

VICEPRESIDENCIA TERCERA DEL GOBIERNO MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL

SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL

Webinar 5 "Use of OWASP ZAP"

Exercises







secretaría de estado de digitalización e inteligencia artificial





INDEX

1. Practical Exercise	
2. Research Exercise	7
2.1. What type of vulnerability has been identified?	
2.3. How would you address the vulnerability?	12
3. Additional exercise	13

FIGURE INDEX

Figure 1 – Proxy settings	3
Figure 2 – Web browsing of the local "test" host	4
Figure 3 – HTTP Headers	4
Figure 4 – Request log	5
Figure 5 – POST Request form	5
Figure 6 – Warning about lacks of CSRF token	6
Figure 7 – bWAPP deployment	7
Figure 8 – bWAPP login	7
Figure 9 – Challenge: OS Command Injection (I)	8
Figure 10 – Challenge: OS Command Injection (II)	8
Figure 11 – POST Request	9
Figure 12 – nslookup output seems similar to server config	9
Figure 13 – Breakpoint 1	0
Figure 14 – Modification of the target parameter 1	0
Figure 15 – Confirmation of injection 1	0
Figure 16 – Source code (commandi.php) 1	1
Figure 17 – Bind shell with netcat 1	2
Figure 18 – Downloading dictionaries 1	3
Figure 19 – Adding new dictionaries 1	3
Figure 20 – Adding new dictionaries 1	4
Figure 21 – Identification of the configuration file "config.inc" 1	4







1. PRACTICAL EXERCISE

Learning HTTP communications in the bWAPP application using a passive approach from a Kali Linux distribution.

The objective of this exercise is to familiarize the student with the configuration of OWASP ZAP for HTTP traffic analysis and to study the communications used with a local domain. The host "test" will serve as a support; we will study the type of parameters sent and received, the method used, the location of web forms, etc. <u>The student will use a passive approach</u>, without using any of the attack features available in OWASP ZAP.

Let's configure the browser proxy to use the localhost address on port 8080. Be sure to select the "Use this proxy server for all protocols" option to include possible SSL traffic in that setting.

← → ♂ ✿	😆 Firefox 🛛 a	bout:preferences#general	80% 🟠	ill\ 🗊	≡
🌂 Kali Linux 🌂 Kali Trainin	ng 🌂 Kali Tools 🌂 K	ali Docs 🌂 Kali Forums 🌂 NetHunter 👖 Offensive Security 🔺 Exploit-DB 🛸 GHDB 👖 MSFU			
	Your organization has preferences.	disabled the ability to change some P Find in Preferences			Ŷ
🔅 General		Connection Settings ×			
Q Search					
 Privacy & Security Firefox Account 	Digital Rights Mar	Configure Proxy Access to the Internet			
	Firefox Update:	Auto-detect proxy settings for this hetwork Use system proxy settings Manual proxy configuration			
	Keep Firefox up to da Version 60.8.0esr (6- Kali Linux distribution	HTTP Progy 127.0.0.1 Port 8080 ✓ Uge this proxy server for all protocols			
	Kali - 1.0 ✓ Automatically up	SSL Proxy 127.0.0.1 Pgrt 8080 ETP Proxy 127.0.0.1 Port 8080			
	Performance	SO <u>C</u> KS Host 127.0.0.1 Port 8080 SOC <u>K</u> S V4 ● SOCKS <u>v</u> 5			
	✓ Use recommende These settings are f	Automatic proxy configuration URL			
	Browsing	No proxy for localhost, 127.0.0.1			
	Use <u>a</u> utoscrolling Use s <u>m</u> ooth scrol Always use the cu	Example: .mozilla.org, .net.nz, 192.168.1.0/24 Do not prompt for authentication if password is saved			l
	Search for te <u>x</u> t w Network Proxy	Proxy <u>D</u> NS when using SOCKS v5			

Figure 1 – Proxy settings

After setting the proxy, you will navigate to the <u>http://test/app/bWAPP/login.php</u> host and verify that OWASP ZAP collects all requests.



