enum

so now we will see nmap results

nmap -sCTV -oN /home/kali/machines/active/love/nmap.txt
10.10.10.239
Starting Nmap 7.91 (https://nmap.org) at 2021-06-10 10:22
EDT
Nmap scan report for
10.10.10.239
Host is up (0.26s
latency).
Not shown: 993 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/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

| 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:
|
NULL:
|_   Host '10.10.14.108' 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
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=6/10%Time=60C22079%P=x86_64-pc-
linux-gnu%r(NU
SF:LL,4B,"G\0\0\x01\xffj\x04Host\x20'10\.10\.14\.108'\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: 2h53m16s, deviation: 4h02m30s, median: 33m15s
| 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: 2021-06-10T07:57:29-07:00
| smb-security-mode:
| account_used: <blank>
| 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: 2021-06-10T14:57:31
|_ start_date: N/A

Service detection performed. Please report any incorrect results at https://-nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 122.02 seconds

vuln script results

nmap --script vuln
10.10.10.239
Starting Nmap 7.91 (https://nmap.org) at 2021-06-10 10:22
EDT
Nmap scan report for
10.10.10.239
Host is up (0.28s
latency).
Not shown: 993 closed
ports
PORT   STATE
SERVICE
80/tcp   open
http
| http-cookie-
flags:
| /:
|
PHPSESSID:
| httponly flag not
set
| /
admin/:
|
PHPSESSID:
| httponly flag not
set
| /admin/-

index.php:
|
PHPSESSID:
|_ httponly flag not
set
| /
Admin/:
|
PHPSESSID:
|_ httponly flag not
set
| http-
csrf:
| Spidering limited to: maxdepth=3; maxpagecount=20;
withinhost=10.10.10.239
| Found the following possible CSRF
vulnerabilities:
|
| Path: http://10.10.10.239:80/

| Form
id:
| Form action:
login.php
|
| Path: http://10.10.10.239:80/login.php

| Form
id:
|_ Form action:
login.php
|_http-dombased-xss: Couldn't find any DOM based
XSS.
| http-
enum:
| /admin/: Possible admin
folder
| /admin/index.php: Possible admin
folder
| /Admin/: Possible admin
folder
| /icons/: Potentially interesting folder w/ directory
listing
| /images/: Potentially interesting directory w/ listing on 'apache/2.4.46

(win64) openssl/1.1.1j php/7.3.27'
http-fileupload-
exploiter:
|
| Couldn't find a file-type
field.
|
| Couldn't find a file-type
field.
|
| Couldn't find a file-type
field.
|
|_   Couldn't find a file-type
field.
| http-slowloris-
check:
|
VULNERABLE:
| Slowloris DOS
attack
| State: LIKELY VULNERABLE
| IDs: CVE:CVE-2007-6750
| Slowloris tries to keep many connections to the target web server open
and hold
| them open as long as possible. It accomplishes this by opening
connections to
| the target web server and sending a partial request. By doing so, it starves
| the http server's resources causing Denial Of Service.
|
| Disclosure date: 2009-09-17
| References:
| http://ha.ckers.org/slowloris/
|_   https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750
http-sql-injection:
| Possible sqli for queries:
| http://10.10.10.239:80/bower_components/jquery/dist/?-
C=M%3bO%3dA%27%20OR%20sqlspider
| http://10.10.10.239:80/bower_components/jquery/dist/?-
C=N%3bO%3dD%27%20OR%20sqlspider
| http://10.10.10.239:80/bower_components/jquery/dist/?-
C=D%3bO%3dA%27%20OR%20sqlspider
| http://10.10.10.239:80/bower_components/jquery/dist/?-
C=S%3bO%3dA%27%20OR%20sqlspider

