How to use OWASP Zed Attack Proxy (zaproxy)

Motivation

Finally, after writing the papers, How to securely isolate Damn Vulnerable Linux with VirtualBox and How to securely isolate Kali Linux with VirtualBox, this paper is dedicaated to the execution of attacking the Web and DataBase services on Damn Vulnerable Linux with Zed Attack Proxy. If you are not familiar with this beautiful, free tool, review it here: <u>http://tools.kali.org/web-applications/zaproxy</u>

Basically, this tool enables Pen Testers an automated method to attack web servers and validate the security level of said.

Test environment layout

My workstation is running Ubuntu 16.10. I am first installing VirtualBox 5.1.6 for Ubuntu, using method 2 below. Damn Vulnerable Linux 1.5 running inside of VirtualBox 5.1. Kali Linux running in inside VirtualBox 5.1.

Setup and deployment

Asuming you followed the previous papers mentioned in Motivation, go ahead and start both virtual machines now.



This is the login screen for Damn Vulnerable Linux. Your user name is root and the password is toor.



Type in "startx &" and hit enter.



This is the initial X11 window system.



Using the left icon, I believe KDE gears, follow the diagram and start the HTTPD service.



Start the MySQL service.



Start the Postgres service.



Start the SSHD service.

Start the Tomcat service.

Now, Switch to the running Kali Linux virtual machine.

Once you authenticate in (username root, password toor), this is what you will see.

You will see this on the initial startup of the application.

Applica	ations 🔻 Pla	ces 🔻 🐧 OWASP	ZAPtio9 🔻			Sun Nov 27,	17:01•					1,2	40) F -
	pplications Places Pla				Untitled Session - OWASP ZAP 2.5.0								
898					Progress	This option can	changed via Tools/i	Options OK					
)	History	🔍 Search 🏾 🏴 Alerts	Output 🛉)									¥.
	🎯 🚳 🍸 Filt	er:OFF											
	Id	Req. Timestamp	Method	URL		Code	Reason	RTT	Size Resp. Body	Highest Alert	Note	Tags	B 4
	Alerts P 0 🖡	0 🕫 0 📢 0								Current Sca	ans 🥮 0 😽 0	0 0 🕷	0 20 0 80

Use the pull down menu, under 03-web-application-analysis, open "owasp-zap".

Click OK.

ti •) € -) 1	1												Nov 27, 17:01 •	Su							Places 🔻	tions 🔻	Applic
										- x	_ 0	-		dd-ons	Manage A									
										-							Marketplace	Ins						
			-	-	_													ZAP	s Online Heli	Report Tools	alvse R	t View Anal	File Edit	
																version	AP is on the latest v	2.5.	1 68 1 1			d Mode	Standard	
																		Add-				es +	Site:	
	~				_						2	Update			ription	A Descr	e	1						
		t	Select	st.	to tes	rmission t	AP) ilications.	r (Z łb appl ly been	oxy s in we ₂cifical	ose		Update Update Update Update Update	ise of Jav t risk leve etween 2 ed Brows g code fr t related i tst a targ tst a targ tst a targ	we Scanner rules nual testing es that make heavy it the changing of all e language files ing the differences b to be used with "2AP Guide and directories usis and directories usis with ZAP Guide in of the ZAP help fil titons passing conter of solve Scanner rules lows you to quickly to enable disabled file Update Sele	elease quality Act ced fuzer for ma s you to spider sil s you to automat lations of the co ags a dialeg show f directory names d browsing of file that Getting Starte sh (master) versis e external applici online menu item release quality Pa des a tab which a hidden fields an Uninstall Sele	The re Advan Allows Transl Displa List of Englis Invoke ZAP 0 The re Provid Show	e scanner rules uzzer Spider text Alert Filters tol anguage Files tory List VI.0 de Browse ing Started with ZAP - English ke Applications he menus kistart kistart sal		Output]	P Alerts	earch	tory	Con Con Con Con Con Con Con Con	
ß		Tags		Note	1	t Alert	Higher	y	p. Body										Method	amp	Timesta	Req. T	Id	
**0 ~0 **0	<mark>〕</mark> 0 ※(0 (3 0	🧼 0 🔻	cans 📢	lurrent Sc											11			0	0 47 0 0	nci 0 ni 0 ni	Alerts 📍	
	0	0 0	9 0 👌	🥶 o 🔻	cans 📢	urrent Sc											11			0	0 12 0	147 0 49 0 49	Alerts 🗚	

If you have internet access, click on Update All.

Applica	tions ▼ Places ▼	Sun Nov 27, 17:02 •	1 52 40 0 -
	tions • Places • Elle Edit View Analyse Beport Iools Qnline Helf Standard Mode • • • • • • • • • • • • • • • • • • •	Manage Add-ons	At A A A A A A A A A A A A A A A A
	Alerts 🗭 0 🏴 0 🛱 0 🛱 0		【 Current Scans 曼 0 号 0 🚴 0 😡 0 🔆 0 ≯ 0 🧩 0

What we see once completed. Click on Close.

Now open the broswer Iceweasal.

Open Preferences.

Under Advanced, Network, click on Settings.

Applica	ations 🔻 🛛 Places 👻 🧊 Icer	weasel 🔻		Su	n Nov 27, 17	:03•			1 👪 🕬 🗲	•
	Kali Linux. an Offe	× 🗰 Prefe		Proferences - Icewases Connection Settings						
	(e) (e) Teeweasel about:p	oreferences#	Configure Proxie	s to Access the Internet			☆ 自 ♥	↓ ☆ ⊝		
	🚡 Most Visited 🔻 🗍 Of	fensive Secu	 No proxy Auto-detect pr <u>U</u>se system pr 	roxy settings for this net <u>w</u> o oxy settings			ng		T CONTRACTOR	
	👩 General	Ad	• <u>M</u> anual proxy	configuration:					_	
	O Search	110	HTTP Pro <u>x</u> y:			8080 🛟			- •	×
		Gen		✓ Use this proxy server for	or all prot		tes			
	Content									
	Applications 🌲	Conn								1
	🗢 Privacy	Config					Settings			
	🖴 Security	Cach	No Durant fair		🗆 Remo	e <u>D</u> NS			ission to test.	/
	C) Sync	Your w	No Proxy for:	7.0.0.1			<u>C</u> lear Now			
	Advanced	<u> </u>							Select	
898	a Auvanceu	Lin	Example: .moz	zilla.org, .net.nz, 192.168.1	.0/24					
D		Offlin	 <u>A</u>utomatic pro: 	xy configuration URL:						
		Your a					Clear <u>N</u> ow		tests while some for the such 740	
		✓ <u>T</u> el	🗆 Do not prompt f	or authentication if passwe	ord is sav	əd	Exceptions		tests while proxying through ZAP.	
		The fo								v
	💡 Iceweasel automatio	cally sends s	onie data to Mozilia :	so mac we can improve you	ur experie	nice.	Choo	se What I Share	ert Note Tags	ra.
										-
										•
	Alerts 🍽 0 🔍 0 🕅 0								Current Scans 🚭 0 👌 0 🎯 0 勝 0 🎤 0 🌞 0 🕴	Ķ0

Change to Manual, input localhost, port 8080. Check the box for "Use this proxy..." and click OK.

Applica	tions 🔻 Places 🔻	🦉 Iceweasel 🔻					Sun Nov 27, 17:0	4•								1	(0)	3 -
						of / - Icewea												
	Index of /	× +																
	G 9 172 20 0	103					c Q Search	<u>ــــــــــــــــــــــــــــــــــــ</u>	☆ ⋹		1 4	ê e	=					
	Most Visited 🔻	Offensive S	ecurity	Kali Linux	Kall Docs	Kall Tools	Exploit-DB	Aircrack-ng	3									
	Index of	f /																
	Name	<u>Last modif</u>	ied	<u>Size</u> <u>Descriptio</u>	D													×
	Parent Directory	/ 18-Jan-200	9 21:58															
	base/	18-Jan-200	9 21:58	-														4
	info.php	18-Jan-200	9 21:58	1k												\leq	2	
· 🧭	nanual/	18-Jan-200	9 21:58	-													> >	
	Date/	18-Jan-200	9 21:58	-										ssion to test.				
	phpmyadmin/	18-Jan-200	9 21:58	-														*
	unicornscan/	18-Jan-200	9 21:58												(-	_		
	webexploitation	<u>pack></u> 18-Jan-200	9 21:58	-											😺 Select.			
898	webexploitation	<u>pack></u> 18-Jan-200	9 21:58	-														
	Apache/1.3.37 Se	erver at bt.exam	ple.net F	Port 80														
														tasta ubila pr	and a through	ab 740		
														tests while pr	oxymig throug	gii ZAP.		
		nescamp		01.02									gnost	lert N	ote T	ags		P
	1 27/11/1	6 17:03:52 0	GET	http://172.20.	0.120/		502	Bad Gateway 3	3 s S me	1.96 KiB			Modium	n				4
	5 2/11/1	01/104/05	561	ncp.//1/2/2020.	0.103/		200		5 1115	1.57 KD			meanan					
	Alerts 🍽 0 🏴 2 🏳 2	ba 0 rad											Cur	rrent Scans 🜷	0 0 6 0	0 👋 0 🧪	°0 🌞 0	₩0
			1000 million (1000 million)				and the second second											-

Now, in the browser, put the IP address of the Damn Vulnerable Linux server, here I have 172.20.0.103. To check, open a terminal and type in "ip a" this will show the address on the DVL virtual machine. Plug that result in here.

In OWASP ZAP, you will see the IP address populate under Sites.