		Ayuda								
ar 💌 🗋 🚂 🖬 📑 🎡		▥ : ::::::::::::::::::::::::::::::::::	0 💢 📖 🗽 📼	🤢 🖲 🔮						
+		🔗 Inicio	Rápido 🔤 Petición	Respuesta 🗢 🛉						
3		Encabeza	miento: Vista Raw	Cuerpo:Vista Raw						
tos		GET here.	//102 168 1 5.0000	(ann/hUADR/login pto HTT	P/1 1					
texto predeterminado		Connectio	n: keep-alive	app/ower/login.php hit	F/1.1					
		DNT: 1								
ttp://192.168.1.5-8888		Upgrade-I User-Aper	nsecure-Requests: 1 t: Mozilla/5.0 (Wir	L idows NT 10.0: Win64: x6	 AppleWebKit/537.36 	(KHTNL, like Gecko) Chrome/80,0,3987	.122 Safari/537.36			
900		Accept: t	ext/html,applicatio	on/xhtml+xml,application	/xml;q=0.9,image/webp,	image/apng,*/*;q=0.8,application/sig	ned-exchange;v=b3;q=0.9	>		
		Sec-Fetch	-Site: none							
P OWAPP		Sec-Fetch	-User: 71							
Po tonts		Accept-La	nguage: es,en;q=0.9	9,es-ES;q=0.8						
images		Cookie: P Host: 192	<pre>HPSESSID=36u5v171bu .168.1.5:8888</pre>	Jime3g3clsls1jv06						
js										
GET:login.php										
E PU stylesheets										
s://192.168.1.5:8888										
🔍 Buscar) 🏴 Aleftas) 🔝 Sa	lida 🕂									
Buscar Pt Alefas Sa Itto: APAGADO E Exportar	lida 💽 🛨									
<mark>€. Buscar PB Alefas</mark>) Sa lite: APACADO € Espotar Marcade Serro Req	lida 🕂	URL	Código	Razón	RTT	Tamaño requerido para el cuerpo	Alerta mayor	Nota	Eliquetas	
C. Buscar Materias C Sa Mitra APAGADO 2 Expostar Marca de tempo Req 1 4/2/2017:74.9	Nida + Mětodo CET	URL IS SEESIAppV0xPPlogin.php	Código	Razón 502 Bad Gateway	RTT 20milisegundos	Tamaño requeido para el cuerpo 422h fea	Alerta mayor	Nota	Eliquetas	
Buscar Mateixa 58 Bir ANGADO Č Expotar 58 Marca de Sempo Reg 1 4/200 1157.49 5 4/200 1158.00 2	Método GET GET	URL http://www.urlia.com/urlia	Código	Razón 502 Bad Galeway 502 Bad Galeway	RTT 20milisejundos 15milisejundos	Tamaño requerido para el cuerpo 4220 feis 4220 feis	Alerta mayor	Nota	Eliquetas	
Buscar PB Aletas S a Ittr: APACADO C Expotur Marca de Samo Rea Marca de Samo Rea 1 4/020 1158 01 6 4/020 1158 01 6 4/020 1158 01 1188 01 1	Hda + H Mitodo GET GET GET	URL http://102.168.15.8888/app/WAPPAogn.php http://122.168.15.8888/app/WAPPAogn.php http://121.06.15.8888/app/WAPPAogn.php	Código	Razón 502 Bad Gateway 502 Bad Gateway	RTT 20milisepundos 15milisepundos	Tamaño requerido para el cuerpo 422h feis 422h feis 422h feis	Aleta may or	Nota	Eliquetas	
Buscar PA Alettas 58 Branc Ark GADO C Expositar 58 Marca de Semeo Reg 1 42020 1157.49 5 42020 1157.40 5 7 42020 1158.00 6 7 42020 1158.01 7	IIda + Método OET OET OET OET	URL Mgu 1712, 164, 15, 8880/app/WAPPAggin.pht Mgu 1712, 164, 15, 8880/app/WAPPAggin.pht Mgu 1712, 164, 15, 8880/app/WAPPAggin.pht Mgu 1712, 164, 15, 8880/app/WAPPAggin.pht	Código	Razón 502 Bas Galeway 502 Bas Galeway 502 Bas Galeway 502 Bas Galeway	RTT Zomilisejundos 15milisejundos 16milisejundos	Tamuño requerdo para el cuerpo 4220 fela 4220 fela 4220 fela 4220 fela	Alerta mayor	Nota	Eliquetas Dom Research 24	-
Buscar PB Aletas S a Iltra APACADO C Expotur Marca de tempo Res 1 4/020 1158 01 4 0/120 1158 01 4 0/120 1158 01 4 0/120 1158 01 5 4/020 1158 01	IIda + Мёйоdо СЕТ СЕТ СЕТ СЕТ СЕТ	URL Mbs / 122 168 1.5 8888/app/WAPPAgin cfb mbs //122 168 1.5 8888/app/WAPPAgin cfb	Cádigo	Racón 502 Bas Galeway 502 Bas Galeway 502 Bas Galeway 502 Bas Galeway 502 Bas Galeway	RTT 20milisegundos 15miliegundos 45miliegundos 20miliegundos 20miliegundos	Tamelo repartó para el cuerpo 422tyles 422tyles 422tyles 422tyles 422tyles	Alerta mayor	Nota	Eliquetas Elimpietas Commenta Soci	cri
Buscar P# Alettas Sis Mirca de Semo Reg 1 4/200 1157.49 5 4/200 1157.49 5 4/200 1158.00 6 4/200 1158.01 1 7 4/200 1158.01 12 4/200 1158.01 12 2 4/200 1158.06 1 <td>HGA + HARON</td> <td>URL Impuritization Impuritization</td> <td>Código</td> <td>Racén 502 Bas Gelevay 502 Bas Gelevay 502 Bas Gelevay 502 Bas Gelevay 503 Bas Gelevay 503 Geleva 503 Geleva 503 Geleva</td> <td>RTT 20millegundos 15millegundos 15millegundos 20millegundos 20millegundos 13millegundos</td> <td>Tamaño reguerdo para el cuerpo 4220 fela 4220 fela 4220 fela 4220 fela 4220 fela 4220 fela 4220 fela 4220 fela 4220 fela</td> <td>Alerta mayor Marta mayor Pi Bajo Pi Bajo</td> <td>Nota</td> <td>Eliquetas Econoce 50 Comment Comment</td> <td>cri</td>	HGA + HARON	URL Impuritization	Código	Racén 502 Bas Gelevay 502 Bas Gelevay 502 Bas Gelevay 502 Bas Gelevay 503 Bas Gelevay 503 Geleva 503 Geleva 503 Geleva	RTT 20millegundos 15millegundos 15millegundos 20millegundos 20millegundos 13millegundos	Tamaño reguerdo para el cuerpo 4220 fela 4220 fela 4220 fela 4220 fela 4220 fela 4220 fela 4220 fela 4220 fela 4220 fela	Alerta mayor Marta mayor Pi Bajo Pi Bajo	Nota	Eliquetas Econoce 50 Comment Comment	cri
Buscar Per Atetas 5 Iltra APAGADO C Expostar Marca de tempo Reg 1 4020 1155 00 6 42020 1155 01 4 4202 1158 01 8 42020 1158 01 9 42020 1158 01 12 42020 1158 01 2 42020 1158 01 23 42020 1158 08 2 42020 1158 08 23 42020 1158 08	Ida + Método GET GET GET GET GET GET	LVIII. Major L/102, 164, 1.5, 8888/insph/104.07M Augins and the strength of the strengh of the strengh of the strength of the strength of the strength	Código Vidyleshe	Reaction 502 Band Galenary 502 Band Galenary 502 Band Galenary 502 Band Galenary 200 Disk 200 Disk 200 Disk	RTT 20milisegundos 15milisegundos 16milisegundos 12milisegundos 12milisegundos 11milisegundos 11milisegundos 10milisegundos 10milisegundos	També preventés para el cuerpo 6220 (nis 6220 (nis 4220 (nis 4220 (nis 4220 (nis 420 (nis 400 (nis) 6 400 (nis) 4 3 300 (nis)	Alerta mayor P Baja P Baja P Baja	Nota	Eliquetas Econo Passonos So Comment Comment	cri
Duccar P# Aretas Sa Maca de tempo Res 1 4/20 1157.49 5 5 4/20 1153.00 6 4/20 1158.01 7.4220 1158.01 7 4/20 1158.01 7.4220 1158.01 1.52.01 15 4/20 1158.01 1.53.00 1.53.00 2 4/20 1158.01 1.53.00 1.53.00 3 4/320 1158.00 32.40320 1158.00 32.40320 1158.00	Hda 1 1	URL Mg. 2012; 163:15.8888/app.014.PPAp.gin.ptm Mg. 2012; 163:15.8888/app.014.PPAp.gin.ptm Mg. 2012; 163:15.8888/app.014.PPAp.gin.ptm	Código vity feshe ectodaug	Racón 502 Bas Galeway 502 Bas Galeway 502 Bas Galeway 200 Bas Galeway 200 Bas Galeway 200 Bas Galeway 200 Bas Galeway 200 Disk 200 Disk 200 Disk	RTT 20milise gundos 15milise gundos 12milise gundos 12milise gundos 12milise gundos 12milise gundos 10milise gundos 10milise gundos	Tamelo requerido para el cuerpo 4220 fes 4220 fes 4220 fes 4220 fes 4220 fes 4220 fes 4220 fes 4220 fes 4230 fes 43300 y fes	Alerta mayor P Bajo P Bajo P Bajo	Nota	Eliquetas Elicando Edit Comment Comment Comment	cri
Buscar Planta 5 Itte: APACADO CF Exposur Marca de tempo Reg 4000 1157.40 5 4.020 1158.00 6 4202 1158.01 9 4.020 1158.01 8 4202 1158.01 9 4.020 1158.01 8 4202 1158.01 9 4.020 1158.01 12 4202 1158.08 12 4200 1158.08 22 4300 1158.08 12 4300 1158.08 12 120 1	Ida + Método GET GET GET GET GET GET	URL Mag. 1742 1641 5 5888/https://mix.0PMagin.pdf Mag. 1712 1641 5 5888/https://mix.0PMagin.pdf Mag. 1712 1641 5 5888/https://mix.0PMagin.pdf Mag. 1712 164 5 58888/https://mix.0PMagin.pdf Mag. 1712 164 5 588888/https:	Código votyleshe wctodaug	Razón 502 Bacón 502 Bacón	RTT Shimisegundos Hamisegundos Hamisegundos 20misegundos 20misegundos Hamisegundos	Tamelo regueido para el cuerpo 127/81 4 4220/84 4 4220/84 4 4020/84 6 4020/84 6 4020/84 6 43.360/84 6	Alerta may or P Mede P Bajo P Bajo P Bajo P Bajo	Nota	Etravetas Form Passeot So Comment Comment	cri

