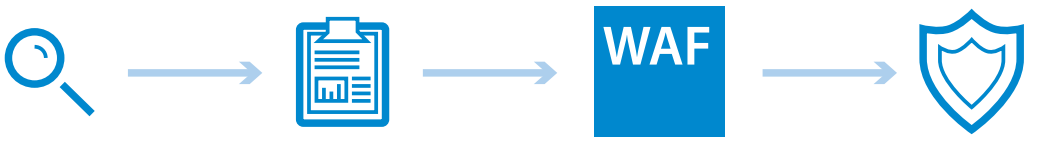
Solution Brief

Web Application Vulnerabilities: from Detection to Remediation with Barracuda Vulnerability Manager and Barracuda Web Application Firewall

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 newly released Vulnerability Manager works along with Barracuda's award-winning Web Application Firewall to make web application vulnerabilities a problem of the past. This solution brief provides a step-by-step overview of the process.

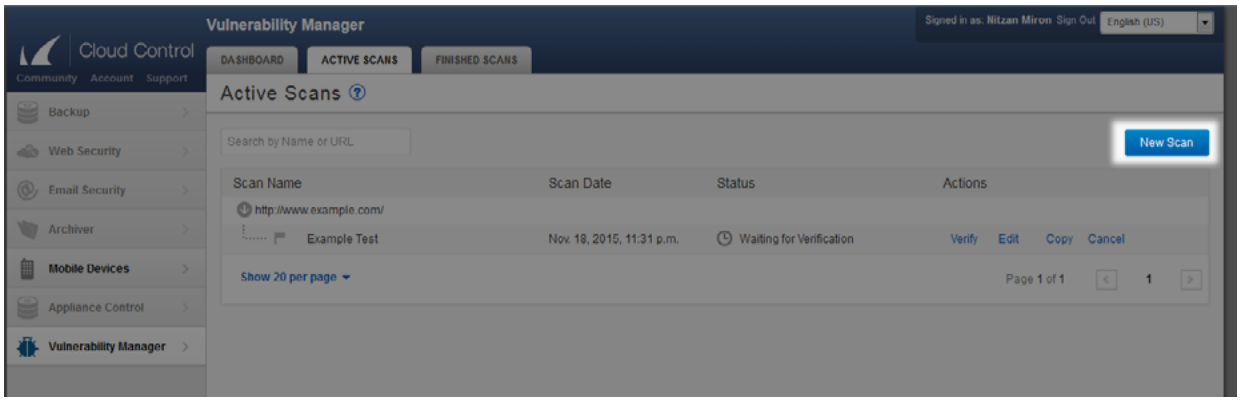
The process of securing your web application can be broken down into these four easy steps:



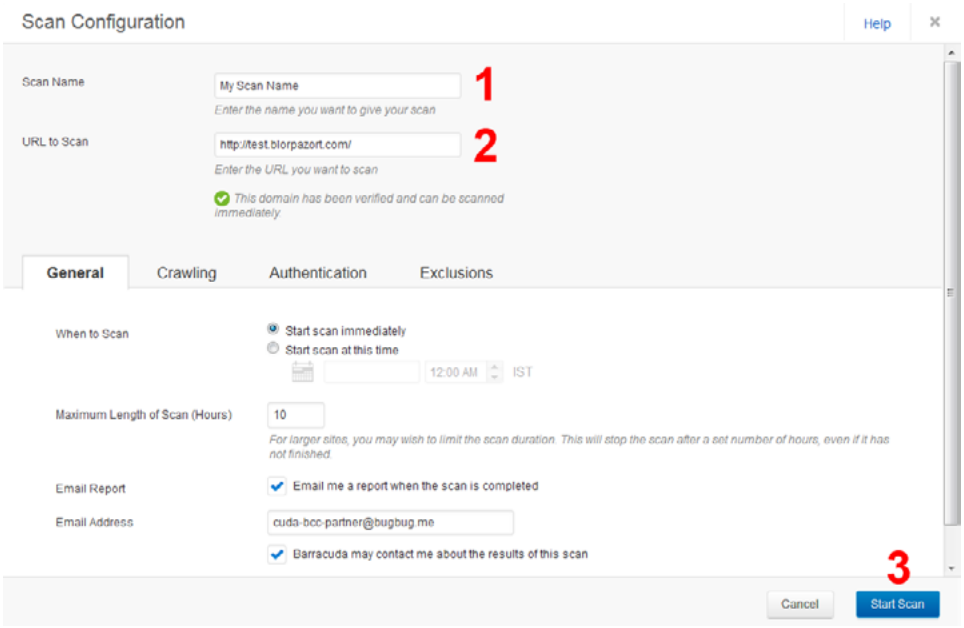
Scan application with BVM → Export report from BVM → Import report into Barracuda Web Application Firewall → Application is Secured

