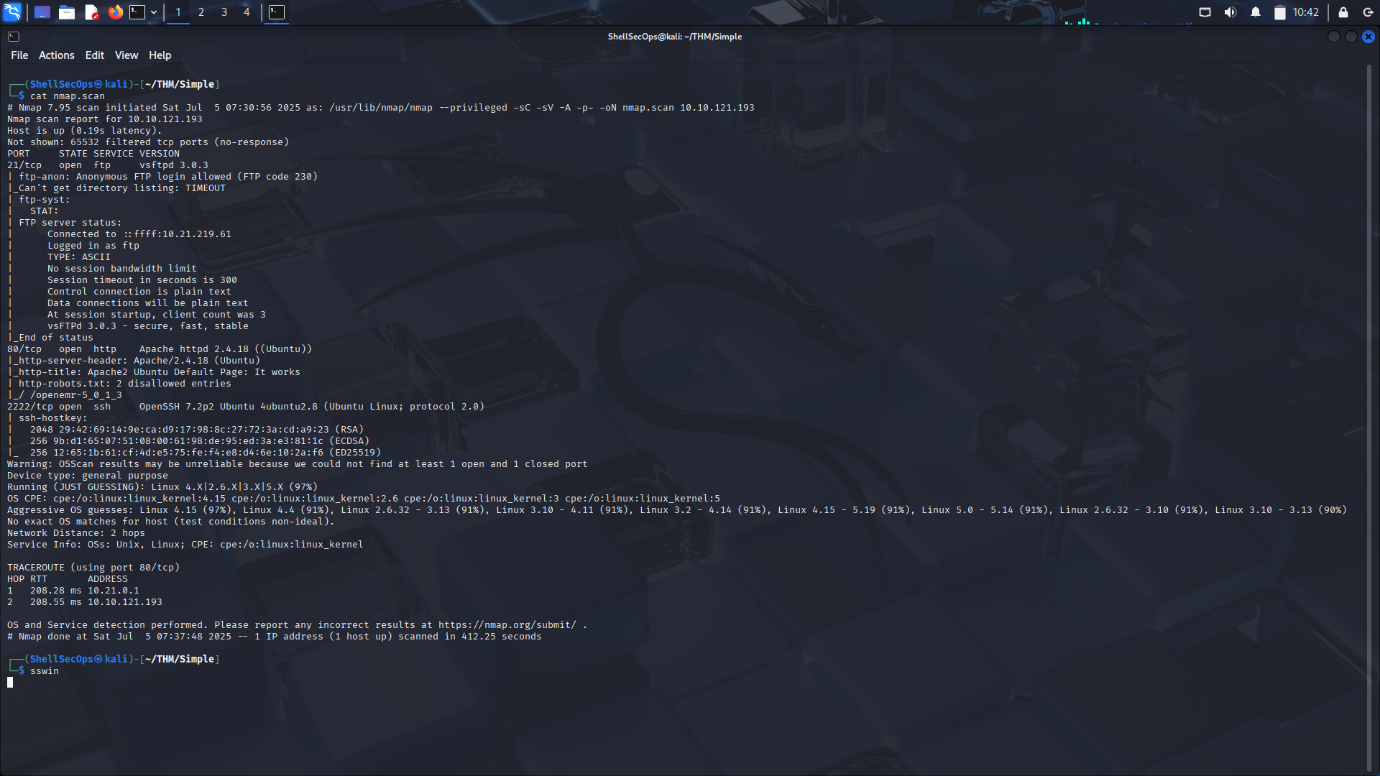
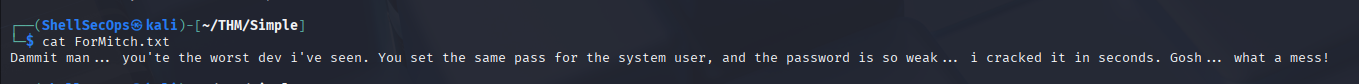
**Simple CTF Walkthrough(T.H.M)**