Figure 2 – Web browsing of the local "test" host

From now on we can study the type of traffic exchanged between the browser and the local host, as well as the technologies used by the same.

For example, we can immediately observe some of the HTTP security headers used by the web server.

🔇 Editor Manual de Peticiones	—	Х
Petición Respuesta		
Encabezamiento: Vista Raw 🔽 Cuerpo:Vista Raw 🔽 🗐 🔲		
HTTP/1.1 200 OK		
Date: Wed, 04 Mar 2020 11:11:33 GMT		
Server: Apache		
Expires: Thu, 19 Nov 1981 08:52:00 GMT		
Cache-Control: no-store, no-cache, must-revalidate		
Pragma: no-cache		
Vary: Accept-Encoding		
X-XSS-Protection: 1; mode=block		
Content-Length: 4023		
Keep-Alive: timeout=5, max=99		
Connection: Keep-Alive		
Content-Type: text/html; charset=UTF-8		
1		

Figure 3 – HTTP Headers

Some of these headers (https://owasp.org/www-project-secure-headers/), such as the use of *X-XSS-Protection*, would make XSS-type attacks difficult by activating certain filters in the browser. Similarly, the *X-Content-Type-Options* header would make it possible to prevent certain types of attacks as a result of "content sniffing" carried out by the browser (http://webblaze.cs.berkeley.edu/papers/barth-caballero-song.pdf). It is recommended that





the student researches and understands the use of these headers for a better understanding of concepts related to web security. In this aspect, the OWASP (Open Web Application Security Project) is one of the best starting points for understanding the basic pillars of web security.

Continuing with the analysis of the host "test", in the information window (History tab) you can see, the type of resources requested when accessing the main URL: CSS, JavaScript, etc.

🛗 Histo	🗮 Historia 🔍 Buscar 🏴 Alertas 📄 Salida 🛨								
o 🛛 🏹	Filtro: A	PAGADO 🥐 Exportar							
ID		Marca de tiempo Req	Método	URL	Código	Razón			
	1	4/3/20 11:57:49	GET	https://192.168.1.5:8888/app/bWAPP/login.php	502	Bad Gateway			
	5	4/3/20 11:58:00	GET	https://192.168.1.5:8888/app/bWAPP/login.php	502	Bad Gateway			
	6	4/3/20 11:58:01	GET	https://192.168.1.5:8888/app/bWAPP/login.php	502	Bad Gateway			
	7	4/3/20 11:58:01	GET	https://192.168.1.5:8888/app/bWAPP/login.php	502	Bad Gateway			
	8	4/3/20 11:58:07	GET	http://192.168.1.5:8888/app/bWAPP/login.php	200	OK			
	12	4/3/20 11:58:08	GET	http://192.168.1.5:8888/app/bWAPP/stylesheets/stylesheet.css	200	OK			
	16	4/3/20 11:58:08	GET	http://192.168.1.5:8888/app/bWAPP/js/html5.js	200	OK			
	32	4/3/20 11:58:08	GET	http://192.168.1.5:8888/app/bWAPP/fonts/architectsdaughter.ttf	200	OK			
	36	4/3/20 12:00:31	POST	https://outlook.office365.com/mapi/nspi/?MailboxId=0b193407-fd64-4c8f-9634-5fe671d6c6ab@ihacklabs.com	200	OK			
	37	4/3/20 12:00:31	POST	https://outlook.office365.com/mapi/nspi/?MailboxId=0b193407-fd64-4c8f-9634-5fe671d6c6ab@ihacklabs.com	200	OK			
	40	4/3/20 12:00:31	POST	https://outlook.office365.com/mapi/emsmdb/?MailboxId=0b193407-fd64-4c8f-9634-5fe671d6c6ab@ihacklab	200	OK			
	41	4/3/20 12:00:31	POST	https://outlook.office365.com/mapi/emsmdb/?MailboxId=0b193407-fd64-4c8f-9634-5fe671d6c6ab@ihacklab	200	OK			
	42	4/3/20 12:00:32	POST	https://outlook.office365.com/mapi/emsmdb/?MailboxId=0b193407-fd64-4c8f-9634-5fe671d6c6ab@ihacklab	200	OK			
	43	4/3/20 12:00:33	POST	https://outlook.office365.com/mapi/emsmdb/?MailboxId=0b193407-fd64-4c8f-9634-5fe671d6c6ab@ihacklab	200	OK			
	44	4/3/20 12:00:33	POST	https://outlook.office365.com/mapi/emsmdb/?MailboxId=0b193407-fd64-4c8f-9634-5fe671d6c6ab@ihacklab	200	OK			
	45	4/3/20 12:00:33	POST	https://outlook.office365.com/mapi/emsmdb/?MailboxId=0b193407-fd64-4c8f-9634-5fe671d6c6ab@ihacklab	200	OK			
	46	4/3/20 12:00:35	POST	https://outlook.office365.com/mapi/nspi/?MailboxId=0b193407-fd64-4c8f-9634-5fe671d6c6ab@ihacklabs.com	200	OK			
	47	4/3/20 12:00:35	POST	https://outlook.office365.com/mapi/nspi/?MailboxId=0b193407-fd64-4c8f-9634-5fe671d6c6ab@ihacklabs.com	200	OK			
	48	4/3/20 12:00:32	POST	https://outlook.office365.com/mapi/emsmdb/?MailboxId=0b193407-fd64-4c8f-9634-5fe671d6c6ab@ihacklab	200	OK			

