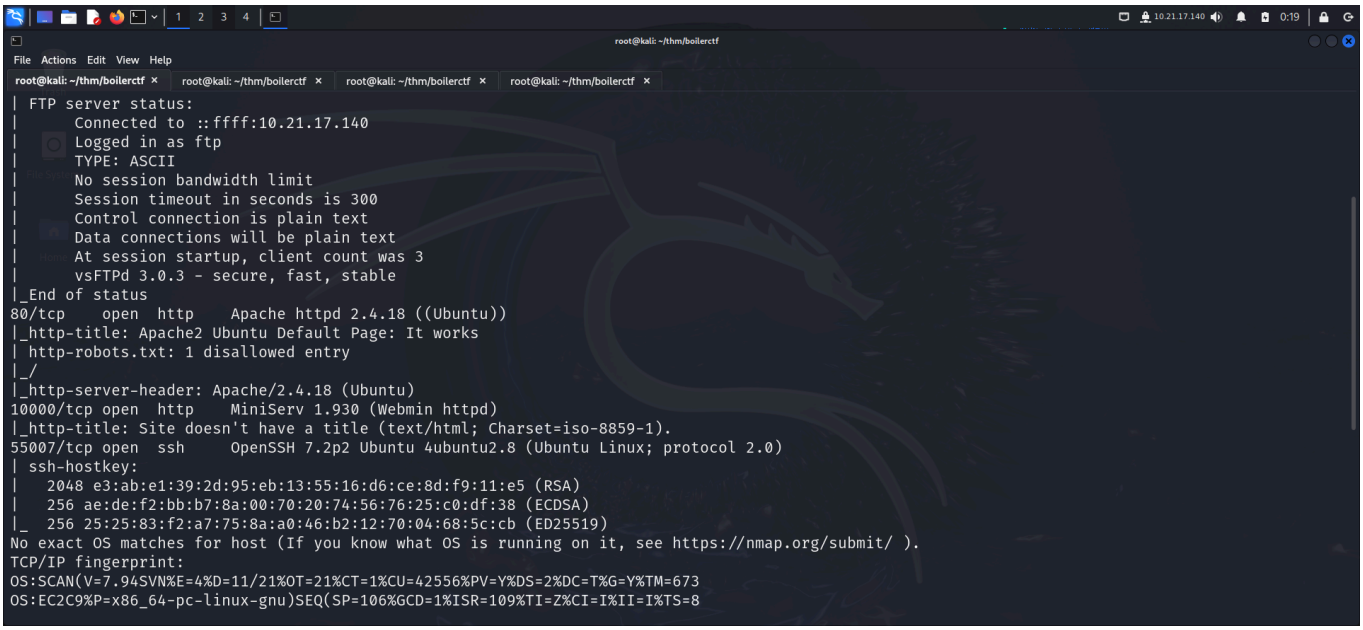
BOILER CTF

Link to machine : https://tryhackme.com/room/boilerctf2

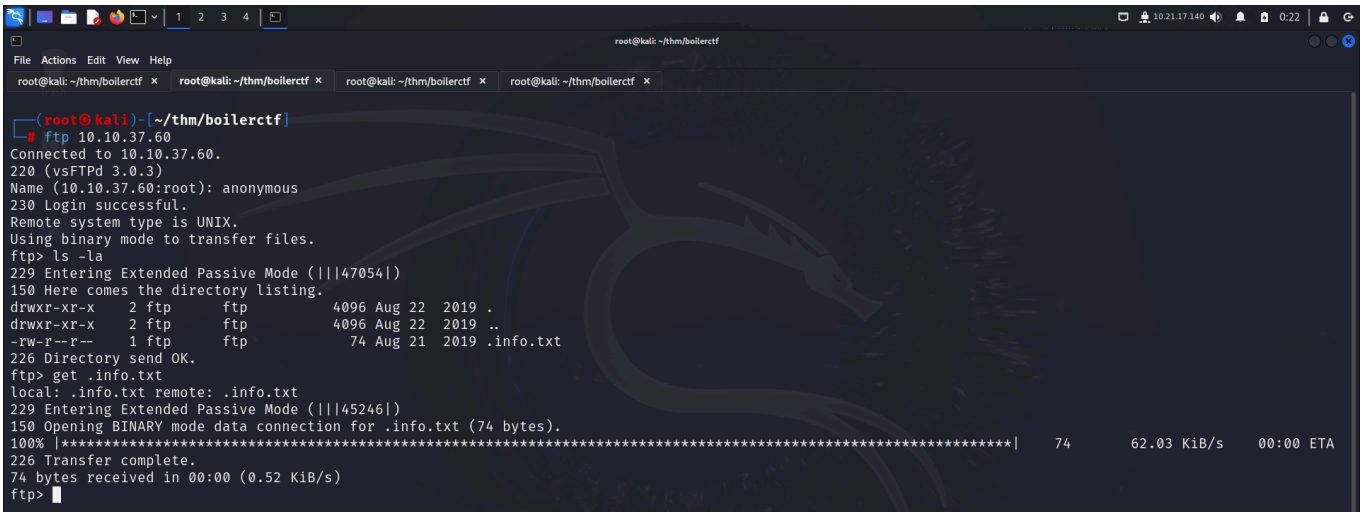
RECONNAISSANCE

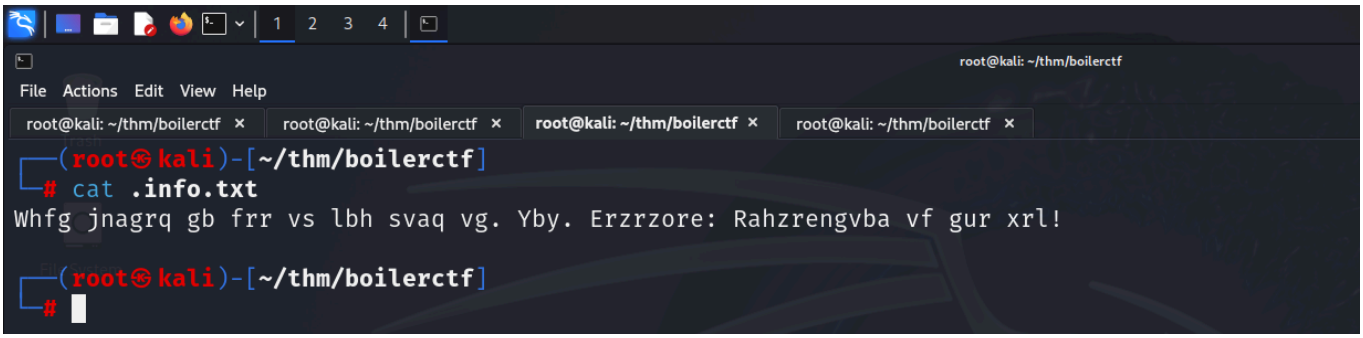
I performed an **nmap** aggressive scan to identify the open ports, services and run default script scan.



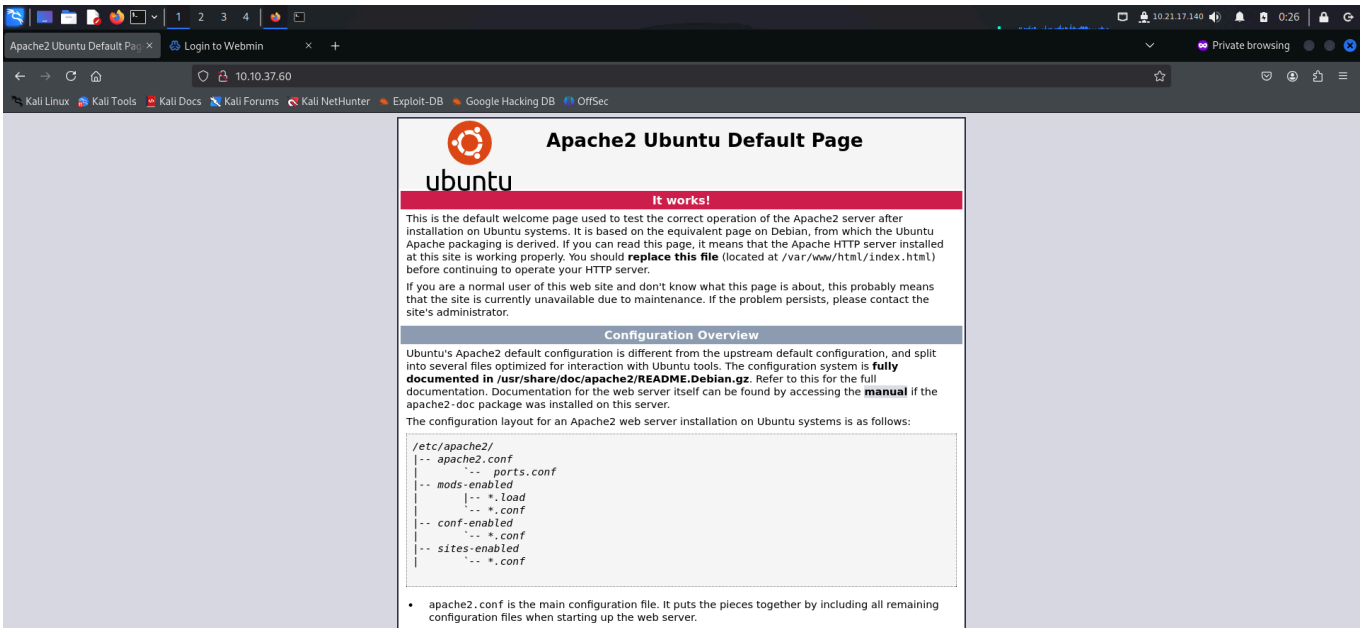
FOOTHOLD

I accessed the **ftp** server and found a txt file. I downloaded it and viewed the contents inside.