| http://10.10.10.239:80/bower_components/jquery/dist/?-C=N%3bO%3dA%27%20OR%20sqlspider
| http://10.10.10.239:80/bower_components/jquery/dist/?-C=D%3bO%3dA%27%20OR%20sqlspider
| http://10.10.10.239:80/bower_components/jquery/dist/?-C=S%3bO%3dA%27%20OR%20sqlspider
| http://10.10.10.239:80/bower_components/jquery/dist/?-C=M%3bO%3dD%27%20OR%20sqlspider
| http://10.10.10.239:80/bower_components/jquery/?-C=M%3bO%3dA%27%20OR%20sqlspider
| http://10.10.10.239:80/bower_components/jquery/?-C=D%3bO%3dA%27%20OR%20sqlspider
| http://10.10.10.239:80/bower_components/jquery/?-C=N%3bO%3dD%27%20OR%20sqlspider
| http://10.10.10.239:80/bower_components/jquery/?-C=S%3bO%3dA%27%20OR%20sqlspider
| http://10.10.10.239:80/bower_components/jquery/dist/?-C=M%3bO%3dA%27%20OR%20sqlspider
| http://10.10.10.239:80/bower_components/jquery/dist/?-C=D%3bO%3dA%27%20OR%20sqlspider
| http://10.10.10.239:80/bower_components/jquery/dist/?-C=S%3bO%3dA%27%20OR%20sqlspider
|_ http://10.10.10.239:80/bower_components/jquery/dist/?-C=N%3bO%3dA%27%20OR%20sqlspider
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-trace: TRACE is enabled
|_http-vuln-cve2017-1001000: ERROR: Script execution failed (use -d to debug)
135/tcp open msrpc
139/tcp open netbios-ssn
443/tcp open https
|_http-aspnet-debug: ERROR: Script execution failed (use -d to debug)
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
| http-enum:
|_ /icons/: Potentially interesting folder w/ directory listing
| http-slowloris-check:
| VULNERABLE:
| Slowloris DOS attack
| State: LIKELY VULNERABLE
| IDs: CVE:CVE-2007-6750
| Slowloris tries to keep many connections to the target web server open and hold
| them open as long as possible. It accomplishes this by opening connections to

| the target web server and sending a partial request. By doing so, it starves
| the http server's resources causing Denial Of Service.
|
| Disclosure date: 2009-09-17
| References:
| http://ha.ckers.org/slowloris/
|_   https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-trace: TRACE is enabled
|_sslv2-drown:
445/tcp open microsoft-ds
3306/tcp open mysql
|_mysql-vuln-cve2012-2122: ERROR: Script execution failed (use -d to debug)
|_sslv2-drown:
5000/tcp open upnp

Host script results:
|_samba-vuln-cve-2012-1182: NT_STATUS_ACCESS_DENIED
|_smb-vuln-ms10-054: false
|_smb-vuln-ms10-061: NT_STATUS_ACCESS_DENIED

Nmap done: 1 IP address (1 host up) scanned in 368.94 seconds

nmap result of complete port scan result

nmap -sCV -p- -oN /home/kali/machines/active/love/nmap_complete.txt
10.10.10.239
Starting Nmap 7.91 (https://nmap.org) at 2021-06-10 10:23
EDT
Stats: 0:29:37 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth
Scan
SYN Stealth Scan Timing: About 81.74% done; ETC: 10:59 (0:06:37
remaining)
Stats: 0:30:51 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth
Scan
SYN Stealth Scan Timing: About 85.84% done; ETC: 10:59 (0:05:05
remaining)
Nmap scan report for
10.10.10.239
Host is up (0.24s
latency).
Not shown: 65453 closed ports, 63 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-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
| 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:
| LPDString,
X11Probe:
|_   Host '10.10.14.108' 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   [21/61]
|_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
| Not valid before: 2021-04-11T14:39:19
|_Not valid after: 2024-04-10T14:39:19
|_ssl-date: 2021-06-10T15:34:23+00:00; +33m14s from scanner time.
| tls-alpn:
|_ http/1.1
7680/tcp open pando-pub?
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=6/10%Time=60C22890%P=x86_64-pc-
linux-gnu%r(X1

SF:1Probe,4B,"G\0\0\x01\xffj\x04Host\x20'10\.10\.14\.108'\x20is\x20not\x20
SF:allowed\x20to\x20connect\x20to\x20this\x20MariaDB\x20server")-
%r(LPDStri
SF:ng,4B,"G\0\0\x01\xffj\x04Host\x20'10\.10\.14\.108'\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: 2h18m14s, deviation: 3h30m00s, median: 33m13s
| 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
| Workgroup: WORKGROUP\x00
|_ System time: 2021-06-10T08:34:05-07:00
| smb-security-mode:
| account_used: <blank>
| 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: 2021-06-10T15:34:11
|_ start_date: N/A

Service detection performed. Please report any incorrect results at https://-
nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 2268.97 seconds

hash-- aab42ca009fed69fa5ee57c52cf5bcf1
open ports

80/tcp   open http   Apache httpd 2.4.46 ((Win64)

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

445/tcp open microsoft-ds Windows 10 Pro 19042 microsoft-ds

3306/tcp open mysql?

