



# Solution Brief

## Deploying the Barracuda Web Application Firewall with the New Vulnerability Remediation Service

Web Application vulnerabilities have become the proverbial punching bag of the internet. A Verizon report found that 35% of security incidents they researched involved web applications—more than any other vector. Unfortunately, web application vulnerabilities have traditionally been difficult to fix and many organizations leave themselves exposed by not correctly securing themselves.

Barracuda's Web Application Firewall is the ideal solution for organizations looking to protect web applications from data breaches and defacement. And now, with the Vulnerability Remediation Service (VRS), it's easier than ever to deploy. This solution brief provides a step-by-step overview of how to use the Vulnerability Remediation Service (VRS) to easily deploy the Web Application Firewall.

There are three steps to deploy the Barracuda Web Application Firewall (WAF) and secure your web applications:

1

Connect WAF to the network

2

Associate backend servers

3

Use VRS to scan and remediate vulnerabilities

### Step 1: Connect WAF to the network

In this step, we assign the WAF an IP address for management and make sure it has access to the Internet as well as to the backend servers it protects. We may also ensure it's running the latest firmware and has the latest security definition updates.

For detailed instructions on how to connect your WAF to the network, please consult the following Campus articles:

- For hardware appliances, see <https://campus.barracuda.com/product/webapplicationfirewall/article/WAF/GetStarted1/>
- For virtual appliances, see <https://campus.barracuda.com/product/webapplicationfirewall/article/WAF/QuickStartGuideVx/>
- For AWS instances, see <https://campus.barracuda.com/product/webapplicationfirewall/article/WAF/AWSDeployQSG/>
- For Azure instances, see <https://campus.barracuda.com/product/webapplicationfirewall/article/WAF/DeployInOldAzurePortal/>

Once the WAF is connected to the network, connect it to Barracuda Cloud Control as well. This allows you to control your WAF from the cloud, and also allows the Vulnerability Remediation Service to apply policy changes to secure your applications. For detailed instructions, consult the following Campus article: <https://campus.barracuda.com/product/webapplicationfirewall/article/WAF/SetUpBCC/>

## Step 2: Associate backend servers

The 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, we tell the WAF which IPs to listen for traffic on and which servers to forward legitimate traffic to.

For detailed instructions on how to create services on your Web Application Firewall, please consult the following Campus article: <https://campus.barracuda.com/product/webapplicationfirewall/article/WAF/GetStarted2/>

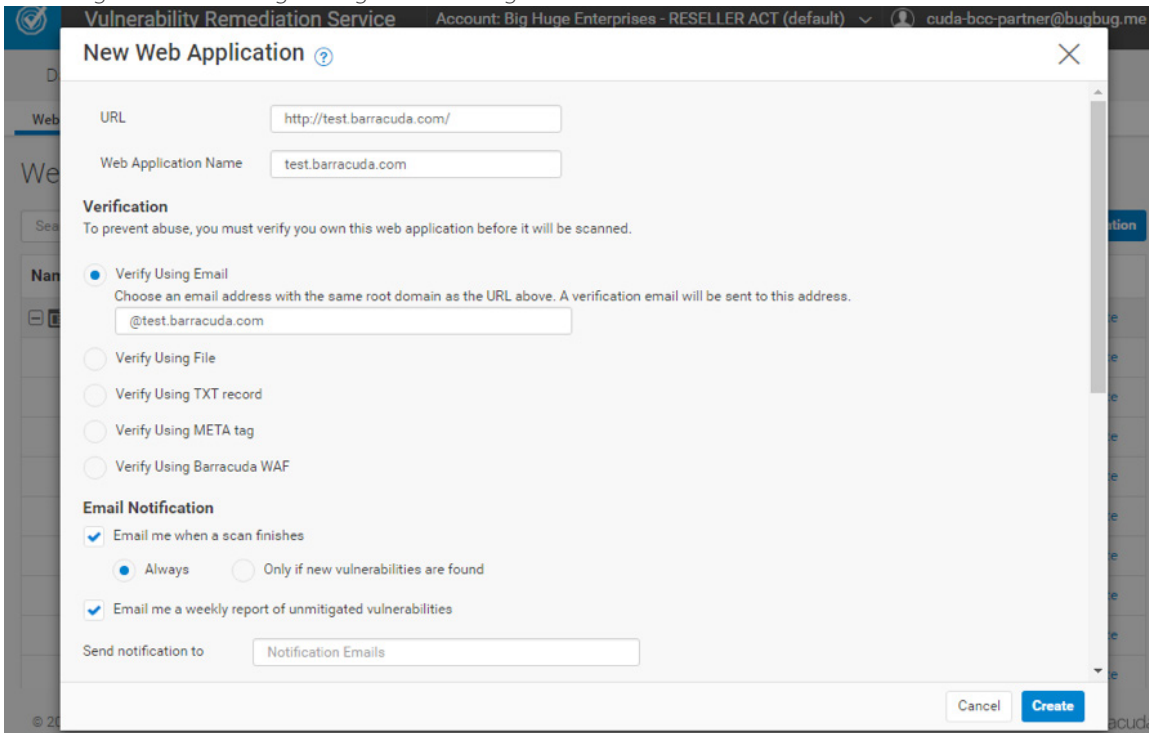
You may initially configure the service you created in Passive Mode, but you must switch it to Active Mode after verifying that the application runs properly. Passive Mode is intended for testing only; in this mode, the Web Application Firewall does not secure your application.