Figure 4 – Request log

Although most of the resources are requested via the web, we can also filter by POST methods to locate entry parameters of interest. For example, the following image shows the information submitted when using one of the web search engines. If we had the corresponding authorization to do a security audit, it would be interesting to test several payloads with these parameters (by means of the fuzzing functionality) to corroborate if they are susceptible to any vulnerability.

									_		
6\1400					Enca	ibezamiento:	Vista Raw 🔻	Cuerpo:Vista	Raw 💌 📘		
DVVAFF	DVVAPP				S Filtro histori	ial				×	-
		* 🚞 P http://192.168.1.5:8888			chimiscos Cola	uccione los fil	roe nacession	ous es musetras	abaia Puede cal	laccionar	
an extremely bugay web app	1	🔻 🚞 🏲 app			varias filas en o	cada element	o. Un elemente	o no es utilizado p	para filtrar si ningu	na de sus	
		T 🔤 🎮 DWAPP			filas es selecci	onada. </th <th>ntrni></th> <th></th> <th></th> <th></th> <th></th>	ntrni>				
		Ponts			Métodos:	Códigos:	Etiquetas	Alertas:	Incluse URL Re	egex:	
		Images			CONNEC 4	100	A Commer	nt Informa *		Ă	+ /5
Loain New User Info Talks & Training Blog		Image: Second			DELETE	101	Form	Low			
		🧾 🏴 GET:login.php			GET	200	Passwor	d Mediur			-
	Editor Manual de Peticiones	Image: Style St			HEAD	201	Script	High		•	
/ Nie w Alexand /		GET:user_new	ephp		OPTIONS	202	SetCook	je at 13	URL Exc Rege	κ.	
New User /	Peticion Respuesta	POST:user_ne	w.php(action	n,email,login,password,pa	PATCH	203		False F			
	Método 💌 Encabezamiento: Vista	-(~		POST	204		Low	1	D	
reate a new user.	POST http://102.168.1.5:8888/app	🗮 Historia 🔍 Buscar 🏼 🏴 Al	ertas S	Salida 🕂	1.75	205	7 -1 7	Mediur			
poin E-mail	Connection: keep-alive	O G Filtro: Encendido Métod	tos 🥐 Expo	rtar	Nature Trener					1	
suario email@dominio.com	Cache-Control: max-age=0	ID Marca de tiempo Reg	Método	URL	reotas ignora						50
	Origin: https://192.168.1.5:8888	36 4/3/20 12:00:31	POST	https://outlook.office3		6	ancelar	Borrar Aplic	ar		1
assword: Re-type password:	DNT: 1	37 4/3/20 12:00:31	POST	https://outlook.office3		_					
	Content-Type: application/x-www-f	40 4/3/20 12:00:31	POST	https://outlook.office3	65.com/mapi/ems	smdb/?Mailbo	xId=0b193407	fd64-4c8f-9634-	5fe671d6c6ab	200 OK	
ecret	Sec-Fetch-Dest: document	41 4/3/20 12:00:31	POST	https://outlook.office3	65.com/map/ems	mdb//Mailbo	xId=00193407	1054-4081-9534-	5fe671d6c6ab	200 OK	
misecreto	Accept: text/html,application/xht	43 4/3/20 12:00:32	POST	https://outlook.office3	65.com/mapi/ems	mdb/?Mailbo	xId=0b193407	fd64-4c8f-9634-	5fe671d6c6ab	200 OK	į.
	Sec-Fetch-Mode: navigate	44 4/3/20 12:00:33	POST	https://outlook.office3	65.com/mapi/ems	smdb/?Mailbo	xld=0b193407	-1d64-4c8f-9634-	5fe671d6c6ab	200 OK	
E-mail activation: III	Sec-Fetch-User: 71	45 4/3/20 12:00:33	POST	https://outlook.office3	65.com/mapi/ems	smdb/?Mailbo	xId=0b193407	-fd64-4c8f-9634-	5fe671d6c6ab	200 OK	6
Create	Accept-Language: es,en;q=0.9,es- Cookie: PHPSESSID=36u5v171bu1me3g	Alertas P0 P1 P7 P3 Pri 3cls1s1jv06	mary Proxy:	localhost 8080							
Please enter all the fieldel	login-usuario&email-email@dominio	.com&password=mipa≸≸w0rd&pas	sword_conf	-mipa\$\$w0rd&secret=r	nisecreto&acti	ion=create					
Flease enter an the netusi	-						-				







As we browse, we will frequently check the alert window to see if ZAP has detected any security issues. In the following image, for example, it informs us that a form without a CSRF token has been detected (<u>https://cheatsheetseries.owasp.org/cheatsheets/Cross-Site Request Forgery Prevention Cheat Sheet.html</u>). In this case, however, the alert does not represent any danger since the form is not related to the execution of potentially harmful actions or the sending of critical information.



Figure 6 – Warning about lacks of CSRF token

By carefully studying the requests intercepted by ZAP we will be able to reconstruct the technologies used by the service. We will also be able to identify the entries that are likely to be vulnerable. Remember, however, that active scanning or using any of the attack features available in ZAP requires the appropriate authorization, otherwise a crime could be committed.





2. RESEARCH EXERCISE

The objective of the exercise is to investigate the HTTP traffic used by a certain web portal and try to take advantage, if possible, of a vulnerability in one of its parameters. Because this type of testing requires prior authorization from the domain owner, a web service will be installed on a Kali instead, and the testing will be performed locally.