**Reconnaissance**:

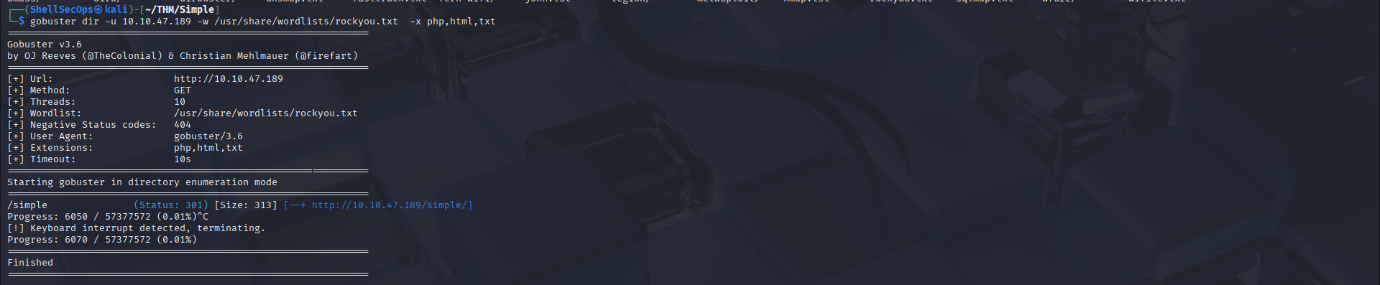
First, let us get information about the target. Scan the machine using nmap

Port no 21(ftp), 80(http), 2222(ssh) are open. Let us jump enumerating these ports.

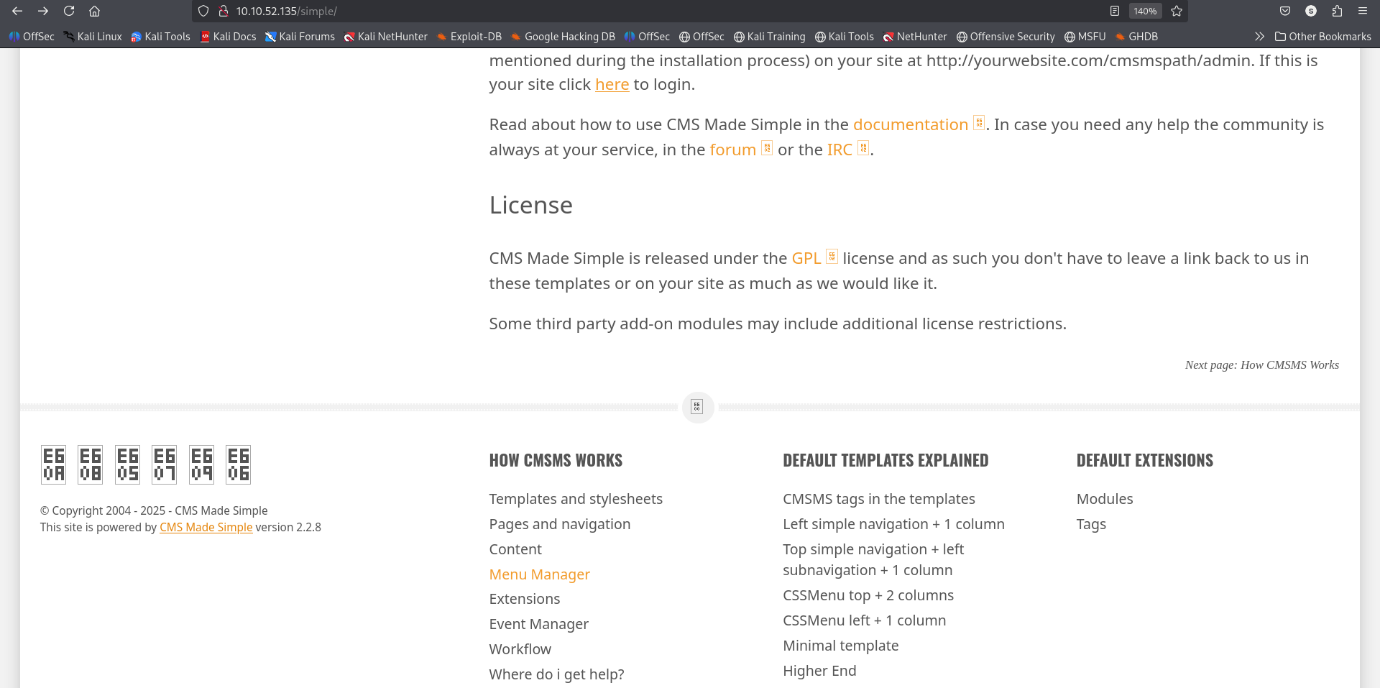
**Enumeration:**

* Ftp: we can log in as anonymous but we a ForMitch.txt file.
* SSH: we cannot login as anonymous so find nothing.
* HTTP: HTTP running apache httpd 2.4.18 So, there is nothing