5000/tcp open http   Apache httpd 2.4.46

80/tcp   open http   Apache httpd 2.4.46

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

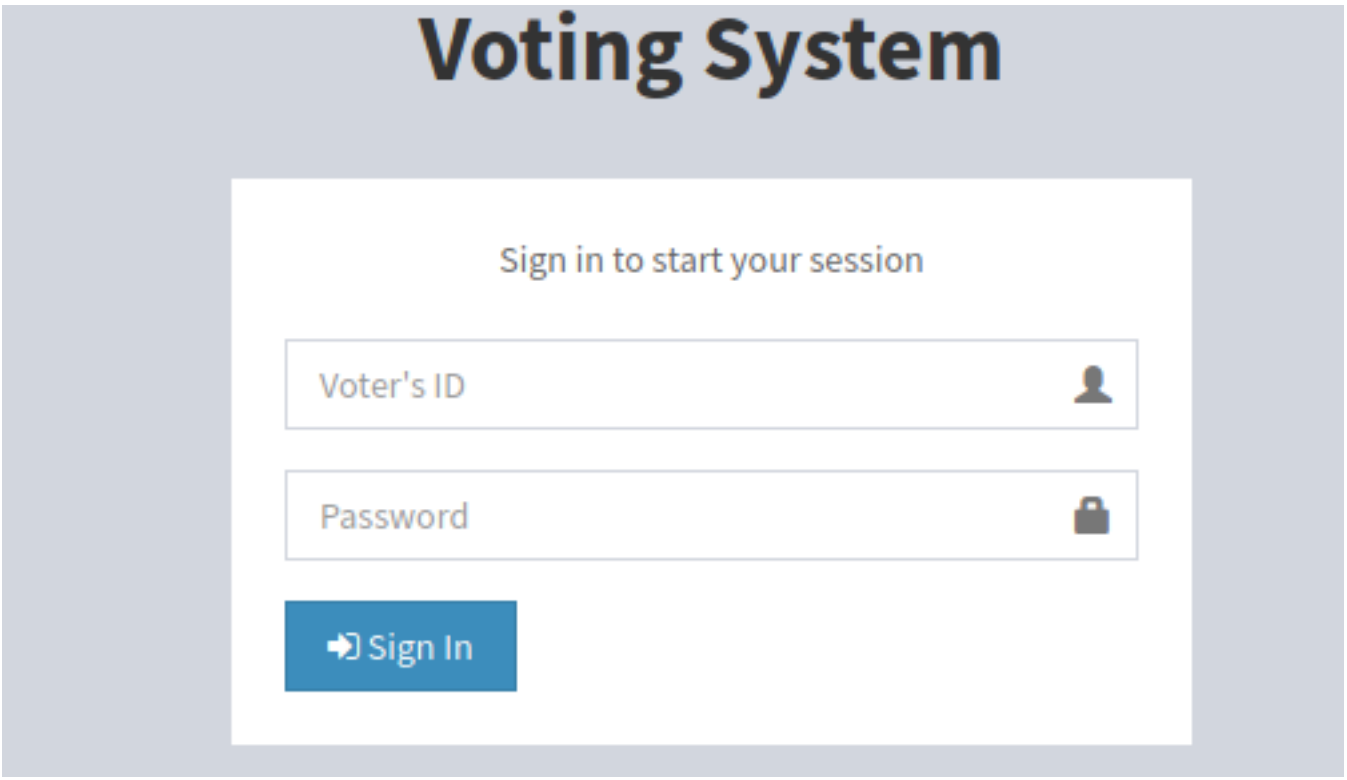
445/tcp   open microsoft-ds Windows 10 Pro 19042 microsoft-ds (workgroup: WORKGROUP)
3306/tcp open mysql?