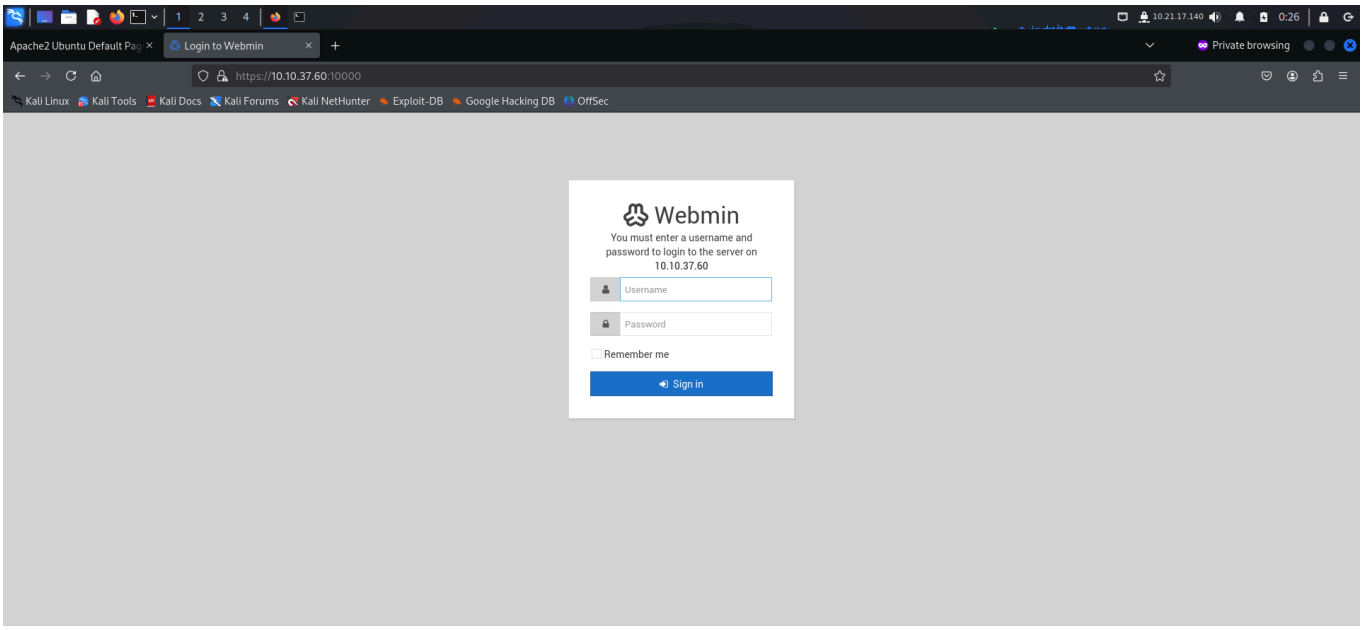




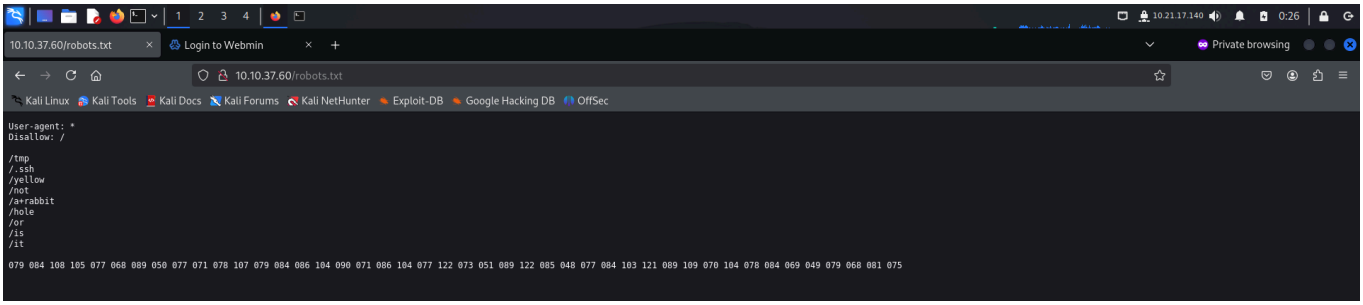
It was rot13. This decodes to `Just wanted to see if you find it. Lol. Remember: Enumeration is the key!`. I then accessed the web application on port 80 and 10000.



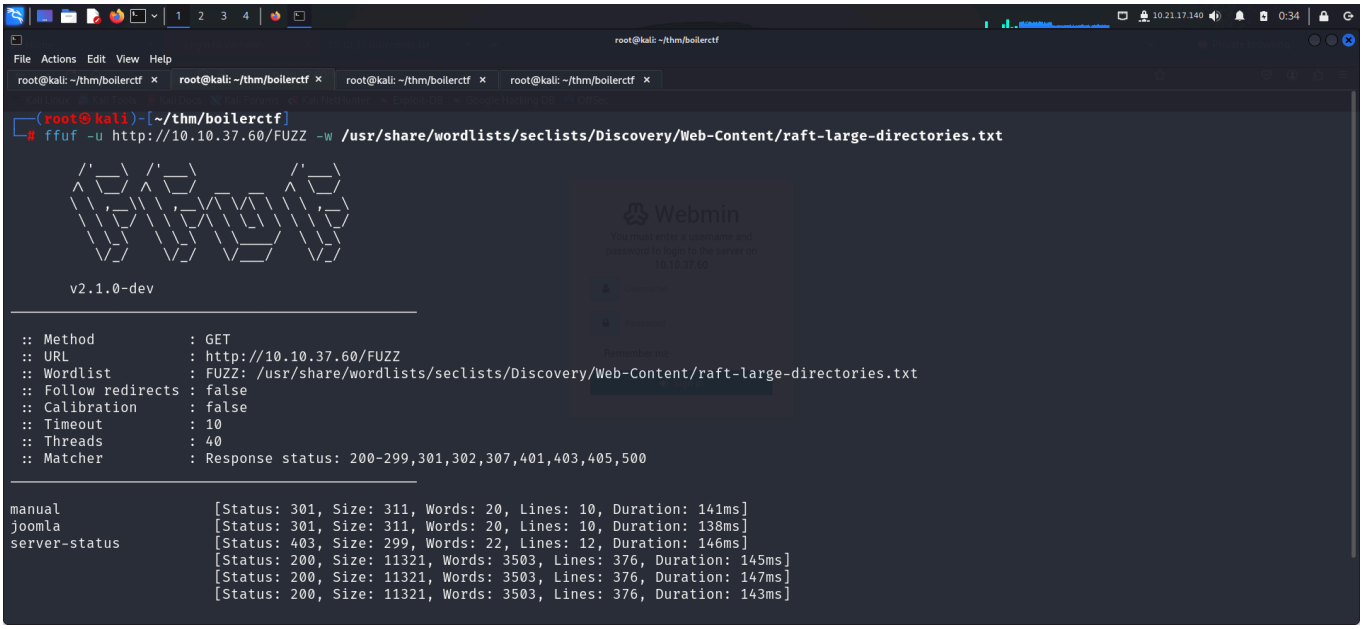
Port 10000 had a login panel.



