

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:



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.

	Vulnerability Manager			Signed in as: Nitzan Miron Sign Out English (US)	
Cloud Control	DA SHBOARD ACTIVE SCANS FINISHED SCANS				
Community Account Support	Active Scans 😨				
Васкор				New Sci	an
Web Security >					_
Email Security	Scan Name	Scan Date	Status	Actions	
Mrchiver >	Example Test	Nov. 18, 2015, 11:31 p.m.	Waiting for Verification	Verify Edit Copy Cancel	
Mobile Devices >	Show 20 per page 👻			Page 1 of 1	-
Appliance Control					
🐞 Vulnerability Manager >					

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.

Scan Configuration	Help			
ican Name	My Scan Name			
E	Inter the name you want to give your scan			
JRL to Scan	est.blorpazort.com/ 2			
E	Inter the URL you want to scan			
	This domain has been verified and can be scanned mmediately			
General Crawling	Authentication Exclusions			
When to Scan	Start scan immediately Start scan at this time 12:00 AM IST			
When to Scan Maximum Length of Scan (Hou	Start scan immediately Start scan at this time 12:00 AM IST Ist For larger allos, you may wish to limit the scan duration. This will stop the scan after a set number of hours, even if it has set finished.			
When to Scan Maximum Length of Scan (Hour Email Report	Start scan immediately Start scan at this time 12:00 AM I IST 15 10 For larger sites, you may wish to limit the scan duration. This will stop the scan after a set number of hours, even if it has not finished. Imail me a report when the scan is completed			
When to Scan Maximum Length of Scan (Hour Email Report Email Address	Start scan immediately Start scan at this time 12:00 AM I IST IsT Is) For larger sites, you may wish to limit the scan duration. This will stop the scan after a set number of hours, even if it has not finished. Is mail me a report when the scan is completed cuda-bcc-partner@bugbug me			

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.

URL to Scan	http://example.com/
	Enter the URL you want to scan
	This domain has not been verified. For security purposes, you must confirm you own an email address at example.com before the scan will start. Enter an email address at example.com that you have access to below:
	@example.com

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.

	Vulnerability Manager	Current Accou	Big Huge Enterprises - RESELLER ACT	Signed in as: Nitzan Miron Sign Out English (US)
	DASHBOARD ACTIVE SCANS FINISHED SCANS			
Backup	Finished Scans 🔊			
Web Security	Search by Name or URL			a Delete
() Email Security	Scan Name	Scan Date	Status	Actions Reports
W Archiver	http://10.8.120.13/ prod 19/01/2016 badstore	Jan. 19, 2016, 1:20 p.m.	38 Vulnerabilities details	Copy View Download-
🛞 Vulnerability Manager 🔿	C http://test.biorpazort.com/			
Mobile Devices >	prod 19/01/2016 test platform	Jan. 19, 2016, 1:19 p.m.	54 Vulnerabilities details	Copy View Download-
Appliance Control	Demo Test Scan	Jan. 19, 2016, 12:53 a	53 Vulnerabilities details	Copy View Download-
	Demo Scan	Jan. 18, 2016, 11:05 p	54 Vulnerabilities details	Copy View Download-

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

Сору	View	Download
		PDF
Сору	View	XML
		CSV
Сору	View	Download -

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.

٩

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

BASIC	SECURITY POLICIES	WEBSITES ACCES	S CONTROL AD	VANCED	Search help topics	
ckups stem Logs	Energize Updates Templates System Configuration	Firmware Update View Internal Patterns Secure Administration	Export Logs Libraries Troubleshooting	Advanced Networking Admin Access Control Vulnerability Reports	Network Firewall Logs High Availability Cloud Control	
sk Manager			_			
sk Manager nport Vuln	erability Report	_	-	_		н
nport Vuln Assessment	erability Report	Demo_Scan	billy assessment	_	-	H
nport Vuln Assessment Scanner Use	erability Report tName ed	Demo_Scan Specify a name for the vulnera Barracuda Vulnerability Select the scanner version us	ibility assessment. Manager	erability assessment report fron	n the drao-down list.	н

- 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.

Manage Vulnerability Assessments				
Assessment Name	Demo_Scan 💌 Load Delete			
Apply To Service	service(10.11.26.99:80)			

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

Secur	Security Policy Recommendation(s) : Demo_Scan								
9	tatus 💌 contains			AND Apply File	save Filte	¢			
14	4 Page 1 of 1 ▷ ▷	Apply Reject Un-Reject	t Settings -						
E	Attack	Attack Group	Severity .	URL	Parameter	Status	Recommendation		
E	SQLinjection	SQL Injection	High	http://test.biorpazort.com/pages/sqli_form_1.php	region	A NEW	Parameter profile with SQL Injection e		
E	RemoteFileInclusion	Remote File Inclusion	High	http://test.biorpazort.com/pages/rfi.php	color	A NEW	No recommendation.		
E	OsCommandinjection	OS Command Injection	High	http://test.blorpazort.com/pages/os_injection_1.php	cmd	A NEW	Parameter profile with OS Command L		
E	BlindOsCommandInjection	Blind OS Command Injection	High	http://test.biorpazort.com/pages/os_injection_2.php	filename	A NEW	Parameter profile with OS Command L		
E	Unvalidated Redirect	Unvalidated Redirect	Medium	http://test.biorpazort.com/pages/redirect_unvalidat	uri	A NEW	No recommendation.		
		Webserver vulnerability	Medium	http://test.biorpazort.com/		A NEW	No recommendation.		
E	ReflectedXSS	Reflected Cross-Site Scripting	Medium	http://test.biorpazort.com/pages/xss_parsing_test	url	A NEW	Parameter profile with XSS enabled f		
E	ReflectedXSS	Reflected Cross-Site Scripting	Medium	http://test.biorpazort.com/pages/rfi.php	color	A NEW	Parameter profile with XSS enabled f		
E	ReflectedXSS	Reflected Cross-Site Scripting	Medium	http://test.biorpazort.com/pages/xss_form_post.php	search	A NEW	Parameter profile with XSS enabled f		
E	ReflectedXSS	Reflected Cross-Site Scripting	Medium	http://test.biorpazort.com/pages/xss_form_get.php	q	A NEW	Parameter profile with XSS enabled f		
E	ReflectedXSS	Reflected Cross-Site Scripting	Medium	http://test.blorpazort.com/pages/page_header_inje	fname	A NEW	Parameter profile with XSS enabled f		
E	ReflectedXSS	Reflected Cross-Site Scripting	Medium	http://test.biorpazort.com/pages/page_header_inje	iname	A NEW	Parameter profile with XSS enabled f		

