# WAF Test Drive Tutorial User Guide

Welcome to our test drive.

EDGENEXUS



pre-sales@edgenexus.io edgenexus.io



### This document will provide you with the information you need to get the most out of your WAF Application firewall test drive



The WAF test drive is a complete web application application security testing and training environment. This includes, Load balancer/ADC, WAF (Web Application Firewall), Zap application attack tool, DVWA (Dam Vulnerable Web Application)

It can be downloaded below (you don't need an Azure account).



The ALB-X has the ability to run containerised applications that can be joined together directly or by using the load balancer proxy.

This image has 3 already deployed but you can always go to Appstore and deploy more.

JetNEXUS	🚠 IP-Services 🕹 Add-Ons X					GUI Status	🕷 Home	telp
Avioxinon 0	⇔ Add-Ons							
IB Library	dvwa1							
Add-Ons			Container Name: dvwa1		Parent Image: DVWA-jetNEXUS_TEST_0	NLY.		
- 🚵 Apps	CONTRACT	<b>II</b> II <b>I</b>	External IP:		Internal IP: 172.31.0.4			
Authentication	DAMAT		External Port:		Started At: 2018-03-05 11:07:53			
Cache			Cr Update	Remove Add-On	Stopped At:			
->\$ flightPATH					Import File: Browse Id Brow	59		
Real Server Monitors					Import Configuration			
- 🔒 SSL Certificates					C Export Configuration			
- Widget								
	waft							
			Container Name: wafl		Parent Image: ietNEXUS-Application-Fire	vall-		_
			External IP:		Internal IP: 172.31.0.5			
		■ II ►	External Port:		Started At: 2018-03-05 11:08:07			
			Cr Update	Remove Add-On	Stopped At:			
					Import File: Browse 🗹 Brow	se		
		C Add-On GUI			Import Configuration			
					C Export Configuration			
	zap1							
			Container Name: zap1		Parent Image: jetNEXUS-OWASP-ZAP-jet	NEX		
		<b>—</b> 11 b	External IP:		Internal IP: 172.31.0.9			
			External Port:		Started At: 2018-03-05 13:40:29			
			Cr Update	Remove Add-On	Stopped At:			
@ View					Import File: Browse 🗠 Brow	59		
🖌 System					C Import Configuration			
F Advanced					C Export Configuration			
🕀 Help 🛛 🕄								

edgenexus.io

The Web Application Firewall is one of several feature add-ons that can be applied to the ALB-X load balancer.



We have tried to make the deployment of the WAF as simple as possible but there are obviously a few things that you can configure to adjust the environment to suit your needs.

We will highlight these settings during the cause of this test drive walk-through.

In a real life scenario the WAF would receive and inspect http requests / traffic from the client and forward or block those requests from reaching your web application depending on whether the request triggered a firewall rule.

We've assumed in the first place you probably don't want to subject your live web application to a malicious attack but do want to see how the WAF operates. (This can be easily changed if you want to test you real servers)

So we have set up a self contained environment to be able to exercise and demonstrate the WAF behaviour.

We have chosen to use 2 widely used security test tools to do this the 'OWASP Zed attack proxy' to be able to generate attack traffic and the 'Damn Vulnerable Web Application' which as its name suggests simulates a web application with many security holes to exploit.

While we will walk through some basic configuration settings here to be able to use these tools, this document should not be regarded as a comprehensive guide to the applications.

We would encourage you to visit each of the tools official online portals for full details if you are not already familiar with their use or operation.



Damn Vulnerable Web Application (DVWA)

As ever you will find several video walkthroughs on YouTube that may also be useful to check out. Both of these tools have been imported quickly and easily onto the ALB-X docker container environment, the same environment that we use to deploy the WAF (and also GSLB).

## **Connectivity Overview**

Virtual machines deployed in the Azure cloud make use of private internal IP addressing (NAT'ed IP's) in the same way as would be deployed in a standard data centre environment.



To gain access to the resource via the public internet a NAT function is performed from the allocated Public IP address to the Private IP address of the virtual machine.

One IP address is allocated to the appliance and different ports are used to access the different resources.

