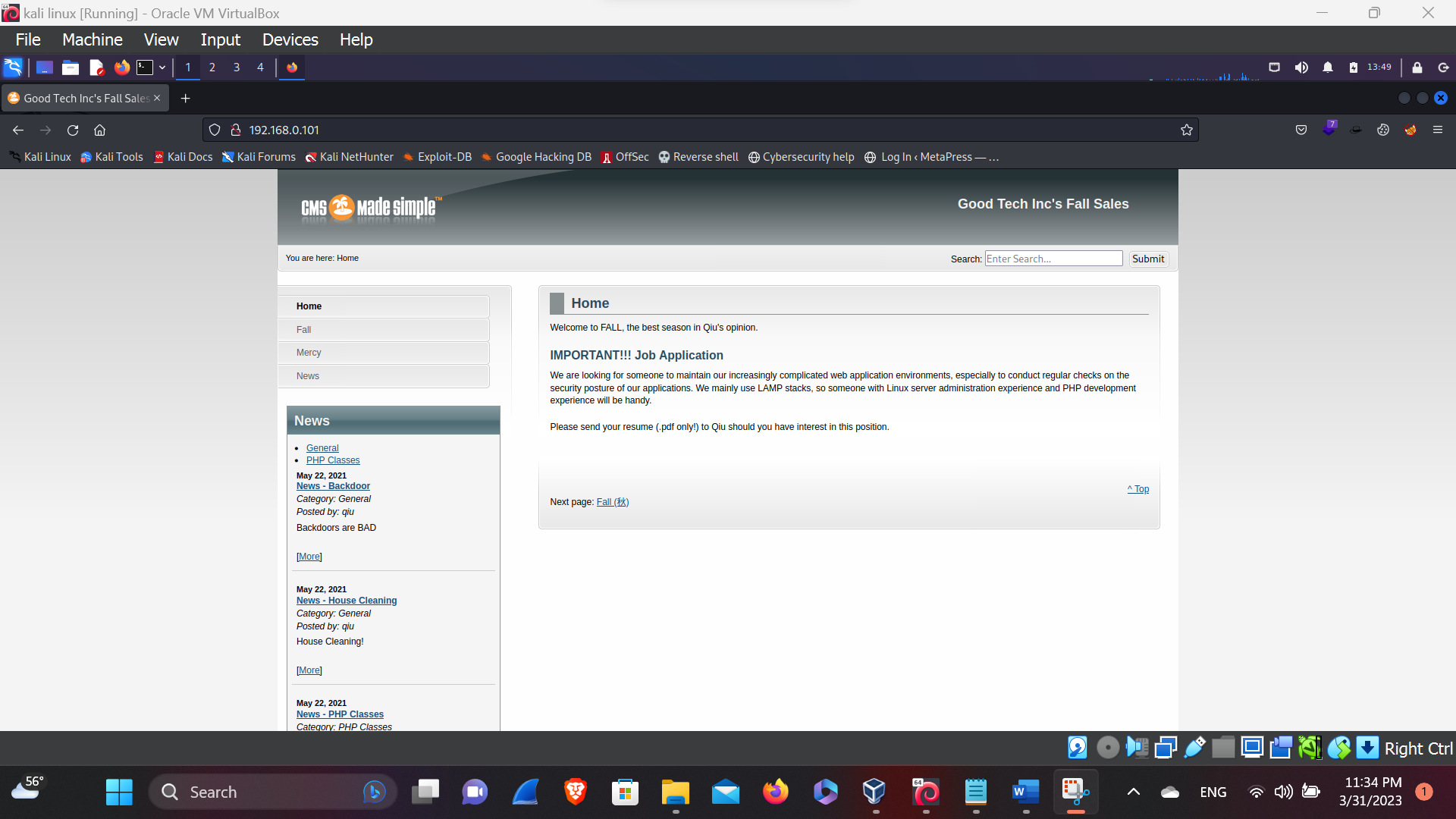
**FALL**

Fall is a simple website that post news and recently it has posted about the job vacancy.



Here, in this above picture we can see the simple website that posted news for the job vacancy.

