







# Sadržaj

1	UVO	D	
2	INST	TALACIJA ALATA OWASP ZAP	4
3	KOR	NŠTENJE ALATA OWASP ZAP	8
	3.1	Konfiguracija HTTP posrednika (eng. <i>HTTP proxy</i> )	9
	3.2	KONFIGURACIJA ZA PRESRETANJE HTTPS PROMETA	
	3.3	KORIŠTENJE OWASP ZAP HTTP POSREDNIKA	
	3.4	ISPITIVANJE SIGURNOSTI POMOĆU ALATA OWASP ZAP	
4	ZAK	LJUČAK	23

Ovaj dokument izradio je Laboratorij za sustave i signale Zavoda za elektroničke sustave i obradbu informacija Fakulteta elektrotehnike i računarstva Sveučilišta u Zagrebu.

Ovaj dokument vlasništvo je Nacionalnog CERT–a. Namijenjen je javnoj objavi te se svatko smije njime koristiti i na njega se pozivati, ali isključivo u izvornom obliku, bez izmjena, uz obvezno navođenje izvora podataka. Korištenje ovog dokumenta protivno gornjim navodima povreda je autorskih prava CARNET-a, a sve navedeno u skladu je sa zakonskim odredbama Republike Hrvatske.



## 1 Uvod

Već duže vrijeme raste broj web aplikacija te se značajan dio našeg privatnog i poslovnog života seli na web. Paralelno tome, raste i broj napada na web aplikacije te su posljedice takvih napada sve značajnije. Kako bi povećali razinu sigurnosti web aplikacija, jedan koristan postupak je ispitivanje njihove sigurnosti iz perspektive napadača.

OWASP Zed Attack Proxy, kraće OWASP ZAP ili samo ZAP, jedan je od najčešće korištenih slobodnih (eng. *free and open source*) alata za ispitivanje sigurnosti web aplikacija. U tu svrhu ga koriste programeri aplikacija, ali i sigurnosni stručnjaci. OWASP ZAP je u suštini HTTP posrednik. U mreži, HTTP posrednik (eng. *HTTP proxy*) se nalazi između HTTP klijenta i poslužitelja, a njegova zadaća je da prenosi, analizira te po potrebi i mijenja HTTP promet koji prolazi kroz njega. U <u>prethodnom dokumentu</u> Nacionalnog CERT-a opisan je sličan alat, Telerik Fiddler – no njegova je glavna primjena ispravljanje grešaka (eng. *debugging*), dok je OWASP ZAP usmjeren na sigurnost.

Kao što i ime kaže, iza ovog alata stoji neprofitna organizacija OWASP (Open Web Application Security Project) koja uz pomoć velikog broja volontera razvija slobodno dostupnu dokumentaciju, alate i metodologije u području web sigurnosti. OWASP ZAP dostupan je na operacijskim sustavima Windows, Linux i macOS. Njegova trenutna inačica je 2.7 te će na toj inačici biti i prikazani primjeri u nastavku dokumenta.



## 2 Instalacija alata OWASP ZAP

U ovom dokumentu bit će objašnjen instalacijski postupak na operacijskom sustavu Windows 10, no postupak je analogan i na ostalim inačicama sustava Windows. Za rad alata OWASP ZAP potrebno je instalirati okruženje za izvođenje programskog jezika Java (eng. *Java Runtime Environment*) koje je moguće preuzeti <u>ovdje</u>. Potrebno je preuzeti odgovarajuću inačicu – u ovom primjeru 64-bitna inačica za operacijski sustav Windows.

Najnoviju inačicu instalacijske datoteke alata ZAP moguće je preuzeti sa službene web stranice na <u>ovoj poveznici</u>. Pritiskom na poveznicu s natpisom **Download now** za odgovarajuću sustav, u ovom slučaju **Windows (64) Installer**, počinje preuzimanje instalacijske datoteke.



Nakon pokretanja preuzete datoteke, ako instalacijski program ne uspije pronaći okruženje za izvođenje programskog jezika Java, prikazat će se poruka s donje slike. U tom slučaju, potrebno je u izborniku datoteka odabrati lokaciju okruženja za izvođenje programskog jezika Java ili instalirati ga, ako to već nije napravljeno.

install4j W	izard X	
3	The install4j wizard could not find a Java(TM) Runtime Environment on your system. Please locate a suitable 64-bit JRE. (minimum version: 1.8)	
	Locate Cancel	



Nakon toga se otvara čarobnjak za instalaciju alata OWASP ZAP. Pritiskom na tipku *Next* prelazi se na sljedeći korak.

🔇 Setup - OWASP Zed Attac	ack Proxy 2.7.0 —				
	Welcome to the OWASP Z Setup Wizard	ed Attac	k Prox	у	
	This will install OWASP Zed Attack Pro wizard will lead you step by step thro Click Next to continue, or Cancel to e	xy on your ( ugh the inst xit Setup.	computer. allation.	The	
		Next >	Ca	ancel	

U ovom je koraku prikazana licenca koju koristi OWASP ZAP. Potrebno je odabrati *I accept the agreement* te pritisnuti *Next* za sljedeći korak instalacijskog postupka.