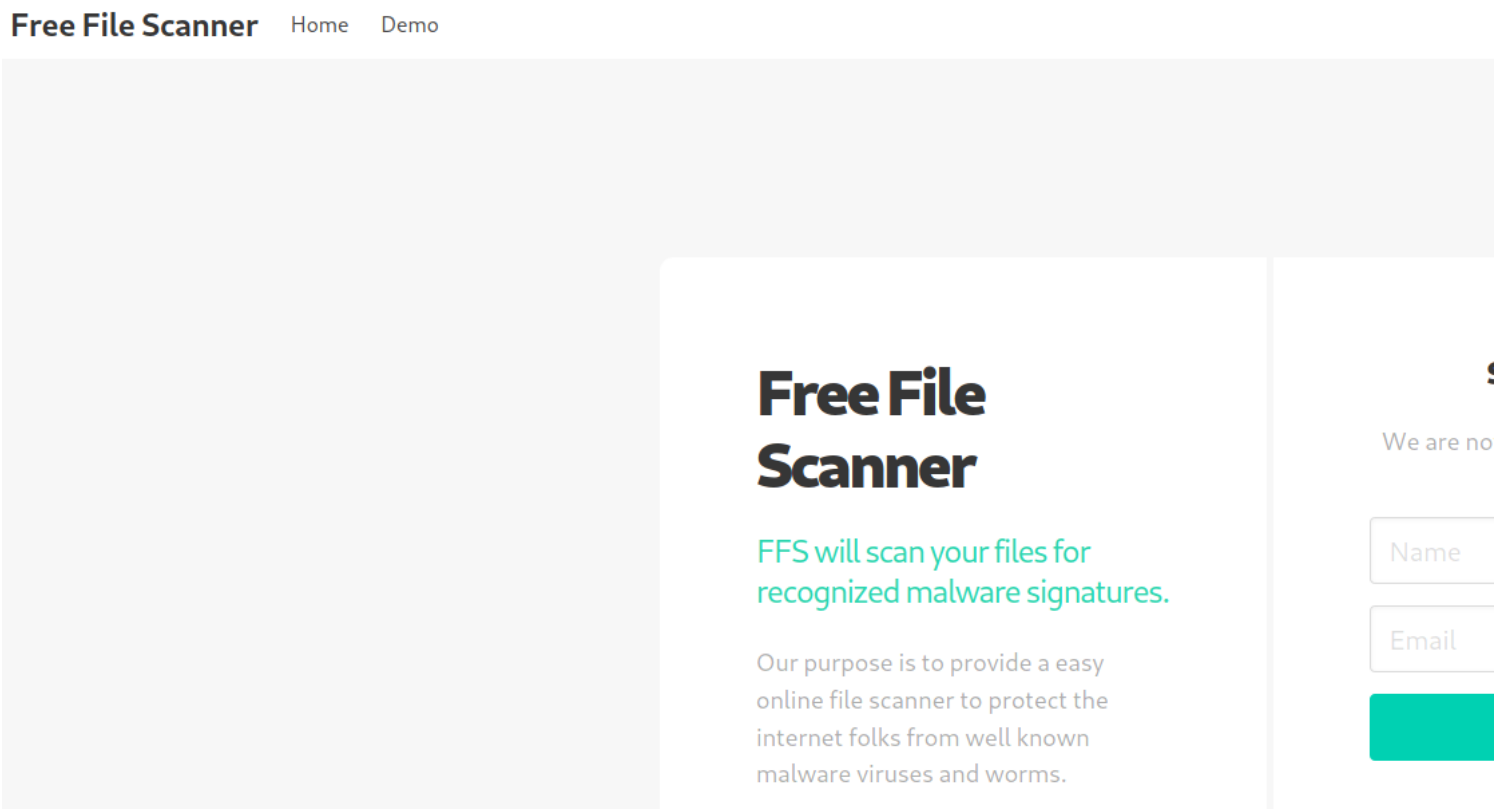
5000/tcp open http   Apache httpd 2.4.46
5040/tcp open unknown
5985/tcp open http   Microsoft HTTPAPI httpd 2.0
5986/tcp open ssl/http   Microsoft HTTPAPI httpd 2.0
7680/tcp open pando-pub
47001/tcp open http

found some domain names

staging.love.htb
www.love.htb;

so going to default page we found this page





love.htb is same but the 2nd domain name took us to this page

lets signup to this

in love.htb we found this
/images (Status: 301) [Size: 330] [--> http://love.htb/images/]

/index.php (Status: 200) [Size:

4388]
/login.php (Status: 302) [Size: 0] [--> index.php]
/home.php (Status: 302) [Size: 0] [--> index.php]
/Images (Status: 301) [Size: 330] [--> http://love.htb/Images/]