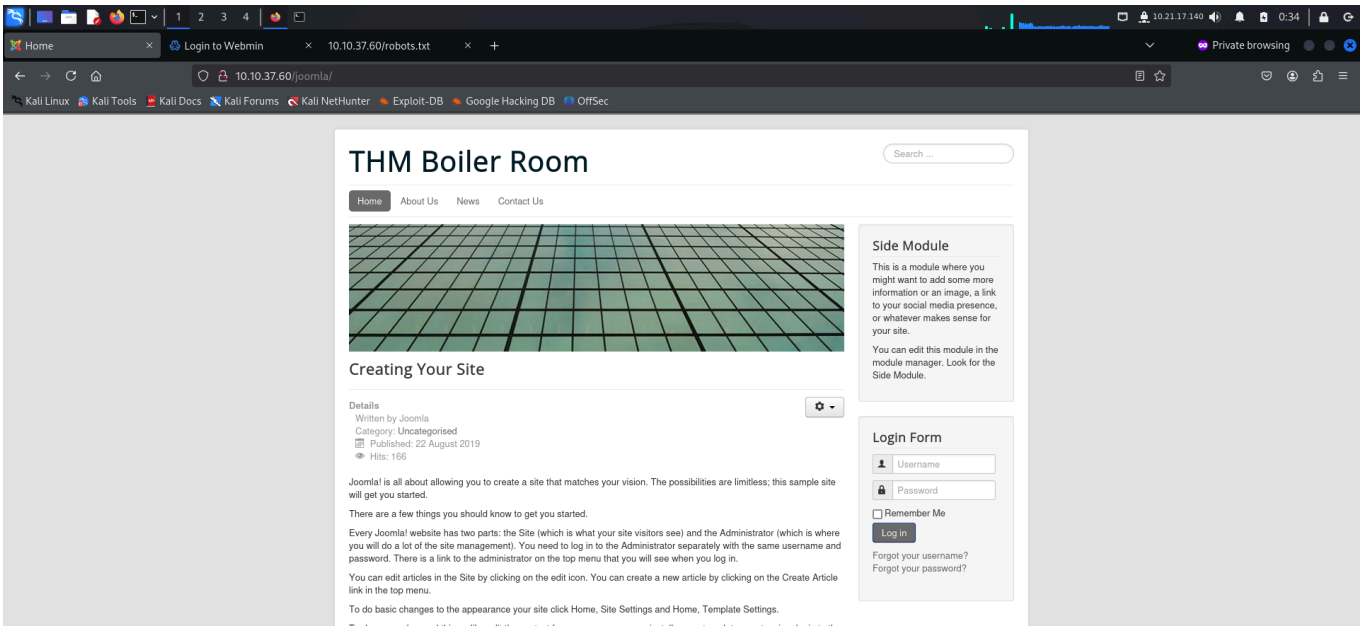
I then viewed *robots.txt* and found multiple endpoints.



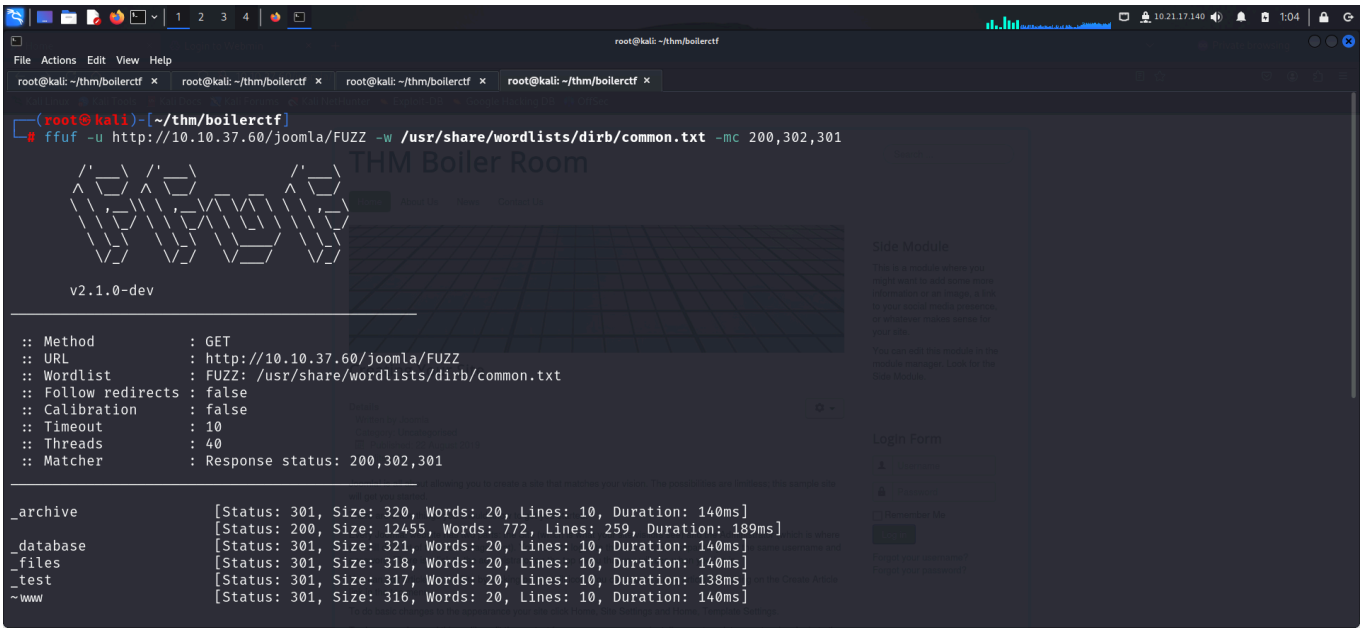
I also ran a directory bruteforce scan using **ffuf** to find more directories.

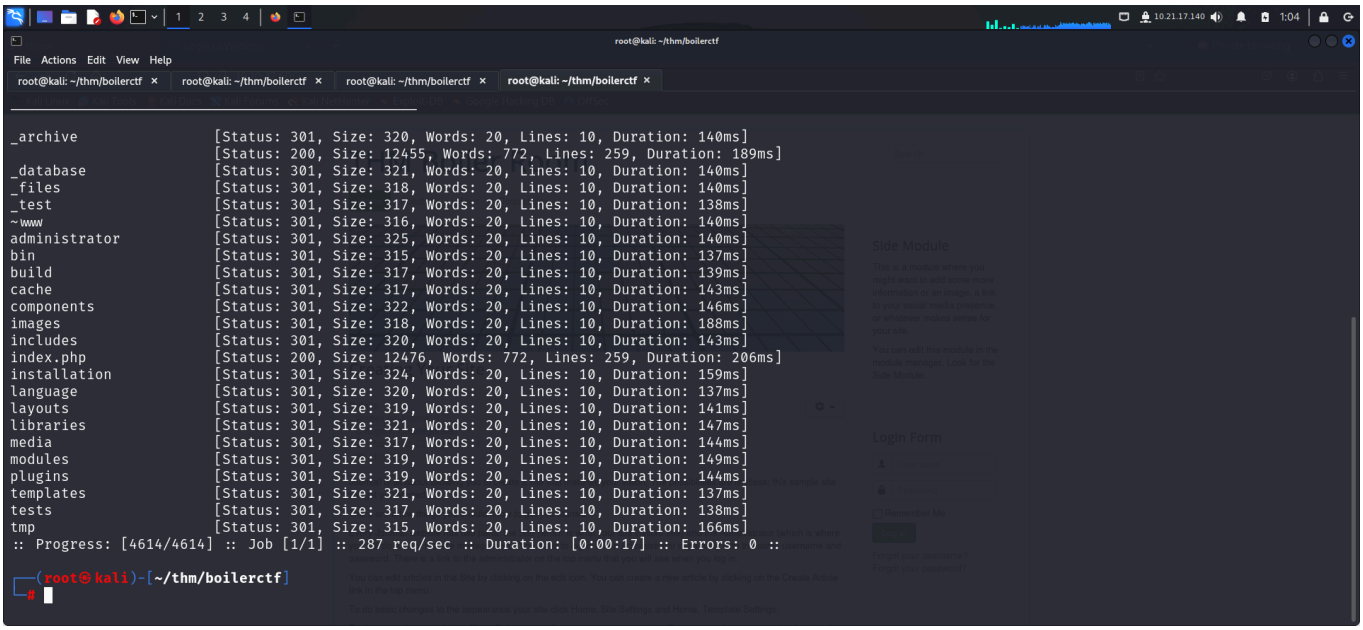


JOOMLA seemed interesting so I accessed it.



I bruteforced files present in the **joomla** directory.



