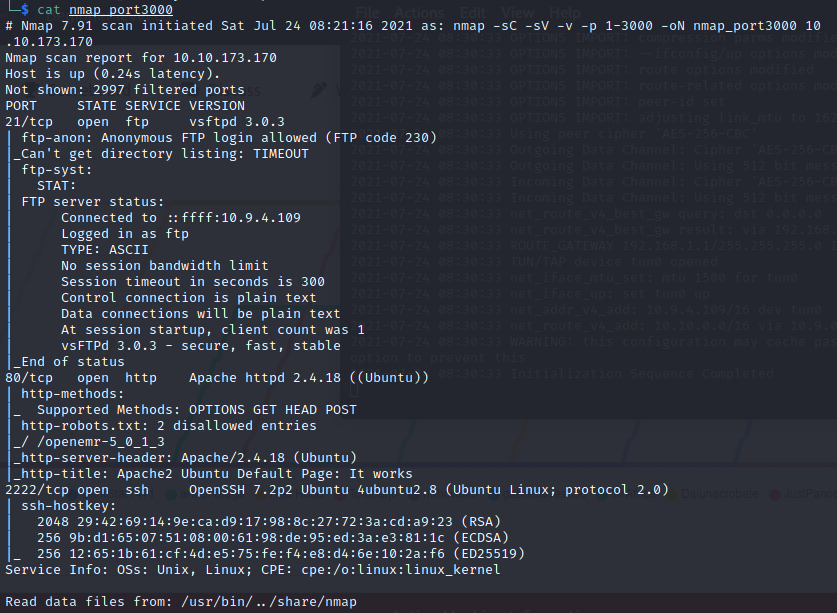
**Simple CTF write-up**

This is a write-up for Simple CTF in TryHackMe which we will exploit web server, try to get a shell for the first flag and elevate our privilege to capture our root flag



**How many services are running under port 1000?**

Always start with nmap with tag –sC –sV for 3000 ports and We’ve found that 21,80 and 2222 ports are currently running so this answer is 2 ports





**What is running on the higher port?**

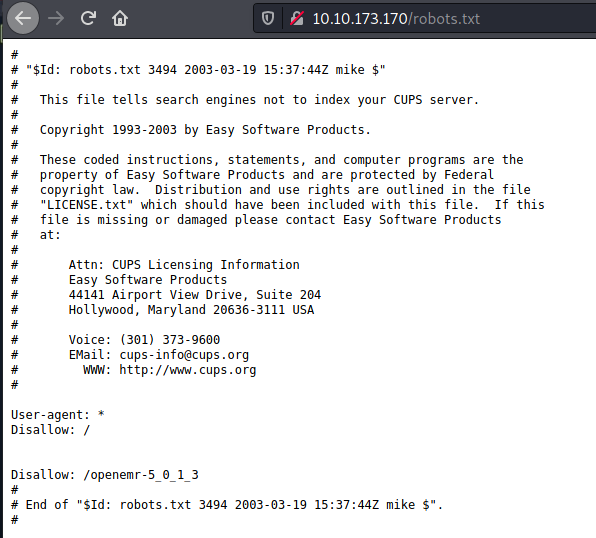
We’ve found that port 2222 is running SSH



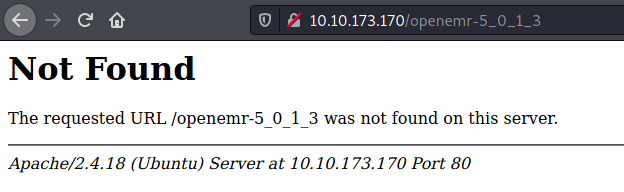
**What's the CVE you're using against the application?**

We found that target machine is running a web server run so we may need to bruteforce directory

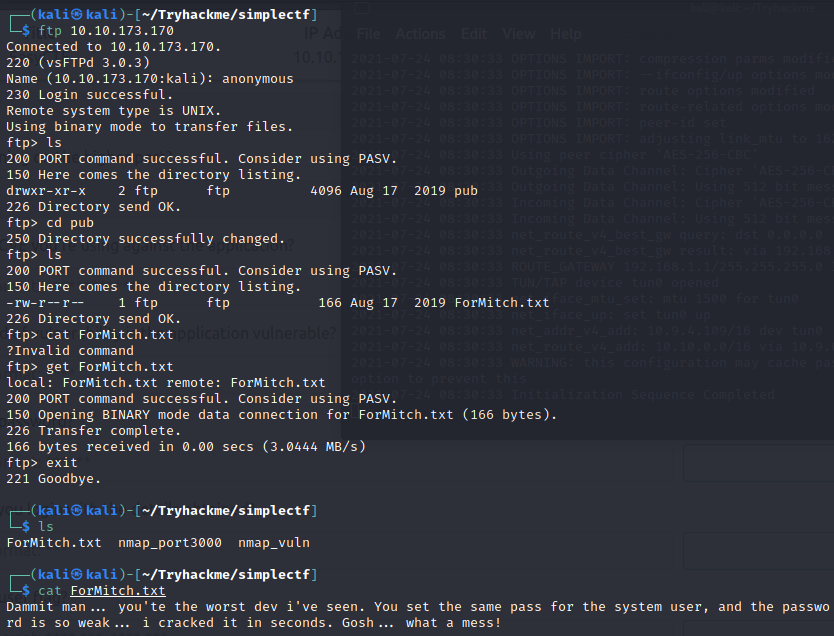
After launching gobuster I’ll look at robots.txt first and file is telling crawler to go to directory 1 directory and we know that this web server was built with CUPS server