Step 1: Scan your application with Barracuda Vulnerability Manager

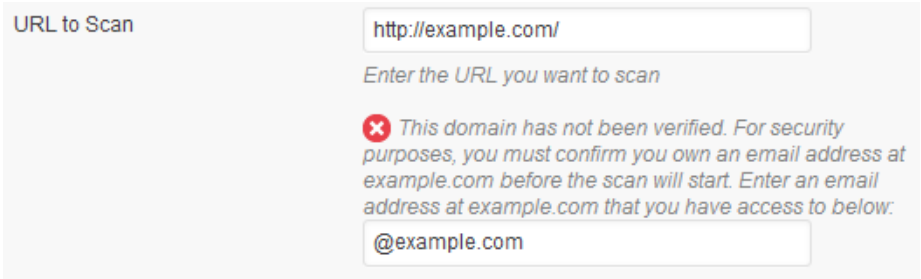
1. Log in to Barracuda Vulnerability Manager at https://bvm.barracuda.com/, using your Barracuda Cloud Control credentials. If you do not have a Barracuda Cloud Control account, you can create one by clicking "Create User."
2. From the Active Scans tab, click New Scan.



3. Enter a scan name (for your future reference), and the URL of the application you wish to scan. If you like, you can browse and configure other scan options, but all are optional. Finally, press Start Scan.

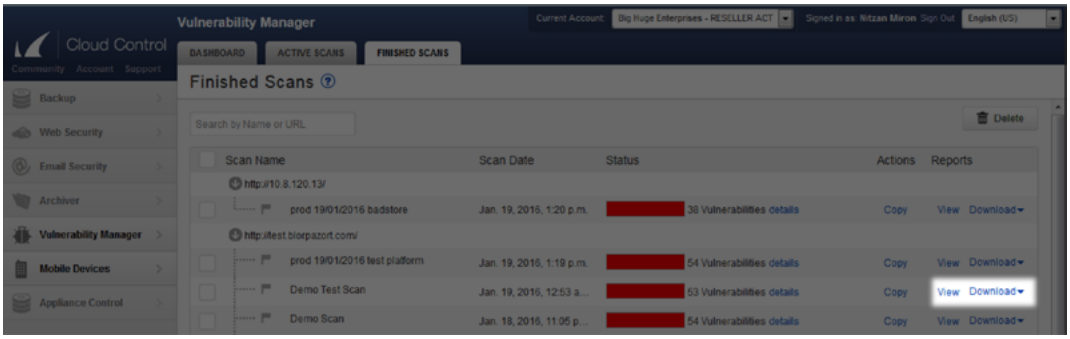


4. If you are scanning a domain for the first time, you will be prompted to verify it in order to prevent abuse. If so, enter an email address on the same domain as you are scanning, to which you have access (for example, if you were scanning example.com you could enter jsmith@example.com). You will need to click the link in the verification email before the scan starts.



Step 2: Export the report from Barracuda Vulnerability Manager

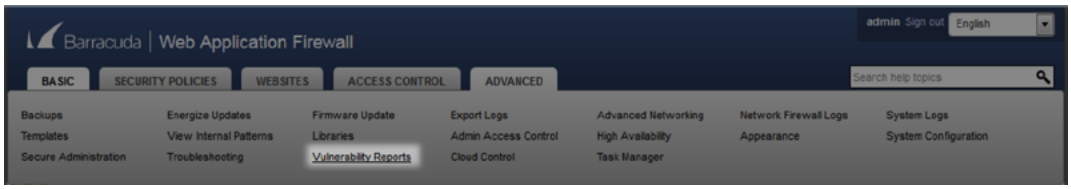
1. Once the scan has finished, log in to Barracuda Vulnerability Manager at https://bvm.barracuda.com/, using your Barracuda Cloud Control credentials.
2. On the Finished Scans tab, find the scan you performed. Click the "View" link to review the report and see which vulnerabilities were found by the scan.