🔇 Setup - OWASP Zed Attack Proxy 2.7.0 —		×
License Agreement Please read the following important information before continuing.	-	
Please read the following License Agreement. You must accept the terms of thi before continuing with the installation.	is agreeme	ent
Apache License Version 2.0, January 2004 http://www.apache.org/licenses/ TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION 1. Definitions. "License" shall mean the terms and conditions for use, reproduction, sed distribution as defined by Sections 1 through 0 of this day ment		~
<ul> <li>I accept the agreement</li> <li>I do not accept the agreement</li> </ul>		
<pre>Instair4j <back next=""></back></pre>	•	Cancel



Zatim je moguće odabrati standardni ili prilagođeni instalacijski postupak. Standardne postavke su u ovom slučaju dovoljne pa je potrebno ostaviti odabranu opciju *Standard installation* te pritisnuti tipku *Next* za sljedeći korak.

🔇 Setup - OWASP Zed Attack Proxy 2.7.0		_		×
Select Installation Type Which type of installation should be performed?				
Select the type of installation that you want to perform. Clic continue.	k Next v	vhen you are	e ready to	)
Standard installation				
O Custom installation				
install4j				
< B	Back	Next >	Ca	ancel

U ovom koraku je moguće provjeriti postavke instalacije. Ukoliko je sve u redu, pritiskom na *Install* započinje postupak instalacije datoteka na računalo korisnika.





Nakon što instalacija završi, prikazuje se zadnji korak čarobnjaka. Klikom na *Finish* instalacijski čarobnjak se gasi te je sada moguće koristiti alat OWASP ZAP.





## 3 Korištenje alata OWASP ZAP

Prečicu na izvršnu datoteku alata OWASP ZAP moguće je naći na radnoj površini sustava ili pretraživanjem u glavnom izborniku. Pri pokretanju OWASP ZAP-a prvo se otvara prozor u kojem je prikazan napredak otvaranja alata. Zbog složenosti alata i velikog broja komponenti, ovaj postupak može potrajati i do minutu na sporijim računalima.



Nakon uspješnog otvaranja alata prikazuje se prozor u kojemu se može odabrati treba li ovu sjednicu korištenja alata pohraniti na računalo ili ne. U ovom slučaju to nije potrebno pa će biti odabrano *No, I do not want to persist this session at this moment in time* te će biti pritisnuta tipka *Start*.

🔇 OWASP ZAP - OWASP ZAP 2.7.0							_		$\times$
<u>File Edit View Analyse Report</u>	<u>T</u> ools <u>O</u> nline <u>H</u> elp								
Standard Mode 💌 📄 블 🔚 🗎	🗉 📄 🎲 🗖 🖻	* 📖 🔳			1 🔒 🥖 💡		10	💥 🖽	
Sites 🕂		🛛 🖗 Quick S	tart 🖉 🔿 Re	quest	Response				
									-
Contexts		Welco	me to t	he	OWASP	Zed /	Atta	ck P	r <b>o</b> :
		7AP is an op	ev to uco intog	otod n	opotration tactin	<del>a tool for fin</del> X	ding vul	nerabilitie	es in
		rejet the ZAD	foreion?			~	bu have	been sp	ecifi
		ISISU III ZAP	Session with nor	o hoo	ad on the ourrant	timesterne	ttack.		
	O Yes, I want to p	ersist this se	ssion with harr	ie bas	ed on the current	umestamp	,		
	Yes, I want to p	ersist this se	ssion but I wan	t to sp	ecity the name a	nd location			_
	No, I do not wa	int to persist t	his session at t	his m	oment in time				
	Remember my	choice and c	lo not ask me a	gain.					
	You can always ch	ange your de	cision via the O	ptions	/ Database scree	en			
History 🔍 Search 🏴 Ale	Help					Start			7 F
🎯 🍛 🍸 Filter: OFF े Export									
Id Req. Timesta Met URI	L		Co Reason	R	Size Resp I	Highest	N Ta	ags	5
Alerts 🍽 0 🏴 0 🏴 0			Cur	rent S	cans 🍑 0  🐺 (	) ) 0 🧕	0 🕷	0 20	₩0

# CERT.hr

Sada se otvorio glavni prozor alata OWASP ZAP te je moguće koristiti njegove značajke, primjerice presretanje HTTP prometa ili ispitivanje sigurnosti web aplikacija.

### 3.1 Konfiguracija HTTP posrednika (eng. *HTTP proxy*)

Kako bi HTTP promet bio usmjeren preko posrednika, tj. preko alata OWASP ZAP, potrebno je izmijeniti određene postavke u web pregledniku. Po pretpostavljenim (eng. *default*) vrijednostima, OWASP ZAP očekuje promet na priključku (eng. *port*) 8080. Tipično, u postavkama web preglednika moguće je ili ručno konfigurirati korištenje posrednika ili koristiti postavke posrednika operacijskog sustava. U ovom primjeru bit će opisano postavljanje posrednika u web pregledniku Google Chrome na operacijskom sustavu Windows 10.

U glavnom izborniku preglednika Google Chrome (ikona s tri točkice u gornjem desnom kutu) prvo je potrebno odabrati *Settings*. Tada je moguće pretražiti postavke pomoću riječi *proxy* te pritisnuti na *Open proxy settings*.





Kako bi se konfiguriralo korištenje posrednika potrebno je pritisnuti *Lan settings*.



Potrebno je označiti *Use proxy server for your LAN*, pod *Address* upisati **localhost** i pod *port* upisati **8080**.