The diagram below shows how the different functions communicate.



	jetNEXUS ADC Load ba	lance and Proxy
dvwa1		
DYWR	Container Name dowel	NOTE: Use Hostnames Not IP, as IP's are dynamically assigned
wafi		
	Container Name weft Internal IP 1723105 Ports: 80, 443	
zapl		
0	Container Name: zap1 Internal IP: 172.31.0.9	

### Docker host name / IP address and IP service connectivity

Add-on applications deployed on the ALB-X communicate with ALB-X through an internal docker0 network interface. They are automatically allocated IP addresses from the internal docker0 pool.



A host name for each instance of add-on application is configured through the ALB-X GUI prior to starting the application.

The ALB-X is able to resolve the dockerO IP address for the application using this internal host name.



Always use the host name when addressing the application containers – IP's may change!

IP services using the Azure eth0 private IP address are configured on the ALB-X to allow for external access to the add-on application. This enables the use of the ALB-X reverse proxy function to perform SSL offload and port translation where required.

So these are all the open ports:

- → ALB-X GUI Management: 27376
- $\rightarrow$  ZAP attack Proxy: 8080 and 8900
- → DVWA: 8070
- Ports 80 and 443 are open to allow direct access to the WAF

## **Accessing the Test Drive GUI**

When you request a test drive a new instance of the WAF test appliance is created in Azure. Once it has started you will be advised the Internet host name to be able to access the Web GUI of the ALB-X platform also the unique user name and password combination.

Your Web Application Firewall Test Drive is ready. You have 8 hours to try the product. Instructions are available in your <u>Test Drive user manual</u>.

#### Here's the basic info:

Test Drive: Web Application Firewall Publisher: jetNEXUS Host Name: jetnexus-water adw.centralus.cloudapp.azure.com User Name: admin Password:

Publisher contact: https://www.edgenexus.io/support/

Go to your Test Drive

Thank you and have a great Test Drive!

Microsoft Azure Marketplace Team

We recommend using the Chrome browser for this purpose.



Access the Server https://host name:27376

As we use a local SSL certificate for the management access you will be prompted in your browser to accept the security alert.

You will see the pre-configure IP services screen once you login.

We have named each of the services to make it easy to identify what they are used for and how you need to construct the link in your browser address bar to access the service, replacing the x.x.x.x with the Azure host name or public IP address. Note it is normal for the Zed Attack Proxy service on port :8090 to show a red health check error until it is started by accessing the proxy management interface on port :8080/zap/.

### ALB-X add-ons

Click on Library in the left menu and select Add-Ons.

JetNEXUS	in IP-Services 4 Add-Ons X			🧐 GUI Status 🗌 Home 🕀	delp
	د Add-Ons				
Services					
ii\ Library	dvwa1				
- 🕂 Add-Ons			Container Name: dvwa1	Parent Image: DVWA-jetNEXUS_TEST_ONLY.	
- 🚵 Apps	(DYWA)		External Port:	Started At 2018-03-05 11-07-53	
- M Authentication			Ct Hodate	Remove Add. On     Stopped At:	
-Xt flightPATH				Import File: Browse	
- 🚯 Real Server Monitors		C Add-On GUI		C Import Configuration	
🔒 SSL Certificates				C Export Configuration	
- Widget					
	wafi				
			Container Name: waft	Parent Image: jetNEXUS-Application-Firewall-	
		■ 11 ►	External IP:	Internal IP: 172.31.0.5	
				Started Ac. 2018-03-05 11:08:07	
			<b>O</b> Update	Remove Add-On     Import File: Browse     The Browse	
		C Add-On GUI		Umport Configuration	
				C Export Configuration	
	zap1				
			Container Name: zap1	Parent Image: jetNEXUS-OWASP-ZAP-jetNEX	
		■ 11 ►	External Pr:	Internal IP: 172.31.0.9	
			de linder	Dependent Add On     Stopped At:	
@ View			• opuate	Import File: Browse	
🖌 System 🕕		C Add-On GUI		C Import Configuration	
F Advanced				C Export Configuration	
C Help					

Here you can see the 3 Add-Ons that have been deployed on the ALB-X platform.

Each has been configured with a container or hostname (waf1, zap1, dvwa1) and you can see the 172.31.x.x dynamic docker0 IP address that was allocated when the application was started.

Note in the Azure environment the Add-On GUI access buttons are not used.

Feel free to click around the rest of the ALB-X GUI interface for familiarity.