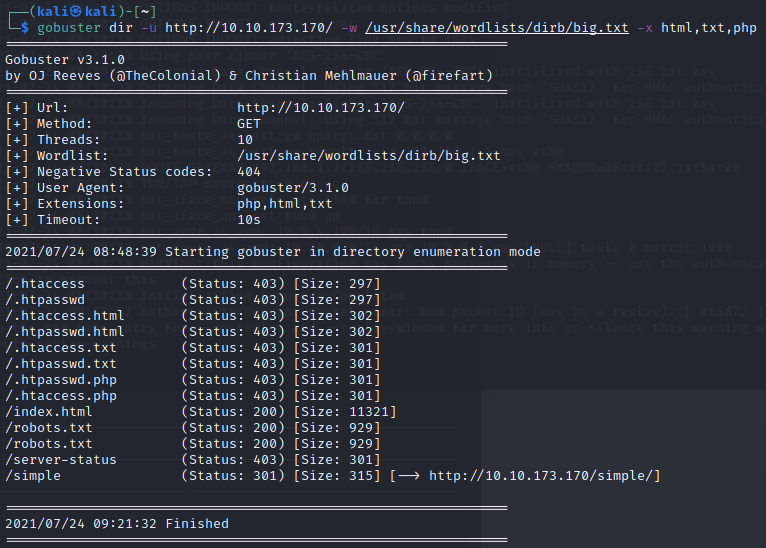
We’re tricked, this directory is gone



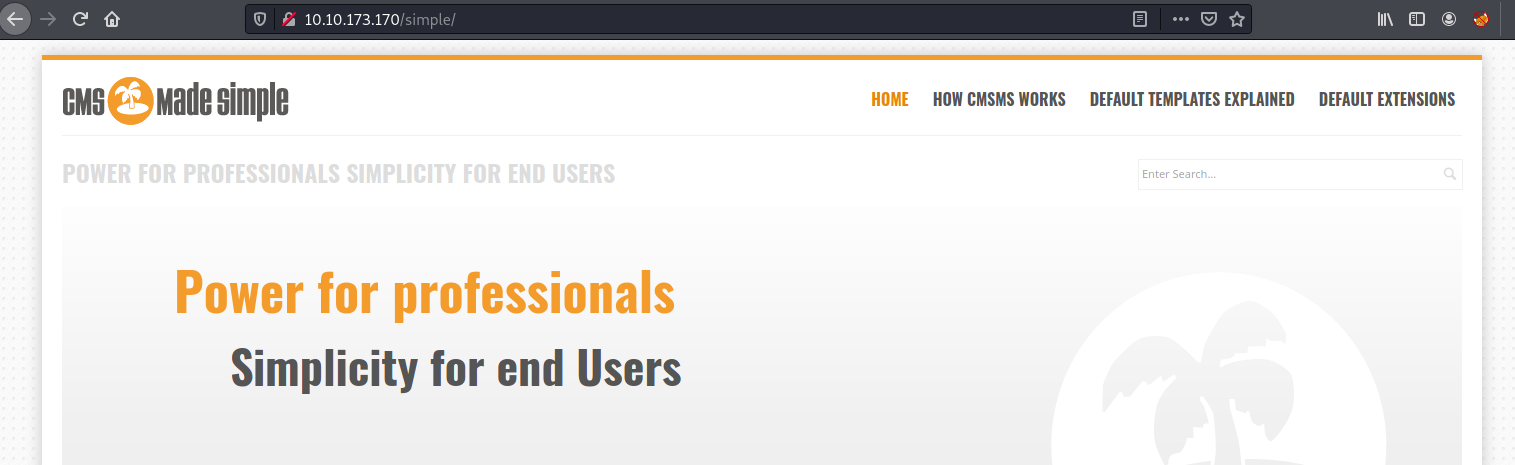
Until now my gobuster still running so I’ll check ftp server first and I’ve found a hint about password



Now back to gobuster /simple look suspicious so let’s check this out



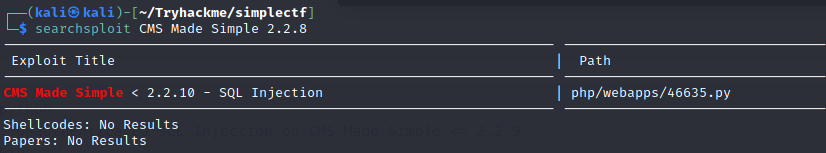
And in /simple is a CMS Made Simple default page which is Open-source management system