Applicat	itions 🔻 🛛 Places 👻 🚷 OWASP ZAP 🕶		Sun Nov 27, 17:04 •		1 ,** 40) 🗲 🔫
	Index of / × +				
	• 172.20.0.103 •		୯ 🔍 Search 🔄 😭	i ♥ ↓ ŵ	
	🐱 Most Visited 🔻 👔 Offensive Security 🔨 Kali I	.inux 🥆 Kali Docs 🔨 Kali Tools	Exploit-DB Aircrack-ng		
	Index of /				
	Eile Edit View Analyse Report Tools Online Help				
	Standard Mode 💌 🗋 😂 🕁 🖿 📄 😳 💷 🌁 📼 💷 🕼				
			Request Response 🖛		
	T Contexts	Welcome t	o the OWASP Zed Attac	k Provy (7	(AP)
. 😭]	Default Context		Spider	×	lications.
	V Sites V P Sites V P http://172.20.0.103	Scope			n given permission to test.
	▶ 🔛 icons	Starting point:	http://172.20.0.1.03/	Soloct	
		Cantant	110/11/22001103	Select	Select
898		Concext:			
D		user:	~		
		Spider Subtree Only	2		
		Show Advanced options			d regression tests while proxying through ZAP.
					*
	🚝 History 🔍 Search р Alerts 📄 Output 🕂				
				[
	Id Req. Timestamp Method URL				Highest Alert Note Tags 🖪
	3 27/11/16 17:04:03 GET http:/	0	Cancel	set Start Scan	Pe Medium
					Ļ
	Alerts 🕫 0 🕫 2 🕫 0				Current Scans 👽 0 👌 0 🎯 0 💥 0 🎤 0 🌻 0 😽 0

Most items in ZAP are right-click sensitive, meaning you can right click to open additional dialogues. Right click under Sites on the IP address and choose: Attack, Spider. Check the box for Spider Subtree Only, and hit Start Scan.

Applicat	tions - Places -		Sun Nov 27, 17:05 •		1 ,2 +
	Index of /				
	172.20.0.103		C Q Search		
	🛅 Most Visited 🔻 👖 Offensive Security	y 🔨 Kali Linux 🔨 Kali Docs 🕚	🔨 Kali Tools 🗽 Exploit-DB 🔄 Aircrack-ng		
	Index of /				
			Untitled Session - OWASP ZAP 2.5.0		
	Eile Edit View Analyse Report Tools Online Hel	p			
	(Standard Mode 💌 📄 😂 🖬 💼 📸 💷 💷		/ 😑 🕪 🕨 🖉 💥 📾 🗽 😖 📼		
	😵 Sites 🕂	💡 Qu	iick Start 🖉 🔿 Request Response⇔ 🕂		
			L L L		
		We	Icome to the OWASP Zed	Attack Proxv (ZAP)	\leq
	Default Context	ZARIO	an easy to use integrated population testing teel for	finding wilperabilities in web applications	
. 🕲 🛛	🔻 🚱 🏴 Sites	ZAFIS	an easy to use integrated penetration testing toor or	inding vulnerabilities in web applications.	
	🔻 🚔 🏓 http://172.20.0.103	Please	be aware that you should only attack applications that	t you have been specifically been given permi	ssion to test.
	GET:base	To quic	kly test an application, enter its URL below and press '	Attack'.	
	GET:beet	1			
BB	W GET-beef(N)	URL to	attack: http://		Select
	GET:beef(M)		Generation Attack		
D	# GET:beef(S)	Progra	ss: Not started		
	# GET:beef(D)	i rogio.	ss. Not started		
	▶ 🔛 ₩ beef				
	GET: docs	For a m	nore in depth test you should explore your application i	using your browser or automated regression t	ests while proxying through ZAP.
	Ref # GET:robots.txt	See the	e help file for more details.		
	B B # CET.siteman.uml	T	_		×
	🛗 History 🔍 Search 🏴 Alerts 📄 Output	₩ Spider 🖉 🛎 🚹			
	Wew Scan Progress: 0: http://172.20.0.103/	• • • • • • • • • • • • • • • • • • • •	24% 🖉 Current	Scans: 1 🗄 URIs Found: 755 🗄 🛅 Show Messaq	jes 🕸
	Processed Meth	nod L	JRI	Flags	
	GET		http://bt.example.net/webexploitation_package_02/joon	halo9/templates/rh OUT_OF_SCOPE	4
	GET GET		http://172.20.0.103/webexploitation_package_02/joom	a109/index.php?ltemi	
	POS"	r i	http://bt.example.net/webexploitation_package_02/joon	nla109/index.php OUT_OF_SCOPE	
	POS"	r ł	http://bt.example.net/webexploitation_package_02/joon	nla109/index.php?ite OUT_OF_SCOPE	
	GET	ł	http://172.20.0.103/webexploitation_package_02/nabo	poll/?N=D	
	GEI GET	1	http://172.20.0.103/webexploitation_package_02/nabop	2011/1M=A	
	GET		http://172.20.0.103/webexploitation_package_02/nabo	poll/?D=A)
	GET	ł	http://172.20.0.103/webexploitation_package_02/nabo	ooll/admin/	
	Alerts 🍋 0 🍋 2 💫 2 🗭 0			Curr	ent Scans 🚭 0 👌 0 🎯 0 勝 1 🎤 0 🌞 0 勝 0

Spider in progress.

Applicat	tions 👻 Places 👻	Sun Nov 27, 17:07●	1 ,2 (0) 🕣 🔻
		index of / - Iceweasel	
	Index of / × +		
	172.20.0.103	여 Q Search ☆ 自 👽 🖡 🎓 😑	
	🛅 Most Visited 🔻 📲 Offensive Security 🔨	ali Linux 🔨 Kali Docs 🔨 Kali Tools 🗽 Exploit-DB 🔍 Aircrack-ng	
	Index of /		
		Untitled Session - OWASP ZAP 2.5.0	
	<u>E</u> ile <u>E</u> dit ⊻iew <u>A</u> nalyse <u>R</u> eport <u>T</u> ools <u>O</u> nline <u>H</u> elp		
	Standard Mode 💌 🗋 😂 层 💷 🚊 🎲 💷 🛎 📼		
	🚱 Sites 🕂	🥖 Quick Start ≉ 🗋 ⇔ Request ໂ Response 🗢 🚺	
		Welcome to the OWASP Zed Attack Proxy (ZAP)	\leq
-	Contexts Default Context	74D is an enabled use interested exected to taking the left finding underset lifetics in use and leading	
9	🔻 🤪 🏴 Sites	ZAP is an easy to use integrated penetration testing tool or innoing vulnerabilities in web applications.	
	▼ 🚔 № http://172.20.0.103	Please be aware that you should only attack applications that you have been specifically been given permission to test.	
	P # GET:base	To quickly test an application, enter its URL below and press 'Attack'.	
		2	
	R W GET:beef(N)	URL to attack: http://	Select
	📄 🏴 🕷 GET:beef(M)	🗲 Attack 🔳 Stop	
2	📄 🏴 🕷 GET:beef(S)	Progress: Not started	
	R # GET:beef(D)		
	R # GET docs		
	► Cons	For a more in depth test you should explore your application using your browser or automated regression tests while prov	ing through ZAP.
	📄 🙉 🗰 GET:robots.txt	See the help file for more details.	_
	🔚 History 🔍 Search 👎 Alerts 📄 Output 🕷 S	ler 🖉 🛪 🛉	
	🕷 New Scan 🛛 Progress: 0: http://172.20.0.103/ 💌 🛽	Loo% Current Scans: 0 : URIs Found: 2156 : E Show Messages	
	Processed Method	URI Flags	8
	POST	http://172.20.0.103/phpmyadmin/scripts/setup.php	4
	POST	http://17.2.00.103/phpmyadmin/scripts/setup.php	
	POST	http://172.20.0.103/phpmyadmin/scripts/setup.php	
	POST	http://172.20.0.103/phpmyadmin/scripts/setup.php	
	GET	http://www.phpmyadmin.net/token=965f99a92057e8595e9b896097b31ffe OUT_OF_SCOPE	
	GET	http://sourceiroige.nervonate/index.php?group_ide/sourceire/sourceire/sourceiroige.nervonate/index.php?group_ide/sourceire/sourceiroige.nervonate/index.php?group_ide/sourceire/sourceiroige.nervonate/index.php?group_ide/sourceire/sourceiroige.nervonate/index.php?group_ide/sourceire/sourceiroige.nervonate/index.php?group_ide/sourceire/sourceire/sourceiroige.nervonate/index.php?group_ide/sourceire/sourceiroige.nervonate/index.php?group_ide/sourceire/sourceire/sourceiroige.nervonate/index.php?group_ide/sourceiroige.nervonate/index.php?grou	
	GET GET	http://172.20.0.103/unicornscan/index.php?sessid=WDtYrQ==!Ub9Zljjp6rF	D
	GET GET	http://172.20.0.103/unicomscan/index.php?sessid=WDtYtw==!Ug6KZgEdjl6	•
	Alerts 🍽 0 🍽 3 🏳 6 🍽 0	Current Scans 🖑 0	🔥 0 🥥 0 勝 0 🎤 0 🧅 0 勝 0

Spider finished.

Right click on the IP, Choose: Attack, Active Scan.

