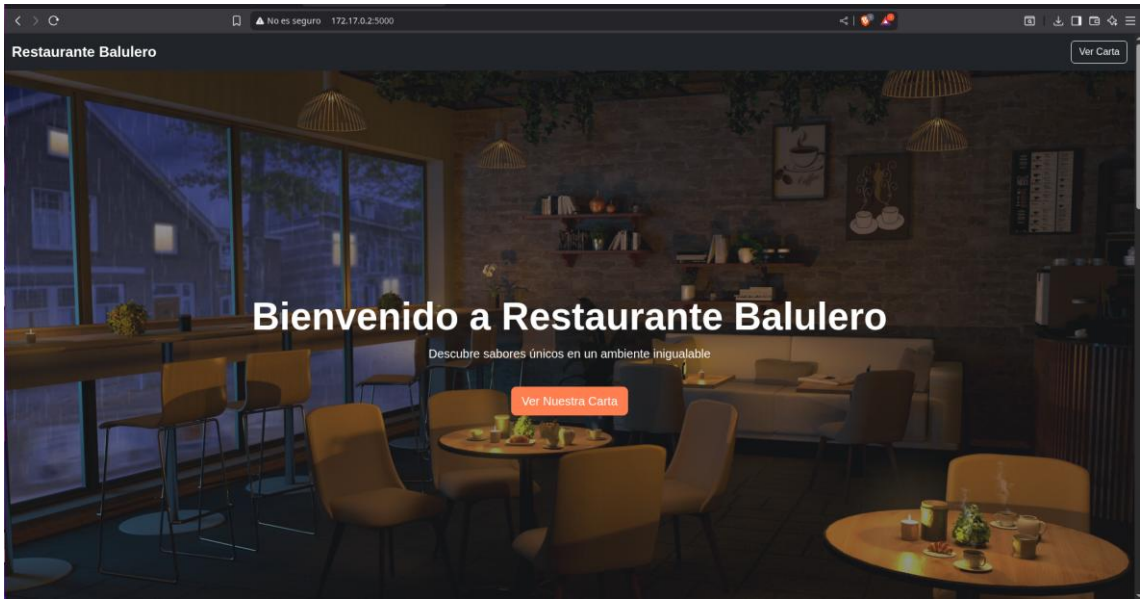
Vamos a desplegar la máquina.

Ahora vamos a hacer un escaneo profundo de los puertos abiertos.

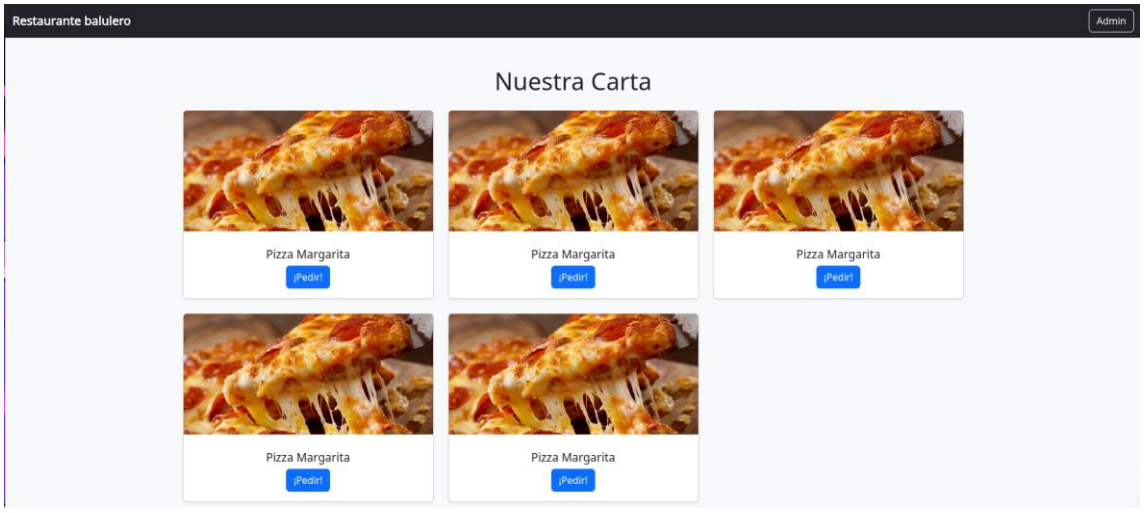
Vemos que cuenta con un puerto 5000, hacemos un escaneo especifico a ese puerto para ver que contiene.

```
❯ nmap -p5000 -sCV -Pn 172.17.0.2
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-08 16:43 CEST
Nmap scan report for 172.17.0.2
Host is up (0.000035s latency).

PORT     STATE SERVICE VERSION
5000/tcp open  http    Werkzeug httpd 2.2.2 (Python 3.11.2)
|_http-title: Restaurante Balulero - Inicio
|_http-server-header: Werkzeug/2.2.2 Python/3.11.2
MAC Address: 02:42:AC:11:00:02 (Unknown)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.41 seconds
```