To proceed with the installation, download the attached bWAPP.zip file and unzip its contents into the /var/www/ directory. Then follow the instructions described in the INSTALL.txt file.

root@k	ali:	/var	/www,	/html/bl	VAPP# ls	-1			
total	19652	2							
drwxrw	xrwx	2	root	root	4096	ene	24	15:12	
drwxrw	xrwx	13	root	root	12288	ene	24	15:12	
-rwxrw	xrwx	1	root	root	5010042	nov	2	2014	bWAPP_intro.pdf
-rwxrw	xrwx	1	root	vboxsf	15058349	ene	24	15:11	bWAPP_latest.zip
-rwxrw	xrwx	1	root	root	325	mar	8	2014	ClientAccessPolicy.xml
-rwxrw	xrwx	1	root	root	200	mar	11	2014	crossdomain.xml
drwxrw	xrwx	2	root	root	4096	ene	24	15:12	
-rwxrw	xrwx	1	root	root	2589	may	12	2014	INSTALL.txt
-rwxrw	xrwx	1	root	root	2491	nov	2	2014	README.txt
-rwxrw	xrwx	1	root	root	8271	nov	2	2014	release_notes.txt
root@k	ali:	'var	-/www,	/html/bl	VAPP# less	s INS	STAL	L.txt	

Figure 7 – bWAPP deployment

After installation verify that you have access to the web platform from your browser and that it is correctly configured to use ZAP as a web proxy.

bWAPP an extremely buggy web	app !	
Login New User Info Talks & Training	Blog	
Login / Enter your credentials (bee/bug). Login: bee Password: Set the security level: low	Vertified and the security Audits & Training	WITH WITH MESSING & CHILDREN WITH MESSING CHILDREN WITH MESSING CHILDREN
Login		

Figure 8 – bWAPP login





Then authenticate yourself to the portal using your default credentials (if these have not been changed):

- Login: bee
- Password: bug

Once authenticated, choose the type of bug, "OS Command Injection" and press the Hack button.

(←) → ℃ ŵ	ⓓ	··· 🛡 🏠	
🔨 Kali Linux 🥆 Kali Training	🕆 Kali Tools 🥆 Kali Docs 🌂 Kali Forums 🌂 NetHunter 🚺 Offensive Security 🛸 Exploit-DB 🛸 GHDB 🚺 MSFU		
bW/ an extre	APP [®] emely buggy web app !	Choose your bug bWAPP v2.2v Set your security level: low v Set Current low	Hack
Bugs Change Part	seword Create User Set Security Level Reset Credito Blog Logout Velocance al / web application, is a free and open source deliberately insecure web application. thusiasts, developers and students to discover and to prevent web vulnerabilities. Imajor Known web vulnerabilities, including all risks from the OWASP Top 10 project stign and educational purposes only. want to hack today?: want to hack today?: Teact) Top Find </td <td>Bee</td> <td></td>	Bee	

Figure 9 – Challenge: OS Command Injection (I)

The user will find the following web portal where he will have to audit, using ZAP, if any of the parameters used are vulnerable. He will also have to describe the type of vulnerability found, its implications and how it would be solved. Students will not be able to use active scanning or any of the attack functions implemented in ZAP (this includes: Spider, fuzzing, predefined navigation, etc.). Only a manual approach can be used to improve their skills in using OWASP ZAP. After correctly identifying the vulnerability, students will be able to study the source code of the vulnerable script.

← → C ŵ () ▲ https://192.168.1.166/commandi.php	🛡 🏠	\ ⊡ ≡
Kali Linux Kali Training Kali Tools Kali Docs Kali Forums NetHunter MOffensive Security Exploit	-DB ≪ GHDB MMSFU Choose your bug WAPP V2.2 Set your security level low ∨ Set Current h	V Hack
Bugs Charge Password Create User Set Security Level Reset Credits / OS Command Injection / DNS lookup: www.nsa.gov Lookup	Blag Lagat Welcant Reg In In E	C

Figure 10 – Challenge: OS Command Injection (II)





Exercise solution:

If you analyze the sent request when you press the "Lookup" button, you can see that the input field (by default, the value <u>www.nsa.gov</u>) is sent via POST with the parameter target.

Sitios 🛨	🔗 Inicio Rápido 🔀 Request & Response 🛨	
0 📮 🗉 📼	Vista Raw 🔹 🔲	Encabezamiento: Vista Raw 💌 Cuerpo:Vista Raw 💌 🔲 🔲
 ▼ Contextos ■ Contextos predeterminado ♥ Sitios ▼ Phttp://192.168.1.166 ■ ♥ Etr.commandi.php ■ ♥ POST:commandi.php(form.target) 	<pre>POST http://192.168.1.166/commandi.php HTP/1.1 Usar-Apent: doxila/5.0 Ktl. Linux /86 kt. rv:60.0 Gecko/20100101 Firefox/60.0 Accept: text/html.application/html+xml_application/xml;q=0.9,*/*;q=0.8 Accept:inguage: en-USe.erg:ep-0.5 Referer: https://192.168.1.166/commandi.php Content-Type: application/xww-form_urlencoded Content-Length: 30 Cookie: PHF2SID=01pnslaphmbfmvs/luipuy11; security_level=0 Content:Type:ure-Request: 1 Host: 192.168.1.166</pre>	HTTP/1.1 200 0K Date: Wed. 20 Jan 2020 12:20:37 GMT Express Thu, J9 Nov J980 08:52:00 GMT Cache-Control: no-store. no-cache, must-revalidate Pragma: no-cache Vary: accept-Encoding Keep-Alive: timeout-5, max-100 Connection: Keep-Alive Content-Type: text/html; charset=UTF-8
		<pre> cp_align="left">Server: 1.1.1.1</pre> Address: 1.1.1.1#53 Non-authoritative answer: www.nsa.gov.edgekey.net. nsa.gov.edgekey.net.canonical name = e16248.dscb.akamaiedge.net. Name: e16248.dscb.akamaiedge.net Address: 95.100.122.124 Name: e16248.dscb.akamaiedge.net Address: 2a02.26f0:15:1:9000::3778 Name: e16248.dscb.akamaiedge.net Address: 2a02.26f0:15:1:8400::3778
		<pre><div id="side"></div></pre>
Bugs Change Password Create U	ser Set Security Level Reset Credits Blog Logout	
/ OS Command Ir	njection /	E in
Server: 1.1.1.1 Address: 1.1.1.1#53 Non-auth nsa.gov.edgekey.net canonical name = e162 Address: 95.100.122.124 Name: e16248.dscl e16248.dscb.akamaiedge.net Address: 2a02.	oritative answer: www.nsa.gov canonical name – nsa.gov.edgekey.net. 48.dscb.akamaiedge.net. Name: e16248.dscb.akamaiedge.net .akamaiedge.net Address: 2a02:26/0:15:1:9000::3/78 Name: 26/0:15:1:8400::3/78	

Figure 11 – POST Request

Note that the result returned by the server matches the output generated by the **nslookup** command:



Figure 12 – nslookup output seems similar to server config

Everything seems to indicate that the web server is using the value sent by the target parameter to run it in the console and return the generated output. What would happen if instead of sending the domain we add a second command in the input? For example, the command: ;ls

To modify this argument on the fly, we will use the break points described in the course, with which we can "stop" the web request before it is sent to the web service.