Applica	tions 👻 Places 👻 🚷 OWASP ZAP 🕇			Sun Nov 27, 17:07 •		1	,≌ 40) ∓ -
	Index of / × 🕂						
	• 172.20.0.103			c 🔍 Search	☆ 自 ♥ ♣ 兪	⊜ ≡	
	Most Visited V Offensive	Security - Kali I	inux 🗅 Kali Doce 🛸 Kali Too	ls Fynloit-DB Aircrack-r			
				IS MEADION DD CANTORNA	19		
	Index of /						
			Untit	led Session - OWASP ZAP 2.5.	.0		
	<u>Eile Edit View Analyse Report Tools O</u>	nline <u>H</u> elp					
	Standard Mode 💌 🗋 😂 🔚 📾 🛒 🖗	ş 💷 🛎 📼 🔳	= = = = 🛋 🖓 🖕 🕨) 🖉 💥 💷 🗽 🔍 🔤			
	😺 Sites 🛨		Ouick Start &	🗢 Request 🕻 Response 🖨 🗍 📥 🗎			
				Active Scan			
	T Contexts		Scope Upput Vectors Curtem Vec			(AP)	
. 🕐	Default Context		Scope Input vectors custom vec	technology Folicy		plications.	
-	🔻 🤪 🏴 Sites		Starting point:	http://172.20.0.103/?D=D/	Select		
200	▼ 🚔 № http://172.20.0.103					in given permission to test.	
	📄 🏁 🤫 GET:base		Policy:	Default Policy	v		
	▶ 🔜 🎮 ₩ base		Context:		v		
	📄 🏁 🕷 GET:beef(N)					Select	
898	📄 🎮 🕷 GET:beef(M)		User:		Y		
O	P # GET:beef(S)		Recurse:	V			
	► CET:Deer(D)		Show advanced options	V			
	🛅 👎 🗰 GET: docs					d regression tests while provving through 74	P
	▶ 🚞 icons					aregreester teste mile prograg triougn E.	
	📄 🏴 🕷 GET:robots.txt						
	😤 History 🔍 Coorsh 📑 Alarta	Output The Enider of	1				
	instory Search Merca	oucput wy spider >	-				
	% New Scan Progress: 0: http://172.2	0.0.103/				Show Messages	\$Q\$
	Processed	Method					6
		POST					A.
	e e e e e e e e e e e e e e e e e e e	POST					
		POST					
		POST		c	ancel Reset Start Scan	CODE	
		GET	https://source	forge.net/donate/index.php?group_id=2	23067&token=965f99 OUT 0	F SCOPE	
		GET	http://172.20.	0.103/unicomscan/index.php?sessid=W	DtYrQ==!WRGIHW45/V		
		GET	http://172.20.	0.103/unicomscan/index.php?sessid=W	DtYrQ==!Ub9ZlJjp6rF)
		GET	http://172.20.	0.103/unicomscan/index.php?sessid=W	DtYtw==!Ug6KZgEdJl6		
	Alerts PO PO PO PO DO					current scans 👽 0 👌 0 🥘 0 🞘	20 🖉 0 🦊 0 🔆 0

Check the box for Advanced Options.

Applica	tions 👻 Places 👻 🚷 OWASP ZAP 👻		Sun Nov 27, 17:08 •			1 😼 🐠 f
	Index of / × +					
	€ ● 172.20.0.103		c Q Search	合自	⊽ ∔ ⋒	• =
	🛅 Most Visited 🔻 👖 Offensive Security 📉 Kali I	Linux – Kali Docs – Kal	i Tools 🛄 Exploit-DB 🔄 Airci	rack-ng		
	Index of /					
	Eile Edit View Analyse Report Tools Online Help					
	Standard Mode 💌 🗋 😂 🔐 📾 📄 🍪 💷 🗷 📼 🕅		▶ ▶ ⊘ 💥 📾 🗽 😡 📼			
		G Ouick Sta)		
	Sires T		Active Scan		×	
			Active South		~	
	🔻 🚍 Contexts	Scope Input Vectors Custo	om Vectors Technology Policy			
S	Default Context		-			plications.
-	🔻 🚱 🏴 Sites	▼ Policy	Policy		۲	
No.	▼ 🚔 № http://172.20.0.103	Lifernation Gathering	Policy: Dofault Po	liev		in given permission to test.
	N W GET:base	Injection	Deradit To			
	N W base	Miscellaneous	Default Alert Threshold: Low	(More potential issue	s flagged)	
	R # GET:beef(N)	Server Security	Default Attack Strength: Low	(Fewer attacks)		Select
	R # GET:beef(M)					
0 B H D	R # GET:beef(S)		Apply Low Infestioid to All	Rules Go		
	🛅 🎮 🗰 GET:beef(D)		Apply Low Strength To All	Rules Go		
:::	🕨 🚞 🎮 🗰 beef		Category	Threshold	Strength	
····]	P # GET: docs		Client Browser			d regression tests while proxying through ZAP.
	icons		Information Gathering	Low	Low	
	P W GET:robots.txt		Injection	Low	Low	
		1	Miscellaneous Server Security	Low	Low	
	History 🔍 Search 🏴 Alerts 🔄 Output 🕷 Spider 🖉		Server Security	2011	2011	
	🕷 New Scan 🗄 Progress: 0: http://172.20.0.103/ 💌 📗 📗					Show Messages
	Processed Method	1				
	e Post	1				
	POST					
	POST					
	POST POST					
	GET POST			Cancel Reset	Start Scan	SCOPE
	GET	https://	sourceforge.net/donate/index.php?grou	up_id=23067&token=96	55f99 OUT 0	DF_SCOPE
	GET GET	http://1	72.20.0.103/unicomscan/index.php?se	ssid=WDtYrQ==!WRGIH	₩45/V	
	GET	http://1	72.20.0.103/unicomscan/index.php?se	ssid=WDtYrQ==!Ub9ZlJj	p6rF	
	GET GET	http://1	72.20.0.103/unicomscan/index.php?se	ssid=WDtYtw==!Ug6KZ	gEdJl6	
	Alerts 🍽 O 🏳 3 🏳 6 🏳 0					Current Scans 🚭 0 👌 0 🎯 0 勝 0 🎤 0 🌻 0 🔅

Click on the Policy tab, and set everything to Low. Then hit the Go buttons. Then Start Scan.

Applica	tions 🔻	Places 🔻			Sun Nov 27, 17:08 •					1 ,**	() F -
				Ir	ndex of / - Iceweasel			_ 0	×		
	Ind	lex of / ×	ŧ								
	¢¢	172.20.0.103			୯ 🔍 Search	☆自	V 🖡 n				
	a Mo	st Visited 🔻 👖 Offensiv	ve Security 🥆 Kali Lir	iux 🔍 Kali I	ocs 🔨 Kali Tools 🕱 Exploit-DB 🔍 Aircrack	-na					
					,	3					
	In	dex of /									
					Untitled Session - OWASP ZAP 2.	5.0					
	Eile E	dit <u>View Analyse Report T</u> ool	ls <u>O</u> nline <u>H</u> elp					_			
	Standa	ard Mode 💌 🗋 🚘 🔚 💷 🗄	·		₽ ♀ ⊖ ▶ ▶ ⊘ 🗶 📾 🐂 😡 🖬						
		tes 📥			Guick Start & Request Responses						
		T T			y quick start > -+ Request Response +						17
	© 📮				Welcome to the OWASP 700		Drow				
	🔻 🗖 C	ontexts		A	welcome to the OWASP Zeo		(Proxy ((ZAP)			5 /
- 🛐 🛛		Default Context			ZAP is an easy to use integrated penetration testing tool	for finding vuln	erabilities in web a	applications			7
		Sites			Please be aware that you should only attack applications t	that you have b	een specifically b	een given p	ermission to test.		
77		B # GET base									
		📄 🙉 🕷 GET:beef			To quickly test an application, enter its URL below and pre	ss 'Attack'.					
	Þ	🚞 🎮 🕷 base			100 Ac este els latte //					-1	
		📄 🏴 🕷 GET:beef(N)			URL to attack: http://				W 5	elect	
898		📄 🏴 🕷 GET:beef(M)			🗳 Attack 📃 Stop						
D		W GET:beet(S)			Progress: Not started						
	▶	N W beef									
		📄 🕫 🗰 GET:docs			For a more in donth test you should employ your application		rouser or outoms	ted rearees	ion toots while proving i	brough 740	
	Þ	icons			Por a more in deprintest you should explore your application	on using your c	rowser of automa	ateu regress	aon tests while proxying	iniougn zwr.	
		📄 🕫 🕷 GET:robots.txt			See the help file for more details.						_
	<u></u>			L							•
	🔡 🛗 Hi	istory 🔍 Search 🛛 🏴 Alerts	📄 Output 🛛 🕷 Spider 👌	Active Scan 🖉 🕴	9 ±						
	. m	New Scan 🗄 Progress: 0: http	://172.20.0.103 🔽 👖 🔲	III 🚪	2%	💚 Currer	it Scans: 1 🗄 Num	requests: 8	00		
	Id	Req. Timestamp	Resp. Timestamp	Method	URL	Code	Reason	RTT	Size Resp. Header	Size Resp. Boo	dy 🖪
		3,856 27/11/16 17:08:29	27/11/16 17:08:29	POST	http://172.20.0.103/olate/details.php?cmd=addco	200	OK OK	28 ms	347 bytes	7.52 KiB	A
		3,857 2//11/16 17:08:29	27/11/16 17:08:29	POST	http://172.20.0.103/olate/details.php?cmd=addco http://172.20.0.103/olate/details.php?cmd=addco	200	OK .	25 ms 24 ms	347 bytes 347 bytes	7.52 KIB 7.52 KIB	
		3.859 27/11/16 17:08:29	27/11/16 17:08:29	GET	http://172.20.0.103/olate/recommend.php?file=thi	200	OK OK	156 ms	146 bytes	2.7 KiB	
		3,860 27/11/16 17:08:29	27/11/16 17:08:29	POST	http://172.20.0.103/olate/details.php?cmd=addco	200	ЭK	21 ms	347 bytes	7.52 KIB	
		3,861 27/11/16 17:08:29	27/11/16 17:08:29	POST	http://172.20.0.103/olate/details.php?cmd=addco	200	ок	23 ms	347 bytes	7.52 KiB	
		3,862 27/11/16 17:08:29	27/11/16 17:08:29	POST	http://172.20.0.103/olate/details.php?cmd=addco	200	ок	22 ms	347 bytes	7.52 KiB	
		3,863 27/11/16 17:08:29	27/11/16 17:08:29	POST	http://172.20.0.103/olate/details.php?cmd=addco	200	OK	22 ms	347 bytes	7.52 KiB	5
		3,864 2//11/16 17:08:29	2//11/16 17:08:29	POST	http://1/2.20.0.103/olate/details.php?cmd=addco	200	UK DK	22 ms	347 bytes	7.52 KIB	2
	Alorte	BIO DIS DIE DIO	2//11/10 17:00:29	FUSI	http://1/2.20.0.103/olace/decans.prip:cmd=addco	200	UK .	20 1115	Current Coope R.O.	7.52 ND	<u> </u>
	Alerts	100 103 100 100							current scans 😵 0 👩	1 🕘 U 🖑 U 🧨 U	🚽 U 🧒 U