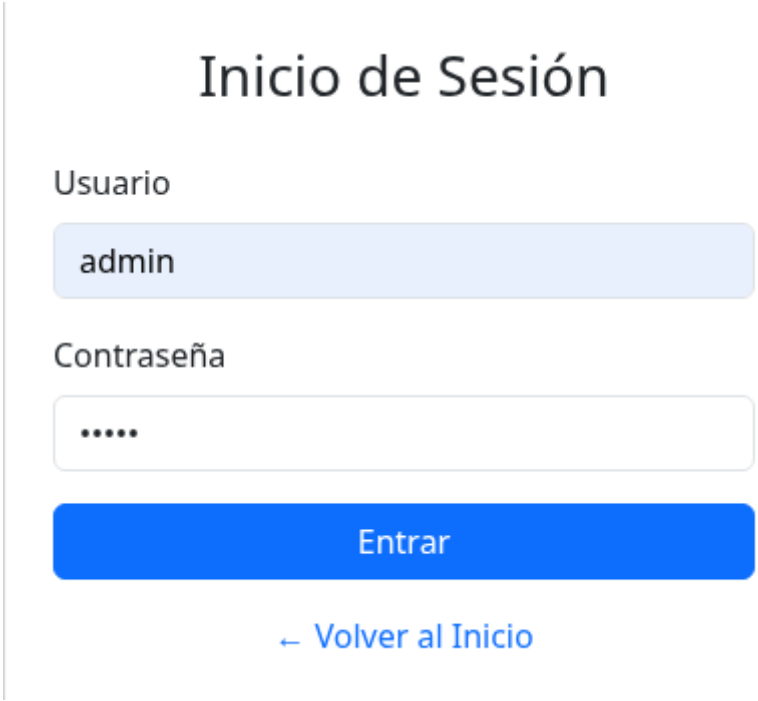
Vemos que es un servidor http, así que vamos a explorar un poco a ver que nos encontramos.



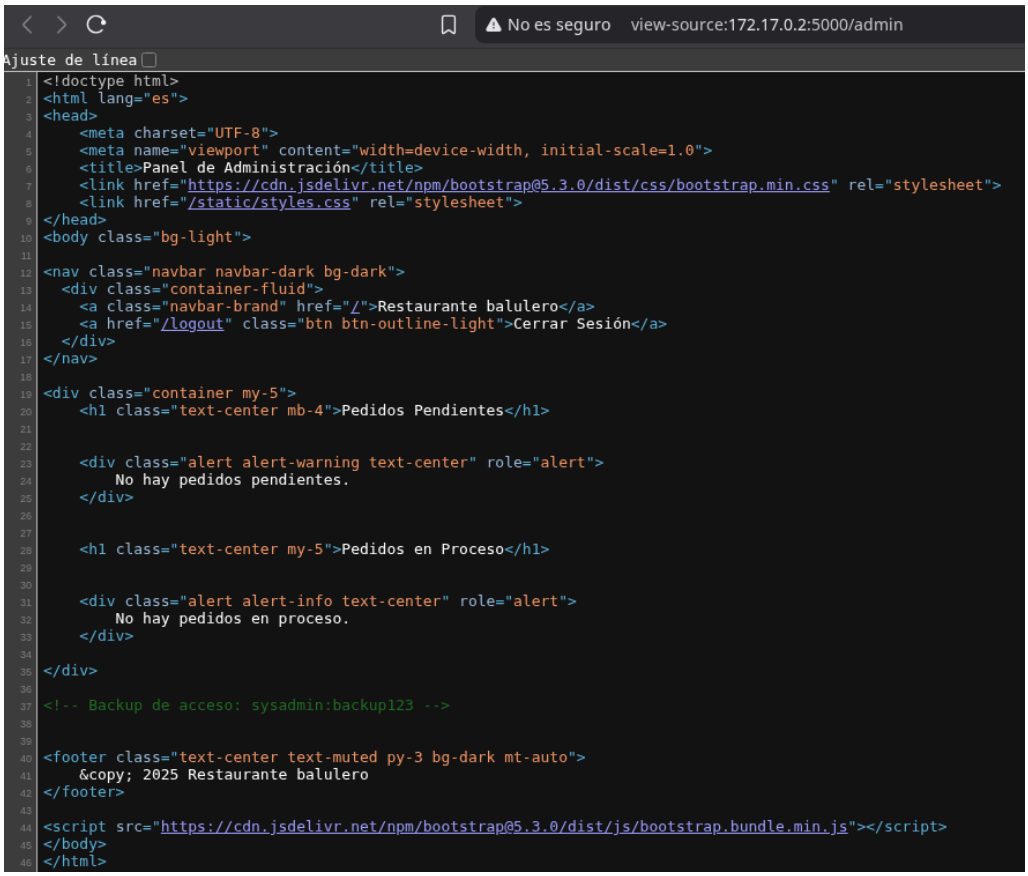
Vemos que hay un botón que pone admin.