/admin (Status: 301) [Size: 329] [--> http://love.htb/admin/]

/Home.php (Status: 302) [Size: 0] [--> index.php]
/plugins (Status: 301) [Size: 331] [--> http://love.htb/plugins/]

/includes (Status: 301) [Size: 332] [--> http://love.htb/includes/]

/Index.php (Status: 200) [Size: 4388]
/Login.php (Status: 302) [Size: 0] [--> index.php]
/examples (Status: 503) [Size: 398]
/logout.php (Status: 302) [Size: 0] [--> index.php]
/preview.php (Status: 302) [Size: 0] [--> index.php]
/dist (Status: 301) [Size: 328] [--> http://love.htb/dist/]

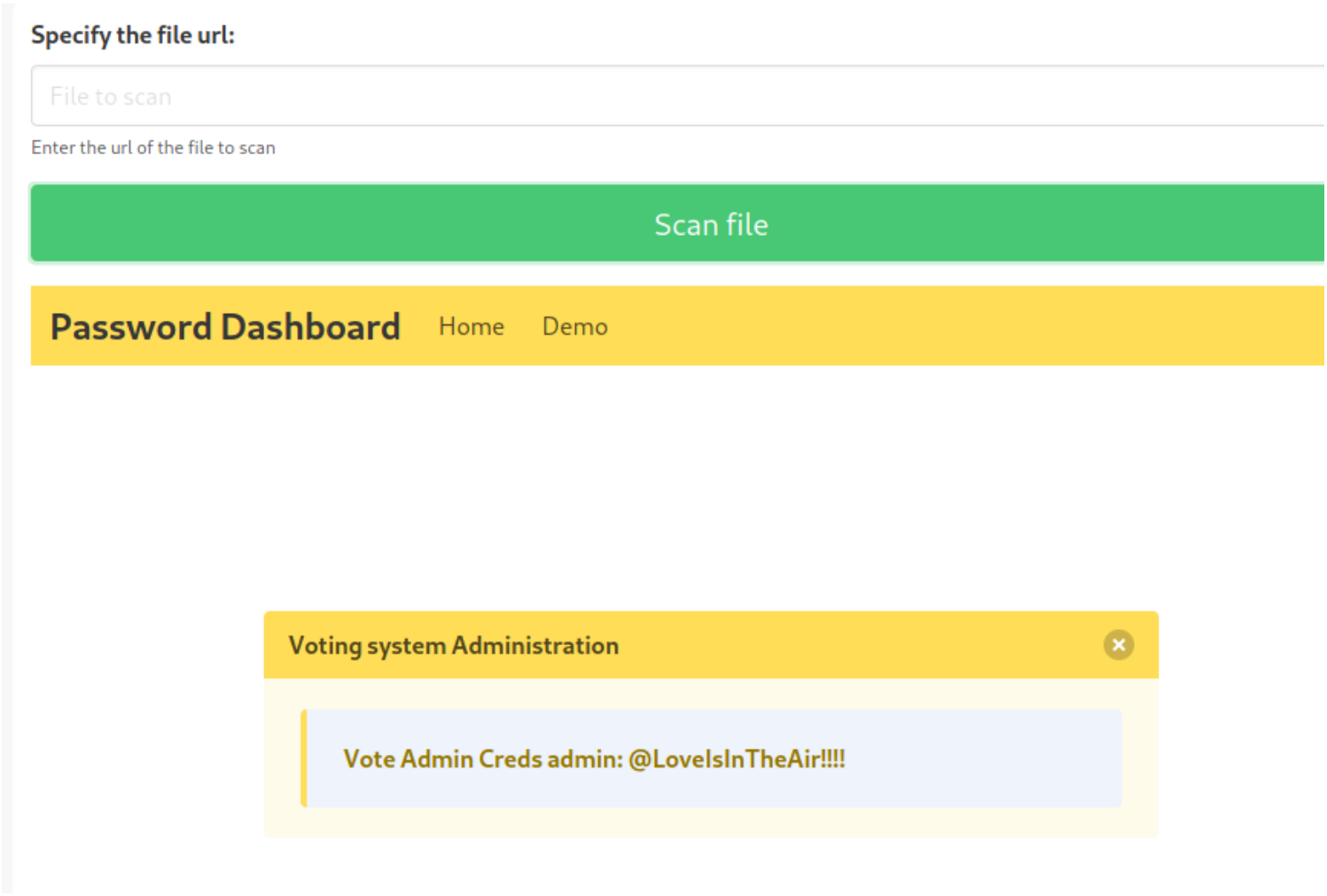
/licenses (Status: 403) [Size: 417]
/IMAGES (Status: 301) [Size: 330] [--> http://love.htb/IMAGES/]