Attack in motion.

Ubunt	tu Desktop								• •	🖉 🛅 🛃 利 5:08 P	м 📃
0	1		File Machine View Input De	vices Help		second and the second			1909		;
	A State of the same	Applic	ations 👻 Places 👻			Sun Nov 27, 17:08 •				1 📲 📢 🖻	
						Index of / - Icewease)		_ 0	×		
10											
	A BAR HAND		🕞 🕘 172.20.0.103				☆ 白 ♥ ♣	ê ⊕	3		
			🛅 Most Visited 🔻 👖 Offensive	e Security 🔨 Kali L	inux 🔨 Kali	Docs 🥆 Kali Tools 🔝 Exploit-DB 📑 Aircrae					
	●●● Machine View Input		Index of /								
2	top - 22:08:55 up 48 min. 1 user.		index or ,			Lintitled Session - OWASP 7AP	25.0				
- 10	Tasks: 91 total, 3 running, 88		File Edit Manual Analysis Depart Taxla	Online Hale		Ontrice Session - OWASE ZAF 2	2.3.0				
	Men: 1032748k total, 304436k us		Elle Edit View Analyse Report Tools	Online Help							-
\odot	Swap: Øktotal, Økus										
😰 🗄	PID USER PR NI VIRT RES		Sites 🛨			Quick Start ☞ Request Response ← +					_
-	2 root 34 19 0 0					Walcome to the OWASP 7	d Attack Brow	(740)			
•	3 root 10 -5 0 0 4 root 11 -5 0 0		▼		*	Welcome to the OWASP 20	a Allack Prox	y (ZAF)			
	5 root 10 -5 0 0	- 🥶 🛛	Default Context			ZAP is an easy to use integrated penetration testing to	ol for finding vulnerabilities in w	veb application:	k.		
	97 root 20 -5 0 0		V = P http://172.20.0.103			Please be aware that you should only attack application	is that you have been specifica	ally been given p	ermission to test.		/
TEX	130 root 20 -5 0 0 131 root 20 -5 0 0	2/	📄 🏁 🤀 GET:base			To quickly test an application, enter its URL below and p	ress 'Attack'.				<
۲	132 root 20 -5 0 0	_	📄 🏲 🗰 GET:beef								
	135 root 20 -5 0 0 137 root 10 -5 0 0	100	F W Dase			URL to attack: http://				Select	
-	159 root 25 0 0 0	898	📄 🎮 🦷 GET:beef(M)			🗳 Attack 🔲 Stop					
•••	161 root 20 -5 0 0	D	📄 🏴 🍀 GET:beef(S)			Progress: Not started					
	162 root 20 -5 0 0 163 root 20 -5 0 0		☐ P ₩ GET:beef(D)								
	164 root 20 5 0 0		► ₩ GET:docs								
S	165 root 20 -5 0 0 166 root 20 -5 0 0		► 🚞 icons			For a more in depth test you should explore your applica	ation using your browser or aut	comated regres	sion tests while proxying	through ZAP.	
	167 root 20 -5 0 0 855 root 11 -5 0 0		☐ P ₩ GET:robots.txt			See the help file for more details.					
Two	874 root 11 -5 0 0 879 root 11 -5 0 0		History Search Nets	📄 Output 🗎 🕷 Spider 🚺	Active Scan #	×+					
-	902 root 11 -5 0 0 903 root 11 -5 0 0		New Scan Progress: 0: http://	172.20.0.103 💽 🔟 🔲		2%	Current Scans: 1 N	ium requests: 1	967		83
	904 root 11 -5 0 0		Id Beg. Timestamp	Resp. Timestamp	Method	URL	Code Reason	RTT	Size Resp. Header	Size Resp. Body	12
BHO	909 root 10 -5 0 0		4,052 27/11/16 17:08:33	27/11/16 17:08:33	POST	http://172.20.0.103/olate/report.php?file=4	200 OK	39 ms	347 bytes	1.81 KiB	
	991 root 18 -4 1808 528		4,053 27/11/16 17:08:33	27/11/16 17:08:33	POST	http://172.20.0.103/olate/recommend.php?file=4	200 OK	21 ms	146 bytes	5.24 KIB	
-	1846 root 18 0 1720 668		4,054 27/11/16 17:08:33	27/11/16 17:08:33	POST	http://172.20.0.103/olate/report.php?file=4	200 OK	27 ms	347 bytes	1.81 KiB	- 1
	1854 root 18 0 1568 384 .		4,055 27/11/16 17:08:33	27/11/16 17:08:33	POST	http://172.20.0.103/olate/recommend.php?ile=4	200 0K	35 ms	247 butos	1 01 VID	- H. R
	1896 root 15 0 1588 384		4,057 27/11/16 17:08:33	27/11/16 17:08:33	POST	http://172.20.0.103/olate/recommend.php?file=4	200 OK	30 ms	146 bytes	5.28 KiB	- H B
	1935 root 18 0 1776 604		4,058 27/11/16 17:08:33	27/11/16 17:08:33	POST	http://172.20.0.103/olate/report.php?file=4	200 OK	20 ms	347 bytes	1.81 KIB	
	1938 root 18 0 1560 492		4,059 27/11/1617:08:33	27/11/16 17:08:33	POST	http://172.20.0.103/olate/report.php?file=4	200 OK	31 ms	347 bytes	1.81 KiB	
	1945 Foot 23 0 2408 1236 1		4,060 27/11/16 17:08:33	27/11/16 17:08:33	POST	http://172.20.0.103/olate/recommend.php?file=4	200 OK	33 ms	146 bytes	5.3 KIB	\mathcal{D}
			4,061 27/11/1617:08:33	27/11/16 17:08:33	POST	http://172.20.0.103/olate/report.php?file=4	200 OK	27 ms	347 bytes	1.81 KiB	
	alis 🖬 🙆 🙆 🡍		Alerts 🍽 0 🍋 3 🏳 6 🕅 0						Current Scans 🚭 0 👌	1 🥥 0 🕷 0 🎤 0 🌞 0	8 0
-	~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~								🖸 📀 🛃 🖆	🗐 🖶 🔟 🔇 💽 Right C	trl
-				1 . M. 1	2 1	A CONTRACTOR	1 N 12		1 4	1 m 1 m	

Starting to see some results. You can see I have DVL in the back ground with top open in a terminal watching the CPU utilization.

The scan is finally done. On my laptop, this took over an hour to run.

Click on the Alerts tab.