## Step 3: Use VRS to scan and remediate vulnerabilities

In this step, we configure the Vulnerability Remediation Service to scan the application and use the scan results to apply security policy changes on the WAF to secure your applications.

### Run a scan of the application

- Log in to the Vulnerability Remediation Service at <https://vrs.barracuda.com/>. Use the same email and password you used to connect your WAF to Barracuda Cloud Control in step 1.
- Click the blue **“New Web Application”** button to create a new web application.
- Configure the following settings in the dialog:



The screenshot shows the 'New Web Application' dialog box in the Vulnerability Remediation Service interface. The dialog has a title bar with a question mark icon and a close button. It contains the following fields and sections:

- URL:** A text input field containing 'http://test.barracuda.com/'.
- Web Application Name:** A text input field containing 'test.barracuda.com'.
- Verification:** A section with the text 'To prevent abuse, you must verify you own this web application before it will be scanned.' and five radio button options:
  - Verify Using Email: Below this is the text 'Choose an email address with the same root domain as the URL above. A verification email will be sent to this address.' and a text input field containing '@test.barracuda.com'.
  - Verify Using File
  - Verify Using TXT record
  - Verify Using META tag
  - Verify Using Barracuda WAF
- Email Notification:** A section with three checked checkboxes:
  - Email me when a scan finishes: Below this are two radio button options:  Always and  Only if new vulnerabilities are found.
  - Email me a weekly report of unmitigated vulnerabilities
- Send notification to:** A text input field containing 'Notification Emails'.
- Buttons:** 'Cancel' and 'Create' buttons at the bottom right.

- Enter the publicly-accessible URL of your web application.
- Enter a name for the application.
- 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, you can use a different verification method.
- Under **Email Notification**, select your email notification preferences.
- Under **Mitigation**, select the Web Application Firewall and Virtual Service that you created in step 2.
- Click **“Create”** to create the web application.

- The Web Applications screen refreshes to show the newly created application, as well as a Default scan. If you would like to edit scan settings, or schedule the scan for a particular time, click Edit on the scan. If you would like to run the scan immediately, click **Run Now**.

Vulnerability Remediation Service Account: Big Huge Enterprises - RESELLER ACT (default) cuda-bcc-partner@bugbug.me

Dashboard Scanner Vulnerabilities Reports

Web Applications Scan Status

### Web Applications ?

Search:  Add Web Application

Name	URL	Schedule	Details	Actions
Test Web Application	http://test.blorpazort.com/			New Scan Clone Edit Delete
Default		Manual	Max depth 3, No Authenticati...	Run Now Clone Edit Delete

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

## Review vulnerabilities on the application

When the scan has completed, log in to VRS and navigate to the Vulnerabilities tab.

Vulnerability Remediation Service Account: Big Huge Enterprises - RESELLER ACT (default) cuda-bcc-partner@bugbug.me

Dashboard Scanner Vulnerabilities Reports

### Vulnerabilities ?

Select a web application to see its vulnerabilities.

Search: sales demo finished 2

Web Application Name	Vulnerabilities	Barracuda WAF	Service	Policy	Actions
Test Web Application	72				View

Show 10 rows First Previous 1 Next Last 1 web applications

Click the name of the web application you created to view vulnerabilities.

Vulnerability Remediation Service Account: Big Huge Enterprises - RESELLER ACT (default) cuda-bcc-partner@bugbug.me

Dashboard Scanner **Vulnerabilities** Reports

### Vulnerabilities on Test Web Application

[Back to Vulnerabilities](#)

Search by Type, URL or Parameter All Time

Mitigate on WAF in: Passive Mode Active Mode Manual Ignore

<input type="checkbox"/>	ID	Last Found	Type	URL	Parameter	Severity	Mitigation	Autofix	Actions
<input type="checkbox"/>	129865	2016-11-11	OS Command Injection	http://test.blorpazort....	cmd	Critical	New		<a href="#">View</a>
<input type="checkbox"/>	129860	2016-11-11	Blind OS Command In...	http://test.blorpazort....	filename	Critical	New		<a href="#">View</a>
<input type="checkbox"/>	129863	2016-11-11	Blind SQL Injection	http://test.blorpazort....	search	Critical	New		<a href="#">View</a>
<input type="checkbox"/>	129850	2016-11-11	SQL Injection	http://test.blorpazort....	region	Critical	New		<a href="#">View</a>
<input type="checkbox"/>	129838	2016-11-11	Blind SQL Injection	http://test.blorpazort....	cityid	Critical	New		<a href="#">View</a>
<input type="checkbox"/>	129859	2016-11-11	SQL Injection	http://test.blorpazort....	search	Critical	New		<a href="#">View</a>
<input type="checkbox"/>	129823	2016-11-11	Known Vulnerable We...	http://test.blorpazort....		High	New		<a href="#">View</a>
<input type="checkbox"/>	129857	2016-11-11	Directory Traversal	http://test.blorpazort....	fname	High	New		<a href="#">View</a>

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

### Fix vulnerabilities

Once you have reviewed the vulnerabilities, select the checkbox to the left of the ones you wish to fix and click "Mitigate on WAF in/Active Mode" above. Security policy changes will be applied to your Web Application Firewall to mitigate these vulnerabilities.