/%20 (Status: 403) [Size: 298]
/INDEX.php (Status: 200) [Size: 4388]

/examples

we found nothing we have to look we finally found that the staging.love.htb we can run localhost to port 5000 which is forbidden to see the page

go to demo

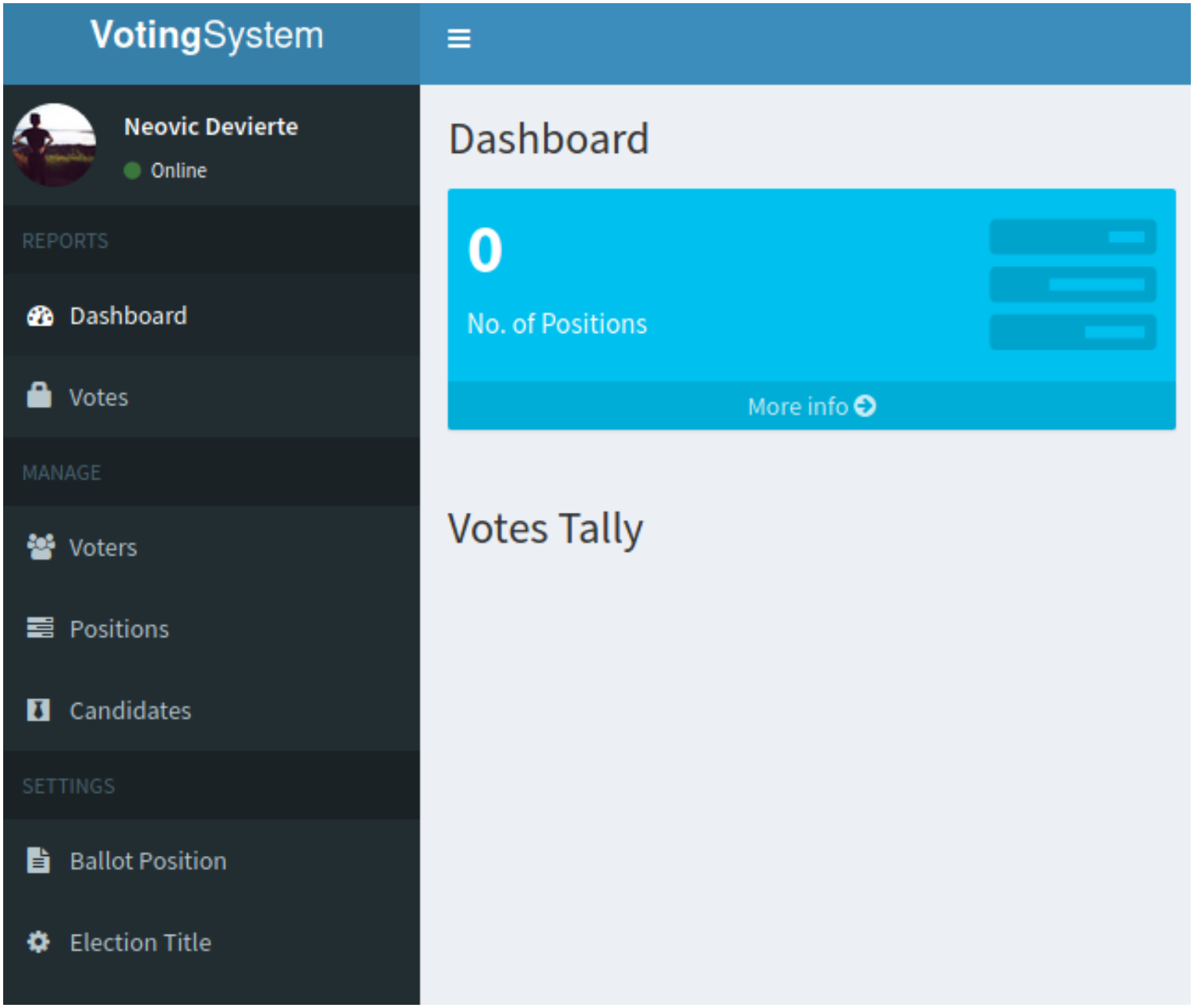


and we found this

credentials which clearly says vote admin creds are **admin: @LoveIsInTheAir!!!!**