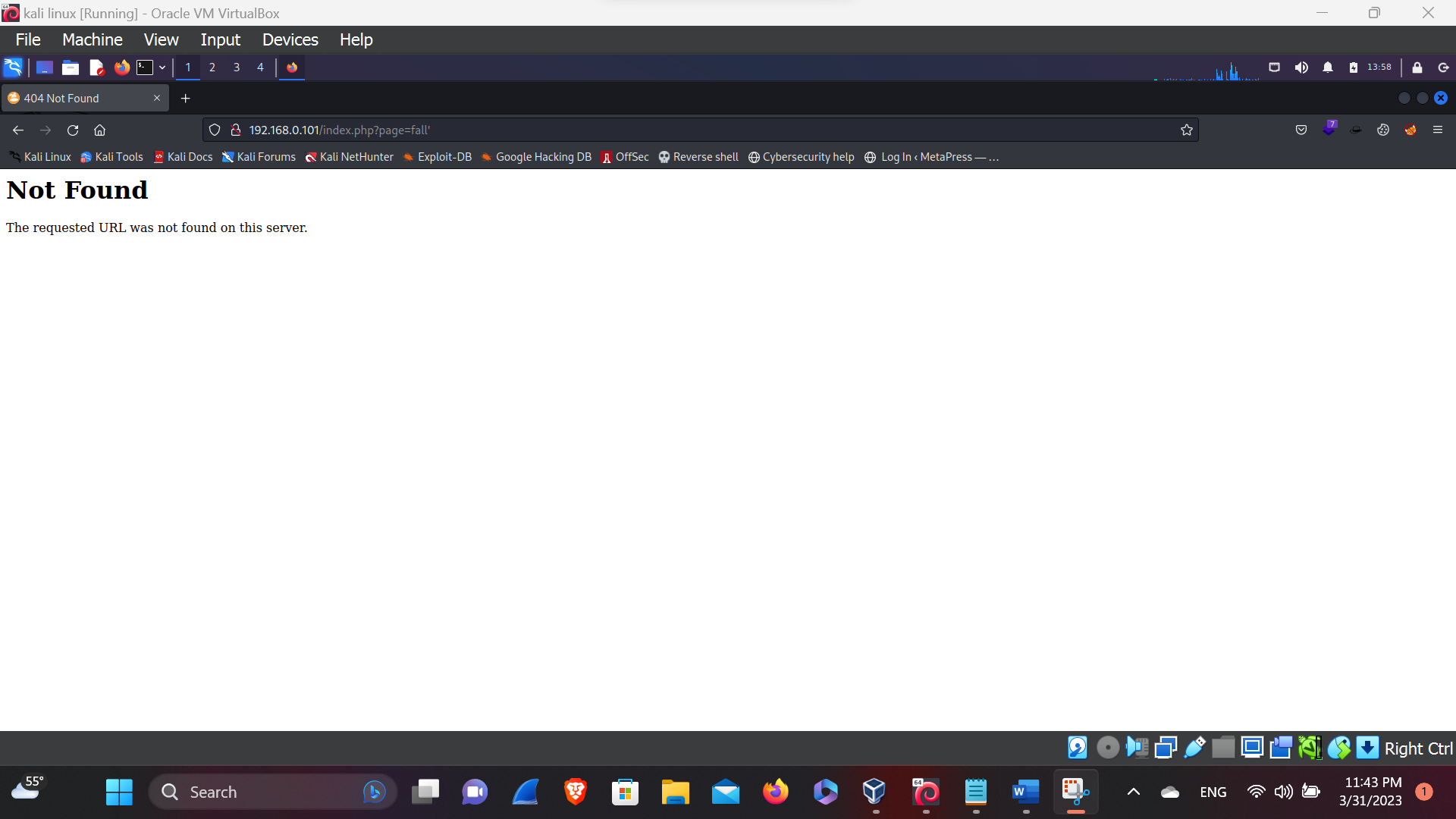
**BUG IMPACT**

Here, by simple job vacancy we can see they uses LAMP stacks, and using the operating system i.e. Linux, webserver (Apache), and they usage pHp for the development. We can see the URL bar by changing the new, the parameters and the hack value get changed, so lets try on the URL bar i.e. URL is given down,