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.

	>>		»
Attack: SQLInjection		Attack:	SQLInjection
Attack Group: SQLInjection		Attack Group:	SQLInjection
IIRI : http://test.biorpazort.com/pages/soli_form_1.php		URL:	http://test.blorpazort.com/pages/soli_form_1.php
Severity: High		Severity:	High
Statue		Status:	
Last lindated		Last llodated	
Last opdated.		cast opdated.	
Attack Information Recommendations		Attack Information	Recommendations
Attack Information	ń	Barracuda Recomme	endation:
CWE-89: Improper Neutralization of Special Elements used in an SQ	L Command ('SQL	Perform the steps below t	o resolve the issue:
Injection')		1. Go to the WEBSITE	S > Website Profiles page. Is for the LIRI, http://dest.blornezort.com/nages/soli_form_1.php
Description Summary		3. Create a Paramete	er profile for the parameter region under the URL profile created in step 2 with the following
The software constructs all or part of an SQL command using externally-influenced in	put from an upstream component,	settings:	
but it does not neutralize or incorrectly neutralizes special elements that could modify	the intended SQL command	a. Type - Sele	ct Input.
when it is sent to a downstream component.		b. Parameter	Class - Select Generic.
		c. Specify app	ropriate values for other parameters and click Save.
Extended Description			
Without sufficient removal or quoting of SQL syntax in user-controllable inputs, the g	enerated SQL query can cause		
those inputs to be interpreted as SQL instead of ordinary user data. This can be used to	alter query logic to bypass		
security checks, or to insert additional statements that modify the back-end database, p	ossibly including execution of	Scanner Recommend	lation:
system commands.			
SQL injection has become a common issue with database-driven web sites. The flaw i	s easily detected, and easily	B	and the second data and the second sector data data data data data data data dat
exploited, and as such, any site or software package with even a minimal user base is	ikely to be subject to an	Frevenung injection require	es keeping unirusted data separate irom commands and queries.
attempted attack of this kind. This flaw depends on the fact that SQL makes no real di	stinction between the control and	The surface dention is to a	as a set. A DY which evolds the use of the interpreter entirche as according a second sized
data planes.		The preferred option is to u	ise a safe AP1 which avoids the use of the interpreter entirely of provides a parameterized
		interface. Be careful with A	tris, such as stored procedures, that are parameterized, but can still introduce injection under
Applicable Platforms		the nood.	
Languages: All		If a parameterized ADI is a	of available, you should carefully escape special characters using the specific scapes writer for
Technology Classes: Database-Server		that interpreter	or available, you should carefully escape special characters using the specific escape syntax for
		that interpreter.	
Common Consequences			
Technical Impact: Read application data	E		
Confidentiality Since SQL databases generally hold sensitive data, loss of confident	iality is a frequent problem with		
SQL injection vulnerabilities.			
Technical Impact: Runass protection mechanism			
Access Control If noor SOL commands are used to check user names and nassword	it may be possible to connect		
to a system as another user with no previous knowledge of the passy	word		
to a system as another over that no pretrots showingge of the pass			

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.

14	Apply Reject Un-Reject Settings+								
	Attack	Attack Group	Severity 🔺	URL	Parameter	Status	Recommendation		
	SQLInjection	SQL Injection	High	http://test.blorpazort.com/pages/sqli_form	region	A NEW	Parameter profile with SQL Injec	-	
	RemoteFileInclusion	Remote File Inclusion	High	http://test.blorpazort.com/pages/rfi.php	color	A NEW	No recommendation.		
	OsCommandInjection	OS Command Injection	High	http://test.blorpazort.com/pages/os_injectio	cmd	A NEW	Parameter profile with OS Com		
	BlindOsCommandInjection	Blind OS Command Injection	High	http://test.blorpazort.com/pages/os_injectio	filename	A NEW	Parameter profile with OS Com		
	Unvalidated Redirect	Unvalidated Redirect	Medium	http://test.biorpazort.com/pages/redirect_u	uri	A NEW	No recommendation.		
		Webserver vulnerability	Medium	http://test.blorpazort.com/		A NEW	No recommendation.		
	ReflectedXSS	Reflected Cross-Site Scrip	Medium	http://test.blorpazort.com/pages/xss_parsi	uri	A NEW	Parameter profile with XSS ena		
	ReflectedXSS	Reflected Cross-Site Scrip	Medium	http://test.blorpazort.com/pages/rfi.php	color	A NEW	Parameter profile with XSS ena		
	ReflectedXSS	Reflected Cross-Site Scrip	Medium	http://test.biorpazort.com/pages/xss_form	search	A NEW	Parameter profile with XSS ena		
	ReflectedXSS	Reflected Cross-Site Scrip	Medium	http://test.blorpazort.com/pages/xss_form	q	A NEW	Parameter profile with XSS ena		

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