

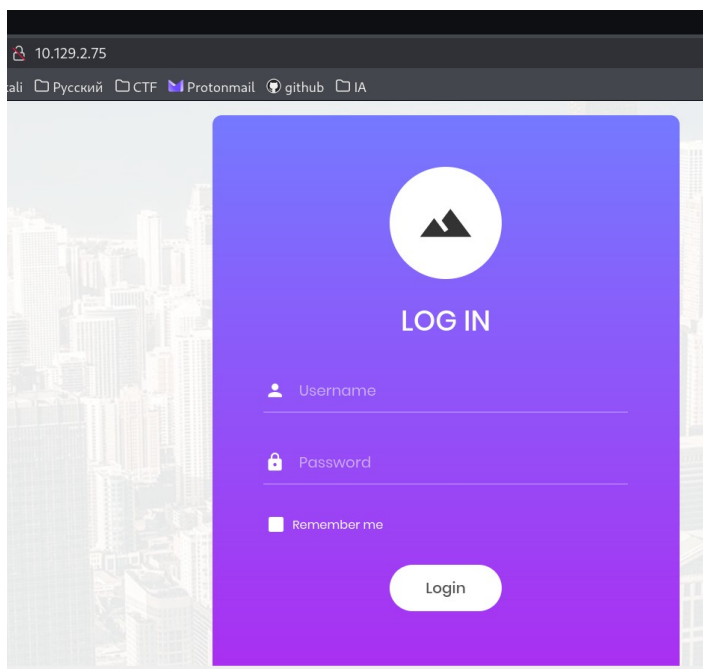
# HackTheBox

**Máquina:** Appointment  
Pablo José Pérez Díez

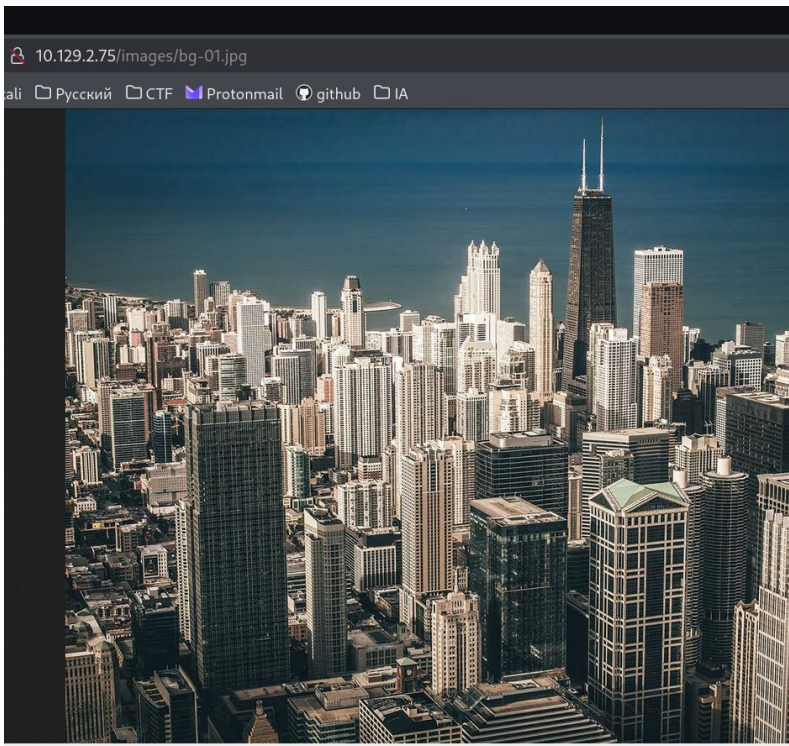
Escaneo Inicial:

```
(pabli@kali)-[~]  
└─$ sudo nmap -sV -sC -O 10.129.2.75  
[sudo] contraseña para pabli:  
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-23 21:26 CEST  
Nmap scan report for 10.129.2.75  
Host is up (0.21s latency).  
Not shown: 999 closed tcp ports (reset)  
PORT      STATE SERVICE VERSION  
80/tcp    open  http      Apache httpd 2.4.38 ((Debian))  
|_http-title: Login  
|_http-server-header: Apache/2.4.38 (Debian)  
Device type: general purpose  
Running: Linux 5.X  
OS CPE: cpe:/o:linux:linux_kernel:5  
OS details: Linux 5.0 - 5.14  
Network Distance: 2 hops
```