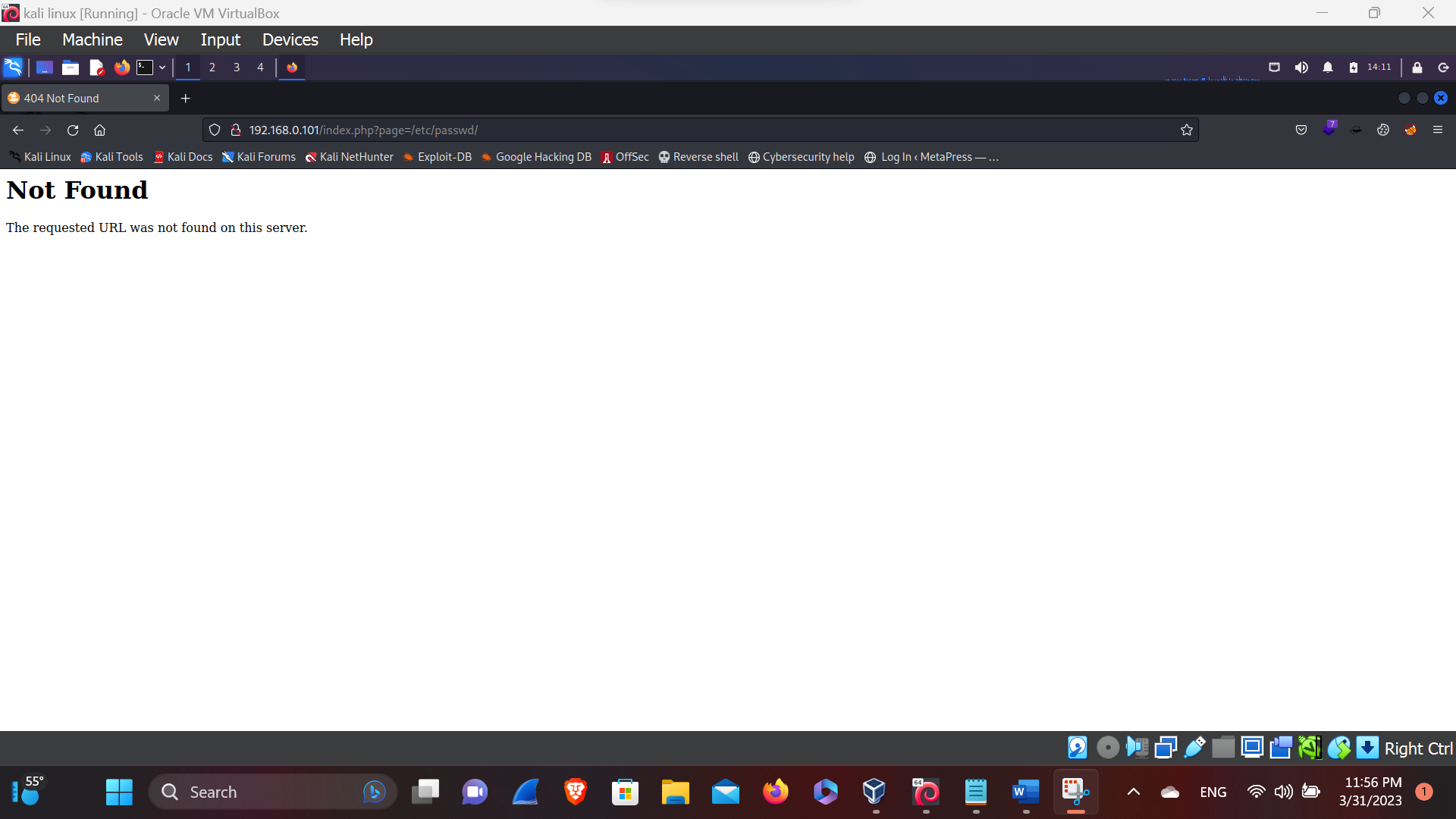
<http://192.168.0.101/index.php?page=fall>

Here, in this above link we can see the parameters provide that can controlled and can be affected by the **Bug Impact** i.e.