Hay un panel para iniciar sesión, como tenemos login admin por predeterminado vamos a intentar con la contraseña admin por probar.



Ahora dentro nos encontramos con un panel, si inspeccionamos la pagina encontraremos un comentario donde nos pone un usuario y su contraseña que intentaremos conectar por ssh.



```
❯ ssh sysadmin@172.17.0.2
The authenticity of host '172.17.0.2 (172.17.0.2)' can't be established.
ED25519 key fingerprint is SHA256:ZcJw57pSEVAGdPKcg6E5FVaWh/s1IMKnuLnTky7h3xQ.
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.
sysadmin@172.17.0.2's password:
Linux 81c7b5c8e31d 6.12.25-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.12.25-1kali1 (2025-04-30) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Mon Sep  8 14:22:01 2025 from 172.17.0.1
sysadmin@81c7b5c8e31d:~$
```

Ahora vamos a ver un poco dentro de este usuario a ver que encontramos.

```
sysadmin@81c7b5c8e31d:~$ ls -la
total 56
drwx——r-- 1 sysadmin sysadmin  4096 Apr 29 12:59 .
drwxr-xr-x 1 root     root      4096 Apr 29 12:56 ..
-rw——————— 1 sysadmin sysadmin   151 Sep  8 14:40 .bash_history
-rw-r--r-- 1 sysadmin sysadmin   220 Apr 29 12:51 .bash_logout
-rw-r--r-- 1 sysadmin sysadmin  3526 Apr 29 12:51 .bashrc
-rw-r--r-- 1 sysadmin sysadmin   807 Apr 29 12:51 .profile
-rw-r--r-- 1 root     root      3809 Apr 29 12:59 app.py
-rw-r--r-- 1 root     root     12288 Apr 29 12:45 restaurant.db
drwxr-xr-x 3 root     root      4096 Apr 28 18:55 static
drwxr-xr-x 2 root     root      4096 Apr 29 13:00 templates
sysadmin@81c7b5c8e31d:~$
```

Encontramos un script que vamos a ver que contiene, vemos una contraseña, así que vamos a ver que usuarios tiene este servidor y ver si pertenece alguien.

```
  edidossysadmin@81c7b5c8e31d:~$ cat app.py
from flask import Flask, render_template, redirect, url_for, request, session, flash
import sqlite3
from functools import wraps

app = Flask(__name__)
app.secret_key = 'cuidaditocuidadin'
DATABASE = 'restaurant.db'

def get_db_connection():
    conn = sqlite3.connect(DATABASE)
    conn.row_factory = sqlite3.Row
    return conn
```

```
sysadmin@81c7b5c8e31d:~$ ls /home/
balulero  sysadmin
```

Nos conectamos y vemos que pertenece a ese usuario, nuevamente vamos a explorar un poco para ver si encontramos algo.

```
sysadmin@81c7b5c8e31d:~$ su balulero
Password:
balulero@81c7b5c8e31d:/home/sysadmin$ cd
balulero@81c7b5c8e31d:~$ ls -la
total 36
drwx------ 1 balulero balulero 4096 Apr 29 12:58 .
drwxr-xr-x 1 root     root     4096 Apr 29 12:56 ..
-rw------- 1 balulero balulero  351 Sep  8 14:40 .bash_history
-rw-r--r-- 1 balulero balulero  220 Apr 29 12:55 .bash_logout
-rw-r--r-- 1 balulero balulero 3572 Apr 29 12:58 .bashrc
drwxr-xr-x 3 balulero balulero 4096 Apr 29 12:57 .local
-rw-r--r-- 1 balulero balulero  807 Apr 29 12:55 .profile
```

Al ver que contiene el fichero .bashrc

```
alias ser-root='echo chocolate2 | su - root'
```

Ahora somos root.

```
root@81c7b5c8e31d:~# whoami
root
```