all of the exclusions within a section of the page.
- By default, all images and videos are excluded.

> 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.

How to Copy Scan Configurations

You can quickly create new scans based on existing scan configurations using the **Copy** option on either the **Active Scans** or **Finished Scans** p age.

1. Go to either the **Active Scans** or **Finished Scans** page, and click **Copy** in the **Actions** column for the scan configuration on which you want to base the new scanner configuration.
2. In the **Scan Configuration**, enter a new **Scan Name**, if you choose. If you choose, change the URL, to perform the same scans on a different web site.
3. Make any necessary adjustments to the remaining settings. If you do not change any configuration parameters, the scan will be identical to the scan you copied.
4. Click **Start Scan**. The scan will either begin immediately or will begin at the designated time.

Active Scans

The **Active Scans** page lists each scan that has been defined by name under the associated URL. Click the arrow to the left of the URL name to display or hide the list of scans. From this page you can view the scan date, current status including scan details.

Search for Scans

To refine the list of scans, begin typing in the **Search** field, or use the navigation tools to move through the list.

Edit a Scan

If the scan is scheduled for a future date and time, click **Edit** to modify the scan configuration.

Verify a Scan (Awaiting Verification)

If the scan **Status** displays as **Waiting for Verification**, an email has been sent to the verification email address configured when the scan was started. If you did not receive this email, click **Verify** to resend the email or specify a different verification email address. For more information on scan verification, refer to Understanding Verification.

If you specified a **Start scan at this time** setting when defining the scan configuration, you must verify the scan on the **Active Scans** page before the scan can run.

Before your scan can be activated, you must verify the scan settings on the **Active Scans** page. A scan awaiting verification displays a status of **Waiting for Verification** on the **Active Scans** page.

Copy a Scan

Click **Copy** to create a new scan, based on the selected scanner configuration. If you choose, change the name to distinguish them.

For additional information on copying a scan, refer to How to Copy Scan Configurations.

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 will finish its current scenario and abort. Note that this may take a few minutes, depending on the length of the current scenario.

Flag a Scan

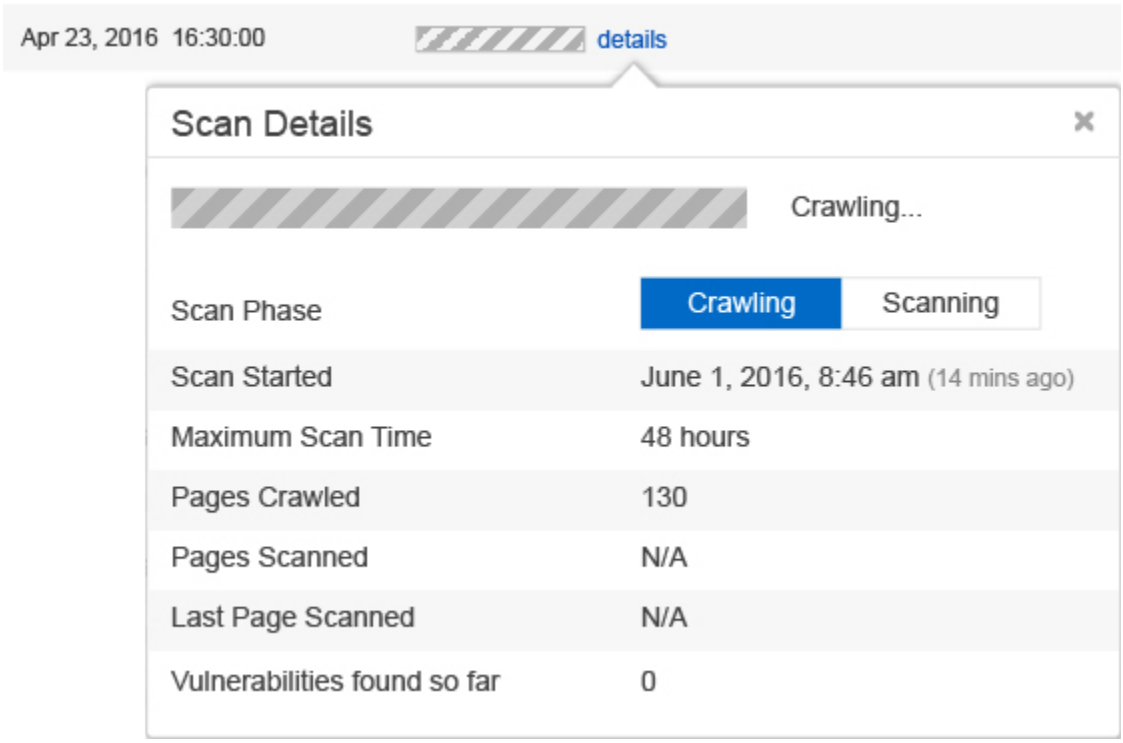
Click the flag icon ( ) to the left of a scan name to mark it in red ( ), so it is easier to find next time you want to view it.