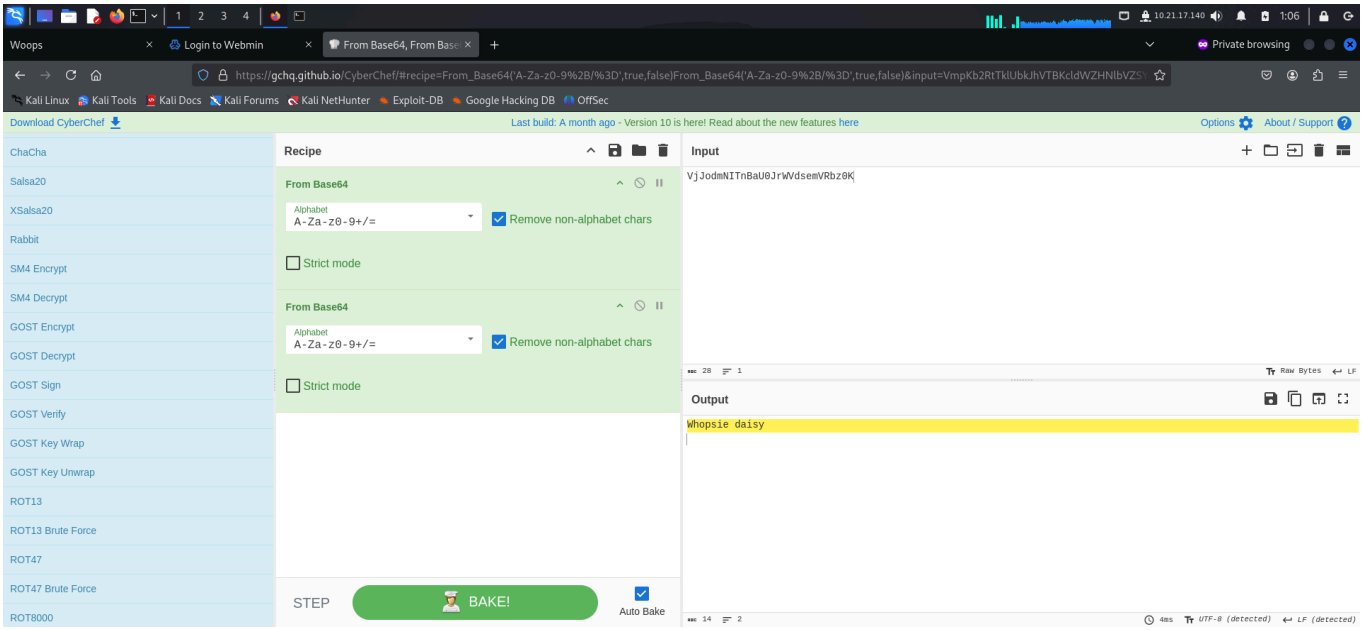


I viewed the different files present in the directory but found nothing interesting at first.

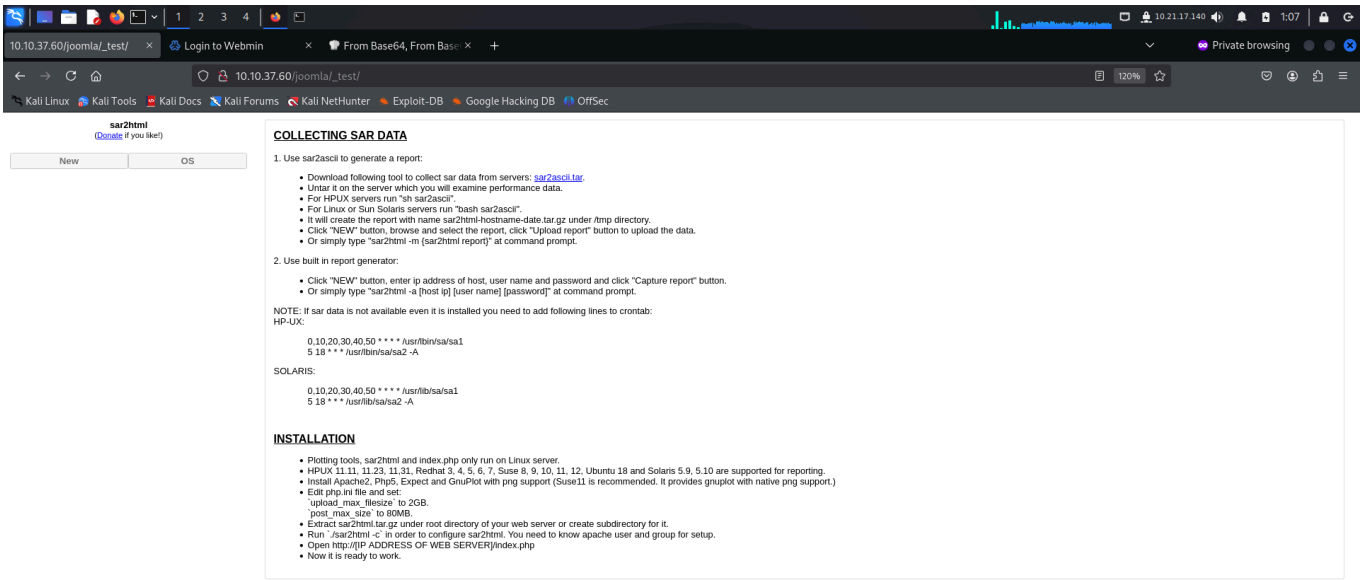
Mnope, nothin to see.

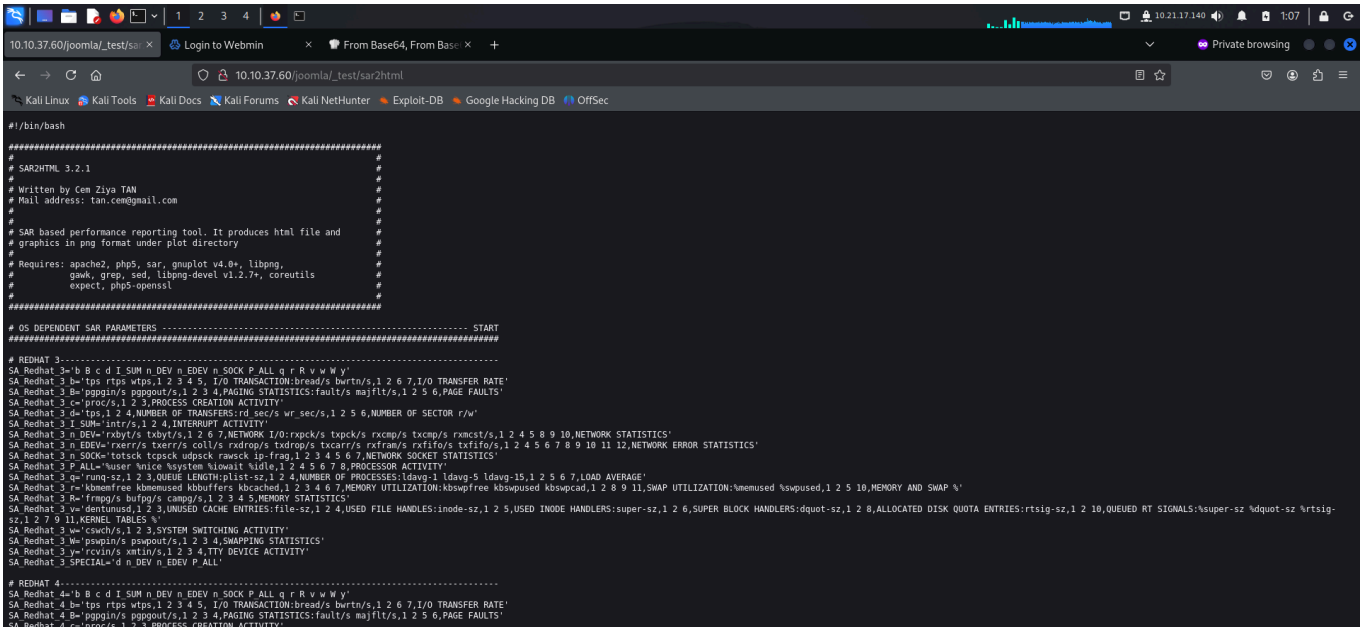
The `_files` endpoint had an encoded text. However, decoding it revealed nothing important.