🐏 Local Area Network (LAN) Settings 🛛 🗙 🗙								
Automatic configuration Automatic configuration may override manual settings. To ensure the use of manual settings, disable automatic configuration. Automatically detect settings Use automatic configuration script								
Address								
Proxy server Use a proxy server for your LAN (These settings will not apply to dial-up or VPN connections).								
Address:     localhost     Port:     8080     Advanced       Bypass proxy server for local addresses								
OK Cancel								



Ovakva konfiguracija dovoljna je za presretanje nezaštićenog HTTP prometa. No danas se sve više koristi HTTPS protokol koji šifrira i štiti mrežni promet između klijenta i poslužitelja. Kada se koristi HTTPS protokol, mrežni promet je zaštićen tako da ga u pravilu nitko ne može presresti – ni napadač, ali ni korisnik koji pokušava legitimno koristiti OWASP ZAP.

#### 3.2 Konfiguracija za presretanje HTTPS prometa

Kako bi pomoću OWASP ZAP-a ipak mogli presretati mrežni promet zaštićen HTTPS protokolom, potrebno je napraviti dodatne korake za konfiguraciju web preglednika odnosno operacijskog sustava. Točnije, potrebno je uvesti TLS certifikat koji je generiran pomoću OWASP ZAP-a. Korištenjem tog certifikata OWASP ZAP može uspješno presretati HTTPS promet.

Za konfiguraciju presretanja HTTPS prometa, potrebno je prvo u glavnom izborniku alata OWASP ZAP odabrati *Tools* pa zatim *Options*, kao što je prikazano na donjoj slici.



Zatim je u lijevom popisu prozora koji se upravo otvorio potrebno odabrati *Dynamic SSL Certificates* te pritisnuti tipku *Generate* kako bi se izradio certifikat.



🔇 Options	×
▼ Options Active Scan	ertificates
Active Scan Input Vectors       Root CA certific         AJAX Spider       Import         Alerts       Import         Anti-CSRF Tokens       Import         API       Import         Applications       Import         Breakpoints       Import         Callback Address       Import         Check For Updates       Import         Connection       Import         Display       Import	MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAhgbCjCk         AiHJrWFDumSJmJFG/tbzCONBmDlJnmpeqLkzKCkOfuzNSqfXBas         E6QWflvlzvboBLlU2r/uqPuPZLZa/uryk6RtCNd0vLS3S7bzC7         BlZjm6afG0G6f0BYFZarTYs+SjPQj6LjcEn0wZ9LYPeVvg2gfh         /5236HrRY4m80YC4QHiSQE8Wj3skDWa2tcw9EW8+o78p/ddpxv8         fL3NCdltouRde1Ahk0+EZ+ye3853SqoBVK3ELnQEU90GXw/ns4c         jQIDAQABo4IBfjCCAXowggEZBQNVHQ4EggEqBIIBJjCCASIwDQ1         BQADggEPADCCAQoCggEBAIYGwownyArg25KP9DhW8gIhya1hQ7r         QZg5S25qXqi5MygpDn7szUqn1wWveVYU11/R6kKG2h0kFn5b5c7         j2S2Wv7q8pOkbQjXdLy0t0u28wu8nhBNm6iEQQoFgQdWY5umnxt         Pkoz0I+i43BJ9MGfS2D31b4NoH4crR76U0sWllt7R/+dt+h60WC         Fo97JA1mtrXMPRFvPqO/Kf3Xacb/CU6Vp1/X3bS9gHy9zQndba1         nt/0d0qqAV5txC50BFPTh18P570HPdvU8Ut7mrhYHI0CAwEAATF
Dynamic SSL Certificates Encode/Decode Extensions Forced Browse Fuzzer Global Exclude URL (Beta) HTTP Sessions JVM Keyboard Language	BTADAQH/MAsGA1UdDwQEAwIBtjAjBgNVHSUEHDAaBggrBgEFBQc AwIGBFUdJQAwDQYJKoZIhvcNAQELBQADggEBAITPFA1XCGdSkpt mTdTDle46ePnAkgacdGLtB/B16ANKHkR5PAiEL72rN3XY+89EJW 8zZOwigVasxFIRAp9APmQVAa+EMYO/JSnTZLbj9hhpQY122zUpP 3EJLuAYJfTVYTGvFCEkgSKFAb8EVRC9xpxM/dIZAfEDW550Fk92 47adA070Ln1228XjhxpL1SNBR8gzIkD27nlom1A+QOKnxx9P+kC +xORNjBgT+doo29oyRZpbleCqKm0jj13ye0ghPwLfcTZ76111QE END CERTIFICATE
Language Local Proxies Passive Scan Rules Reset to Factory Defaults	Cancel OK

Zatim treba odabrati *Save* kako bi certifikat bio pohranjen u datoteku na računalu korisnika.

🔇 Save		×
Look <u>I</u> n:	certs	
File <u>N</u> ame:	owasp_zap_root_ca.cer	
Files of <u>T</u> ype:	All Files	
		Save Cancel

Nakon što je datoteka s certifikatom pohranjena na računalo, taj certifikat je potrebno uvesti u operacijski sustav tj. web preglednik. I u ovom primjeru korišten je web preglednik Google Chrome te operacijski sustav Windows 10. U postavkama preglednika Google Chrome moguće je pretražiti pojam *certificate* te zatim pritisnuti na *Manage certificates* kako bi se otvorila aplikacija za upravljanje certifikatima.





