WRITEUP - LA CASA DE L'INJECTION.

- **Category**: Web
- **Level:** : Medium

Description: Le professeur est attarpé par la police d'Espagne, et il a besoin de toi pour trouver deux document sur leur système privé. Ces documens contient le flag qui va innocenter le Professor. Tu vas travailler avec l'equipe de Casa del Papel pour ca.

Step 1 : Download the docker image

- The docker images is available on my docker hub.

```
Link : https://hub.docker.com/repositories/razafindraibe
```

```
sudo docker pull razafindraibe/la_casa_de_injection:latest
```

- Run the container :

```
sudo docker run -d -p 8080:5000 -p 21:21 -p 21100-21110:21100-21110
razafindraibe/la_casa_de_injection:latest
```

```
┌──(malaso㉿kali)-[~]
└─$ sudo docker run -d --name casadelpapel2 -p 8080:5000 -p 21:21 -p 21100-21110:21100-21110 razafindraibe/la_casa_de_injection
dc027061c925dbbac74a17fd53afbc7e1c8e7c1ec71e1c4ca0607d65cd0ef9d3
```

Step 2 : Reconnaissance

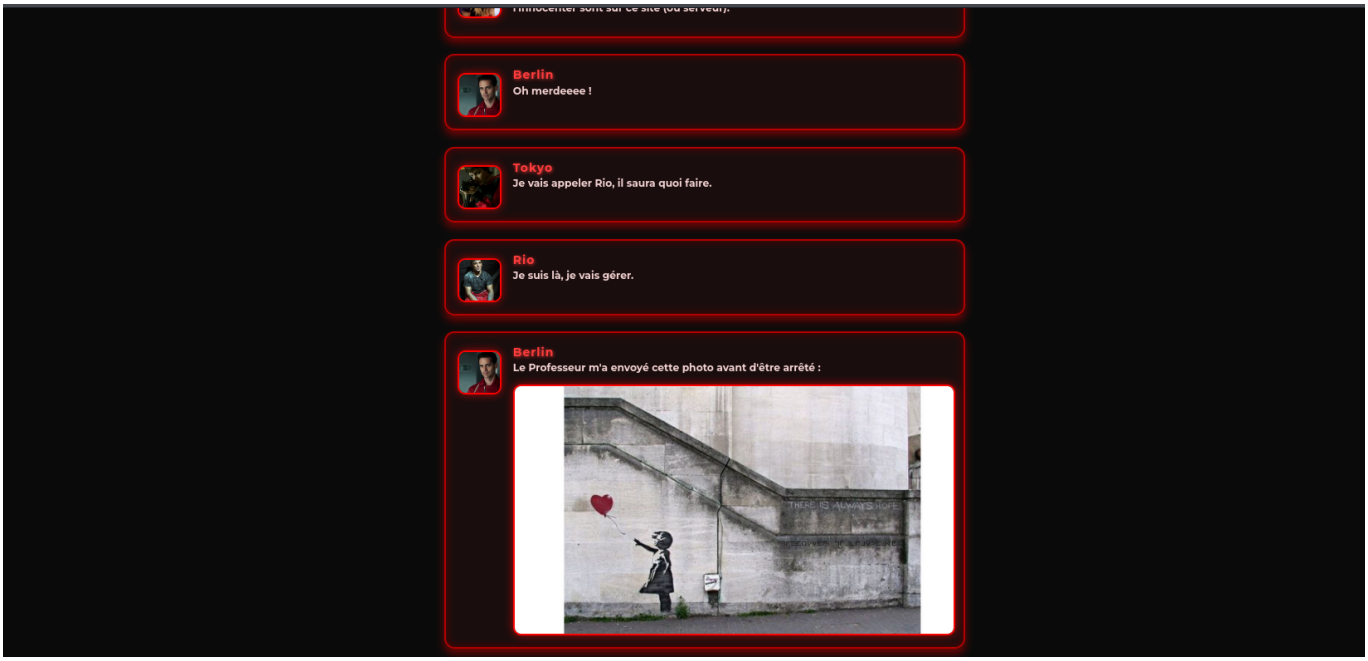
1 - Let's start with a simple IP scan using : nmap

```
┌──(malaso㉿kali)-[~]
└─$ sudo nmap -sC -sV -Pn 127.0.0.1
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-18 16:32 +01
Nmap scan report for localhost (127.0.0.1)
Host is up (0.0000030s latency).
Not shown: 998 closed tcp ports (reset)
PORT     STATE SERVICE VERSION
21/tcp   open  ftp     vsftpd 3.0.5
8080/tcp open  http    Werkzeug httpd 3.1.3 (Python 3.10.12)
|_http-server-header: Werkzeug/3.1.3 Python/3.10.12
|_http-title: Blog Interne \xE2\x80\x93 Casa de Papel
Service Info: OS: Unix
```