VjJodmNITnBaU0JrWVdsemVRbz0K

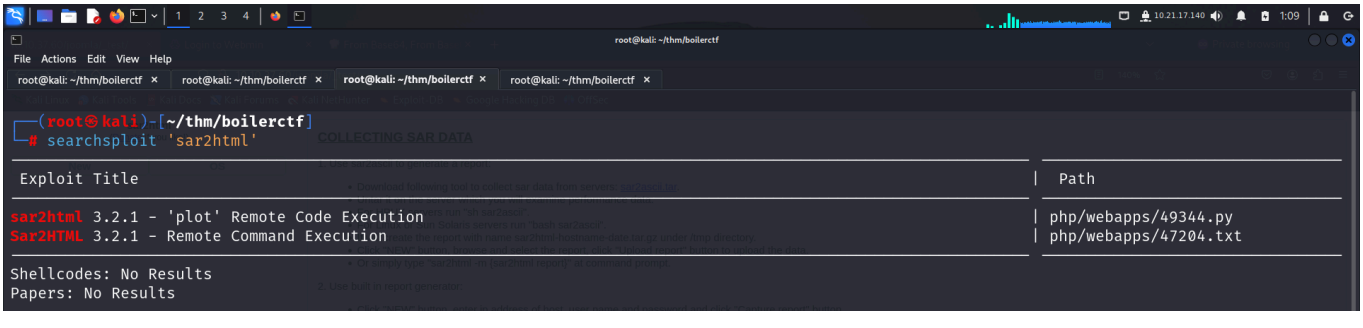


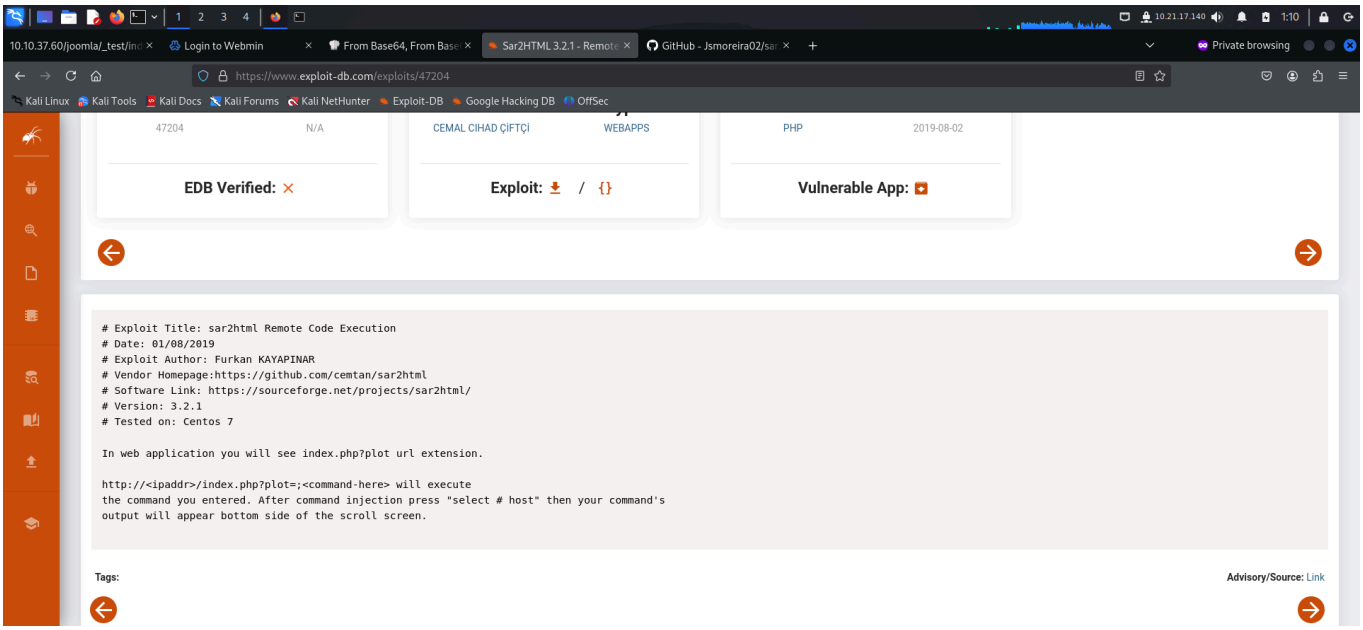
I continued looking at the files present in the *joomla* directory and found the version of a web based tool in the source code of `_test`.

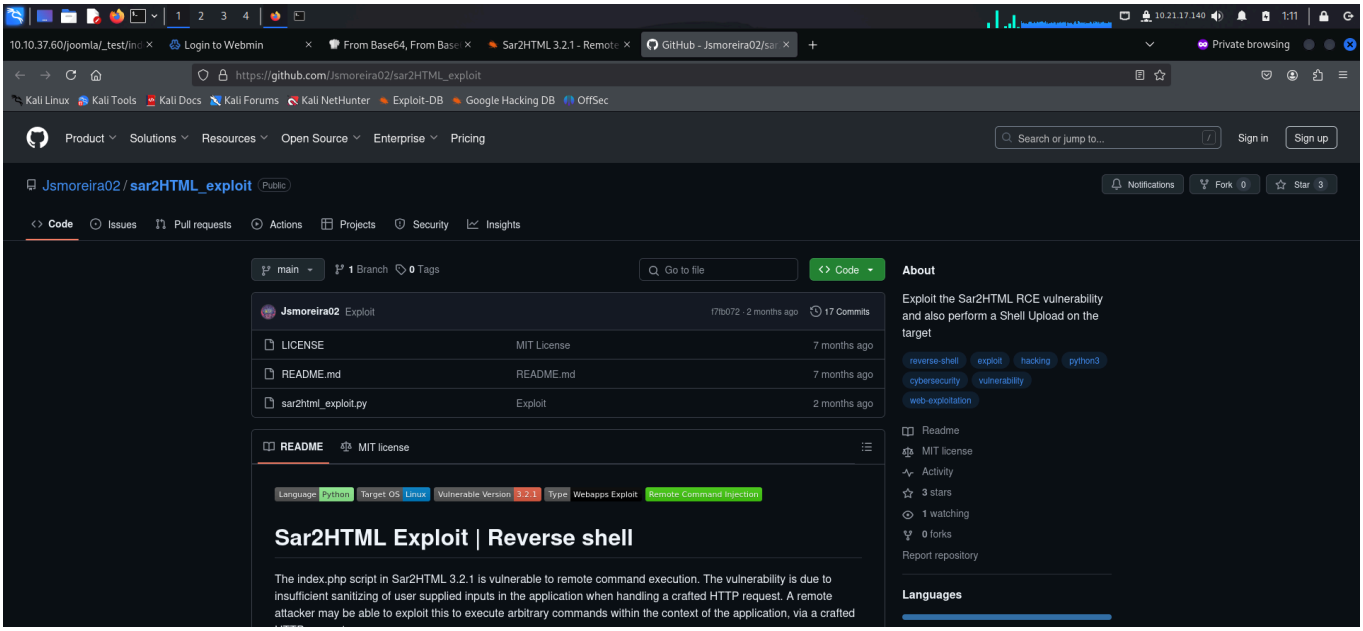




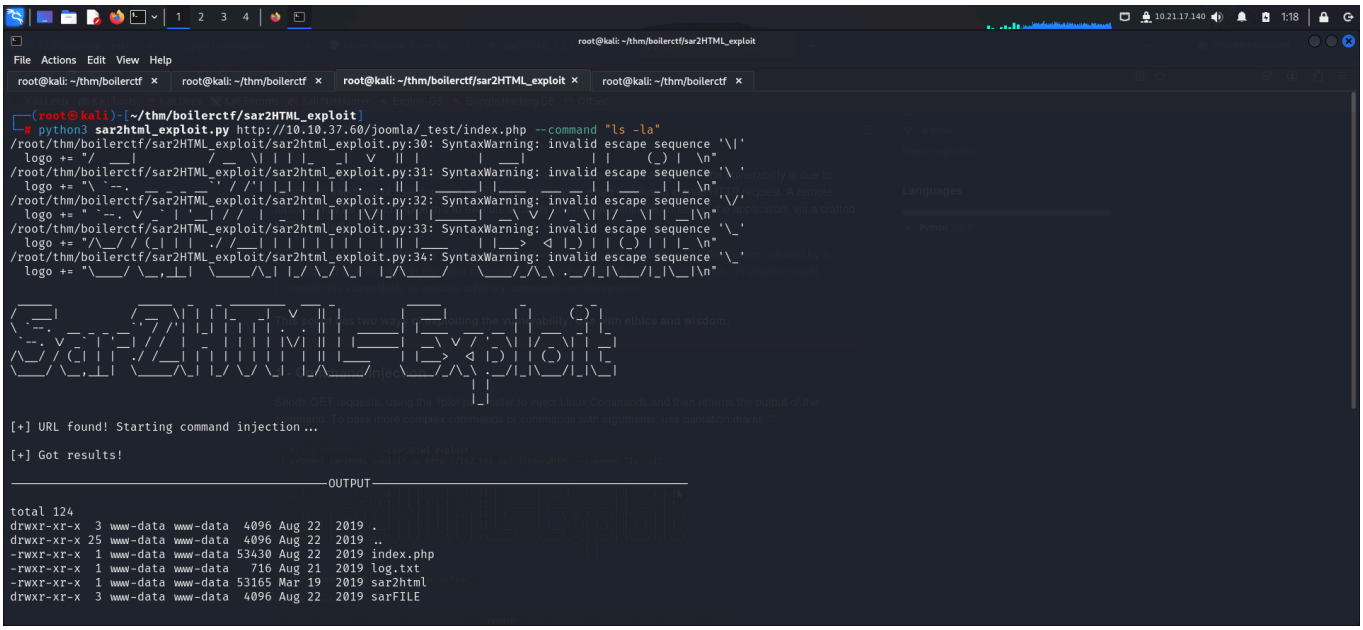
I looked for exploits and found an **RCE**.

