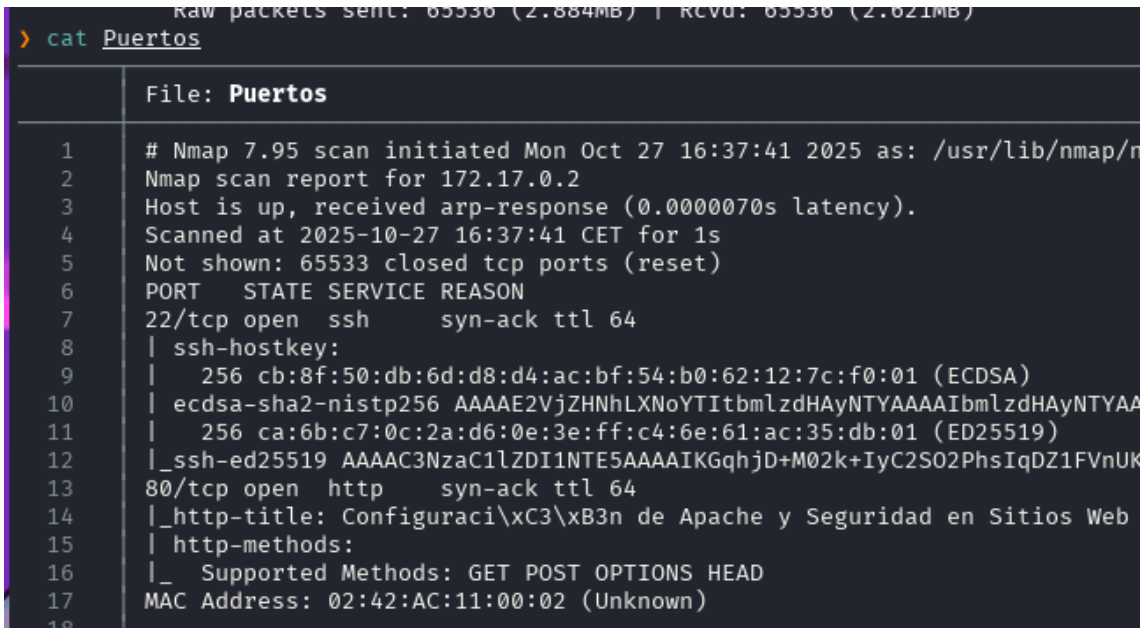
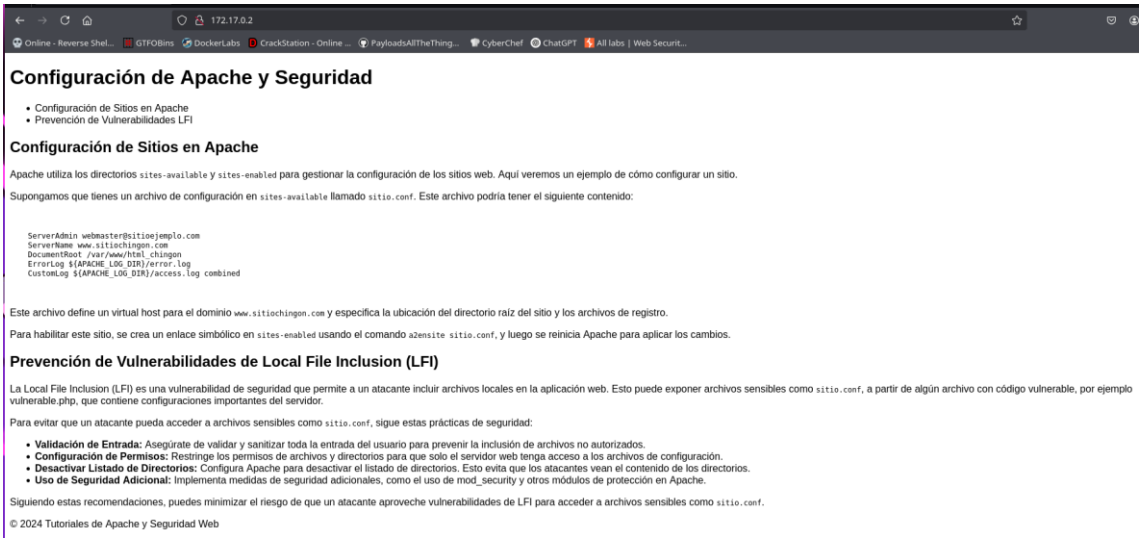
Vamos a desplegar la maquina vulnerable.

Haremos un escaneo profundo de los puertos abiertos del servidor.