GOBIERNO DE ESPAÑA VICEPRESIC TRECERA I UNIVETERE DE ASUMUT VTRANSFO	DEL GOBIERNO DEL GOBIERNO OS ECONOMICOS OS ECONOMICOS DE DIGITALIZA E INTELIGENCI	E ESTADO ICIÓN A ARTIFICIAL	\$in ci	be_	TU AYUDA EN CIBERSEGURIDAD
 http://192.168.1.166 P GCT.commandi.phpform.target) P ADT.commandi.phpform.target) P ap images P ap images P CCT.login.php P stylesheets 	target-sev.nsa.goviform-submit Atara Incluir en contexto Marara como un contexto Ejecutar aplicación Excluir del contexto seleccionado Excluir del contexto seleccionado Open URL in tronser Mostrar en la pagina de historial Ver en el navegador Copie las URL al portapables Eliminar Administrar Tag Exportar Todas las URLs a un fichero Exportar Todas las URLs a un fichero	Suprimir	Añadir punto de interrupción oblicación: URL iartido: Regex integui 92.168.1166/cor morar caso: 2 2 2 2 2 2 2 2 2 2 2 2	Content-Type: text/htm Break Point) wmmandi.php Guardar Cancelar div id="side">	ml: charset=UTF-8 erver: 1.1.1.1 wrr: Baanae = nna.gov:edgekey.net. gaanaidge.net 24 Jaanaidge.net 1:9400:13778 .akamaidge.net

Figure 13 – Breakpoint

After creating the breakpoint we'll click on the "Lookup" button again and replace the content of the "target" parameter with the following string:

Sillos T	🦻 Inicio Rapido 🛛 🔀 Request & Response 🛛 💥 Punto de interrupción 🛛 🛨
© , C .	Método 🝸 Encabezamiento: Vista Raw 🝸 Cuerpo:Vista Raw 💌 📄 📄
▼ ○ Contextos P ■ Contexto predeterminado Ht ₩ Sitos ₩ Sitos ₩ Nitos ₩ P <td< td=""><td>PQST http://102.168.1.166/commandi.php HTTP/1.1 http://102.168.1.166/commandi.php HTTP/1.1 http://102.168.1.166/commandi.php HTTP/1.1 kccept.text/html.maplication/xhtml.mml.application/xml:q=0.9.*/*:q=0.8 kccept.text/html.application/x-hum.form.urlencoded Content-Length.ig Content-Length.ig Content-Length.ig Content-Length.ig Content-Length.ig Content-Length.ig Content-Length.ig Content-Length.ig Content-Length.ig Content-Length.ig Content-Length.ig Content-Length.ig Content-Length.ig Content-Length.ig Content-Length.ig Content-Length.ig Content-Length.ig ContentLength.ig Conte</td></td<>	PQST http://102.168.1.166/commandi.php HTTP/1.1 http://102.168.1.166/commandi.php HTTP/1.1 http://102.168.1.166/commandi.php HTTP/1.1 kccept.text/html.maplication/xhtml.mml.application/xml:q=0.9.*/*:q=0.8 kccept.text/html.application/x-hum.form.urlencoded Content-Length.ig Content-Length.ig Content-Length.ig Content-Length.ig Content-Length.ig Content-Length.ig Content-Length.ig Content-Length.ig Content-Length.ig Content-Length.ig Content-Length.ig Content-Length.ig Content-Length.ig Content-Length.ig Content-Length.ig Content-Length.ig Content-Length.ig ContentLength.ig Conte

Figure 14 – Modification of the target parameter

Note that this would execute the command: nslookup www.nsa.gov;ls (in Linux the ';' character allows concatenation of several commands). After forwarding the request to the destination, we can see that we have indeed managed to recover the list of files on the server, which would confirm the type of vulnerability.

	bWAPP - OS Command Injection - Mozilla Firefox						
Analizar Reporte Herramientas Import En línea Ayuda	💈 Búsquedas INCIBE 🗴 🍃 Línea de Ayuda en Cil 🗴 🍃 Contacto INCIBE 🛛 🛪 😺 bWAPP - OS Comma 🗙 🔅 Preferences						
🔗 Inicio Rápido 🛛 🛱 Request & Response 🗋 💥 Punto de interrupción 🗍 🛨							
Vista Raw 🔻 😑 🔚 Encabezamiento: Vista Raw 💌 Cuerpo:Vista Raw 💌	🕆 Kali Linux 🥆 Kali Training 🥆 Kali Tools 🌂 Kali Docs 🌂 Kali Forums 🌂 NetHunter 👖 Offensive Security 🛸 Exploit-DB 🛸 GH						
POST HTTP/L1 200 0K http://192.168.1.166/com Date: Wed. 29 Jan 2020 12:48:47 GMT mandi.php HTTP/L1 Server: Apache/2.4.41 (Debian) User-Agent: Norlla/S.0 Expres: Thu. 19 Nov 1981 08:52:00 GMT [X11]: Linux X86_641 // VI Cache-Control: no-store. no-cache. must-revalidate pireforx/00 Mayris Accept-Encoding Accept: text/html. Keep-Alive: timeout-5, max-100 application/Mail:q0-9, V Content-Lengts: I6631	Choose your bug WWAPP V2.2						
Accept:Language: en.US, enr,q=0.5 Referer: https://192.168.1.166/c0 Moress: 1.1.1.1853 Address: 1.1.1.1853 Address: 0.1.1.1.853 Moress: 0.1.1.1.1853 Moress: 0.1.1853 Moress: 0.1.11,11,1853 Moress: 0.1.1853 Moress: 0.1.11,11,11,11,11,11,11,11,11,11,11,11,1	Bugs Change Password Create User Set Security Level Reset Credits Blog						
Habilitado Tipo	information_disclosure_1.php information_disclosure_2.php information_disclosure_3.php						









With this information we can answer the following questions:

2.1. What type of vulnerability has been identified?

The vulnerability corresponds to a command injection: as described by OWASP (<u>https://owasp.org/www-community/attacks/Command_Injection</u>), this type of attack:

"is possible when an application passes insecure data provided by the user (forms, cookies, HTTP headers, etc.) to a system shell. In this attack, the operating system commands provided by the attacker are usually executed with the privileges of the vulnerable application. Command injection attacks are possible largely due to insufficient input validation".