### WAF GUI

As it is the WAF functionality that you are interested in it would make sense now to take a look at the WAF GUI.



The WAF Management as you can see from the IP services naming runs on port :88 to which you must add the path /waf/ when entering address in your browser.

When you do you will be presented with the login screen.



The default user name and password combination is admin / jetnexus. When logged in you will see the following screen.



This dashboard shows a summary of the events that have been triggered by the WAF in the last 24hrs. As this is a pre configured test drive we have already set the details of the host to be protected on the Management page.

🖉 ALB-X-1 X 🔅 Webswing X 🗅 jetNEXUS Web Applicatic X			Cli	7	-		×
← → C ③ 10.4.9.33:88/waf/management.php	☆		0	0	ABP 🖉	13	:
🥑 jetNEXUS WWW 🥊 ESXi 👌 WAF SQL Inj 👌 WAF URL 👌 Pre-Auth 👌 SNI1 👌 SNI2 🗅 GSLB demo 🗅 V	VAF Manage		,	>	Other	bookma	arks
HOME EVENTS FILTER FIREWALL DOS EVASION	MANAGE	MENT	Logge	ed Use	er: Admii	1   Logou	ut 🔺
Config Real Server / VIP							
Info Info Info Info Info Info Info Info							
Requests Keep-Alive Carabled Disabled							
Proxy Preserve Host Enabled     Disabled							
Absolute URL to Relative URL							
Convert specified absolute URL to a relative URL in response body (strip host address part of the URL)							
Client IPs Forwarding							
header generated by a reverse proxy at the following IP address							
Log Storage ☞ Store Local Logs							
Store Remote Logs							
Update configuration							
							-

The test drive has dynamically obtained the Azure private interface IP address and set this in the real server / VIP configuration box along with port :8070 the port we have chosen to use to access the DVWA web server. As this is a pre configured test drive we have already set the details of the host to be protected on the Management page.



The Real server /VIP is the address:port of the application or Virtual server that we are protecting.

Please feel free to change the IP address here to point to your own server.



Note to support HTTPS traffic externally you will need to send the traffic via an ALB-X service in the similar way to how we have configured access the DVWA server.

Whilst here we should take a look at the WAF Firewall page. This is where you set the mode of operation and can see which rules have been detected and allows for white listing of rules that you don't want to block.

The rule set loaded by default is the OWASP core ruleset. This contains details of literally thousands of different attack vectors as maintained by OWASP.

-	OWASP COLE I dieset		
	ALE-X-WAF x		- an
	← → C 0 51.143.137.162.88/wa//frewall.php		x 🛛 🕅 🛆 🦸
	jetNEDUS WWW 🥐 ESXi J WAF SQL Inj J WAF URL J Pre-Auth J SN1 J SN12 J GSLB demo 🗋 WAF Manage 🥥 jetNEXUS Login		
	Fivewall Control OSabibid © Datation adh © Datation adh blochag	comme actuality fixing fitherings, books	arran an ann Mhill
	Matched Rules Whitelisted Rules 92035 (Hist Insets is a numet: P address) 920110 (Dactory Listing) 580110 (Dactory Listing) 580110 (Dactory Listing) 580110 (Dactory Listing) 680110 (Dactory Listin		
	Manually add rule IDs to whitelist		
	Creation rules before OWASP CBS # User defined rules and settings. # These custom rules will be applied before OWASP CRS rules.		
	Custom rules after OWASP CRS # User defined cules and settings. # These custom rules will be applied after OWASP CRS rules.		

The screen shot above shows the WAF running in the default detect only mode. Please change this to detect and blocking mode in the test drive so the WAF will actively block any attacks. Currently you shouldn't have any events but once you do they will be displayed like this.