Otvaranjem kartice *Trusted Root Certificate Authorities* u otvorenom prozoru moguće je vidjeti postojeće certifikate te na računalo uvesti certifikat OWASP ZAP-a. Čarobnjak za pokretanje uvoza certifikata otvara se pritiskom na tipku *Import*.



itermediate Certi	ification Au	uthorities	Trusted Root (	Certification Aut	horities	Trusted Publ	•	
Issued To		Issued B	у	Expiry Date	Friend	y Name	^	
AddTrust Ex	ternal	AddTrust	t External CA	30/05/2020	The US	ERTrust		
🔄 AffirmTrust (	Comme	AffirmTru	ust Commercial	31/12/2030	AffirmT	Frust Com		
Baltimore Cy	berTru	Baltimore	CyberTrust	13/05/2025	DigiCer			
🔄 Certum CA		Certum C	CA	11/06/2027	Certum	Certum Certum Trusted		
Certum Trus	ted Ne	Certum T	rusted Netw	31/12/2029 Cert	Certum			
Class 3 Publi	c Prima	Class 3 P	ublic Primary	02/08/2028	VeriSig	n Class 3		
Copyright (c)	) 1997	Copyrigh	t (c) 1997 Mi	31/12/1999 M	Microso	crosoft Timest		
DigiCert Assu	ured ID	DigiCert	Assured ID R	10/11/2031	DigiCer	rt		
E DigiCert Glob	bal Roo	DigiCert	Global Root CA	10/11/2031	DigiCer	rt	×	
Import	Export	R	emove			<u>A</u> dvan	ced	
		s						
ertificate intende	ea purpose							
ertificate intende	ea purpose							

U čarobnjaku za uvoz certifikata potrebno je pritisnuti *Next* za sljedeći korak.

🔶 😺 Certificate Import Wizard	×
Welcome to the Certificate Import Wizard	
This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.	
A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.	
To continue, click Next.	
Next Canc	al

Sada je klikom na tipku **Browse** potrebno odabrati datoteku s certifikatom kojega je generirao OWASP ZAP.



Nakon odabira datoteke potrebno je pritisnuti **Open** kako bi se zatvorio prozor za odabir datoteke te *Next* za sljedeći korak.

💿 Open									×
← → • ↑ 📘	> This	s PC → Deskto	op > CERT > cert	s v	5	Search certs			Q
Organise 🔻 🛛 N	ew folder	r						•	•
📌 Quick access	^	Name	^		[	Date modified		Туре	
Desktop	*	🔄 owasp_z	ap_root_ca.cer		2	7/08/2018 14:18		Security	Certificate
Downloads	*								
🔮 Documents	*								
Pictures	*								
CERT	*								
slike									
slike									
slike									
ZAP Proxy									
a OneDrive									
	¥ .	<							>
	File <u>n</u> a	me: owasp_za	p_root_ca.cer		~	X.509 Certifica	ate (*	.cer;*.crt)	$\sim$
						<u>O</u> pen		Cano	el:

U ovom koraku nije potrebno ništa mijenjati, dovoljno je pritisnuti Next.

CERT.hr



Sada se prikazuje zadnji korak čarobnjaka u kojemu su ispisane sve odabrane postavke te je pritiskom na tipku *Finish* potrebno završiti postupak uvoza certifikata.

÷	Certificate Import Wizard		×
	Completing the Certific	cate Import Wizard	
	The certificate will be imported after	you dick Finish.	
	You have specified the following set	tings:	
	Certificate Store Selected by User	Trusted Root Certification Authorities	
	Content	Certificate	
	File Name	C:\Users\Lobel\Desktop\CERT\certs\owasp_zap_roo	
	<	>	
		<u>F</u> inish Cance	el



Pojavljuje se prozor s upozorenjem da na računalo pokušavamo instalirati certifikat kojemu sustav Windows ne može potvrditi porijeklo. Kako je taj certifikat maloprije generiran alatom OWASP ZAP, možemo mu vjerovati te će se pritiskom na tipku **Yes** certifikat instalirati na računalo.

Security W	/arning	×
	You are about to install a certificate from a certification authority (CA) claiming to represent: OWASP Zed Attack Proxy Root CA Windows cannot validate that the certificate is actually from "OWASP Zed Attack Proxy Root CA". You should confirm its origin by contacting "OWASP Zed Attack Proxy Root CA". The following number will assist you in this process: Thumbprint (sha1): D6847C39 6EA0196E 239E6D60 AF45454C 0E563F86	
	Warning: If you install this root certificate, Windows will automatically trust any certificate issued by this CA. Installing a certificate with an unconfirmed thumbprint is a security risk. If you click "Yes" you acknowledge this risk. Do you want to install this certificate?	
	<u>Y</u> es <u>N</u> o	

Sada je prikazana poruka u kojoj piše da je uvoz certifikata uspješan te je nakon ovoga moguće presretati HTTPS promet alatom OWASP ZAP.



#### 3.3 Korištenje OWASP ZAP HTTP posrednika

Nakon prethodne konfiguracije, otvaranjem web stranica u pregledniku, automatski se bilježe te prikazuju HTTP zahtjevi i odgovori u sučelju alata OWASP ZAP.

U donjem dijelu prozora u kartici *History* nalazi se popis svih HTTP zahtjeva. Dvoklikom na bilo koji zahtjev prikazuje se njegov sadržaj u kartici *Request* u gornjem desnom dijelu prozora, kao što je prikazano na sljedećoj slici.