---

2 - Let's access the site :

```
http://localhost:8080
```



We accessed the blog of the group.

El Profesor sent a photo to **Berlin** before his arrest.

Hmmm... it seems to be about steganography.

3- Download the photo

Just click on it and it will be downloaded.

- Hint : Pigpen Cipher

Good job! We have credentials, either for FTP or for a login.

---

4 - Let's try to connect by ftp on port 21

```
ftp 127.0.0.1
```

- username: professor
- password: graciastokyo

```
┌──(malaso㉿kali)-[~]
└─$ ftp 127.0.0.1
Connected to 127.0.0.1.
220 (vsFTPd 3.0.5)
Name (127.0.0.1:malaso): professor
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

```
get document1.txt
```

```
ftp> ls
229 Entering Extended Passive Mode (|||21109|)
150 Here comes the directory listing.
-rwxr-xr-x    1 1000     1000           21 Aug 18 00:51 document1.txt
226 Directory send OK.
ftp> get document1.txt
local: document1.txt remote: document1.txt
229 Entering Extended Passive Mode (|||21108|)
150 Opening BINARY mode data connection for document1.txt (21 bytes).
100% |*****************************************************************************************************************************************************************
226 Transfer complete.
```

Bravo !! We got the first document

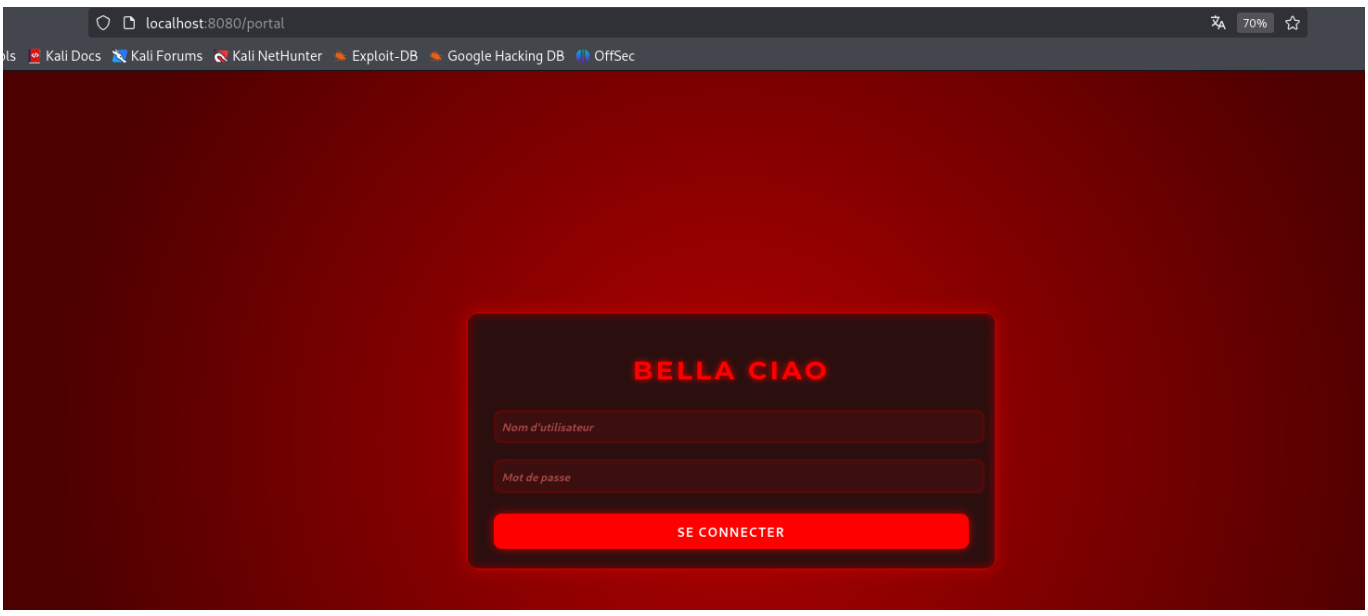
```
┌──(malaso㉿kali)-[~]
└─$ cat document1.txt
flag{[redacted]
```

Step 3 : Search the second document !

Let's continue our exploration with gobuster