÷ -	G G	10.4	.9.33:88/	/waf/eve	nts.php			
J je	INEXUS W	ww 🧧	ESXi	U WAF S	SQL Inj 🥑 W	AF URL 🥑 Pre-	Auth 🕑 SNI1 🔮 SNI2 🗋 GSLB demo 🗋 WAF Manage 🥥 jeth	IEXUS Login
					15:58:40	42852	Method <u>SELT</u> Park <u>Autorchalitestotic Mind?</u> guery-guery/Stemos/t-SET-Y-5/780%7D Status Code: <u>403</u> (Forbidden)	found with ARGS super, cound/timeder (7 (0))     Emende Command Execution: White Command Emission (Matched Data:     [Imeed: found within ARGS query: query)(Imeed/7 (0))     Hoburds Anomaly Score: Exceeded (Total Score; 13)     Host Ihader is a numeric (F2 Address (10.4 9.30))     Host Ihader is a numeric (F2 Address (10.4 9.30))     Host Ihader is a numeric (F2 Address (10.4 9.30))     Host Ihader is a numeric (F2 Address (10.4 9.30))     Host Ihader is a numeric (F2 Address (10.4 9.30))     Host Ihader is a numeric (F2 Address (10.4 9.30))     Host Ihader is a numeric (F2 Address (10.4 9.30))     Host Ihader is a numeric (F2 Address (10.4 9.30))     Host Ihader is a numeric (F2 Address (10.4 9.30))     Host Ihader is a numeric (F2 Address (10.4 9.30))
	<u>Details</u>		WAF.	2	2018-03-05 15:58:40	<u>172.31.42.1</u> 42770	Hostname: <u>10.4.9.33</u> , Port: 80, Method: <u>POST</u> , Path: <u>(login.php</u> Status Code: <u>302</u> ( <i>Found</i> )	Host header is a numeric IP address (10.4.9.33)
	<u>Details</u>	8	WAF.	2	2018-03-05 15:58:40	<u>172.31.42.1</u> 42868	Hostname: <u>10.4.9.33</u> , Port 80, Method <u>(SE)</u> , Park <u>sylveratikitieskold</u> ? query-queryRichoust-%2FT-%780%7D Status Code: <u>403</u> ( <i>frontiden</i> )	Remote Command Execution: Unix Command Injection (Matched Data Jineout Numl with ARGS query, exery/timeout // (0) Remote Command Execution: Vindous Command Injection (Matched Data Jineout Numl Xoore: Exected of Unit Score: 13) Hosh Indonei Janomi, Score: Exected of Unit Score: 13) Hosh Indonei Janomi, Score: Exected of Unit Inform (Score: 13) Hosh Indonei Xoore: Score: Score (11) Scole: 10, Score: Romotol (11) all Inform (Score: 13) Scole: 10, Score: Romotol (11) all Inform (Score: 13) Hosh Indonei Xoore: 11)
	Details	8	<u>WAF</u>	2	2018-03-05 15:58:39	172.31.42.1 42868	Hostname: 10.8.9.33, Port 80, Method (2017, Park, <u>submethalisestodi</u> ?? Query-query:NScienced+%2F1-%780%7D%26 Status Code: <u>403</u> (Forbidden)	Remote Command Execution: Link: Command Injection (Matched Data & Alimecut Fourd with ARSS Query: ouery dameeut /7 (0)8. Remote Command Execution: Window Command Injection (Matched Data & Armeout Down of Window Command Injection (Matched Data & Armeout Down of Window Command Injection (Matched Data Host Index Injection Command Injection (VIII) Host Index Injection Command Injection (VIII) Host Index Injection Command Injection (VIII) Host Index Injection Command Injection (VIII) Science Data (VIIII) Science Data (VIIII) Science Data (VIIII) Host Index (Link) Katel (VIIII) Katel (VIIIII) Katel (VIIII
	<u>Details</u>	8	WAF.	2	2018-03-05 15:58:39	<u>172.31.42.1</u> 42868	Hostname: 10.4.9.33. Port 80, Method (SET, Pani, <u>Auferralitäiseskal, bind</u> /7 queerjaeuery/Normout-%2FT+%780%7D Status Code: <u>403</u> ( <i>Forbidden</i> )	Bernote Command Execution: Unix Command Injection (Matched Data Jimeout Naura Winh ARGS Query: carey/Direcol.77 (0) Bernote Command Execution: Windows Command Injection (Matched Data Jimeout David with ARGS Query: carey/Direcol.77 (0) Inhomand Namuthy Xoore Executed (Total Backson: 18) Hold Inhold Ramathy Xoore Executed (Total Backson: 18) Status 253:-0 (NH-0) Lin-15 RCC-0 PWIN-0 HTTP-0 SICSS-0). Path Traverse Altabal. (L.)
	<u>Details</u>	8	WAF.	2	2018-03-05 15:58:39	<u>172.31.42.1</u> 42852	Hostname: 10.4.9.33. Port 80, Method (§E.T. Parn: <u>cytomerabilites/sold</u> ? query-query/Structs-12, F1-%780%7D Status Code: <u>403</u> ( <i>franciden</i> )	Bernote Command Execution: Unix Command Infection (Matched Data Jimeout Dawa ethin ARGS Query, cayer/primeout /7 (0)) Bernote Command Command Infection (Matched Data (Inneout Dawa) with ARGS Query, query/primeout /7 (0)) Infolmedia a zumeric (IP addites) (104.4.3.5) Infol Intelle is a Innersic (IP addites) (104.4.3.5) Infol Intelle is a Innersic (IP addites) (104.4.3.5) Infol Intelle Intelle Intelle Intellection (Intellection Intellection) Double JASSI (IP Intellection) (IP and Intellection) Addites (L))