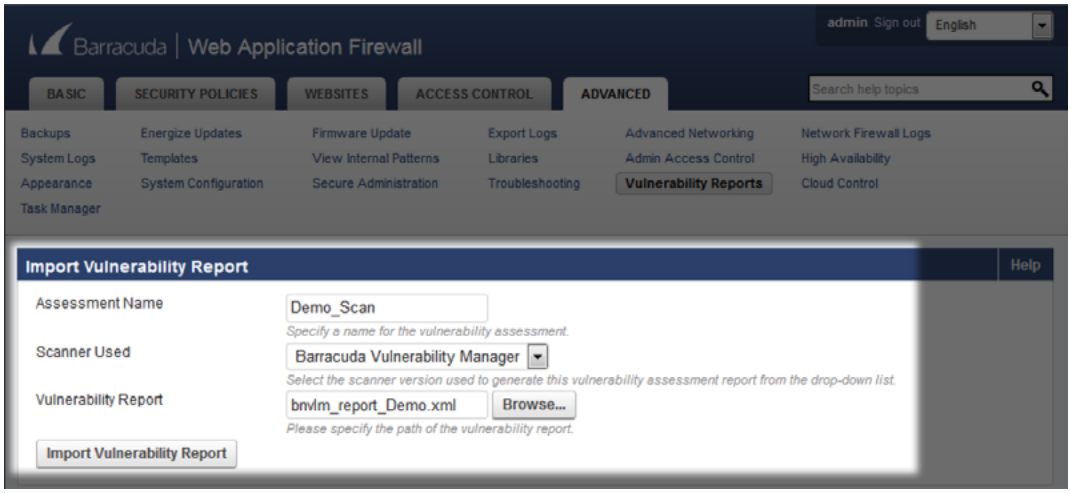
3. After reviewing the report, click Download > XML to download the report in XML format.

Step 3: Import the report into Barracuda Web Application Firewall

1. Log in to your Barracuda Web Application Firewall's web management console using administrator credentials.



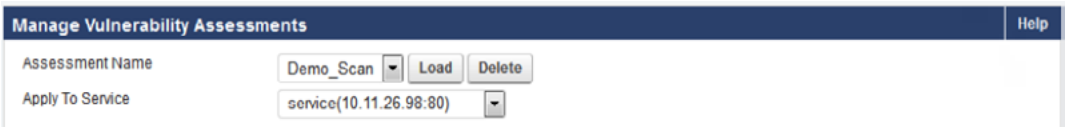
2. Click the Advanced tab, and click Vulnerability Reports.



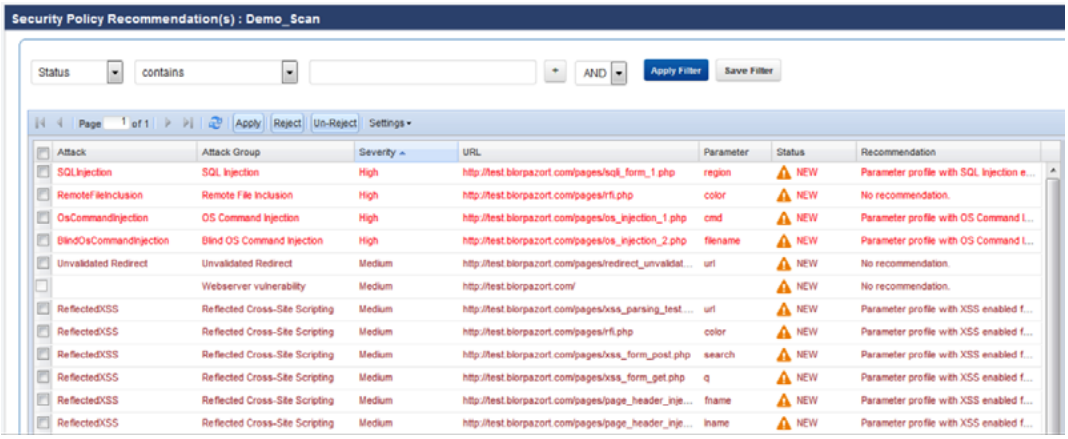
3. In the Import Vulnerability Report pane, enter an assessment name (for your future reference), select Barracuda Vulnerability Manager as the Scanner Used, and select the XML file you downloaded in the previous step. Click Import Vulnerability Report.
4. Note: The assessment name cannot contain spaces.