```
┌──(malaso㉿kali)-[~]
└─$ gobuster dir -u http://127.0.0.1:8080 --wordlist /usr/share/wordlists/dirb/common.txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://127.0.0.1:8080
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/portal               (Status: 200) [Size: 2861]
Progress: 4614 / 4615 (99.98%)
===============================================================
Finished
===============================================================
```

We have */portal* . It seems important.

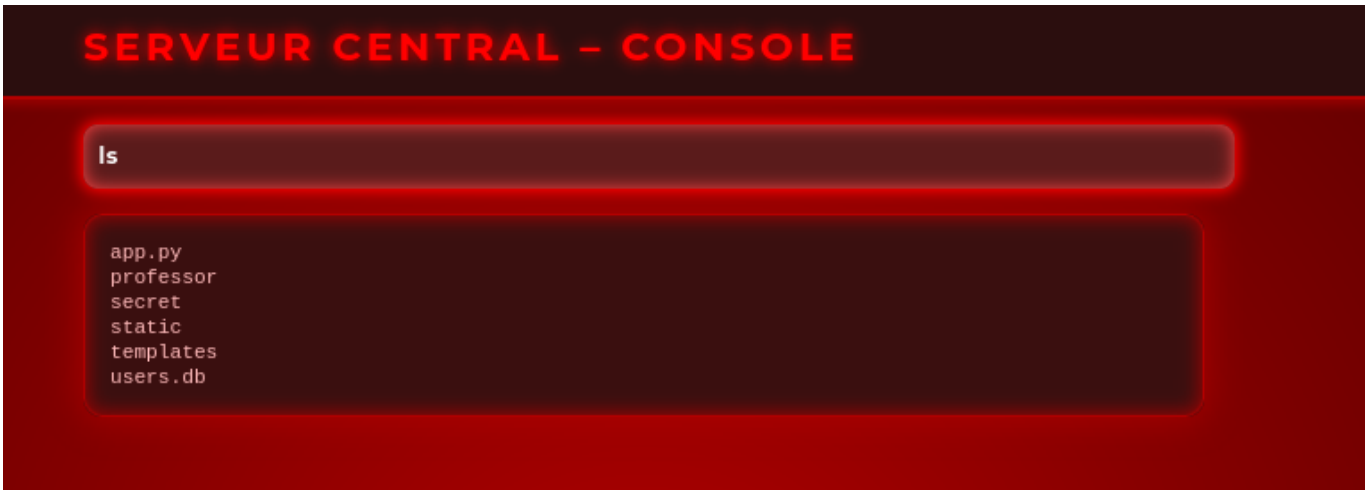


It's a login page

Step 4 : Injection

As the name of the challenge is **LA CASA DE L'INJECTION**, maybe the website is vulnerable to SQL injection.

Boom!! It worked, and we accessed the **WEB SERVER COMMAND PANEL**



/secret and **/professor** are interesting .

Unfortunately .. We can't use cat. Let's try with another one.

Hummmmm... it's not the second document. Let's take a look on /professor

Bingo !!!!

We combined document1 and document2 contents, got the flag, and saved the Professor.