edgenexus.io

You are able to apply a filter to the events screen to be able to hone in on specifics events you are interested in observing.

sett	or lodavi ) Classa Filkan				
	Filter Editor				×
	General		Anomaly Scoring		
16	Date From	2018-03-01 00:00:00	Total Score	2 1	
n	Date To	2018-03-01 23:59:59	SQLi Score	2 1	
C	Sensor	Not All Sensors	XSS Score	2 1	
n	Target Hostname	Not	Dula Timing (in miliagoanda)		
l: C	Client IP	Not	Duration	2 1	
	Client IP Country Code	Not	Combined	2 1	
1	Client IP AS Number	Not	Phase 1	2 1	
	Action	Not All Actions	Phase 2	2	
	Event Severity	Not All Severities	Phase 3	2 1	
Ł	Engine Mode	Not All	Phase 4	2 1	
1	HTTP Method	Not 🗌 All Method 🔹	Phase 5	2 7	
	Path	Not	Storage Read	2 7	
	HTTP Status	Not All Status	Storage Write	2 1	
	User ID	Not	Logging	2 1	
	Rule ID	Not	Garbage Collection	2 1	
	Tag	Not All Tags			
	Web App Info	Not 🔲			
	Marked as False Positive	<b></b>			
	Preserved Events	<b>T</b>			
	Unique ID				
Ŀ			_		
				Apply Filter Cancel Clear Filter	
					111

### Zed Attack Proxy

Whilst we recommend using the Chrome browser for the management access to the appliances you will want to use another browser to generate the test traffic and I'd recommend Firefox for this purpose.



ZAP is started by connecting your management (Chrome) browser to :8080/zap/. When you do this you will first see the first ZAP webswing initializing screen.



This will change to the next ZAP startup.





And then you have the option to choose whether you want to persist the session, so it can be loaded again afterwards. For the test drive this probably isn't required.



Once this is complete ZAP will be running and the LED on the 8090 IP service will change from Red to Green showing the TCP health check is passing as port :8090 is now open.



We now need to configure the browser to use a proxy. You can now configure your Firefox web traffic browser to use the ZAP Public IP address and port :8090 as the Network Proxy.

onfigure Proxie	es to Access the Internet		
No proxy			
Auto-detect p	roxy settings for this net <u>w</u> ork		
Use system pro	oxy settings		
Manual proxy	configuration		
HTTP Pro <u>x</u> y	XXXX	<u>P</u> ort	8090 ÷
	<ul> <li>Use this proxy server for all protocols</li> </ul>		
SS <u>L</u> Proxy	XXXX	P <u>o</u> rt	8090
ETP Proxy	XXXX	Po <u>r</u> t	8090
SO <u>C</u> KS Host	X.X.X.X	Por <u>t</u>	8090
	SOC <u>K</u> S v4 O SOCKS <u>v</u> 5		
<u>N</u> o Proxy for			
localhost, 12	27.0.0.1		
Example: .moz	illa.org, .net.nz, 192.168.1.0/24		
Automatic pro	xy configuration URL		

Replace X.X.X.X with the Public IP of your test drive.

### DVWA access via ZAP Proxy

You should now be able to access DVWA using the Firefox traffic browser via the ZAP Proxy and the WAF by entering the host name or Public IP address of your Test Drive using the standard web port :80 either http://X.X.X.X or something like



http://jetnexus-wafturcokjygzudw.centralus.cloudapp.azure.com

You should see a screen like this.