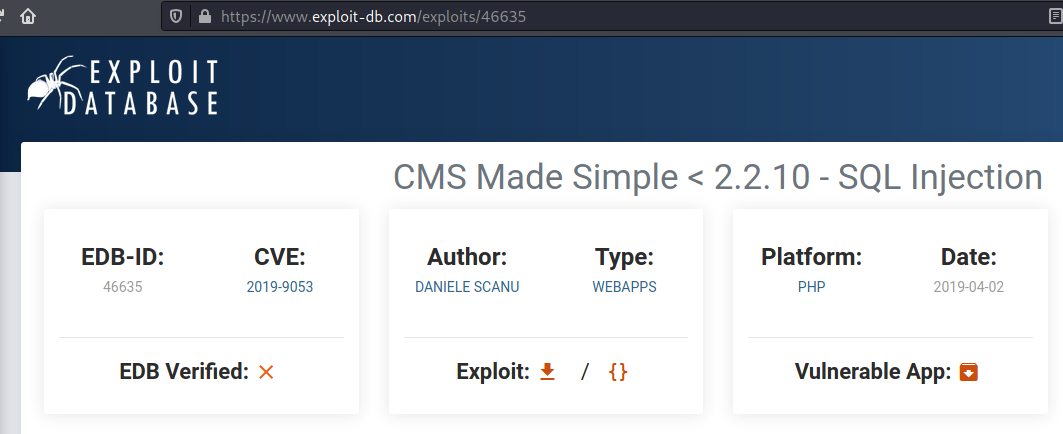
And we will know version of this CMS when we scrolled to the bottom



Time to use searchsploit to search public exploit for this version and we’ve found only 1 which is SQLi



Search in exploit-db we will get CVE number





**To what kind of vulnerability is the application vulnerable?**



**What's the password?**

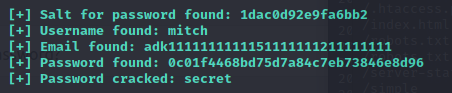
Now it’s time to exploit using this script but first this script is for python 2.7 and python 2.7 that built-in kali linux we don’t have termcolor library so we need to copy termcolor.py to python 2.7 library



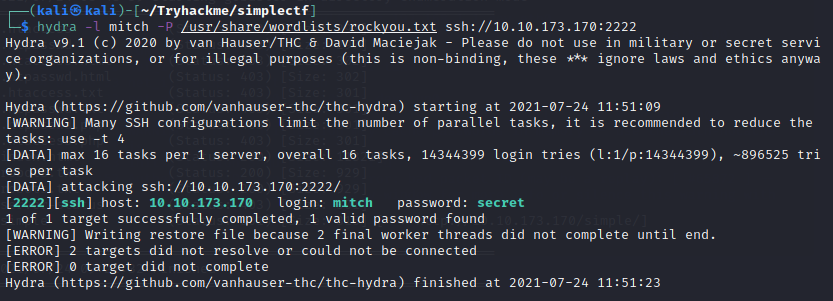
Now we know the drill , run this script with tag –u for the url , -c for cracking password and–w for wordlist



Waiting for eternity for this script, sometimes we don’t get cracked password and we need to run it all-over again and after many attempt I finally got the hashed password for mitch user



Actually we don’t even need that script, we can guess that mitch is username and ssh port is opened sowe can use hydra to guessing password



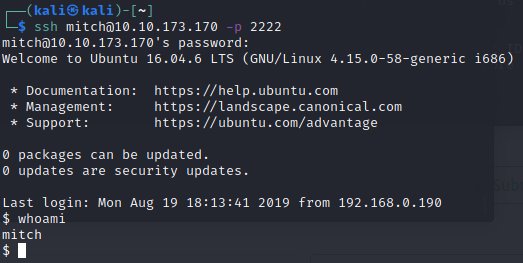


**Where can you login with the details obtained?**

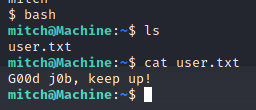


**What’s the user flag?**

Now we need to connect to target machine via ssh



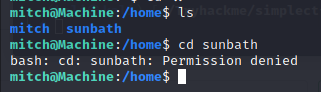
Now capture our first flag! It’s in directory when we connected





**Is there any other user in the home directory? What's its name?**

Go to home directory and we found sunbath





**What can you leverage to spawn a privileged shell?**

Now let’s find a way to elevate our privilege with sudo –l and we found that we can use vim with root privilege without password





**What’s the root flag?**

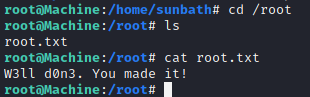
Use sudo vim to spawn root shell







And capture root flag in root directory!





All answers and flags