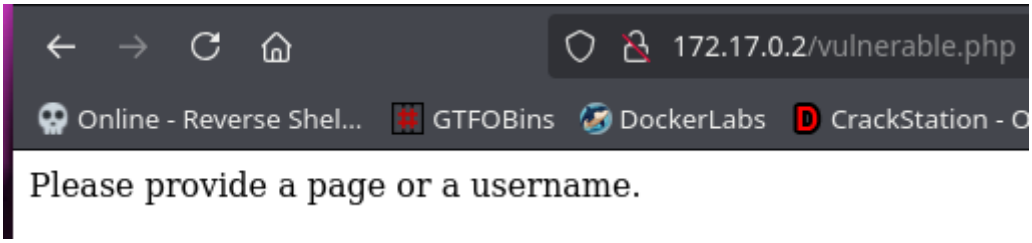
Vemos que tiene el servicio http, así que exploraremos la página.

Tenemos que quedarnos con **sites-available** y **sitio.conf**



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

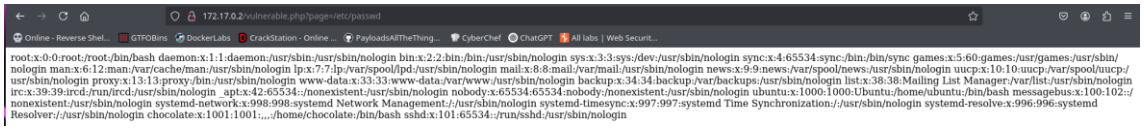
Encontraremos un fichero vulnerable.php



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

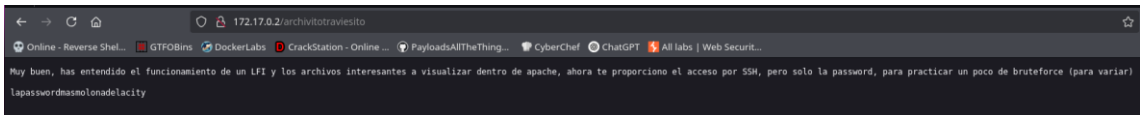
Una vez lo tenemos, aplicamos los filtros.

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

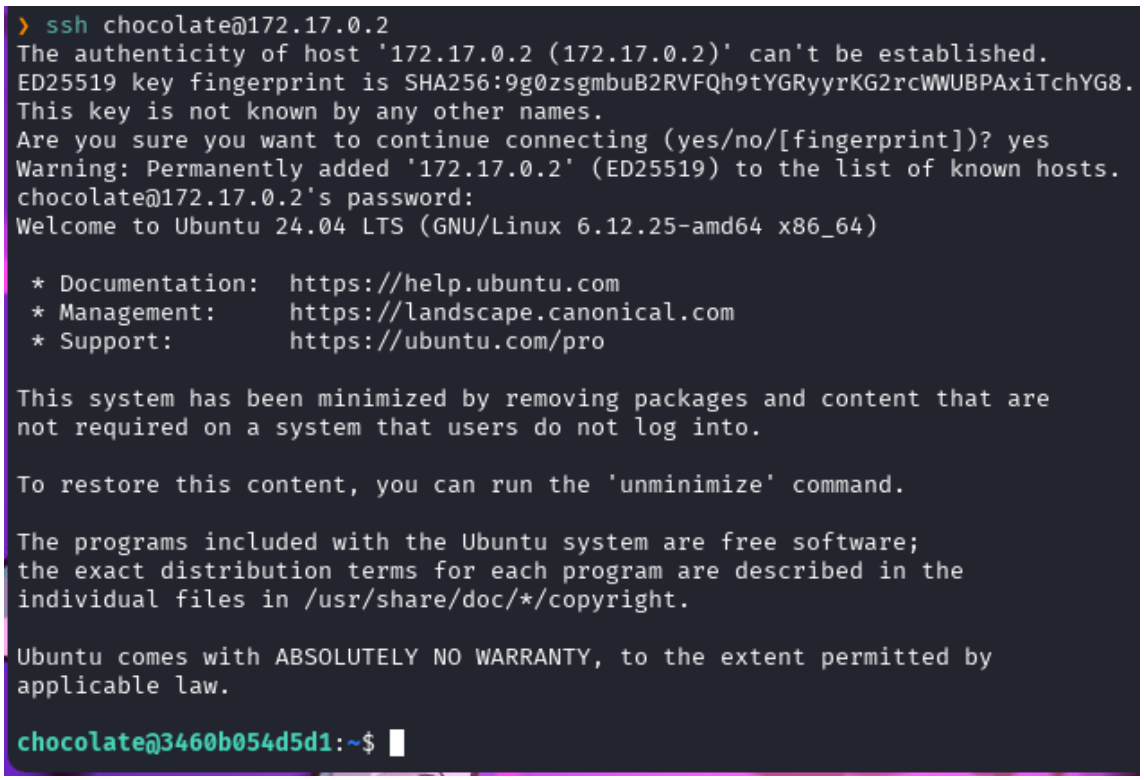


Exploramos la ruta que antes nos indicaba la página índex.

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



Nos conectamos por ssh al usuario.



Con sudo -l vemos que tenemos el binario sed. Asi 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 '1e exec sh 1>&0' /etc/hosts
```

Ejecutamos el comando y vemos que ahora somos root.