	DYWA
Setup DVWA         Instructions         About	<section-header>  Descendence for the formation of the series of the the below to create or reset your database.   Che data carrier of make surve you have the correct user credentials in: var/www.thml.config.config.con.ep.   Che database already exists, it will be cheared and the data will be reset.   Che database already exists, it will be cheared and the data will be reset.   Che database already exists, it will be cheared and the data will be reset.   Che database already exists, it will be cheared and the data will be reset.   Che database already exists, it will be cheared and the data will be reset.   Descendence allow of the operation o</section-header>
	Damn Vulnerable Web Application (DVWA) v1.9

Click on Create / Reset Database.

Create / Reset Database	
Database has been created.	
'users' table was created.	
Data inserted into 'users' table.	
'guestbook' table was created.	
Data inserted into 'guestbook' table.	
Setup successful!	
Please <u>login</u> .	
Damn Vulnerable Web Application (D\	WA) v1.9

Login to DVWA with default credential admin / password.

	DVWA
Username	
admin	
Password	
••••••	
	Login

You will now be logged into DVWA as admin.



#### Home

Instructions

Setup / Reset DB

#### Brute Force

Command Injection CSRF File Inclusion File Upload Insecure CAPTCHA SQL Injection SQL Injection (Blind) XSS (Reflected) XSS (Stored) DVWA Security

PHP Info

About

Logout

#### Welcome to Damn Vulnerable Web Application!

Damn Vulnerable Web Application (DVWA) is a PHP/MySQL web application that is damn vulnerable. Its main goal is to be an aid for security professionals to test their skills and tools in a legal environment, help web developers better understand the processes of securing web applications and to aid both students & teachers to learn about web application security in a controlled class room environment.

The aim of DVWA is to practice some of the most common web vulnerability, with various difficultly levels, with a simple straightforward interface.

#### General Instructions

It is up to the user how they approach DVWA. Either by working through every module at a fixed level, or selecting any module and working up to reach the highest level they can before moving onto the next one. There is not a fixed object to complete a module; however users should feel that they have successfully exploited the system as best as they possible could by using that particular vulnerability.

Please note, there are **both documented and undocumented vulnerability** with this software. This is intentional. You are encouraged to try and discover as many issues as possible.

DVWA also includes a Web Application Firewall (WAF), PHPIDS, which can be enabled at any stage to further increase the difficulty. This will demonstrate how adding another layer of security may block certain malicious actions. Note, there are also various public methods at bypassing these protections (so this can be see an as extension for more advance users)!

There is a help button at the bottom of each page, which allows you to view hints & tips for that vulnerability. There are also additional links for further background reading, which relates to that security issue.

#### WARNING!

Damn Vulnerable Web Application is damn vulnerable! Do not upload it to your hosting provider's public html folder or any Internet facing servers, as they will be compromised. It is recommend using a virtual machine (such as <u>VirtualBox</u> or <u>VMware</u>), which is set to NAT networking mode. Inside a guest machine, you can downloading and install <u>XAMPP</u> for the web server and database.

#### Disclaimer

We do not take responsibility for the way in which any one uses this application (DVWA). We have made the purposes of the application clear and it should not be used maliciously. We have given warnings and taken measures to prevent users from installing DVWA on to live web servers. If your web server is compromised via an installation of DVWA it is not our responsibility it is the responsibility of the person/s who uploaded and installed it.

#### More Training Resources

DVWA aims to cover the most commonly seen vulnerabilities found in today's web applications. However there are plenty of other issues with web applications. Should you wish to explore any additional attack vectors, or want more difficult challenges, you may wish to look into the following other projects:

- **bWAPP**
- NOWASP (formerly known as Mutillidae)
- OWASP Broken Web Applications Project

The default security level for DVWA is 'Impossible' so it will not exhibit any vulnerabilities. You should set the level to low by clicking on the DVWA Security menu selecting Low from the drop down and clicking submit.



Home

About

Logout

Instructions

Setup / Reset DB

Brute Force
Command Injection
CSRF
File Inclusion
File Upload
Insecure CAPTCHA
SQL Injection
SQL Injection (Blind)
XSS (Reflected)
XSS (Stored)
DVWA Security
PHP Info

DVWA Security 🖗

#### Security Level

Security level is currently: impossible.