😧 Untitled Session - OWASP ZAP 2.7.0 – 🗆 🗙							×			
File Edit View Analyse Report Tools Online Help										
Image: State in the second										
Default Context	GET http://192.168	.0.25/mu	tillidae/	styles/d	dsmoothmenu/dds	noothmenu-v.c:	ss HTTP/	1.1		
	User-Agent: Mozill	a/5.0 (V	lindows NT	10.0; W	in64; x64) Appl	WebKit/537.30	5 (KHTML	, like G	ecko)	
	Chrome/68.0.3440.1	06 Safar	i/537.36							
• • • http://192.168.0.25	Accept: text/css,*	/*;q=0.] 2 168 0	25/mutil1	idae/						
GET:mutillidae	Accept-Language: e	n-US,en;	q=0.9	1000						
🕨 🔛 🏴 mutillidae	Cookie: showhints=	1; PHPSE	SSID=n6qm	eedcdi3k	kn2hk5ob0fidml					
	Host: 192.168.0.25									
🛗 History 🔍 Search 📔 Alerts 📄 Output 🕂										
Id Reg. Timestamp Method URL		Code	Reason	RTT	Size Resp. Body	Highest Alert	Note	Tags		R
1 27/08/18 14:32:58 GET http://192.168.0.25/r	nutillidae/	200	OK	28 ms	52.984 bytes	P Medium		Form, Hi	dden. S	cr 🔺
3 27/08/18 14:32:58 GET http://192.168.0.25/n	nutillidae/styles/global-st	200	OK	36 ms	12,022 bytes	P <sup>D</sup> Low		Comme	nt	
4 27/08/18 14:32:58 GET http://192.168.0.25/r	nutillidae/styles/ddsmoot	200	ОК	14 ms	2,281 bytes	P Low		Comme	nt	
8 27/08/18 14:32:58 GET http://192.168.0.25/n	nutillidae/styles/ddsmoot	200	ОК	440	1,188 bytes	🏴 Low		Comme	nt	
9 27/08/18 14:32:58 GET http://192.168.0.25/r	nutillidae/javascript/jQuer	200	ок	7 ms	5,000 bytes	P Low		Comme	nt	
13 27/08/18 14:32:58 GET http://192.168.0.25/n	nutillidae/javascript/dds	200	ок	14 ms	57,254 bytes	P Low		Script, C	ommen	t
15 27/08/18 14:32:58 GET http://192.168.0.25/n	nutillidae/javascript/dds	200	ОК	67 ms	8,639 bytes	P Low		Comme	nt	
16 27/08/18 14:32:58 GET http://192.168.0.25/n	nutillidae/javascript/book	200	OK	26 ms	1,064 bytes	P Low		Comme	nt	
19 27/08/18 14:32:59 GET http://192.168.0.25/n	nutillidae/javascript/jQuer	200	ок	9 ms	267,739 bytes	P Low		Hidden,	Script, C	o
20 27/08/18 14:32:59 GET http://192.168.0.25/r	nutillidae/javascript/jQuer	200	OK	3 ms	11,337 bytes	P <sup>D</sup> Low		Comme	nt	
21 27/08/18 14:32:59 GET http://192.168.0.25/r	nutillidae/javascript/jQuer	200	ОК	4 ms	9,845 bytes	P Low				
45 27/08/18 14:33:19 GET http://192.168.0.25/r	nutillidae/index.php?pag	200	OK	52 ms	53,207 bytes	P Medium		Form, Pa	assword	
40 2000400 201200 (91 ) http://doi.org/10.10.001/20100000000000000000000000000										

Osim zahtjeva, moguće je vidjeti i sadržaj HTTP odgovora klikom na karticu *Response*. U gornjem dijelu kartice nalaze se zaglavlja, dok je u donjem dijelu tijelo HTTP odgovora.