Scan Stages

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

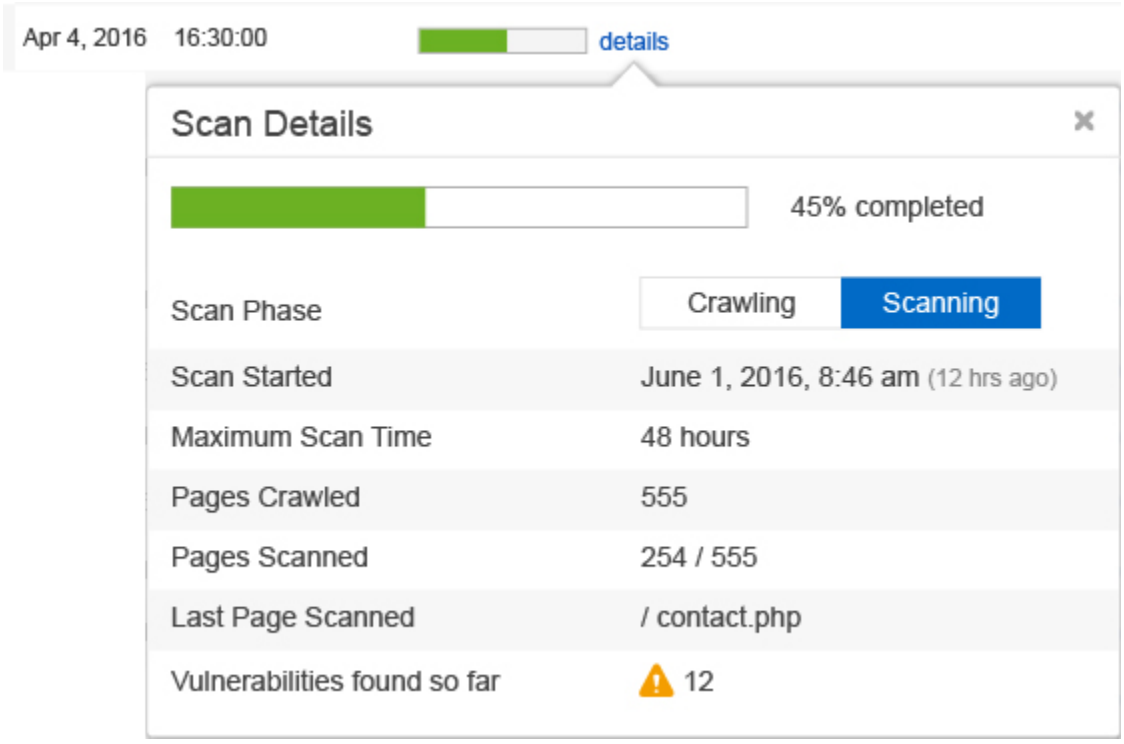
Crawling Stage

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

Once discovery is complete, the scan begins and the scan time duration bar indicates the scan is in progress:



Review vulnerabilities, scans in progress, and finished scans on the Dashboard page.

Finished Scans

The **Finished Scans** page lists each completed scan by name under the associated URL. Click the arrow to the left of the URL name to display or hide the list of scans.

On this page, you can view the date and time the scan was completed and the scan status, including details about vulnerabilities found during the scan.

Viewing Basic Scan Status

The **Status** bar is color coded, so you can see basic information at a glance. Colors include:

- **Red** – Maximum level of vulnerabilities found is *critical.*
- **Yellow** – Maximum level of vulnerabilities found is *medium.*
- **Gray** – Maximum level of vulnerabilities found is *low.*

The length of the **Status** bar correlates to a weighted measure of the severity and number of vulnerabilities found. Longer bars correlate to the measure of vulnerabilities on your web application.

The **Status** section also displays problems including:

- **Error During Scan** – Indicates scan did not complete successfully.
- **Scan Cancelled** – Indicates scan was cancelled manually.

If a scan did not run to completion, you can view a partial report to see results from the areas that were scanned.