You can set the security level to low, medium, high or impossible. The security level changes the vulnerability level of DVWA:

- Low This security level is completely vulnerable and has no security measures at all. It's use is to be as an example of how web application vulnerabilities manifest through bad coding practices and to serve as a platform to teach or learn basic exploitation techniques.
- Medium This setting is mainly to give an example to the user of bad security practices, where the developer has tried but failed to secure an application. It also acts as a challenge to users to refine their exploitation techniques.
- 3. High This option is an extension to the medium difficulty, with a mixture of harder or alternative bad practices to attempt to secure the code. The vulnerability may not allow the same extent of the exploitation similar in various Canture The Flags (CTEs) competitions.
- exploitation, similar in various Capture The Flags (CTFs) competitions.
  4. Impossible This level should be secure against all vulnerabilities. It is used to compare the vulnerable source code to the secure source code.
- Priority to DVWA v1.9, this level was known as 'high'

Low V Submit

#### PHPIDS

PHPIDS v0.6 (PHP-Intrusion Detection System) is a security layer for PHP based web applications

PHPIDS works by filtering any user supplied input against a blacklist of potentially malicious code. It is used in DVWA to serve as a live example of how Web Application Firewalls (WAFs) can help improve security and in some cases how WAFs can be circumvented.

You can enable PHPIDS across this site for the duration of your session.

PHPIDS is currently: disabled. [Enable PHPIDS]

[Simulate attack] - [View IDS log]

DVWA is now all primed and ready for use as a vulnerability test target.

### **Using ZAP**

There are a few steps to follow to set up ZAP to first spider the DVWA application and then perform an attack. We would refer you to the several online resources for details on how to set this up rather than regurgitate the information here.

### Youtube Video



This YouTube video walks the precise steps and is what I followed myself in the process of setting up this test drive. Note it runs rather fast so I recommend slowing the video by half or a quarter.

Where it refers to setting your browser proxy to localhost, you have already performed the necessary configuration steps above.

### **Viewing the Results**

When you have performed the attack you should be able to view the results in both the ZAP Proxy and WAF GUI's. Here you can see the vulnerabilities tree that was spidered and then attacked as the admin user.

🔇 Untitled Session - OWASP ZAP 2.	7.0								
<u>E</u> ile <u>E</u> dit <u>V</u> iew <u>A</u> nalyse <u>R</u> eport <u>T</u> ools <u>O</u> nline <u>H</u> elp									
Standard Mode 💌 🗋 🖨 📰 💼	) 🔅 💷 💻 🗖 🗖 🗖	□ 🗆 🖶 💋 💡 🕒 🕨 🖉 🗶 📾 🐂 📼 🛛 🛛 💿							
🚱 Sites 🕂									
Restingin php(Login pd		Welcome to the OWASP							
B      B      GET:robots txt	🔍 Active Scan								
P # GET:sitemap.xml	Scope								
P # GET:vulnerabilities									
▼ 3 P vulnerabilities	starting point:	http://10.4.9.33/vulnerabilities/							
o P GET:brute	Policy:	Default Policy							
o 🕷 GET:captcha									
o 😻 GET:csrf	Context:	http://10.4.9.33							
o P GET:exec	User:	admin							
適 🕷 GET:fi									
適 🕷 GET:sqli	Recurse:								
🤘 🕷 GET:sqli_blind	Show advanced options								
o 🕷 GET:upload									
o 😽 GET:view_help.php									
o 😽 GET:view_source.php									
o Ketter (1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.									
o 😽 GET:xss_r									
o 😽 GET:xss_s									
joine abilities(C)									
🛗 History 🔍 Search 🏴 Alerts		=							
₩ New Scan 🗄 Progress: 1: Context:		1							
URLs Added Nodes Messages	0	Cancel Reset Start Scan							
Processed Meth		1.090							



By looking at the WAF GUI you can see the attacks that were detected and blocked.