🔌 Untitled Session - OWASP ZAP 2.7.0 – 🗆 🗙							×			
Eile Edit View Analyse Report Iools Online Help										
Standard Mode 💌 🗋 😂 📰 👘 🖄 💷 💆 📟 🖿 🚍 🖃 👘 🔛 👘 👘 👘 👘 👘 👘										
Sites 🛨		Quick Start 🔿	Request Response	÷ +						
◎ □ ■ □		Header: Text V Bo	dy: Text 💌 🔲							
Contexts Contexts Context Con	<pre>Header.Text V Body.Text V Header.Text Body.Text Body.Text Body.Text Body.</pre>									
General Protocol      Filter: OFF      Frequencies	Calpar (a) opraci									
Id Reg Timestamp Method	LIDI		Code Reason	PTT	Size Resp. Body	Highest Alert	Note	Tage		Æ
1 27/09/19 15:00:47 CET	https://www.owoon.org/	magac/7/72/01//ASP	200 OK	2.02 c	1 797 727 bitoc		Note	Commo	nt	
6 27/09/19 15:09:57 CET	http://102.169.0.25/muti	llidae/index.nbn2nad	200 OK	2.03 S	52 /10 bytes	Medium		Eorm H	liddon S	
9 27/08/18 15:09:57 CET	http://192.168.0.25/muti	llidae/styles/global.st	200 OK	5 me	12,022 bytes			Comme	induen, c	
11 27/08/18 15:09:57 GET	http://192.168.0.25/muti	llidae/styles/ddsmoot	200 OK	36 ms	2 281 hytes	RUL ow		Comme	ant	
15 27/08/18 15:09:57 GET	http://192.168.0.25/muti	llidae/iavascrint/book	200 OK	16 ms	1.064 bytes	RULow		Comme	ent	
16 27/08/18 15:09:57 GET	http://192.168.0.25/muti	llidae/javascript/dds	200 OK	31 mg	8 639 bytes	RUL ow		Comme	ant	
17 27/08/18 15:00:57 CET	http://102.168.0.25/muti	llidae/javascript/dds	200 OK	7 me	57 254 hytes	RI Low		Scrint (	ommer	
19 27/09/19 15:09:57 CET	http://102.169.0.25/muti	llidae/javascript/iQuer	200 OK	10 me	5 000 bytes	PLOW		Comme	ont	" J
19 27/08/18 15:09:57 GET	http://192.168.0.25/muti	llidae/styles/ddsmoot	200 OK	14 me	1 188 hytes	RULow		Comme	ent	
20 27/08/18 15:09:57 GET	http://102.168.0.25/muti	llidae/iavascrint/iOuer	200 OK	20 ms	267 739 hutes	R Low		Hidden	Scrint (	20
31 27/08/18 15:09:58 CET	http://192.168.0.25/muti	llidae/iavascript/jQuer	200 OK	3 me	11 337 hytes	RULow		Comme	ent	
33 27/08/18 15:09:58 GET	http://102.168.0.25/muti	llidae/javascript/jouer	200 OK	3 ms	9.8/5 hytes	R Low		Comme		
44 07/00/40 45:40:04 OFT	http://100.160.0.0E/multi	llidee/index.nhp0nea	200 0K	16 mg	E0 004 hites	Di Madium		Form U	liddon C	<b>T</b>
Alerts 🍽 0 🔑 1 🔑 5 🔑 0					Current S	cans 🌞 0   🐺 0	0 6	o 😸 💿 🕘	0 / 0	₩0



Mijenjanje HTTP zahtjeva jedna je od glavnih značajki OWASP ZAP-a. Mijenjanje zahtjeva izrazito je korisno za ispitivanje funkcionalnosti i sigurnosti web aplikacija. OWASP ZAP- om moguće je izmijeniti bilo koji dio HTTP zahtjeva, od primjerice HTTP kolačića (eng. *cookies*) do podataka poslanih u tijelu zahtjeva.

Osnovne tipke za rad s presretanjem i izmjenom HTTP zahtjeva nalaze se u alatnoj traci pri vrhu sučelja OWASP ZAP-a. Tri ikone koje će biti potrebne za ovu funkcionalnost označene su na donjoj slici.

🔇 Untitled Session - OWASP ZAP 2.7.0					_		×
<u>File Edit View Analyse Report Tools Online Help</u>		_					
Standard Mode 💌 🗋 😓 🕞 💷 📄 🌼 💷 🗷 📼 🏾		🧕 💡 🥥		🔀 🖽 🗽 📼	0	<b>G</b>	
Sites 🕂	Quick Start 🖈 🔿 Request	Response 🖛	<b>+</b>				

Klikom na zeleni krug (prvu ikonu s lijeva), krug poprima crvenu boju. To označava da sada OWASP ZAP zaustavlja svaki HTTP zahtjev kako bi ga bilo moguće izmijeniti prije slanja poslužitelju. Primjerice, nakon pritiska na zeleni krug, otvaranje neke web stranice (u web pregledniku) će u sučelju OWASP ZAP-a prikazati zaustavljeni zahtjev u kartici **Break**.





Bilo koji dio zahtjeva sada je moguće izmijeniti. Nakon izmjene, pritiskom na ikonu desno od kruga (srednju od tri prethodno označene ikone) zahtjev će biti poslan, te će se svaki sljedeći zahtjev također ovako zaustaviti. Pritiskom na krajnje desnu ikonu od tri prethodno označene, zahtjev će biti poslan, no OWASP ZAP sada neće više zaustavljati sljedeće zahtjeve.

#### 3.4 Ispitivanje sigurnosti pomoću alata OWASP ZAP

Prije objašnjenja postupka, bitno je naglasiti kako se **ispitivanje sigurnosti web** aplikacije smije raditi isključivo uz dopuštenje vlasnika.

Postoje dva načina ispitivanja sigurnosti web aplikacija u alatu OWASP ZAP: pasivno skeniranje i aktivno skeniranje.

Pasivno skeniranje je automatski uključeno te ga je po potrebi moguće isključiti u postavkama. U pasivnom skeniranju, OWASP ZAP samo analizira promet koji putuje kroz njega. Primjerice, dok korisnik otvara i koristi neku web stranicu s OWASP ZAP-om kao posrednikom, OWASP ZAP će analizirati promet te na temelju njega bilježiti pronađene sigurnosne propuste. Rezultate skeniranja moguće je vidjeti u kartici *Alerts* u donjem dijelu glavnog prozora OWASP ZAP-a. Tamo je zabilježen popis mogućih sigurnosnih propusta kategoriziranih po vrsti. Pritiskom na pojedinu ranjivosti u toj kartici prikazuju se dodatne informacije kao što je prikazano na donjoj slici.





Za razliku od pasivnog skeniranja, aktivno skeniranje zapravo napada web aplikaciju na razne načine te tako pokušava otkriti ranjivosti. Najlakši način za pokretanje aktivnog skeniranja je upisivanje URL-a u polje na kartici **Quick Start** te pritisak na tipku **Attack**.