Encontramos un servidor Apache, visualizando la pagina en el navegador encontramos un formulario de login:



Utilizando Gobuster descubrimos directorios a los que tenemos acceso, como la carpeta images donde se encuentra esta foto:



La descargamos y examinamos sus metadatos con exiftool:

```
$ exiftool bg-01.jpg
ExifTool Version Number      : 13.25
File Name                    : bg-01.jpg
Directory                   : .
File Size                    : 252 kB
File Modification Date/Time  : 2025:08:23 21:58:49+02:00
File Access Date/Time       : 2025:08:23 21:58:49+02:00
File Inode Change Date/Time  : 2025:08:23 21:58:49+02:00
File Permissions             : -rw-rw-r--
File Type                    : JPEG
File Type Extension          : jpg
MIME Type                    : image/jpeg
Exif Byte Order              : Little-endian (Intel, II)
Quality                      : 30%
XMP Toolkit                  : Adobe XMP Core 5.3-c011 66.145661, 2012/02/06-14:56:27
Creator Tool                 : Adobe Photoshop CS6 (Windows)
Instance ID                  : xmp.iid:C5D6C071E29411E795568C4CCECE807D
Document ID                  : xmp.did:C5D6C072E29411E795568C4CCECE807D
Derived From Instance ID     : xmp.iid:C5D6C06FE29411E795568C4CCECE807D
Derived From Document ID     : xmp.did:C5D6C070E29411E795568C4CCECE807D
DCT Encode Version           : 100
APP14 Flags 0                : [14], Encoded with Blend=1 downsampling
APP14 Flags 1                : (none)
Color Transform               : YCbCr
Image Width                  : 1280
Image Height                 : 939
```

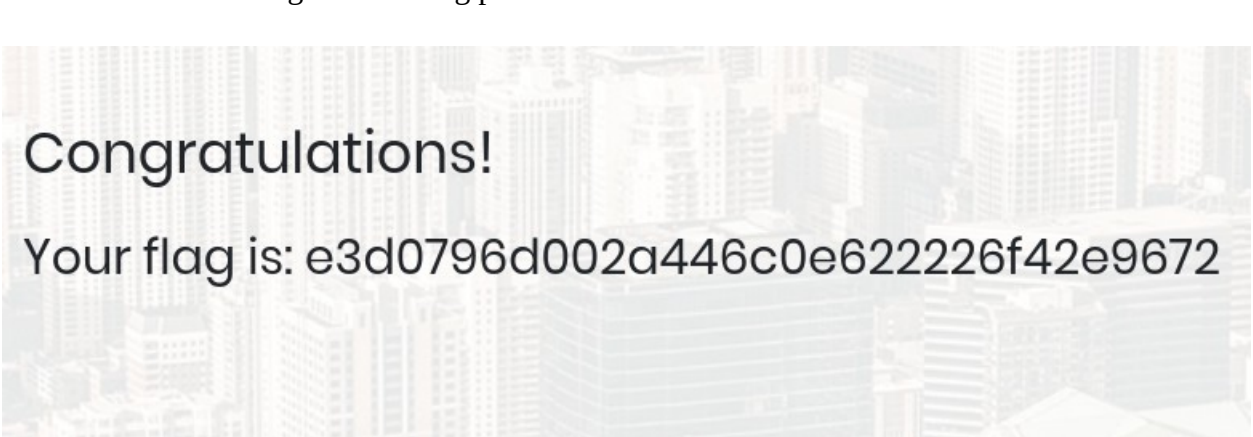
No hemos encontrado información útil y tampoco parece que se trate de una técnica de esteganografía, por lo que solo nos queda como posible entrada el formulario de la pagina principal.

[illegible]

Si la aplicación está mal hecha se adjuntara literalmente lo que añadamos en el formulario a la query SQL, por lo que en este caso realmente se estaría ejecutando algo similar a esto:

SELECT \* FROM user WHERE user.username = 'admin' # → a partir de aquí quedaría ignorado

Como vemos simplemente con introducir un usuario válido nos serviría para entrar. De esta manera conseguimos la flag para terminar el CTF.



Congratulations!

Your flag is: e3d0796d002a446c0e622226f42e9672

Your flag is: e3d0796d002a446c0e622226f42e9672