Searching For and Deleting Scans

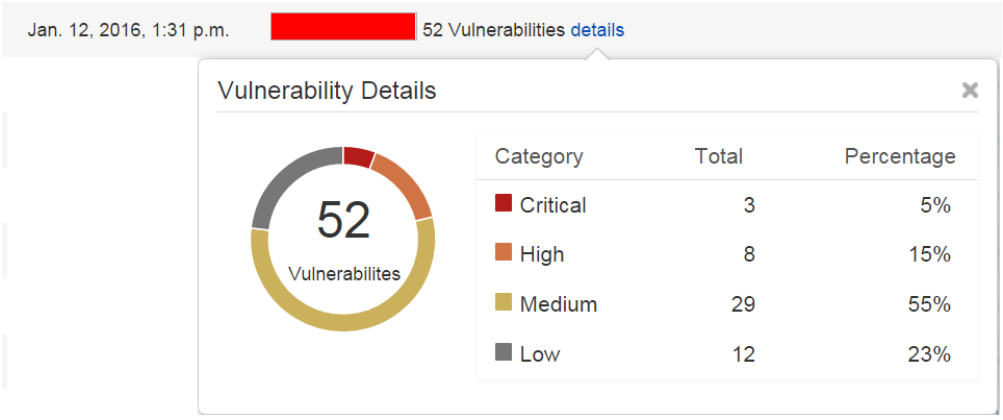
To refine the list of scans, begin typing in the **Search** field, or use the navigation tools to move through the list.

You can select one or more check boxes next to scan names, then click **Delete** to remove the selected scans, or select the check box to the left of the **Scan Name** heading at the top of the table, and then click **Delete** to remove all scans listed in the **Finished Scans** table.

Viewing Scan Vulnerability Details

The **Status** field displays based on the scan outcome:

- **No Vulnerabilities Found** – Indicates scan completed successfully and found no vulnerabilities.
- ***n* Vulnerabilities** – Indicates the scan completed successfully and found *n* number of vulnerabilities. Click **details** for more information:



Copying a Scan

To run a scan again, or to create a similar version of the same scan, in the **Actions** column, click **Copy** in the appropriate row of the **Finished Scans** table.

When you click **Copy**, the **Scan Configuration** window appears, pre-filled with the information from the original scan you copied. At this point, you have two options:

- **To run the same scan again –** If you choose, change the scan name. Do not make any changes to the configuration parameters. Click **Start Scan**.
- **To run a similar scan –** If you choose, change the scan name. Change some of the configuration parameters. Click **Start Scan**.

The **Copy** function is the same on the **Finished Scans** and **Active Scans** pages.

Viewing Reports

Click **View** in the **Reports** column to view the Barracuda Vulnerability Manager Report for the selected scan. The report appears. Refer to the following articles for information on understanding and working with reports:

- Understanding Barracuda Vulnerability Manager Reports
- Interacting with the Barracuda Vulnerability Manager Reports

Downloading Reports

lick **Download** and select to download the report to your local system as a PDF, XML, or CSV file.

You can import an XML file into the Barracuda Web Application Firewall. Refer to Integrating with Barracuda Web Application Firewall for details.

Flagging a Scan

Click the flag icon () to the left of a scan name to mark it in red (), so it is easier to find next time you want to view it.

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 Manager reports contain a comprehensive set of details to help your web application developers to determine how to resolve existing vulnerabilities.

Here is a sample report PDF to give you an idea of the information provided by a scan.

In this section

- Understanding Barracuda Vulnerability Manager Reports
- Interacting with the Barracuda Vulnerability Manager Reports
- How to Customize Barracuda Vulnerability Manager Reports

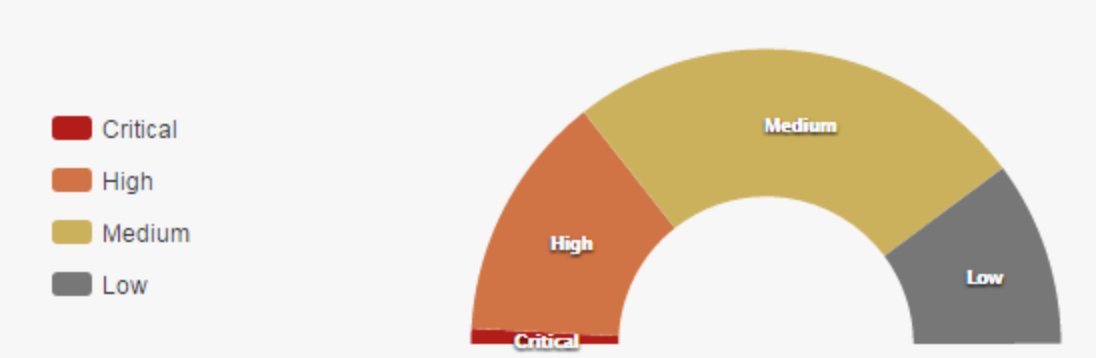
Understanding Barracuda Vulnerability Manager Reports

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.