😧 Untitled Session - OWASP ZAP 2.7.0 — 🗆 🗙							
File Edit View Analyse Report Tools Online Help							
Standard Mode 💌	Standard Mode 🔹 🗋 🐂 🖬 👘 🔅 🕄 👘 👘 👘 👘 👘 👘 👘 👘 👘 👘 🖉 🖉 🖉 👘 🐘 🖉 🗶 🐘						
Sites 🕂		🥰 Quick Start 🖋 🔿 Request 🕅 Response⇔ 🏾 🛨					
0 🗔 🗊 🖪							
		Welcome to the OWASP Zed Attack Proxy (ZAP)					
Default Contex	đ	······································					
🔻 🚱 Sites	-	ZAP is an easy to use integrated penetration testing tool for finding vulnerabilities in web applications.					
► 📄 🏴 http://192.1	68.0.25	Please be aware that you should only attack applications that you have been specifically been given pe	rmission				
		To quickly test an application, enter its URL below and press 'Attack'.					
		URL to attack: http://192.168.0.25	Se 🚱				
		Attack Ston					
		Progress: Spidering the URL to discover the content					
		For a more in depth test you should explore your application using your browser or automated regressi	ion tests v				
		Explore your application: Launch Browser JXBrowser					
			7.6				
History 🔍 Soor	rch 🔲 Alarta 📄 C						
History - Sea							
₩ New Scan : Progre	ess: 0: http://192.168.0	0.25 🔽 🕕 🔚 📕 🎒 💮 🛒 Current Scans: 1 🗄 URLs Found: 948 🗄 Nodes Added: 166 🗄 🦧 Export	ŝĝi				
URLs Added Node	s Messages						
Processed	Method	URI Flags	1				
<u> </u>	GET	http://192.168.0.25/mutillidae/styles/ddsmoothmenu/?C=D;O=A					
	GET	http://192.168.0.25/mutillidae/styles/ddsmoothmenu/readme.txt					
	GET	nttp://192.168.0.25/webservices/?C=N;O=D					
	GET	nttp://192.168.0.25/webservices/?C=M;O=A					
	GET	nttp://192.168.0.25/webservices/?C=S;O=A					
	GEI	http://192.168.0.25/webservices/?C=D;O=A					
	GEI	nttp://192.168.0.25/webservices/soap/	_				
	GET	http://192.108.0.25/webservices/test/00_N/0_D					
	GET	nttp://192.158.0.25/webservices/restr/C=N;U=D					
	GET	http://192.108.0.25/websefvices//cst//C=A					
	GET	http://192.108.0.25/websetvices/resv/ro=5,0=A	_				
	GET	http://192.106.0.20/webset//CESI/CED,UEA					
Alerts 🏴 0 🏴 2 🏴 5	hn 0	Current Scans 😻 0 👌 0 🥥 0 🕷 1 🥕	0 🕷 0				

OWASP ZAP prvo pokušava otkriti koji sve URL-ovi postoje na web aplikaciji, pa ih zatim po završetku toga aktivno skenira. U donjem dijelu prozora alata OWASP ZAP u kartici *Active Scan* vidljiv je napredak aktivnog skeniranja.

<b>W</b> Untitled Session - OWASP ZAP 2.7.0			- 0	×	
Eile Edit View Analyse Report Iools Online Help					
Standard Mode 💌 🗋 😂 🕁 💷 📑 🌼 💷 🗷 📼		) Ø 💢 🖩 🖿 🗌	0 6 6		
Sites +	Gerick Start ≉ 🔿 Request Cresponse	• [+]			
				/	
T Contexts	Welcome to the OWASP	<sup>9</sup> Zed Attack Pr	oxy (ZAP)		
Default Context	ZAP is an easy to use integrated penetration testin	na tool for findina vulnerabilitie	s in web applications.	5	
🔻 🚱 Sites		,			
https://www.paypalobjects.com	Please be aware that you should only attack applic	cations that you have been spe	ecifically been given permission to te	st. 🔪	
▼ 🚞 № http://192.168.0.25	To quickly test an application, enter its URL below	and press 'Attack'.			
GET:mutillidae	the second second second second second				
🔻 🚞 🏴 mutillidae	URL to attack: http://		Select		
images			- Oblect		
GET:index php(page)	Stack	Stop			
B investing	Progress: Not started				
P avascipt					
Fª styles					
### https://www.google.hr	For a more in depth test you should explore your application using your browser or automated regression tests while proxying				
	Explore your application: Launch Browser J	xBrowser 🔻			
(L)	•			7.6	
🛗 History 🔍 Search 🏾 💾 Alerts 🗋 📄 Output 🚺 Active So	an 🖉 🛪 🚹				
Mew Scan   Progress: 0: http://192.168lidae/index.php	II II II II 100%	🥑 Current Scans: 0 🗄	Num requests: 113 🦧 Export	ŝ	
Id Reg. Timestamp Resp. Timestamp Method	JRL Co	de Reason RTT	Size Resp. Header Size Resp. B	ody 📑	
167 27/08/18 15:37:12 27/08/18 15:37:12 GET	http://192.168.0.25/mutillidae/index.php?pag	200 OK 15 ms	189 bytes 44,881 bytes	4	
168 27/08/18 15:37:12 27/08/18 15:37:12 GET	http://192.168.0.25/mutillidae/index.php?pag	200 OK 17 ms	189 bytes 44,869 bytes		
169 27/08/18 15:37:12 27/08/18 15:37:12 GET	http://192.168.0.25/mutillidae/index.php?pag	200 OK 16 ms	189 bytes 44,875 bytes		
170 27/08/18 15:37:12 27/08/18 15:37:12 GET	http://192.168.0.25/mutillidae/index.php?pag	200 OK 16 ms	189 bytes 44,887 bytes		
171 27/08/18 15:37:12 27/08/18 15:37:12 GET	http://192.168.0.25/mutillidae/index.php?pag	200 OK 17 ms	189 bytes 44,893 bytes		
172 27/08/18 15:37:12 27/08/18 15:37:12 GET	http://192.168.0.25/mutillidae/index.php?pag	200 OK 31 ms	189 bytes 55,071 bytes	_	
17.3 27/08/18 15:37:12 27/08/18 15:37:12 GET	http://192.168.0.25/mutilidae/index.php?=	200 OK 17 ms	189 Dytes 52,984 bytes		
174 27/08/18 15:37:12 27/08/18 15:37:12 GET	http://192.168.0.25/mutilidae/index.php?page=	200 OK 33 MS	189 bytes 51,676 bytes	-	
176 27/08/18 15:37:12 27/08/18 15:37:12 GET	http://192.168.0.25/mutilidae/index.php?pag	200 OK 17 ms	189 hytes 44,521 bytes		
177 27/08/18 15:37:12 27/08/18 15:37:12 CET	http://192.168.0.25/mutillidae/index.php?pag	200 OK 17 ms	189 hytes 44 521 hytes		
178 27/08/18 15:37:12 27/08/18 15:37:12 GET	http://192.168.0.25/mutillidae/index.php?pag	200 OK 31 ms	189 bytes 44 521 bytes		
	the second s				