lications 🔻 Places 👻 🛞 OWASP ZAP 👻			Sun Nov 27, 17:55●			, 2 1 40) 9 -	
Index of /	× +						
♦ 172.20.0.1	03		c Q Search	<u>ሰ</u>	rê ♥ ♣ ♠ ₽ ≡		
🛅 Most Visited 🔻	👖 Offensive Security 🔨 Kali Linu:	x 🔨 Kali Do	cs 🔨 Kali Tools 🙀 Exploit-DB 🕥 Aircrac	k-ng			
Index of	1						
Index of	1		Untitled Session - OWASP 7AP 2	5.0			
File Edit View Analyse	e Report Tools Online Help		Edit Alert	×			
Standard Mode							
😡 Sites 🕂		Cross Site	Scripting (Reflected)	5			
		URL:	http://172.20.0.103/webexploitation_package_02/cypl				
		Risk:	High				
Contexts		Confidence:	Low				A
V Sites		Parameter:	login				
🔻 📫 👭 http://172.20	0.0.103	Attack	" <script>alert(1):</script>	nath-	/		
📄 🔑 🗰 GET:ba	se		Societ dereta statistic	puti-	, 		
№ ₩ GET:be	et	Evidence:	" <script>alert(1);</script>	st-chec	k=0, pre-check=0		
P a w GET:be	ef(N)	CWE ID:					٧
📄 🔑 🕷 GET:be	ef(M)	WASC ID:		assword FROM cyphor_users WHERE nick='"" <script>alert(1);</script> '			
📄 🏴 🕷 GET:be	ef(S)	Description:		SQL sy	ntax; check the manual that corresp ne l)	ponds to your MySQL server versi	on for the
📄 🏴 🗰 GET:be	ef(D)	Cross-sit	e Scrinting (XSS) is an attack technique that involves e	dmin@do	main.ext] and specify the exact	t error message.	
P P W Deel	rs.	attacker	supplied code into a user's browser instance. A brows				
▶ 🧰 icons		instance	can be a standard web browser client, or a browser of				
📄 🏴 🗰 GET:rol	bots.txt	Other Info:					
P # GET:sit	emap.xml						
🛛 🛗 History 🏾 🔍 Searc	h 🗍 🏴 Alerts 🖈 📋 📄 Output 🏾 💥 Spider 🏹 👌 .	Ac					
o 😡	Cros	s					A
🔻 📄 P Cross Site Sc	ripting (Reflected) (41)	Solution		age_02/	cyphor/index.php		
POST: http://	172.20.0.103/webexploitation_packa Risk:	Joidton					
POST: http://	172.20.0.103/webexploitation_packa Confi	de Phase: A	rchitecture and Design Ited library or framework that does not allow this weak				J
GET: http://	72.20.0.103/vebexploitation_packat Attac	k: occur or	provides constructs that make this weakness easier to				ľ
GET: http://172.20.0.103/olate/files.php?cat=5&ct Eviden		Defenses					
GET: http://172.20.0.103/phpmyadmin/index.php? WASC I		Reference:					
GET: http://172.20.0.103/webexploitation_package Descr		cr http://pro	ects.webappsec.org/Cross-Site-Scripting	¥			
GET: http://1	72.20.0.103/webexploitation_package		Capcal Cau	kereun	nlied code into a user's browser instar	nce. A browser instance can be a s	tandard
		eb uruwaer urer	it, or a prowser object embedded in a soltware produc	ch as th	he browser within WinAmp, an RSS read	der, or an email client. The code its	elf is
Alerts 🏴 7 🏴 5 🏴 6	in 0 ما				Cur	rrent Scans 🐺 0 👌 0 🥥 0 勝 0	20 🜞 0 🔆 0

Expand on the first vulnerability. Dig through the details. This information is great for ruling out false positives.

Continue exploring the vulnerabilities.

cations 👻 Places 🔻 🚷 OWASP ZAP 👻	Sun Nov 27, 17:57●	,₩ 1 40) €
Inc	dex of / - Iceweasel	_ = ×
Index of / × +		
G 9 172 20 0 103	c Q Search 🔿 🖻	
👼 Most Visited 🔻 👖 Offensive Security 🔨 Kali Linux 🥆 Kali Do	ocs 🕆 Kali Tools 🛄 Exploit-DB 📑 Aircrack-ng	
Index of /		
Index of /		
<u>Eile E</u> dit ⊻iew <u>A</u> nalyse <u>R</u> eport <u>T</u> ools <u>Q</u> nline <u>H</u> elp	Edit Alert ×	
Standard Mode 💌 🗋 블 🕁 📖 🝵 🍪 💷 🛎 🖿 🔲 🔲 🔲		
Sites 🛨	Path Traversal	
	URL: http://172.20.0.103/webexploitation_package_02/php	
X Contexts	Risk: High	
Default Context	Confidence: Medium	
🔻 🤬 🕫 Sites	Parameter: forwarder	
▼ 🚔 🏴 http://172.20.0.103	Attack modules nhp	
C W GET:base	(
	Evidence:	
R # GET:beef(N)	CWE ID:	
R # GET:beef(M)	WASC ID:	
📄 🉉 🕷 GET:beef(S)	Description	
📄 🏁 # GET:beef(D)	Description:	
▶ 🧮 🕫 ₩ beef <	The Path Traversal attack technique allows an attacker access 1	59-1*>
📄 🔑 🕷 GET: docs	commands that potentially reside outside the web document ro	
Icons	Aller and have a she with a second second stars show a second sec	
R # GET:sitemap.yml	Other Info:	Site's
🔚 History 🔍 Search 👎 Alerts 🖈 📄 Output 🕷 Spider 🦂 Active Scan 🕛		
💿 📦 Path Traversal		
▶ 📄 🂫 Cross Site Scripting (Reflected) (41)	Colution	I/modules.php?name=Surveys
▶ 📄 🂫 External Redirect	Solution.	
Path Traversal Confidence: Decomposition	Assume all input is malicious. Use an "accept known good" input	
Post: http://172.20.0.103/webexploitation_packat Parameter:	whitelist of acceptable inputs that strictly conform to specification not strictly conform to specifications, or transform it into somether	
Evidence:		
► CWE ID:	Reference:	
WASC ID: Description:	http://www.house.com/Dath_Tourist	
► 📄 🂫 Application Error Disclosure (201)	nttp://projects.webappsec.org/Path-Traversal	
► 📄 P Directory Browsing (42) The Path Travers	Cancel Save	ommands that potentially reside outside the web document root directory.
An attacker may		ine contents of arbitrary files anywhere on the web server. Any device that
Alerts PV / PV 5 PV 6 PV 0		Current Scans 😍 0 👌 0 🥥 0 💥 0 🤌 0 🍀

More on Path Traversal.

Applications 👻 Places 👻 🚷 OWASP ZAP 🕶	Sun Nov 27, 17:57•	,1 40) F 🗸
li li	ndex of / - Iceweasel	_ _ ×
	C 🔍 Search 😭 🖆	
- Most Visited - Offensive Security - Kali Linux - Kali I	Docs 🕆 Kali Tools 🗰 Exploit-DB 🖾 Aircrack-no	
	Anordox ing	
Index of /		
Indoir of ,		
	Untitled Session - OWASP ZAP 2.5.0	×
Eile Edit View Analyse Report Tools Online Help	Edit Alert ×	
Standard Mode 💌 🗋 😂 🖬 📑 🛱 💷 🗖 📼 🗉 🖬 🖬		l
Sites 🛨	Risk: High	
	Confidence: Medium	
🔻 🗖 Contexts	Parameter: forwarder	
Default Context	Dr Attack: http://www.google.com/	
V 🚱 P4 Sites	C Evidence: <title>Google</title>	
• • • • • • • • • • • • • • • • • • •		
P # GET:beef	P:	ort/accounts/answer/151657?hl=en for more info."
🕨 📄 🏴 🕷 base	SF WASC ID:	l 4
Retribute Retribu	Description:	
M W GET:beef(M)	Remote File Include (RFI) is an attack technique used to exploit	s and more. Google has many special features to help you find exactly what
📄 🏴 🗰 GET:beef(D)	mechanisms in web applications. When web applications take us etc.) and pass them into file include commands, the web application	e="robots"> <meta content="<br"/>
▶ 🚞 🖻 🕷 ₩ beef	n instrution and Alexande materians and	r"> <title>Google</title> <script></script>

More on Remote File Inclusion.

tations 👻 Places 🔻 💸 OWASP ZAP 👻	Sun Nov 27, 17:58 •	بة (1 e) e -
Ir	ndex of / - Iceweasel	_ = ×
Index of / x +		
0 0 172.20.0.103	e 🤉 Search 🛛 🛱 🖿	
🛅 Most Visited 🔻 👖 Offensive Security 🔨 Kali Linux 📉 Kali I	Docs 🥆 Kali Tools 🛄 Exploit-DB 🔍 Aircrack-ng	
Index of /		
Index of /		
Eile Edit View Analyse Report Tools Online Help	Edit Alert ×	
Standard Mode 💌 🗋 😂 🕁 💷 🝵 🎡 💷 🗷 📼 🗉 📼 💷 📼		
😺 Sites 🛨	Remote OS Command Injection	
	URL: http://172.20.0.103/unicornscan/index.php?action=vie	
T Contexts	Risk: High	
Default Context	Di Confidence: Medium	
🔻 🦦 🏴 Sites	St Parameter: action	
▼ 🚔 № http://172.20.0.103	St Attack: viewdata:start-sleep -s 5	k9o+I=; path=/
N # GET:base	E Didence	pre-check=0
▶ 🛄 🏴 ₩ base	Pi	pro shoek o
📄 🏁 🕷 GET:beef(N)	P: CWE ID:	_
Ref # GET:beef(M)	yt wasc id:	
R # GET:beef(D)	Description:	
▶ 🧰 № ₩ beef	Attack technique used for unauthorized execution of operating	
P # GET:docs	attack is possible when an application accepts untrusted input system commands in an insecure manner involving improper dat	
Icons R # GET:robots.txt		
🔁 🏴 🗰 GET:sitemap.xml	Other Info:	
🗯 History 🔍 Search 👎 Alerts 🖈 📄 Output 🕷 Spider 👌 Active Scan	T.	
© 🎱 Remote OS Com	nm.	
Cross Site Scripting (Beflected) (41)		a%3Bstart-sleep+-s+5
► 📄 🂫 External Redirect	Solution:	
▶ 📄 🂫 Path Traversal Confidence:	If at all possible, use library calls rather than external processes	
Remote File Inclusion Parameter: Attack:	desired functionality.	
GET: http://172.20.0.103/unicornscan/index.php?		
► 🚔 P SQL Injection (5) CWE ID: WASC ID:	Reference:	
Server Side Include (2) Description:	http://cwe.mitre.org/data/definitions/78.html	
Application Error Disclosure (201) Attack technig Attack technig	aue	attack is possible when an application accepts untrusted input to build
operating system	tenSave	and/or improper calling of external programs.
Alerts 🏴 7 🔑 5 🔑 6 🟴 0		Current Scans 💀 0 👌 0 🎯 0 勝 0 🏓 0 🌞 0 🔻