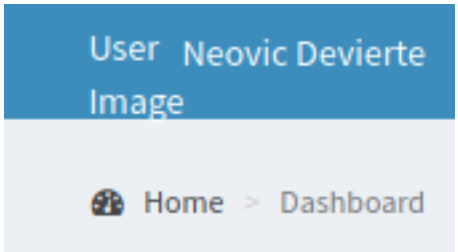
lets try to login using the credentials

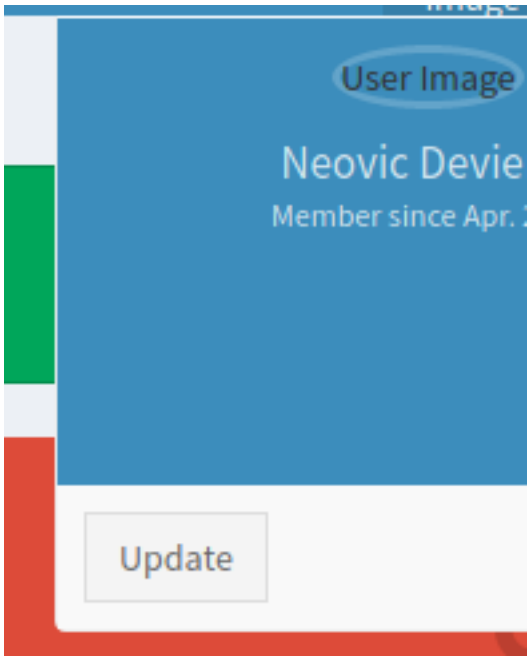
go to http://love.htb/admin/ because we have admin credentials