Također, OWASP ZAP sada sam pronalazi sigurnosne propuste te ih je, kao i kod pasivnog skeniranja, moguće pregledati u kartici *Alerts*.

🔌 Untitled Session - OWASP ZAP 2.7.0 — 🗆 🗙						
File Edit View Analyse Report Tools Online Help						
(Standard Mode 💌 🗋 😂 🕞 💷 💼 🎲 💷 🎩	= □ □ □ = 🛔 💋 ♀ 🕒  🖉 🖉 🐜 🔤 🛛 ④ ⑤ 🚱					
Sites +	Guick Start      A Request Response					
Contexts	Welcome to the OWASP Zed Attack Proxy (ZAP)					
Default Context	74P is an easy to use integrated genetration testing tool for finding vulnerabilities in web applications					
🔻 🥯 Sites	Zw is an easy to use integrated penetration testing too for infoling vulnerabilities in web approactions.					
https://www.paypalobjects.com	Please be aware that you should only attack applications that you have been specifically been given permission to test.					
http://192.168.0.25	To quickly test an application, enter its URL below and press 'Attack'.					
📄 🏴 GET:mutillidae						
🔻 🚞 🏴 mutillidae	URL to attack: http://					
images	4ttack Stop					
📄 🏴 GET:index.php(page)	Progress: Not started					
Javascript						
Image: Styles						
Image: Physical Action in the second seco	For a more in depth test you should explore your application using your browser or automated regression tests while proxying					
	Explore your application: Launch Browser JxBrowser					
🔚 History 🔍 Search 📔 Alerts 🖉 📄 Output 👌 Active	e Scan 🛉					
	Path Traversal					
V 🚔 Alerts (9)	URL: http://192.108.0.25/mutilidae/index.pnp?page=%2FetC%2Fpasswd Bisk: N Hinh					
Cross Site Scripting (Reflected)	Confidence: Medium					
GET: http://192.168.0.25/mutillidae/index.php?page=ja	Parameter: page					
GET: http://192.168.0.25/mutillidae/index.php?page=%	Attack: /etc/passwd					
Arrame-Options Header Not Set (3)	Evidence: rootx:0:0					
P Cookie No HttpOnly Flag	WASCID: 33					
P Cookie Without Secure Flag	Source: Active (6 - Path Traversal)					
P W Incomplete or No Cache-control and Pragma HTTP Header B Private IP Disclosure (0)	er Set Description:					
P Web Browser XSS Protection Not Enabled (3)	The Path Traversal attack technique allows an attacker access to files, directories, and commands that					
X-Content-Type-Options Header Missing (25)	potentially reside outside the web document root directory. An attacker may manipulate a URL in such a way					
that the web site will execute or reveal the contents of arbitrary files anywhere on the web server. Any device						
Alerts 🏴 2 🟴 1 🟳 6 🏴 0	Current Scans 🧅 0 😽 0 🔗 0 🛞 0 🧩 0 🧩 0 🧩 0 🗰 0					



## 4 Zaključak

OWASP ZAP je moćan HTTP posrednik koji značajno olakšava ispitivanje sigurnosti web aplikacija. Osim funkcionalnosti HTTP posrednika, OWASP ZAP ima niz drugih funkcionalnosti usmjerenih na ispitivanje sigurnosti web aplikacija.

Iako OWASP ZAP koriste i sigurnosni stručnjaci, alat je prilagođen i korisnicima koji ne znaju puno o sigurnosti. Primjerice, OWASP ZAP koristan je autorima web aplikacija jer im na lagan način omogućuje osnovno ispitivanje sigurnosti razvijene aplikacije. OWASP ZAP sam po sebi ima mnoštvo funkcionalnosti, no uz njih, moguće ga je i proširiti dodacima (eng. *plugins*) te na taj način dodatno povećati korist alata.