More on Remote OS Command Injection.

itions 👻 Places 👻 🚷 OWASP ZAP 👻	Sun Nov 27, 17:58 •	j ≌ 1 •0)
Index of / × +		
	අ Q Search ☆ 🖨 ♥ =	
😁 🚡 Most Visited 🔻 📲 Offensive Security 🚿	Kali Linux 🕆 Kali Docs 🕆 Kali Tools 🗼 Exploit-DB 🔄 Aircrack-ng	
Index of /	Edit Alert	×
	SQL Injection	
<u>Eile 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	III). http://0.72.20.0.102/webevplaitation_package_02//epsplai.07/indev.php?tamid=26/id=06/imit=2.26/imitstart=16.antion	som content6 tor
Standard Mode 💌 🗋 😂 🖬 📾 🚔 🍪 🖃 🛎 📼	Contemportation	-com_concentatas
🚱 Sites 🛨	High	
0 📮 🖸 🖸	Confidence: Medium	
Contexts	Parameter: limit	
Default Context	Attack: 3-2	
🔻 🤮 🏴 Sites	Evidence:	
 # http://1/2.20.0.103 # GET/base 	CWE ID:	
📄 🎮 🗰 GET:beef	WASC ID:	
🕨 🧰 🎮 🗰 base	Description:	
P # GET:beef(N)		
P # GET:beef(S)	sqL injection may be possible.	
📄 🏴 🕷 GET:beef(D)		
▶ 🔜 № ₩ beef	Other Info:	
⊨ ₩ ₩ GE1:docs		
📄 🉉 🗰 GET:robots.txt	The parameter value being modified was NOT stripped from the HTML output for the purposes of the comparison	
📄 🕫 # GET:sitemap.xml		
🔚 History 🔍 Search P Alerts 🖈 📄 Output 🕷	spider Solution:	
© 😂	Sc Constant distribution of the set of the s	
🕨 📄 🎮 Remote File Inclusion	UF UF DI Not das cliente side input, even in dere is client side validation in pace.	view
Remote OS Command Injection	Ru if the application uses JDBC, use PreparedStatement or CallableStatement, with parameters passed by ?'	
V P SQL Injection (5) GET: http://172.20.0.103/webevploitation_page	Pa Reference:	
POST: http://172.20.0.103/webexploitation_page	Att	
GET: http://172.20.0.103/webexploitation_pac	kag P Ev Intersi/www.owasp.org/index.php/10p10_2010-A1	T
GET: http://172.20.0.103/webexploitation_pac BOST: http://172.20.0.103/webexploitation_pac	kag(w/	Cancel Save
Site include (2)	Description:	
► 📄 🍋 Application Error Disclosure (201)	SQL injection may be possible.	
	7	
Alerts Pa / Pa 5 W 6 Pa 0	Current Scans	👽 0 👌 0 🥥 0 🐺 0 🧭 0 👙

More on SQL Injection.

tions 👻 Places 👻 🚷 OWASP ZAP 👻			Sun Nov 27, 17:58 •	,u	1	0) 🖸
Index of / × +						
172.20.0.103			c 🔍 Search 😭 🖻	♥ ♣ ♠ ≡		
🛅 Most Visited 🔻 👖 Offensive Security 🔨 I	Kali Linux 🔷 Kali D	c	Edit 4			
Index of /		SQL Injectio	1			
		URL:	http://172.20.0.103/webexploitation_package_02/joomla10	17/index.php?Itemid=25&id=7&option=com_content§ion	nid=3&tas	
File Edit View Analyse Report Tools Online Help		Risk:	High			
Standard Mode 💌 🗋 🚂 🖶 🖿 🖄 💷 🗷 📼		Confidence:	Medium			_
Sites +		Parameter:	sectionid			
		Attack:	5-2			-
T Contexts	A I	Evidence:				
Default Context		DE CWE ID:				
🔻 🤪 🎮 Sites						
Http://172.20.0.103		Description				
R # GET:beef						
🕨 🔛 🎮 🗰 base		SQL inject	ion may be possible.			
GET:beef(N)						_
GET:beef(S)						
📄 🏴 🗰 GET:beef(D)		Other Info:				
► 🧰 🎮 🕷 beef		The origin	al page results were successfully replicated using the expr	ession (5-2) as the parameter value		
E I icops		The para	neter value being modified was NOT stripped from the HTML	output for the purposes of the comparison		
Restauration (Construction)						
📄 🕫 🗰 GET:sitemap.xml	Y					
🔚 History 🔍 Search 👎 Alerts 🖈 📄 Output 🕷 S	pider 👌 Active Scan	Solution:				
· · · · · · · · · · · · · · · · · · ·	SOL Injection	Do not tr	st client side input, even if there is client side validation in	place.		-
Employee File Inclusion	URL:	h If the app	, type check all data on the server side. ication uses JDBC, use PreparedStatement or CallableState	ement, with parameters passed by '?'		-
Remote OS Command Injection	Risk:	If the app	ication uses ASP, use ADO Command Objects with strong t	ype checking and parameterized queries.		
🔻 🚞 🍋 SQL Injection (5)	Confidence: I	Reference:				
GET: http://172.20.0.103/webexploitation_packs	Attack:					
GET: http://172.20.0.103/webexploitation_pack	Evidence:	https://w	w.owasp.org/index.php/Top_TU_2010-A1 w.owasp.org/index.php/SQL_Injection_Prevention_Cheat_Sh	eet		
GET: http://172.20.0.103/webexploitation_pack	wASCID: 1	G				
POST: http://172.20.0.103/webexploitation_pac	Ca Description:				L	
m reserver side include (2) m reserver side include (2)	SOL injection m	a				
	A line of the l	1		Cancel	Save	
Alerts 🍽 7 🍽 5 💬 6 🔍 0				Current Scans 💀 0 👌 0 🍥 0	₩0 20 1	۵ 🧼

A POST action for SQL Injection.