If we access the web directory and open the script *commandi.php* we can corroborate that the script is invoking the *nslookup* command through the insecure function *shell_exec* (<u>https://www.php.net/manual/es/function.shell-exec.php</u>) without applying any kind of validation or filter to the target parameter.

	<label for="target">DNS lookup:</label> <input id="target" name="form" submit"="" type="text" value="submit"/> Lookup
	form> php
if {	(isset(\$_POST ["target"]))
	<pre>\$target = \$_POST["target"];</pre>
	<pre>if(starget == "") {</pre>
	echo " Enter a domain name ";
	else
	<pre>echo "" . shell_exec("nslookup " . commandi(\$target)) . "";</pre>
}	
?>	
<div i<="" th=""><th>d="side"></th></div>	d="side">
<a <a <a< th=""><th><pre>href="http://twitter.com/MME_IT" target="blank_" class="button"> href="http://be.linkedin.com/in/malikmesellem" target="blank_" class="button"> href="http://www.facebook.com/pages/MME-IT-Audits-Security/104153019664077" target="blank_" class="button"></pre></th></a<></a </a 	<pre>href="http://twitter.com/MME_IT" target="blank_" class="button"> href="http://be.linkedin.com/in/malikmesellem" target="blank_" class="button"> href="http://www.facebook.com/pages/MME-IT-Audits-Security/104153019664077" target="blank_" class="button"></pre>

Figure 16 – Source code (commandi.php)

2.2. What kind of implications does it have?

An attacker could execute all sorts of commands and thus completely compromise the web server. For example, if instead of executing an "Is" the attacker had executed "*nc -I -p 2222 -c /bin/bash*" he would install a bind shell as a backdoor.



Figure 17 – Bind shell with netcat

2.3. How would you address the vulnerability?

We recommend using the guidelines described by the OWAS project (<u>https://cheatsheetseries.owasp.org/cheatsheets/OS Command Injection Defens</u> <u>e Cheat Sheet.html</u>).

These countermeasures are summarized in:

- Avoid directly invoking commands.
- Escape and filter the values provided to the commands.
- Parameterization along with proper validation of input parameters.







3. ADDITIONAL EXERCISE

Taking advantage of the installation of the local web service used in the previous research section, in this exercise users will learn how to add new dictionaries to ZAP for the discovery of new web resources.

A repository of special interest for this exercise is the project at Github Fuzzdb since it gathers many dictionaries within the *predictable-filepaths* directory (<u>https://github.com/fuzzdb-project/fuzzdb/tree/master/discovery/predictable-filepaths</u>) for many web technologies; for example, for CMS (Drupal, Joomla, WordPress, etc.), login files commonly used for different platforms, etc.

If we want to make use of these dictionaries we can either download them manually from Github or clone the whole repository locally.



Figure 18 – Downloading dictionaries

Later, if we want to add some of these dictionaries to ZAP, to be able to be used with the functionality "Predefined navigation", we will go to the menu "Tools -> Options" and later we will select the dictionary that we want (in the following image the raft-large-directories.txt dictionary has been selected). Note that from this menu we can also configure if we want to include file navigation, the extensions we want to include and other performance related parameters, for example, the number of threads to use. If we want to integrate more dictionaries we will repeat the same process.

Sitios 🛉	🐓 Inicio Rápido 🛛 🗯 Request & Response 🕺 Pr	unto de interrupción 🖉	* +			
Contexts Contexts Contexts Portage Portage	dre Strección de llamadas de regreso Escaneo Activo Escaneo Pativo Estadisticas Estadisticas Estadisticas Estadisticas Estadistes Estadistes Estadistes Guzer Glubal Ader Filtern.	Navegación Pred Número de hilos (t 0 20 M Recursiva: Archivo por defect Agregar archivo pa	opiciones efinida residu concurrentes por sitio: 40 60 80 100 2: ra Navegación Predefinida: por de surbisor	120 140 160 1 raft-large-directories-lowercase.txt Seleccione el archivo	80 200	
	HUD Linguage Mostrar Newspackn Preddmida Proxes locales Proxes locales Proxes locales Auto Sea Launch Register Replacer	Extensiones de arc File extensions to i Fail Case String:	Buscar en: filename-dirname-brutet 3CharExtBrute.txt CommonWebExtensions.txt Copy_of.txt Extensions.Backup.txt Extensions.Common.txt	Abrir force Extensions.Compressed.txt Extensions.Mostcommon.txt Extensions.Skipfih.txt raft-large-directories.txt raft-large-directories.txt	Cafe Cafe Cafe Cafe Cafe Cafe Cafe Cafe	NO] Número de peticiones:1617 🖗 Exportar
	seemium Seziones de la HTTP Spider(Arana) Tectado Tokensı anti CSRF Vectors de entrada del Escaner Activo WebSockets Zest	<i>,</i>	Nombre de archivo: raft-large-directorio Archivos de tipo: Navegación Predel	es.txt Inida Abrir C	3 ×	e se re Tamaño requerido para el cuerpo Obytes 5.152bytes 943bytes 278bytes 60.190bytes
	WebSockets Zest				Abrir	Abrir. Cancelar

Figure 19 – Adding new dictionaries





Once the dictionaries are added, we will select the resource from which we want to discover new directories and, by right clicking, we will select the option "Defined navigation directory" within the Attack menu. Notice that in the lower window the previously added dictionaries will appear and we will be able to select any of them.