just the default Apache2 web page running on Ubuntu, so I tried Dir brute-forcing using gobuster and found something interesting. We find a /simple dir and robots.txt.

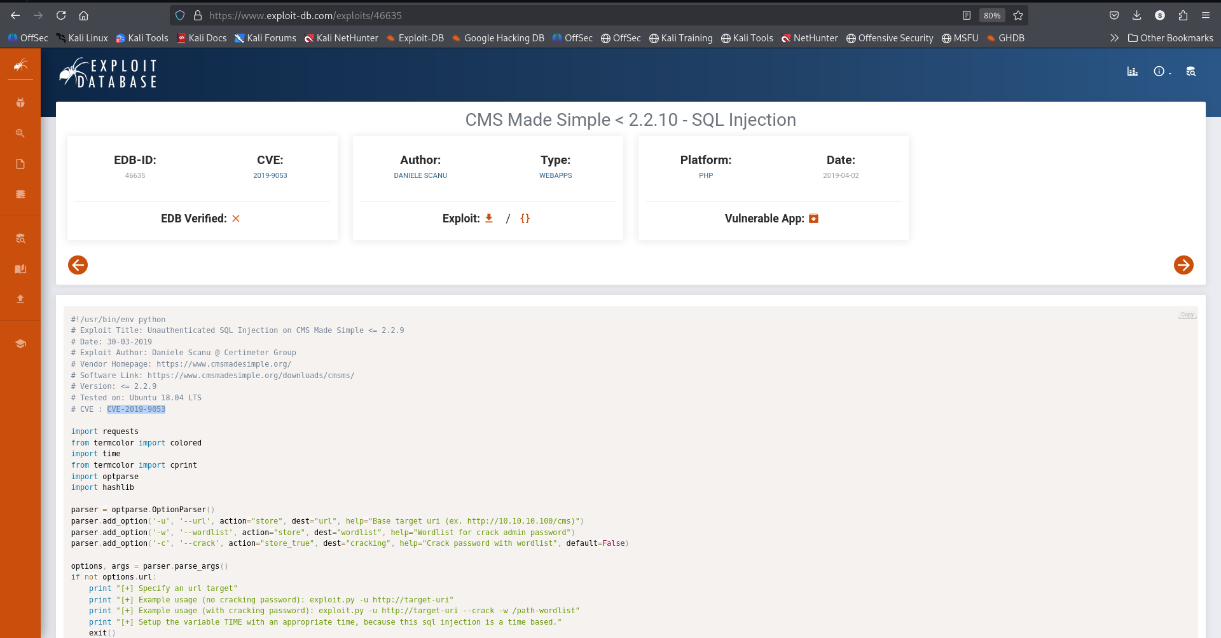


As we can see, there is a simple directory open on the web server.

So, our next step is to browse the /**simple**.

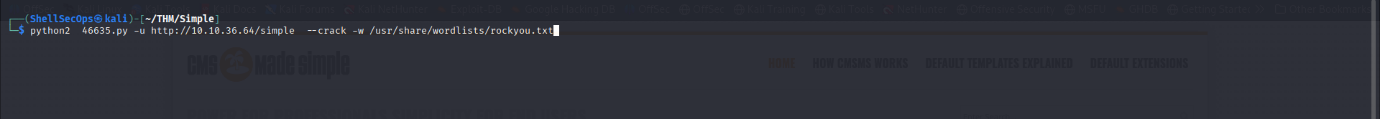
/simple is running a CMS Made Simple (Content Management System) version 2.2.8. which is a vulnerable versiEon we found an exploit against this service version <https://www.exploit-db.com/exploits/46635> .