Index of / - Conversed	spplications 🔻 🛛 Places 👻 🐧 OWASP ZAP 👻			Sun Nov 27, 17:59 •		,≝ 1 ♦) ÷ ▼
172.200.01 172.200.01 10 Central Country Kali Linux Kali Doos Kali Tools (Exploible) Advertised (Central Country Kali Linux Kali Doos Kali Tools (Exploible) Define Country Kali Linux Kali Doos Kali Tools (Exploible) Define Country Kali Linux Kali Doos Kali Tools (Exploible) Define Country Kali Linux Kali Doos Kali Tools (Exploible) Define Country Kali Linux Kali Doos Kali Tools (Exploible) Define Country Kali Linux Kali Doos Kali Tools (Exploible) Define Country Kali Linux Kali Doos Kali Tools (Exploible) Define Country Kali Linux Kali Doos Kali Tools (Exploible) Define Country Kali Linux Kali Doos Kali Tools (Exploible) Define Country Kali Linux Kali Doos Kali Tools (Exploible) Define Country Kali Linux Kali Doos Kali Tools (Exploible) Define Country Kali Linux Kali Doos Kali Tools (Exploible) Define Country Kali Linux Kali Doos Kali Tools (Exploible) Define Country Kali Linux Kali Doos Kali Kali Kali Tools (Exploible) Define Country Kali Linux Kali Doos Kali Kali Kali Tools (Exploible) Define Country Kali Linux Kali Doos Kali Kali Kali Kali Kali Kali Kali Kali						
172.200.103 C Search C Search C Search C Search C Search C C Search C C Search C C Search C C C Search C C Search C C C Search	Index of / × +					
Model Visited Colorestive Security Kall Linux Kall Dots Kall Dots Kall Dots Kall Dots Index Of / Standard Models Security Kall Dots Kall Dots Kall Dots Kall Dots Kall Dots Standard Models Security Kall Dots Kall Dots Kall Dots Kall Dots Kall Dots Standard Models Security Kall Dots Ka				a Q Saarah 👌 🖨		
Most Visited Offensive Security Kall Linux Kall Doos Kall Tools & Exploit 2B WArchacking Index of / Under Security Kall Linux Kall Doos Kall Tools & Exploit 2B WArchacking Edit Contexts Findex of / Under Security Kall Linux Kall Doos Kall Tools & Exploit 2B WArchacking Edit Alert Findex of / Under Security Kall Linux Kall Doos Kall Tools & Exploit 2B WArchacking Edit Alert Findex of / Under Security Kall Linux Kall Doos Kall Tools & Exploit 2B WArchacking Edit Alert Findex of / Under Security Kall Linux Kall Doos Kall Tools & Exploit 2B WArchacking Edit Alert Findex of / Find	0 172.20.0.103				• • • • =	
Index of / Standard Wey Analys Expert Tools On the Left Standard Wey Analys Expert Tools State	🛅 Most Visited 🔻 👖 Offensive Security 🔨 Kali Linux	x 🔷 Kali Do	ocs 🔍 Kali T	'ools "Exploit-DB Aircrack-ng		
Interest of f Interest of f <td< td=""><td>Index of /</td><td></td><td></td><td></td><td></td><td></td></td<>	Index of /					
Life Gat Verw Analyse Beyont Jooks prime Help Standard Mode Ele Gat Verw Analyse Beyont Jooks prime Help Standard Mode Ele Gat Verw Analyse Beyont Jooks prime Help Standard Mode Ele Gat Verw Analyse Beyont Jooks prime Help Standard Mode Ele Gat Verw Analyse Beyont Jooks prime Help Standard Mode Ele Gat Verw Analyse Beyont Jooks prime Help Final Final	Index of /					
Eld Lyw Analyse Beport Tools goline Belo Standard Model Candidard Context						_
Sundard Mode	Eile Edit ⊻iew Analyse Report Tools Online Help			Edit Alert		
Solution	Standard Mode 💌 🗋 😂 🕞 📖 📄 🎡 💷 🗷 🖾 💷 🗔		Conver Cide In	aduda		1
URL Inttr://12.20.103/into.pip?=#s3c%21=#s2=#s2+cm#s30%221=#s2=#s2=*s2 Pak: High Contexts High Contexts Parameter Parameter Parameter Attack: Root R SETbeef(N) Parameter <	🚱 Sites 🛨		Server Side in	iciude		
Private Contexts Ordinance: Medium Pranter: <		ſ	URL:	http://172.20.0.103/info.php?=%3C%21%23EXEC+cmd%3	D%22ls+%2F%22-%3E	
Default context Parameter: Para	🔻 🦳 Contexts		Risk:	High		
Parameter: Paramete	Default Context		Confidence:	Medium	• •	
Inttp://2220.0105 Inttp://2220.0105 Inttp://22200.0105 Intp://22200.0105 Intp:/	🔻 🚱 🎮 Sites	S	Parameter:		•	
Widence: Widen	V N http://172.20.0.103	ô	Attack:	Root /usr		
Weence: <td>GET.base</td> <td></td> <td></td> <td></td> <td></td> <td></td>	GET.base					
P P P P <td>▶ ■ ₩ ₩base</td> <td></td> <td>Evidence:</td> <td></td> <td></td> <td></td>	▶ ■ ₩ ₩base		Evidence:			
Image: Settime file WSC ID; 31 Image: Settime file Image: Settime file Description: Image: Settime file Description: Image: Settime file Image: Settime file Image: Settime file Description: Image: Settime file Image: Settime file Description: Image: Settime file Image: Settime file Image: Settime file Image: Settime file Image: Settime file Image: Settime file Image: Settime file Image: Settime file Image: Settime file Image: Settime file Image: Settime file Image: Settime file Image: Settime file Image: Settime file Image: Settime file Image: Settime file Image: Settime file Image: Settime file Image: Settime file Image: Settime file Image: Settime file Image: Settime file Image: Settime file Image: Settime file Image: Settime file Image: Settime file Image: Settime file Image: Settime file Image: Settime file Image: Settime file Image: Settime file Image: Settime file Image: Settime file Image: Settime file Image: Setime file Image: Setime file<	📄 🏴 🕷 GET:beef(N)	1	CWE ID:		97 🗘	
Bescription: B	📄 🎮 🕷 GET:beef(M)	<	WASC ID:		31 🚔	
P # GET:best(D) Certain parameters may cause Server Side Include commands to be executed. This may allow database connection or arbitrary code to be executed. Certain parameters may cause Server Side Include commands to be executed. Certain parameters may cause Server Side Include commands to be executed. GeT: http://22.20.01.03/webexplotation_package GeT: http://22.20.01.03/webexpl	📄 🏴 🕷 GET:beef(S)		Description			
Certain parameter: Certain para	📄 🕫 🗰 GET:beef(D)	b				l r
Cancel Sove 10 be executed.	▶ 🛄 🙉 ₩ beef	b	Certain par	ameters may cause Server Side Include commands to be exe	cuted. This may allow	
Constant in the server side include (2) Server Si	M W GET: docs	a	database c	connection or arbitrary code to be executed.		
Bergericher Tampering (12) Beschler Tampering (12	GET:robots tyt	a				
History Search Relates Output Spider Active San Server Side Includ Server Side Include Server Side Include (2) Remote OS Command Injection Solution: Solution: On trust client side input and enforce a tight check in the server side. Disable server side Solution: On trust client side input and enforce a tight check in the server side. Disable server side Solution: Solution: On trust client side input and enforce a tight check in the server side. Disable server side Solution:	P # GET:sitemap.xml	v .	Other Info:			
History Saletti Output Splice Attitue scalar Server Side inclusion Server Side inclusion URL: Solution: Solution: Do not trust client side input and enforce a tight check in the server side. Disable server side Disable server side Solution: Do not trust client side input and enforce a tight check in the server side. Disable server side Disable server side Solution: Do not trust client side input and enforce a tight check in the server side. Disable server side Disable server side Solution: Do not trust client side input and enforce a tight check in the server side. Disable server side Disable server side Solution: Do not trust client side input and enforce a tight check in the server side. Disable server side Disable server side Solution: Do not trust client side input and enforce a tight check in the server side. Disable server side Disable server side Solution: Do not trust client side input and enforce a tight check in the server side. Disable server side Disable server side Solution: Do not trust client side input and enforce a tight check in the server side. Disable server side Disable server side Solution: Do not trust client side input and enforce a tight check in the server side. Disable server side Disable server side Solution:	🗮 History 🔍 Search 🎆 Alasta 👌 🗅 Output 👾 Saidar 🔪	Active Coop	#EXEC</td <td>cmd="ls /"></td> <td></td> <td></td>	cmd="ls /">		
Severe Side Indud • @ Remate File Inclusion • @ Remate File Inclusion • @ Remate Side Include • @ Remate Sid	Bristory Search Jewierts & Boutput as spider 67	Active Scall	an wenee			
Image: Server Side Includes URL: Bisk: Condence: Premote 95 Command Injection Bisk: Condence: Parameter: Attack: Ever Side Include (2) Confinetric: Parameter: Attack: Ever Side Include (2) Image: Content Side Side Control Side Side Control Side Side Side Side Side Side Side Side	Serve Serve	er Side Includ				
Image: Confidence: Parameter: Aders: R7_05_5 R.0	Remote File Inclusion		Solution:			
Image: Server Side include (2) Do not trust client side input and enforce a tight check in the server side. Disable server side includes. Image: Server Side include (2) Server Side include (2) Image: Server Side include (2) Server Side include (2) Image: Server Side include (2) Server Side include (2) Image: Server Side include (2) Server Side include (2) Image: Server Side include (2) Server Side include (2) Image: Server Side include (2) Server Side include (2) Image: Server Side include (2) Server Side include (2) Image: Server Side include (2) Server Side include (2) Image: Server Side include (2) Server Side include (2) Image: Server Side (2) Server Side (2) Image: Serve	Remote OS Command Injection Risk:					
GET: http://22.20.0103/nfophp?=%3C%21-%22 GET: http://22.20.0103/nfophp?=%3C%21-%22 GET: http://22.20.0103/nfophp?=%3C%21-%22 GET: http://22.20.0103/nfophp?=%3C%21-%22 GET: http://22.20.0103/nfophp?=%3C%21-%22 For Directory Browsing (42) P Parameter Tampering (12) P Session Din URL Rewrite (15) Certain parameter Certain parameter Cancel Save Out to be executed.	P P Squinjection (5)	meter:	Do not trus	st client side input and enforce a tight check in the server sid	e. Disable server side	
GET: http://172.20.0.103/webexplotation_package Evidence: CWE ID: Reference: Wask: Dp: Directory Browning (42) P Parameter Tampering (12) Evidence: Certain parameter Certain parameter Cancel Save Out to be executed. Cencel	GET: http://172.20.0.103/info.php?=%3(%21-%23	:k:	includes.			ľ
Application Error Disclosure (201) As C Dis	GET: http://172.20.0.103/webexploitation package Evide	nce:				
Cancel Save Det to be executed.	► 📄 🎮 Application Error Disclosure (201)	ID:	Reference:			
Alers 7, 5, 5, 6, 0	Directory Browsing (42)	cription:	http://www	carleton ca/dmcfet/html/esi.html		
Alerts N7 N5 D6 N0	▶ 📄 🂫 Parameter Tampering (12)		neep://www.	carrecon.ca/~uncregneniyaa.ntilli	¥	
	Ce	ertain paramet			Cancel Save	ode to be executed.
	Alerte 017 015 016 010	_			Current Car	

More on Server Side Include.