> **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 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.

Interacting with the Barracuda Vulnerability Manager Reports

You can interact with the online report to keep track of your reactions to the threats described in the report. Your changes are saved, so you will be up to date each time you view the report from the **Finished Scans** page.

Click the current **Severity** level to change it, based on your organization's perception of the threat. Values include:

- **Critical**
- **High**
- **Medium**
- **Low**
- **False Positive**

When you change the **Severity** level, a note appears in the report, pointing out that the **Severity** was changed and its original value.

Any changes to **Severity** are reflected in the charts in the report.

Change the **Status** of an issue, to track your actions on an issue. Click the current status and change it to one of the following values:

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

Click **Add Notes**/**Edit Notes** to add your thoughts on an issue, and return to edit them later. All of your notes will be saved, so you can see them each time you open the report.

How to Customize Barracuda Vulnerability Manager 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 **Show Customize Options** to display the **Customize Appearance** section.
2. Click **Browse** to upload an image. Note that image must be a PNG, GIF, or JPG that is less than 50k in size.
3. In the **Customize 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.

Integrating with Barracuda Web Application Firewall

Barracuda Vulnerability Manager integrates with Barracuda Web Application Firewall to make it easier to address web application vulnerabilities detected by the scans. When the Barracuda Web Application Firewall receives the imported scan report, it creates one or more Security Policy Recommendations. The administrator can apply these Recommendations to modify applicable security policy settings or configurations to mitigate the reported vulnerabilities.

To integrate with the Barracuda Web Application Firewall, create an XML version of the appropriate scan.

1. Navigate to the **Finished Scans** page.
2. Locate the scan you want to import into the Barracuda Web Application Firewall.
3. In the same row as that scan, select **Download**, then **XML**.

You will use the XML file to import into the Barracuda Web Application Firewall.

Refer to Mitigating Website Vulnerabilities using Vulnerability Scanners for information on importing the file.

Troubleshooting

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

In this Section

Allowing Barracuda Vulnerability Manager IP Addresses

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

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

How to Allow Barracuda Vulnerability Manager IP Addresses

Consult the technical documentation associated with your protection element for instructions for 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 Manager 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 Manager 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 Barracuda Vulnerability Manager. When blocked, Barracuda Vulnerability Manager cannot access your application, typically causing the scan abort with an error.

Some protection elements may 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 Barracuda Vulnerability Manager; all web application vulnerability scanners require the same procedure. In fact, to be compliant with the PCI Security Standard, you *must* allow IP addresses. 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 Barracuda Vulnerability Manager 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 may receive the following message in your scan report:

> *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, Barracuda Vulnerability Manager 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 may cause it to change the password to the account it is using to log in. Once this happens, the scanner will see that it can no longer log in using the credentials you provided, and abort the scan.

How to Fix It

Find any forms on your application that may 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 **Finished Scans** page, find the failed scan.
2. In the same row of the table, click the **Copy** link for that scan. This will create a copy of the failed scan.
3. In the **Scan Configuration** window, choose whether to keep the same scan name or type a new name.
4. Select the **Exclusions** tab.
5. Under **Exclude URL patterns**, enter the URLs of each of the above forms and click **Add**.
6. Click **Start Scan** 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 may appear to be malicious, but it is not.

You are seeing this message because you entered the IP address of a Barracuda Vulnerability Manager scan node into your browser. Barracuda Vulnerability Manager 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.

While traffic generated by a web application vulnerability scan may look malicious, it is not. Traffic generated by Barracuda Vulnerability Manager is specially engineered to determine if a vulnerability exists while causing no damage to the application being scanned. Although certain firewalls may 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 Barracuda Vulnerability Manager yourself, you may cancel the scan at any time by clicking **Cancel** on your **Active Scans** page. If you did not run the scan yourself, another authorized person (such as your IT provider) may be running the scan. Ask your IT personnel. If you need help, contact BVM_Support@barracuda.com.

Avoiding Possible Scanning Side Effects

During the scan process, Barracuda Vulnerability Manager 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 Barracuda Vulnerability Manager scan, use the **Exclusions** tab to exclude IP addresses, URL patterns, and file extensions.
- **Back up your data first.** If you are concerned about your data, back it up before starting a scan.

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