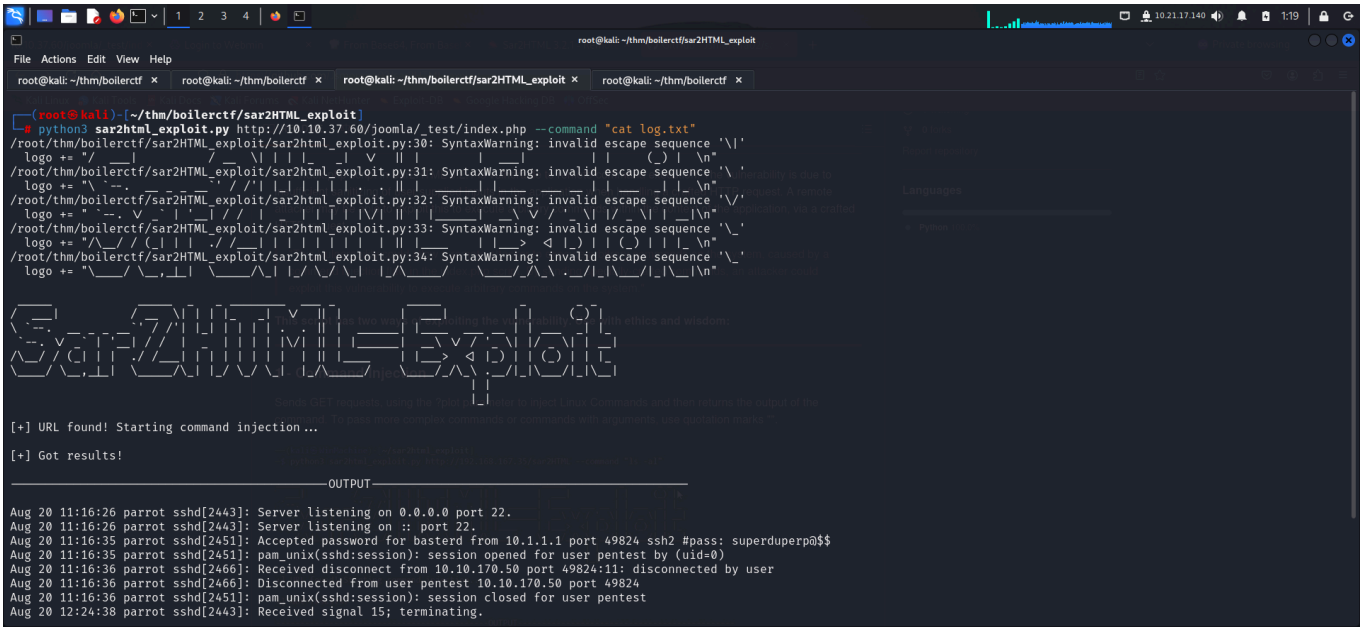




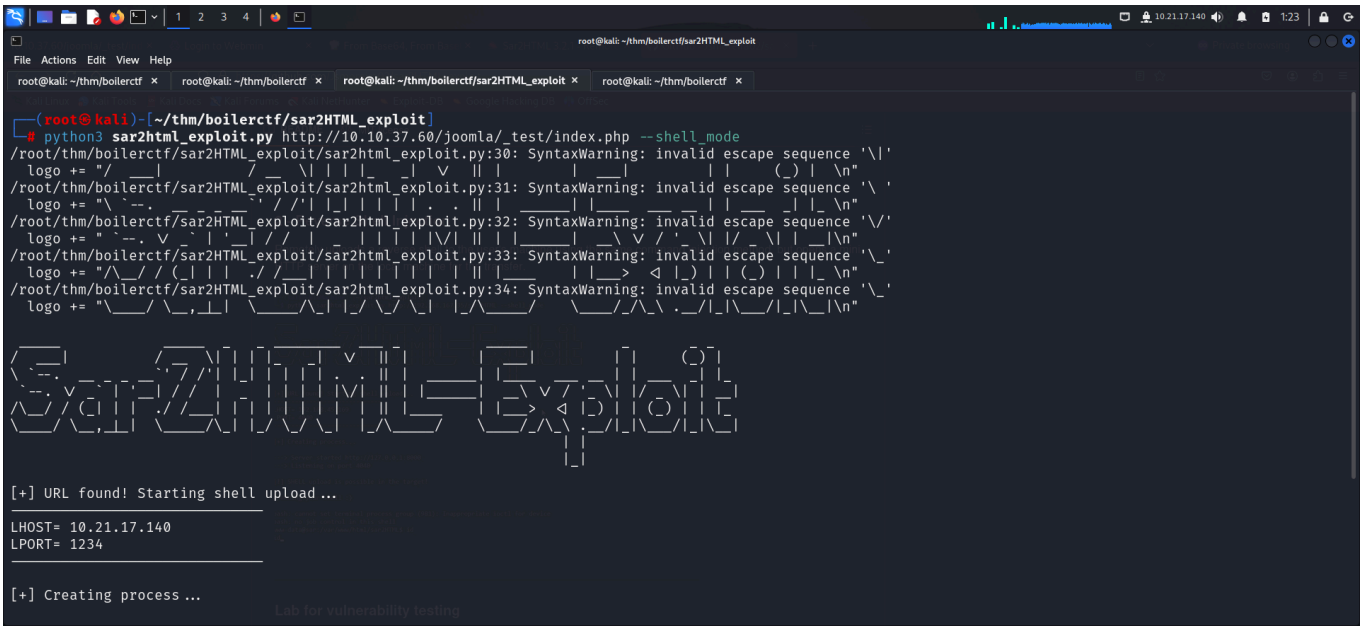


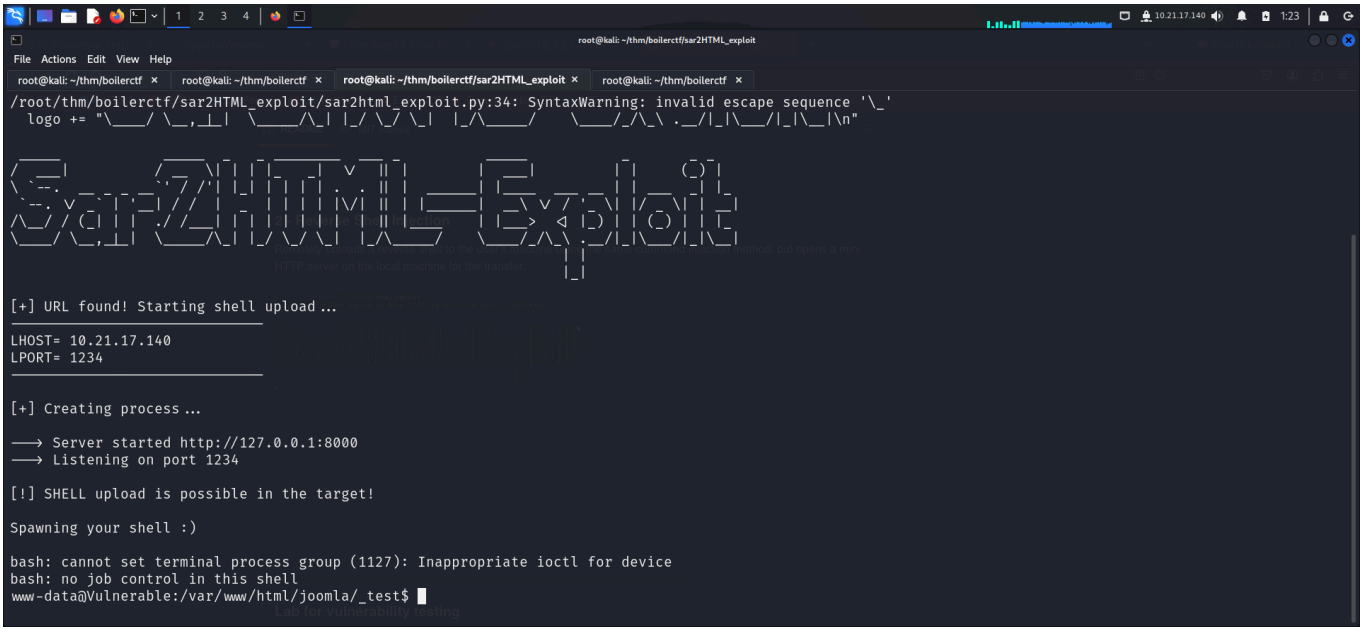
I used the exploit to execute os commands on the target and found the username and password of a user in the log file.