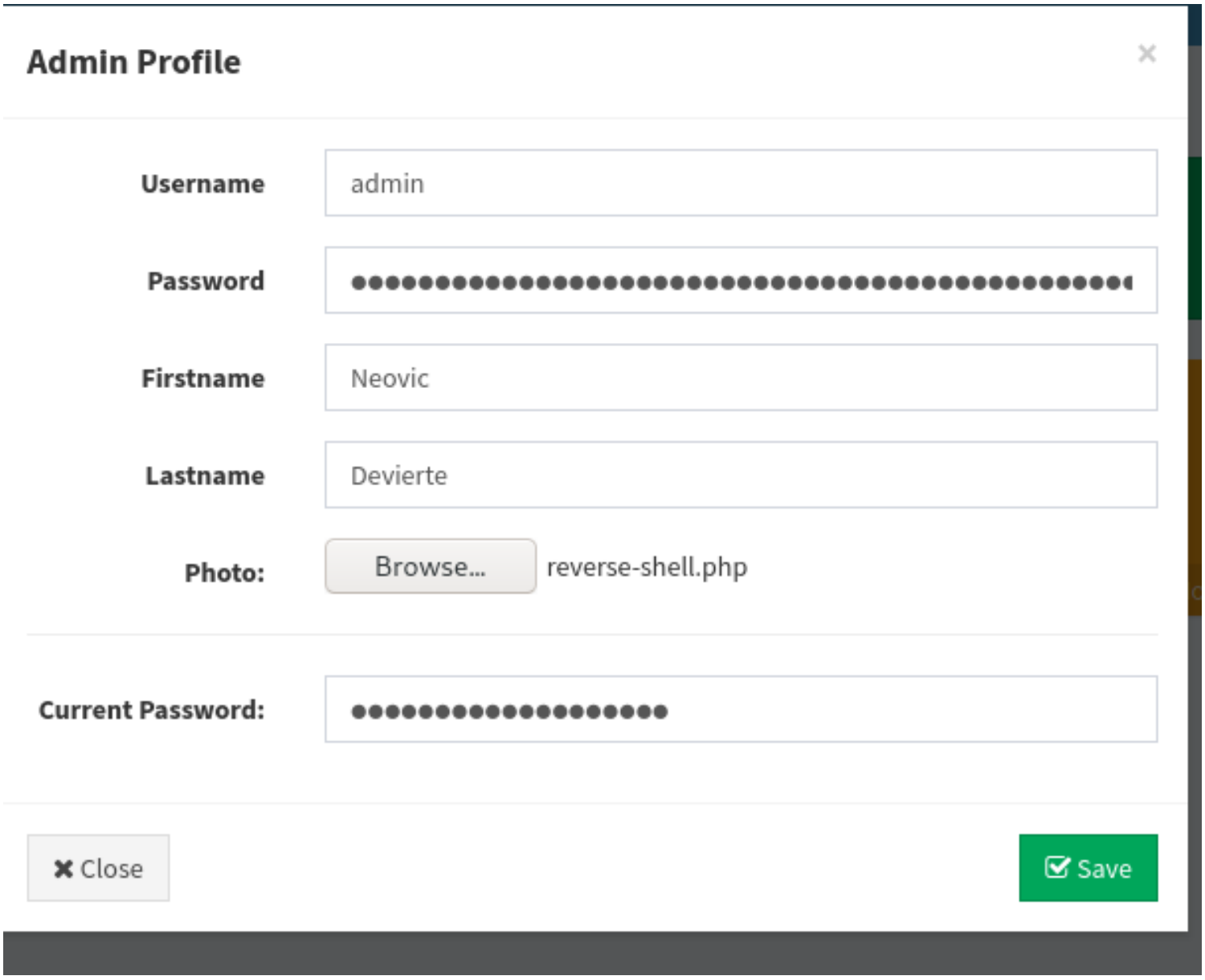


and we have a login

we went to top right and saw to update profile we updated it with a reverse shell





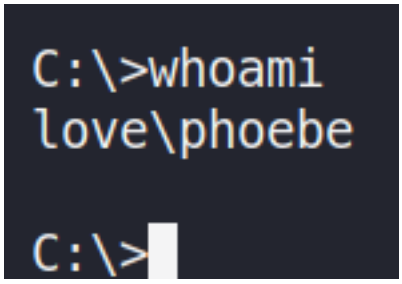


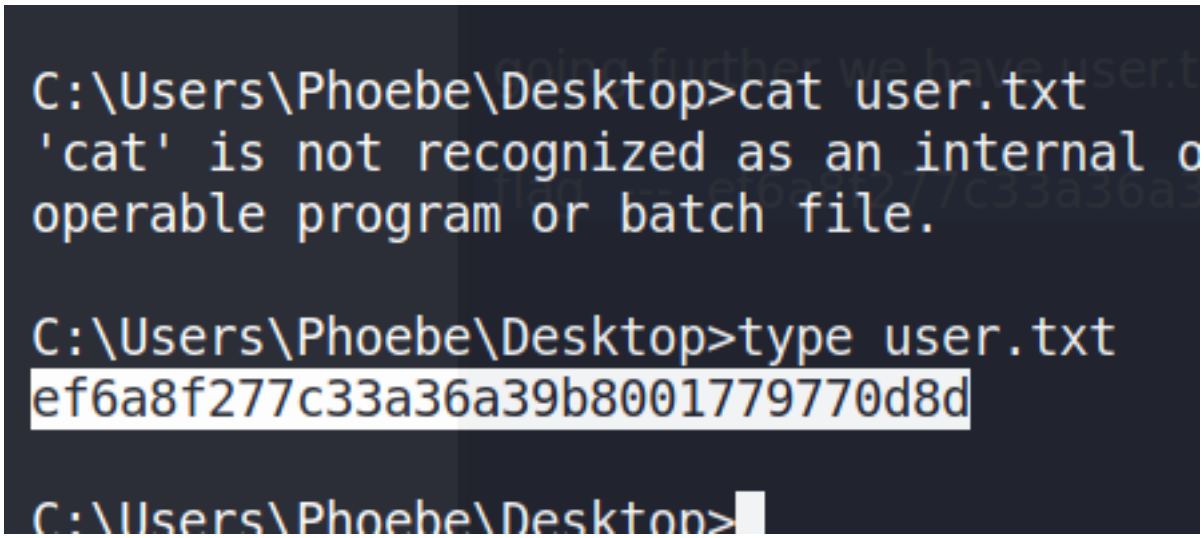
and now lets enable listner

https://github.com/ivan-sincek/php-reverse-shell/blob/master/src/minified/-

[php_reverse_shell_mini.php]

this reverse shell works





going further we have user.txt

flag --- ef6a8f277c33a36a39b8001779770d8d