► 💭 https://192.168.1.166:80	🗮 Historia 🔍 Buscar	👎 Alertas 📄 Salida	a 🎤 Navegación Pre	definida 🖈 🛎 🖣	Þ	_			
Mathematical Science (192,168,1,166) Mathematical Science (192,168,1,166)	Sitio: 192.168.1.166:80	💌 Lista:	raft-large-directories.t	txt 🔽	▶ 00 🖬 📕	4 %		Escaneo actual:1 Número de peticiones:2908	^a Exportar
	Marca de tiempo Req	Marca de tiempo de R	a ha	and the second second		Código	Razón	Tamaño que se requiere para el encabezamiento	Tamaño requerido para el cue
	29/1/20 16:35:38	29/1/20 16:35:38	rait-large-directories-	lowercase.cxc	.166:80/admin/	200	OK	173bytes	3.160bytes
	29/1/20 16:35:38	29/1/20 16:35:38	rait-large-uirectories.		1.166:80/images/	200	OK	172bytes	5.152bytes
	29/1/20 16:35:38	29/1/20 16:35:38	directory-list-1.0.txt		.166:80/	302	Found	172bytes	Obytes
	29/1/20 16:35:38	29/1/20 16:35:38	GET	http://192.168.1	1.166:80/js/	200	OK	172bytes	1.554bytes
	29/1/20 16:35:38	29/1/20 16:35:38	GET	http://192.168.1	1.166:80/logs/	200	OK	171bytes	940bytes
	29/1/20 16:35:38	29/1/20 16:35:38	GET	http://192.168.1	1.166:80/db/	200	OK	171bytes	939bytes
	29/1/20 16:35:39	29/1/20 16:35:39	GET	http://192.168.1	1.166:80/javascript/	403	Forbidden	161bytes	278bytes
	29/1/20 16:35:39	29/1/20 16:35:39	GET	http://192.168.1	1.166:80/js/html5.js	200	OK	266bytes	2.394bytes
	29/1/20 16:35:39	29/1/20 16:35:39	GET	http://192.168.1	1.166:80/documents/	200	OK	172bytes	2.310bytes
	29/1/20 16:35:39	29/1/20 16:35:39	GET	http://192.168.1	1.166:80/js/jquery-1.4.4.min.js	200	OK	269bytes	78.601bytes
	29/1/20 16:35:39	29/1/20 16:35:39	GET	http://192.168.1	1.166:80/apps/	200	OK	171bytes	943bytes
	29/1/20 16:35:39	29/1/20 16:35:39	GET	http://192.168.1	1.166:80/fonts/	200	OK	172bytes	2.591bytes
	29/1/20 16:35:39	29/1/20 16:35:39	GET	http://192.168.1	1.166:80/js/json2.js	200	OK	268bytes	17.347bytes
	29/1/20 16:35:39	29/1/20 16:35:39	GET	http://192.168.1	1.166:80/logs/visitors.txt	200	OK	253bytes	310bytes
	29/1/20 16:35:39	29/1/20 16:35:39	GET	http://192.168.1	1.166:80/js/xss_ajax_1.js	200	OK	266bytes	2.887bytes
	29/1/20 16:35:39	29/1/20 16:35:39	GET	http://192.168.1	1.166:80/icons/	403	Forbidden	161bytes	278bytes
	29/1/20 16:35:39	29/1/20 16:35:39	GET	http://192.168.1	1.166:80/icons/	403	Forbidden	161bytes	278bytes

Figure 20 – Adding new dictionaries

As detailed in the webinar, the discovery of directories and files through the "Predefined Navigation" functionality is very useful for identifying unreferenced resources. Sometimes, these resources allow us to access directories that, by mistake or carelessness, have been made public and that offer information about the platform, technologies used or any other type of sensitive data about the configuration of the web service. The following image shows one of the configuration files identified thanks to one of the dictionaries; the file "config.inc" located in the root directory. Note that it includes access credentials to a certain database.

😡 Sitios 🛨		🗲 Inicio Rápido 🛛 🗮 Request & Response	•						
	Vi	sta Raw 💌 📃 🔲		Encabezamiento: Vista Raw 💌 Cuerpo:Vista Raw 💌					
T Contextos Contexto predeterminado C Contexto predeterminado P Sitio Pige https://fonts.gstatic.com Pige https://www.gstatic.com Pige https://www.goojb.com Pige https://wwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwww	Acc Acc Coc Upg Hos	http://192.168.1.166/config.inc HTT r-Agent: Mozila/5.0 (X1): Linux x86 ept: text/httl.application/xhttl+x91 ept-Language: en-US.en;q=0.5 Kie: MP#SESD=riilqbi4ctgb49htft9uv nection: keep-alive rade-Insecure-Requests: 1 t: 192.168.1.166	P/1.1 _64; nv:60.0) Gecko/20100101 Firefox/60.0 _application/xml:q=0.9.*/*;q=0.8 tlrgn	MTTP/1.1.200.0K Dote: Wel. J2: an 2020 15:18:54 CMT Server: Apache/2.4.41 (Debian) Last-Modified Thu. 01 Ray 2014 09:11:54 CMT ETag: J30c-4F35bff31a80° Accept:Ranges: bytes Content-Length: 780 Memp-Alive: timeott5, nax=100					
 Fintps://googleads.g.doubleclick.net Fintps://googleads.g.doubleclick.net 				Mozilla Firefox			0.0	0	
► ► ► ► ► ► ► ► ► ► ► ► ► ► ► ► ►		192.168.1.166/config.inc × +		P102108 F 11 ET0X				_	
• GET confin inc		w	0 nttps://192.108.1.106/config.inc		8	V W	III\ (L)	=	
▼ ■ R → http://192.168.1.166		🔨 Kali Linux 🌂 Kali Training 🌂	Kali Tools 🌂 Kali Docs 🌂 Kali Forums 🌂 NetHu	nter 👖 Offensive Security 🌭 Exploit-DB 🛸 GHDB	MSFU				
GET:admin		php</td <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td>nse (</td>							nse (
apps		/*							
📋 者 GET:apps									
📑 🏁 GET:config.inc		It helps security enthusiasts, dev	, is a free and open source deliberately insecure velopers and students to discover and to prevent w	web application. web vulnerabilities.					
► 🛄 db		bwAPP covers all major known web w	vulnerabilities, including all risks from the OWAS	SP Top 10 project!					
🗋 🎤 GET:db		It is for security-testing and edu	carconac purposes oncy.						
documents		Enjoy!							
GET:documents		Malik Mesellem							
Ponts		Twitter: @MME_IT							
GET:fonts	CIPL	bWAPP is licensed under a Creative	e Commons Attribution-NonCommercial-NoDerivatives	4.0 International License (http://creativecommons.or	rg/licenses	s/by-nc-nd/4.0/). Copy	right © 2014 MME	BVBA.	
GETHCONS	310	All rights reserved.							
∠ GET:Images	29 Mi	n +/							para el cuerpo
GET-invacation	29	// Connection settings	1						
GET-is	29	<pre>/l \$server = "localhost";</pre>							
E B B B	29	<pre>\$password = "loveZombies";</pre>							_
GET:login.php	25	\$database = "bWAPP_BAK";							
▶ iii login.php	29	/1 7>	-						
GET:logs	29								
► 🔛 logs	29	/1/20 10:42:11 29/1/20 10:42:11	OE1 N(tp://192.108.1.106:80/doct	uments/DWAPP in 200 OK 242Dytes			/.418.2280	vies	

Figure 21 – Identification of the configuration file "config.inc"