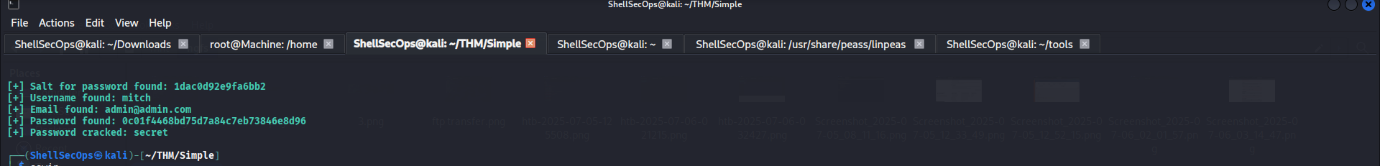
**Exploitation:**



Basically, this is a Sql-injection vulnerability which provide username and password.

After exploiting this vulnerability, we found username and password.

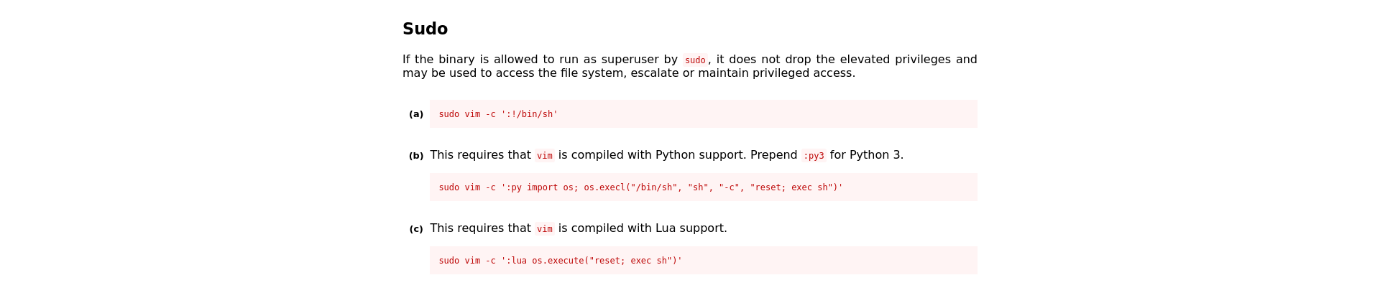


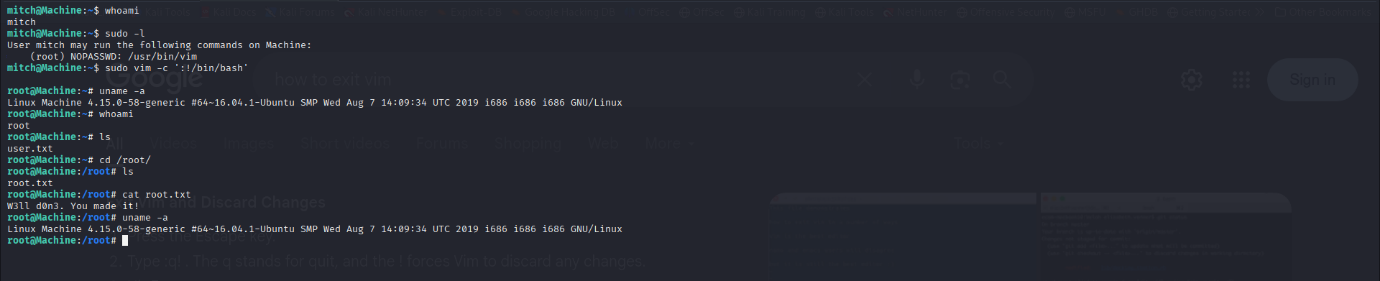


After I got username and password **mitch: secret.**  I tried to login via ssh and I got user shell.

Here I found user.txt flag.

After that for privilege escalation I tried to check sudo permission by using sudo -l command and guess what I found that mitch can run vim as sudo, so i tried GTFOBin resources [https://gtfobins.github.io/](https://gtfobins.github.io/%20) for shell escaping and I found a way of shell escaping through vim.





After using shell escaping technique, we got root.

And we are done! Hope you enjoyed my writeup and get to know some new tricks. Onto the next one my friends!