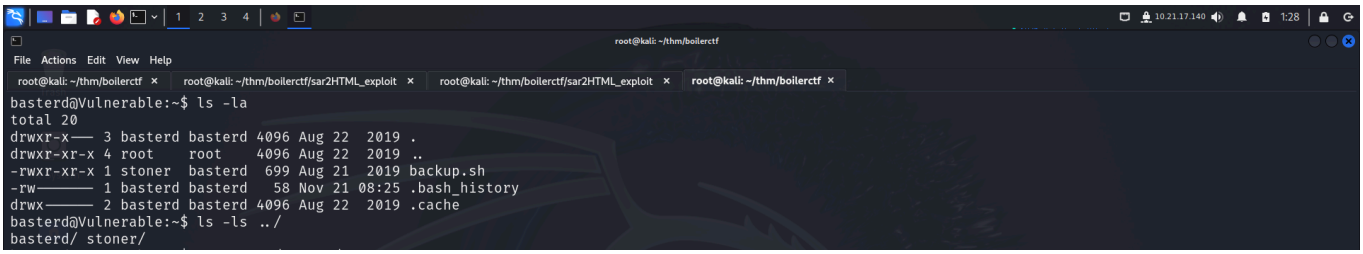
This exploit also allowed us to spawn an interactive shell as **www-data**.

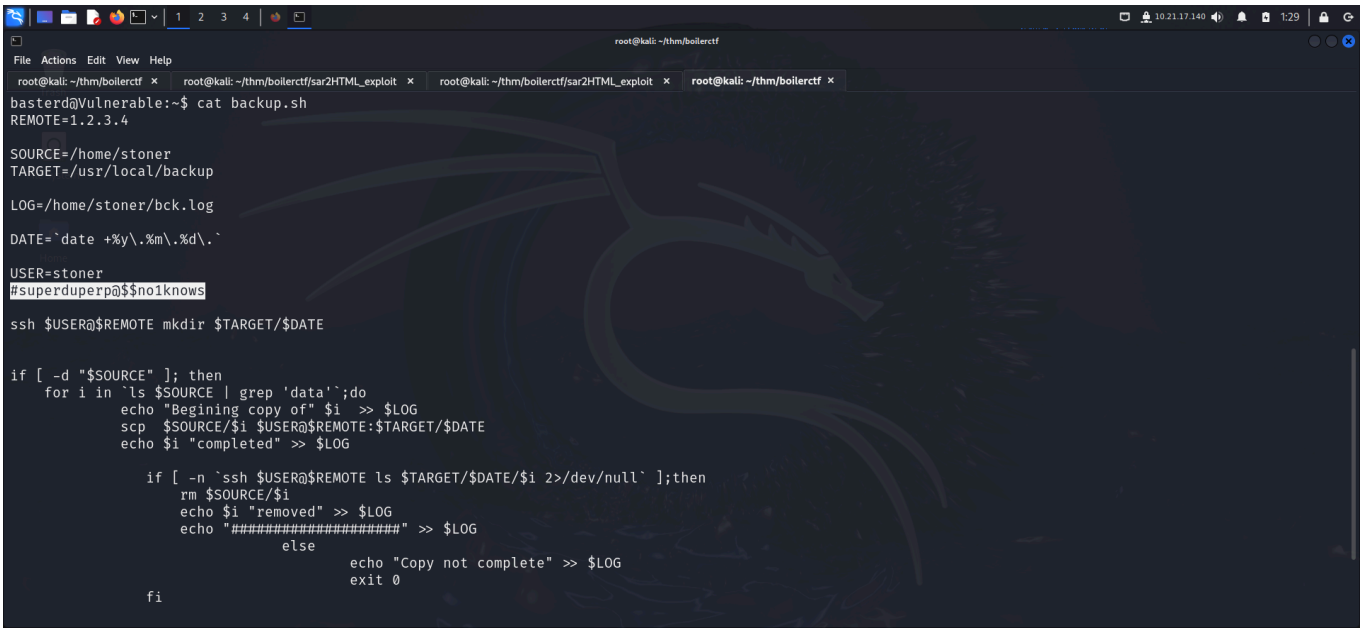




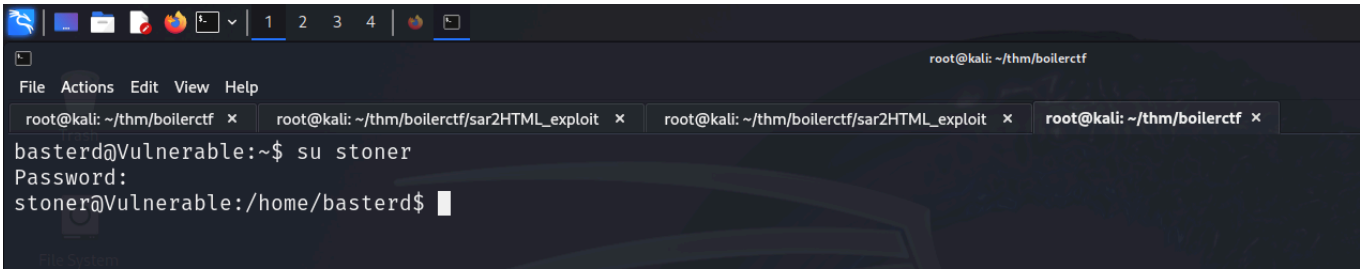
I used the credentials found from the log file to get shell access on the target and spawned a pty shell using **python**.

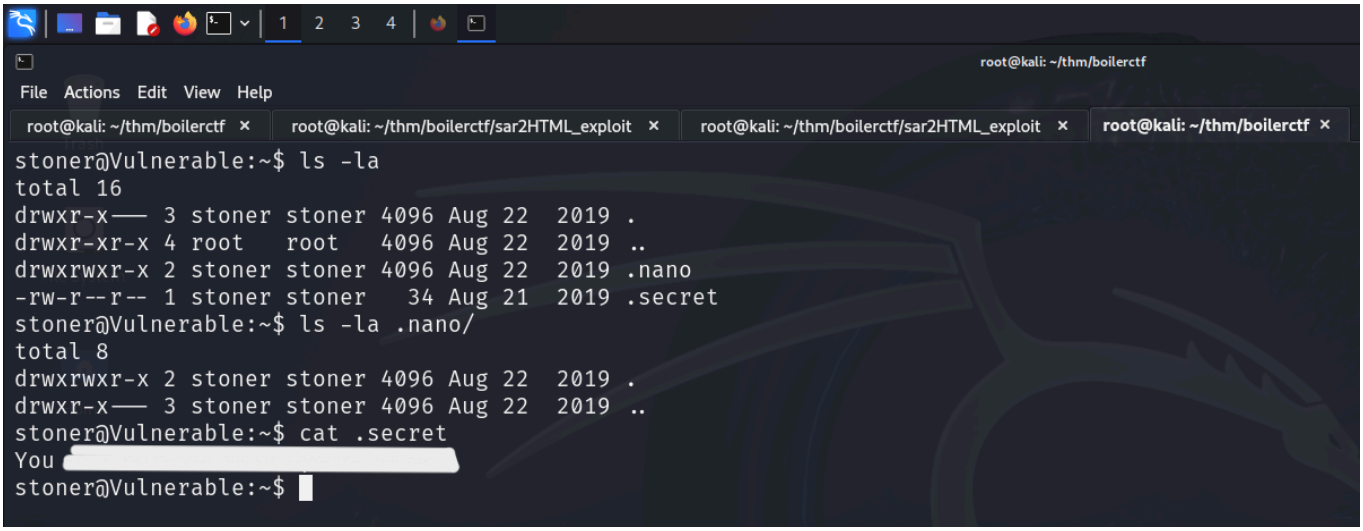
I analyzed the **backup.sh** script and found the credentials of another user.