Step 4: Fix the vulnerabilities

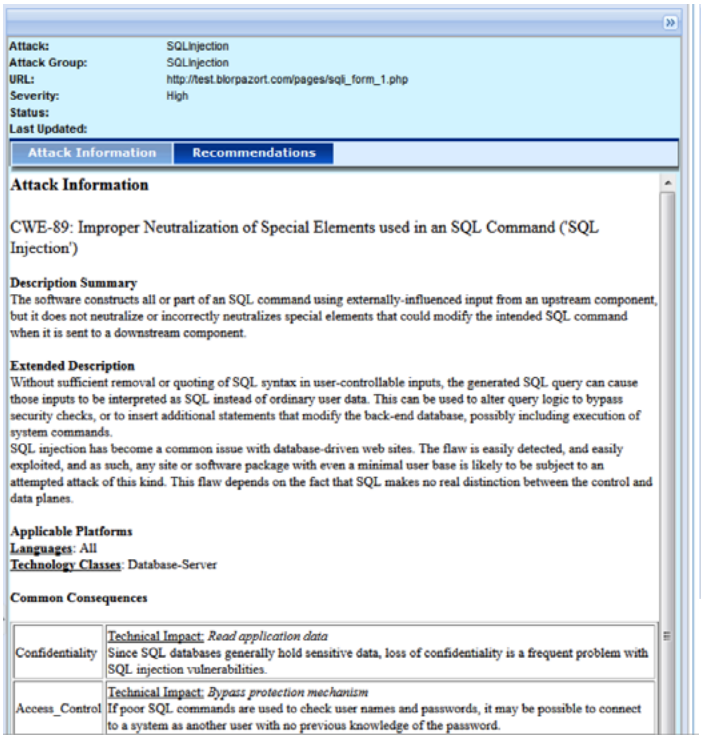
1. On the same Vulnerability Reports pane from the previous section, in the Manage Vulnerability Assessments pane, select the assessment name you chose in the previous section and click Load. Then select the service on the Barracuda Web Application Firewall that serves the application you scanned.

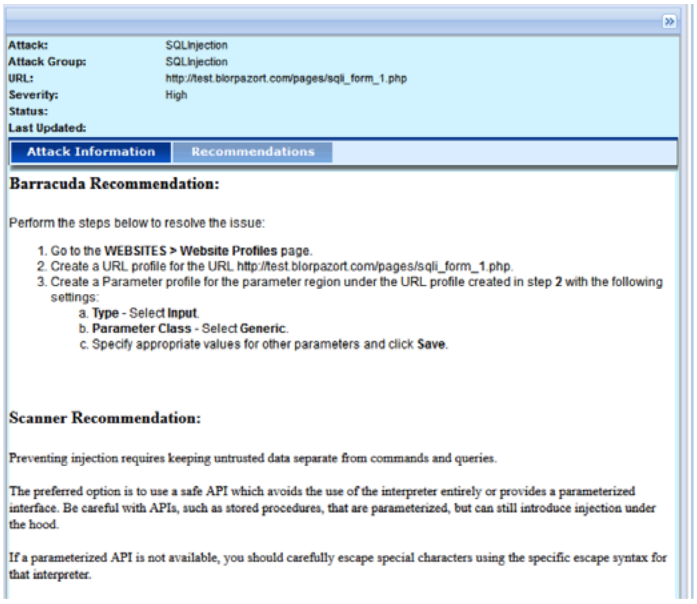


2. Scroll down to the Security Policy Recommendations pane and review the vulnerabilities found.

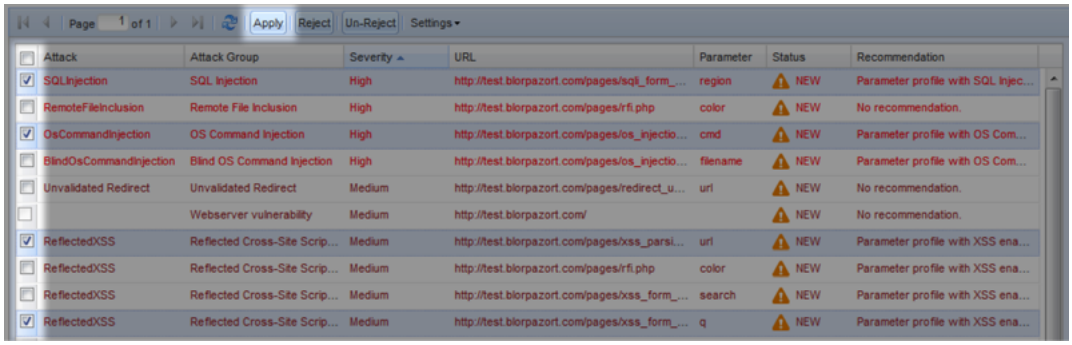


3. You may click any vulnerability to pop up a pane with more information. The pane's Attack Information contains information on the vulnerability, whereas the Recommendations tab contains information on how the Barracuda Web Application Firewall will remediate the vulnerability.





4. After reviewing the vulnerabilities, check the boxes next to the vulnerabilities you wish to have the Barracuda Web Application Firewall fix and click Apply.



5. Congratulations! Your Barracuda Web Application Firewall has now fixed the vulnerabilities, and your application is secure.