Firewall Control Disabled Detection only Detection and blocking	
Matched Rules 322115 (Remote Command Execution: Windows Command Injection) 322120 (Remote Command Execution: Windows PowerShell Command Found) 32130 (Remote Command Execution: Unix Shell Expression Found) 322150 (Remote Command Execution: Unix Shell Code Found) 932160 (Remote Command Execution: Unix Shell Code Found) 933160 (PHP Injection Attack: High-Risk PHP Function Call Found) 941100 (XSS Attack Detected via libinjection) 941100 (NoScript XSS InjectionChecker: HTML Injection) 941180 (Node-Validator Blacklist Keywords) 94180 (Node-Validator Blacklist Keywords)	Whitelisted Rules
Manually add rule IDs to whitelist	
# User defined rules and settings. # # These custom rules will be applied before OWASP CRS rules. #	
Custom rules after OWASP CRS	~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
# User defined rules and settings. # # These custom rules will be applied after OWASP CRS rules. #	
Update configuration	

jetNEXUS Web Application Firewall

Back in the ZAP proxy window you can see that the attacks received a 403 error response from the WAF blocking their progress through to the DVWA server.

	= History	🔍 Search р Ali	erts 📄 Output 🛛 🕷 Spider 🕽	👌 Active Scan 🖉	* +					
0	🕮 👌 New S	Scan : Progress: 2	: http://10.0.0vulnerabilities	💽 🕞 💷 🚺	40%		ダ Current Scans: ]	Num requests: 244		ŝĝ
	d	Req. Timestamp	Resp. Timestamp	Method	URL	Code	Reason	RTT	Size Resp. H	Size Resp. B
	2,593	28/02/18 16:22:20	28/02/18 16:22:20	GET	http://10.0.0.246/dvwa/vulnerabilities/sqli/?id=%		03 Forbidden	60 ms	226 bytes	179 bytes 🔒
	2,595	28/02/18 16:22:20	28/02/18 16:22:20	GET	http://10.0.0.246/dvwa/vulnerabilities/sqli/?id=%		103 Forbidden	53 ms	226 bytes	179 bytes 🏠
	2,597	28/02/18 16:22:20	28/02/18 16:22:20	GET	http://10.0.0.246/dvwa/vulnerabilities/sqli/?id=%2		103 Forbidden	53 ms	226 bytes	179 bytes 🚽
	2,599	28/02/18 16:22:20	28/02/18 16:22:20	GET	http://10.0.0.246/dvwa/vulnerabilities/sqli/?id=%5		103 Forbidden	48 ms	226 bytes	179 bytes
	2,601	28/02/18 16:22:20	28/02/18 16:22:20	GET	http://10.0.0.246/dvwa/vulnerabilities/sqli/?id=Win	:	200 OK	84 ms	353 bytes	1.49 KiB
	2,603	28/02/18 16:22:20	28/02/18 16:22:20	GET	http://10.0.0.246/dvwa/vulnerabilities/sqli/?id=Win	:	200 OK	82 ms	353 bytes	1.49 KiB
	2,605	28/02/18 16:22:20	28/02/18 16:22:20	GET	http://10.0.0.246/dvwa/vulnerabilities/sqli/?id=%2		103 Forbidden	51 ms	226 bytes	179 bytes
	2,607	28/02/18 16:22:20	28/02/18 16:22:21	GET	http://10.0.0.246/dvwa/vulnerabilities/sqli/?id=%		103 Forbidden	84 ms	226 bytes	179 bytes
	2,609	28/02/18 16:22:21	28/02/18 16:22:21	GET	http://10.0.0.246/dvwa/vulnerabilities/sqli/?id=%2		103 Forbidden	47 ms	226 bytes	179 bytes 🔻
	Inducty       Querter       Paters       Output:       W Option       Active Juliar       Image: Control of the second									

The WAF is performing its intended role to protect the attacks on the application server.

### **DOS – Denial of Service**

In addition to being able to block thousands of hack attacks, the WAF is also able to filter some DOS attack behavior from reaching sensitive web servers.



jetNEXUS Web Application Firewall

## Experiment

Hopefully, you will find this test drive useful to be able to discover the ease of setting up the Edgenexus ALB-X Web Application Firewall implementation.





We would encourage you to experiment some more with the interface and you could always temporarily divert some live traffic through the WAF in detection mode to see what attacks are potentially being made to your own published applications, you might be surprised!

We welcome your feedback and would be glad to assist with setting up your own production WAF implementation.

# Thank you.

We really hope you enjoy your Edgenexus ALB-X Web Application Firewall implementation.

We would welcome any questions you may have to

### pre-sales@edgenexus.io

0808 1645876

(866) 376-0175

edgenexus.io

EDGENEXUS

Copyright © 2021 Edgenexus