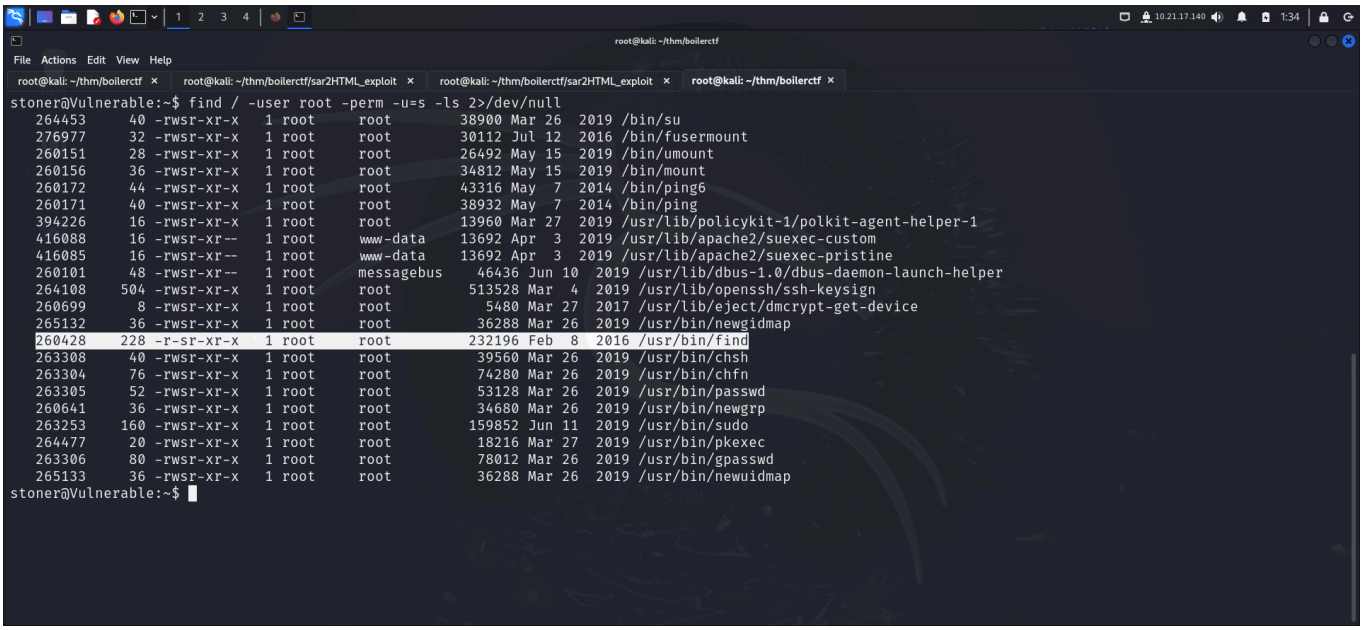
I quickly switched user and was able to capture the first flag from *stoner*'s home directory.



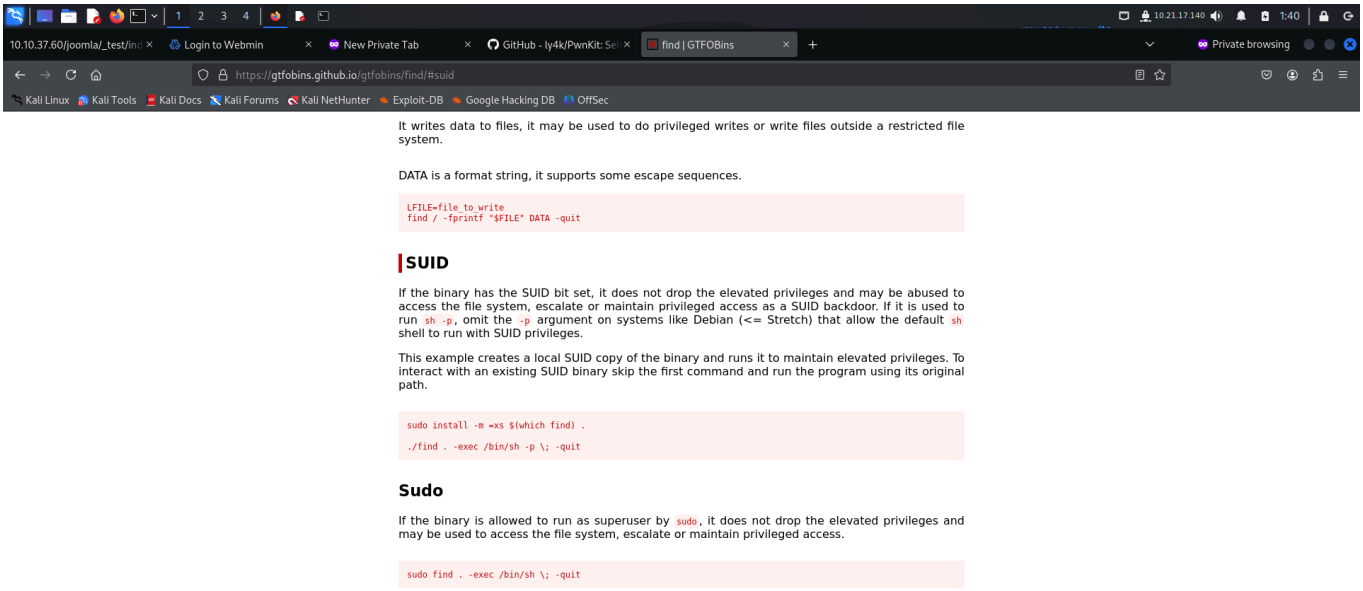


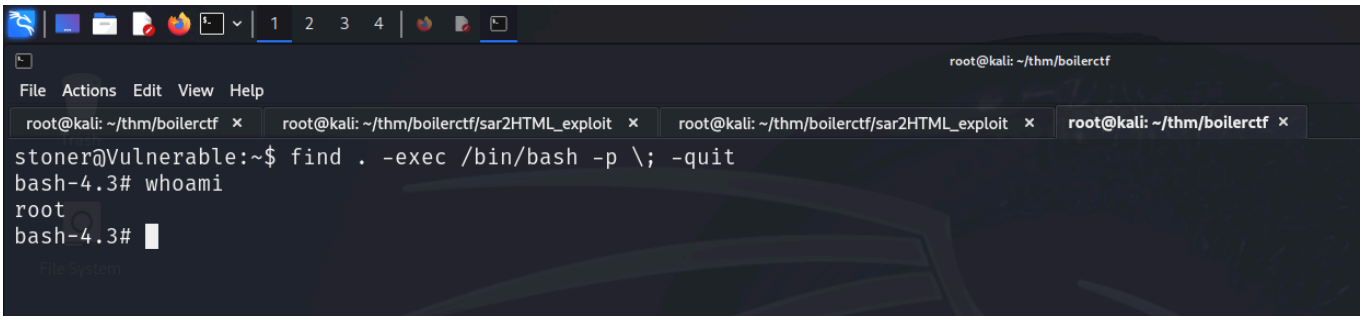
PRIVILEGE ESCALATION

I then looked for binaries with **suid** bit set and found the **find** command.

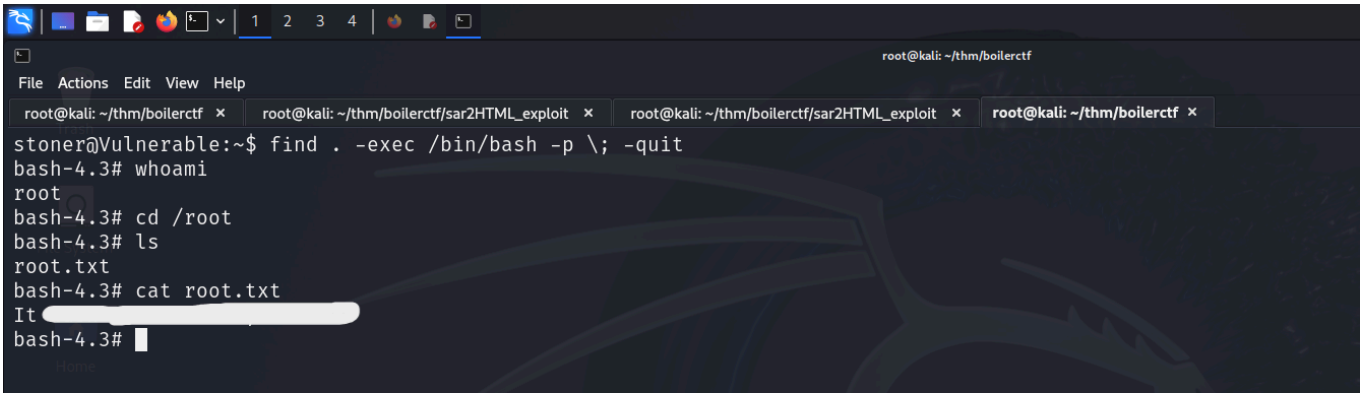


Since this was uncommon, I visited **gtfobins** and found a way to exploit this in order to get root access.





After getting root access, I was able to capture the root flag from the */root* directory.



That's it from my side :)
Happy hacking!