Index of / - Lownake	oplications 👻 Places 👻 🚷 OWASP ZAP 👻		Sun Nov 27, 17:59 •		,¥ 1 40) € ▼
VI 12.20.010 Vi 12.20.010 Vi 10 V	Index of / x +				
Widt Visited					
Mode V Visited V Ordensive Security V Kali Linux V Kali Dools V Kali Tools V Kali Dools V Kali Tools V Kali Dools V Kali D	• • 172.20.0.103		e 🔍 search		
Index of / District Scatter using line in the first scatter of the first scatte of the first scatter of the first scatter of the firs	🔚 Most Visited 🔻 👖 Offensive Security 🔨 Kali	Linux 🖄 Kali Do	ocs 🥆 Kali Tools 🛄 Exploit-DB 🔍 Aircrack-n		
Interest of 1 Interest of 2000 Interest of 2000 Interest of 2000 If Edit Lyter Analyse Beport Look prime Lyter Edit Alert Interest of 2000 Interest of 2000 If Edit Lyter Analyse Beport Look prime Lyter Application Error Disclosure Interest of 2000 Interest of 2000 If Edit Lyter Analyse Beport Look prime Lyter Application Error Disclosure Interest of 2000 Interest of 2000 If Edit Lyter Analyse Beport Look prime Lyter Application Error Disclosure Interest of 2000 Interest of 2000 If Edit Lyter Analyse Beport Look prime Lyter Application Error Disclosure Interest of 2000 Interest of 2000 If Edit Lyter Analyse Beport Look prime Lyter Application Error Disclosure Interest of 2000 Interest of 2000 If Edit Lyter Interest of 2000 Interest of 2000 Interest of 2000 Interest of 2000 If Edit Lyter Interest of 2000 Interest of 2000 Interest of 2000 Interest of 2000 If Edit Lyter Interest of 2000 Interest of 2000 Interest of 2000 Interest of 2000 If Edit Lyter Interest of 2000 Interest of 2000 Interest of 2000 Interest of 2000 If Edit Lyter Interest of 2000	Index of /				
Until de Session - OWASP 24.9-2.5.0 a x Bé dit Meer Analyse Beport Tools Dohne Bélp Bé dit Alert Bé dit Alert Pé dit alors Dohne Bélp Bé dit Alert Pé dit alors Pé dit	Index of /				
bill yww Anlyse Repert. Tools Online Lefe Edit Alort A standard Mode P standard Mode					
Standard Mode Image: Contents Image: Contents Image: Contents Image: Content Image: Contents	<u>Eile Edit View A</u> nalyse <u>R</u> eport <u>T</u> ools <u>O</u> nline <u>H</u> elp		Edit Alert	×	
Application Error Disclosure Parameter:	Standard Mode 💌 🗋 😂 🕁 💷 🛒 🎲 💷 🗷 📼 🔲				
With thtp:///22.20.0.03/ Produkt context Produkt co	😵 Sites 🛨	ſ	Application Error Disclosure		
Pack Pack Pack Pack <td></td> <td>(</td> <td>URL: http://172.20.0.103/</td> <td></td> <td></td>		(URL: http://172.20.0.103/		
Conditiones </td <td></td> <td></td> <td>Risk: Medium</td> <td></td> <td></td>			Risk: Medium		
Bites B	Default Context		Confidence: Medium		
Image: State of the	🔻 🚱 🙉 Sites	S	Parameter:		
P w GET:base	▼ 🚔 № http://172.20.0.103				
K GET:beef Kusses Ku	📄 🏴 🗰 GET:base	ä	Attack:		
CVE ID: 200 CVE VACC ID: 13 CVACC ID: 13	📋 🏴 🕷 GET:beef		Evidence: Parent Directory		
Image: Stripper (M) Image: Stripper (M) Image: Stripper (M) Image: Stripper (M) <td>▶ III № # base</td> <td></td> <td>CWE ID:</td> <td>200</td> <td></td>	▶ III № # base		CWE ID:	200	
We define the state of the	GET:beef(N)				
Conservation C	GET:beef(S)		WASC ID:	13 🗸	
A reference: Confidence: For http://72.20.0103/7b-A Geff: http://72.20.0103/7b-A	GET:beef(D)		Description:		
K GETrobots.txt the produced the unhanded exception. This information K HEF=* 7%+**Last modified / A H	▶ 🔜 🍋 ₩ beef		This page contains an error/warning message that may	A 100 100 100 100 100 100 100 100 100 10	
Cons	📄 🙉 🗰 GET: docs	4	disclose sensitive information like the location of the fil	e D	
W GET: notes, normal information can be control of the file that produced the unhanded exception. This cancel Gave We cancel Gave W Getting the produced the unhanded exception. This cancel Gave We cancel Gave	▶ 🧰 icons	<	that produced the unhandled exception. This informati	on 🔽 📝 🗛 🗛 HRE	H="?M=A">Last modified <a hheh="</th">
Image: Search Release Could and Release	📄 🙉 🗰 GET:robots.txt	<u> </u>	Other Info:		-
History Search National Search National Search National Search National Search National Search Sear	🛛 🏴 🍀 GET:sitemap.xml	<u> </u>		ry 18- Jan - 2009 21:	58 -
Application Error Olaclosure (20) URL: Bak: Confidence: Parameter: Attack: Confidence: GET: http://172.20.0103/N=A	🔚 History 🔍 Search р Alerts 🖈 📄 Output 🏽 🕷 Spide	r 🚺 👌 Active Scan 🕇 🖣			
V fin M Application Error Disclosure (20) GFT: http://172.20.0103/Tb=A GFT: http://172.20.0103	◎	Application Error I			* ×
GFT: http://172.00.0103/D=0 Risk: GFT: http://172.00.0103/D=0 Confidence: GFT: http://172.00.0103/D=0 Risk: GFT: http://172.00.0103/D=0 Reference: GFT: http://172.00.0	🔻 🛱 🔑 Application Error Disclosure (201) 🔹 🔺	URL:	C		
GET: http://172.20.0103/TD=A Confidence: Parameter: GET: http://172.20.0103/TD=A Confidence: Parameter: Attack GET: http://172.20.0103/TD=A Beriew the source older this page. Implement custom provide a unique error relevance GET: http://172.20.0103/TD=A GET: http://172.20.0103/TD=A Extense: GET: http://172.20.0103/TD=A GET: http://172.20.0103/TD=A Extense: GET: http://172.20.0103/TD=A GET: http://172.20.0103/TD=A Extense: GET: http://172.20.0103/TD=A GET: http://172.20.0103/TD=A Extense: GET: http://172.20.0103/TD=A GET: http://172.20.0103/TD=A Extense: Farence: WASC (D): Description: Information can GET: http://172.20.0103/TD=A Extense: Confidence: Farence: Confidence: Farence: Confidence: Farence: Confidence: Farence: Farence: Farence: Confidence: Farence:	GET: http://172.20.0.103/	Risk:	Solution:		
GET: http://72.20.0103/7b=0 GET: http://72.20.0103/7k=A GET: http://72.20.00.0103/7k=A GET: http://72.20.00.000/7k=A GE	GET: http://172.20.0.103/?D=A	Confidence:	Review the source code of this page. Implement custor	n 🔺	
GET: http://17.2.0.0.103/M=A GET: http://17.2.0.0.103/M=A GET: http://17.2.0.0.103/M=D GET: http://17.2.0.0.103/N=D GET: http://17.2.0.0.103/S=D GET: http://17.2.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.	GET: http://172.20.0.103/?D=D	Parameter:	error pages. Consider implementing a mechanism to		P
GEI: http://12.20.0103/N=D CWE ID: WASC ID: GET: http://17.20.0103/N=D GET: http://17.20.0103/N=D Befrence: WASC ID: Description: This page contain information can GET: http://17.20.0103/N=D This page contain information can GET: http://17.20.0103/N=D This page contain information can Alerts P7: P5: P6: P0 Cancel Save	GET: http://172.20.0.103/?M=A	Evidence:	provide a unique error reference/identifier to the client		
Wasc ID: Description: Gef: http://72.20.0109/N=A Bescription: Gef: http://72.20.0109/N=A This page contain formation can Cancel Save the location of the file that produced the unhandled exception. This contain formation can Alerts 77 PS P6 P0 Current Scans Go 0	GET: http://172.20.0.103/?M=D	CWE ID:	Reference:		
GET: http://17.22.00.103/rS=D Description: This page containformation can Alerts #7 P5 P6 © 0 Description: This page containformation can Cancel Save the location of the file that produced the unhandled exception. This rormation can Cancel Save the location of the file that produced the unhandled exception. This rormation can Cancel Save the location of the file that produced the unhandled exception. This rormation can Cancel Save the location of the file that produced the unhandled exception. This rormation can Cancel Save the location of the file that produced the unhandled exception. This rormation can Cancel Save the location of the file that produced the unhandled exception. This Cancel Save the location of the file that produced the unhandled exception. This could be a failse positive Cancel Save the location of the file that produced the unhandled exception. This could be a failse positive Cancel Save the location of the file that produced the unhandled exception. This could be a failse positive Cancel Save the location of the file that produced the unhandled exception. This could be a failse positive Cancel Save the location of the file that produced the unhandled exception. This could be a failse positive Cancel Save the location of the file that produced the unhandled exception. This could be a failse positive Cancel Save the location of the file that produced the unhandled exception. This could be a failse positive Cancel Save the location of the file that produced the unhandled exception. This could be a failse positive Cancel Save the location of the file that produced the unhandled exception. This could be a failse positive Cancel Save the location of the file that produced the unhandled exception. This could be a failse positive Cancel Save the location of the file that produced the unhandled exception. This could be a failse positive Cancel Save the location of the file that produced the unhandled exception. This could be a failse positive Cancel Save the location of the file that produced the	GET: http://172.20.0.103//N=A	WASC ID:			
Gen Internation 2001 100 100 100 100 100 100 100 100 10	GET: http://172.20.0.103//N=D	Description:			
Alerts P7 P5 P6 P0	GET: http://172.20.0.103//S=A	This name contai		the location of the file that pro	duced the unbandled exception. This
Alerts 107 105 106 100 (2017) 100		information can t	Cancel	save could be a false positive if the e	rror message is found inside a documentation
	Alerts 10 7 10 5 10 6 10 0			Cu	rrent Scans 👨 0 👌 0 🥥 0 🗰 0 🏓 0 🗰 0

Medium findings, Application Error Disclosure.

If you have an https sites that requires authentication, right-click on the IP address, Include in Context, and New Context.

Add your credentials here and hit the button Add.

Conclusion

By following this narrative, you've successfully run a web scan against a very vulnerable server with a lot of findings to explore and take to the next level with actively exploiting, and if you are wise, understanding how to close on the web servers side. There is more to do here. I recommend if you have 2 network interfaces on your Kali Linux virtual machine, i.e. one for NAT and one for Host-only, to disable the NAT interface when you are not updating the server. This takes discipline. But, this action will make sure you don't have stray packets going out to web sites that might press legal charges against you when they discover them and turn those over to law enforcement. The choice is yours; I prefer to error on the side of caution.