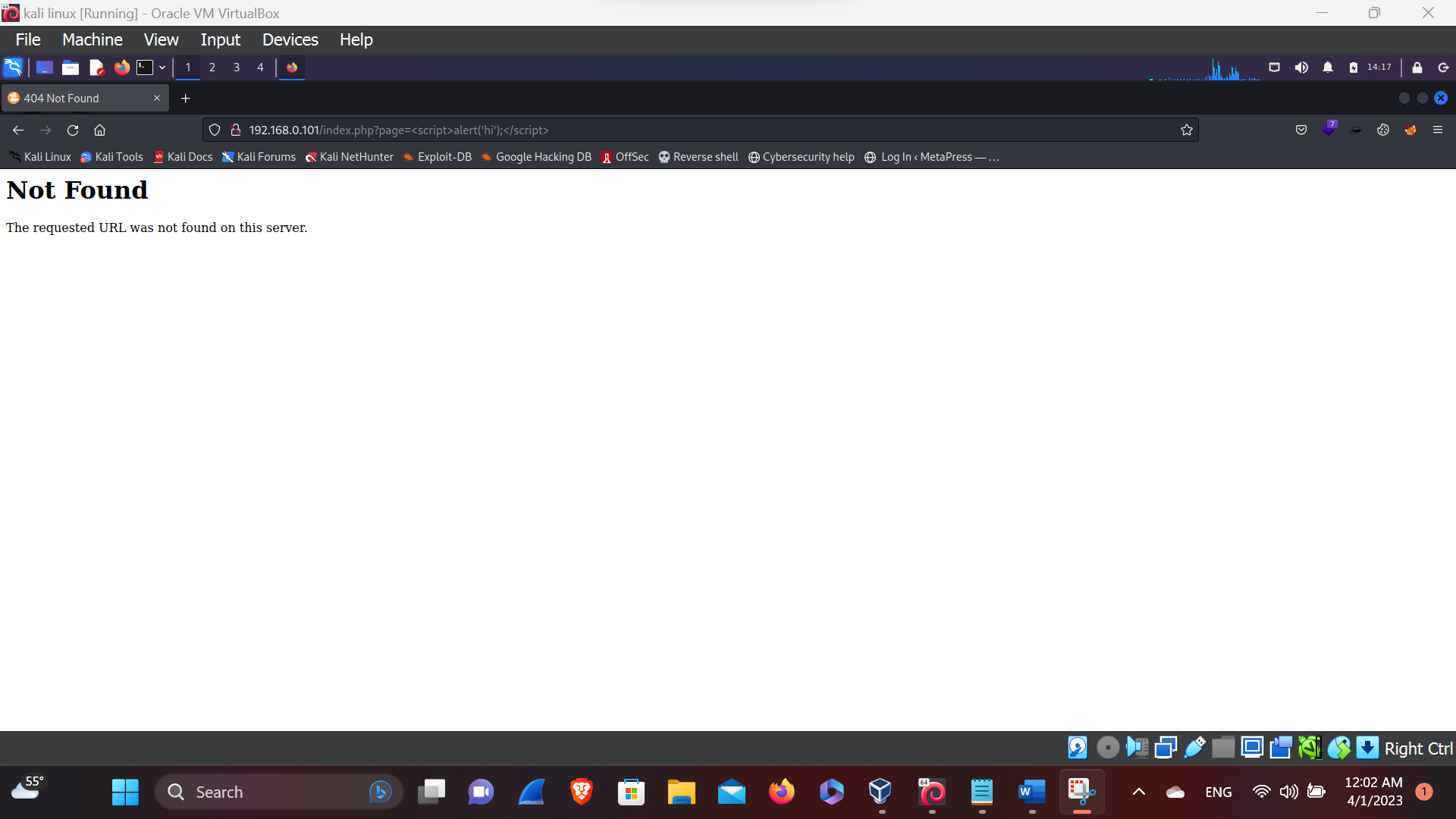
* SQL Injection
* LFI – Local File Inclusion
* Directory Transversal
* XSS to Session hijacking
* RCE – Remote Code Execution

So, let’s try for the SQL injection in the given parameters:

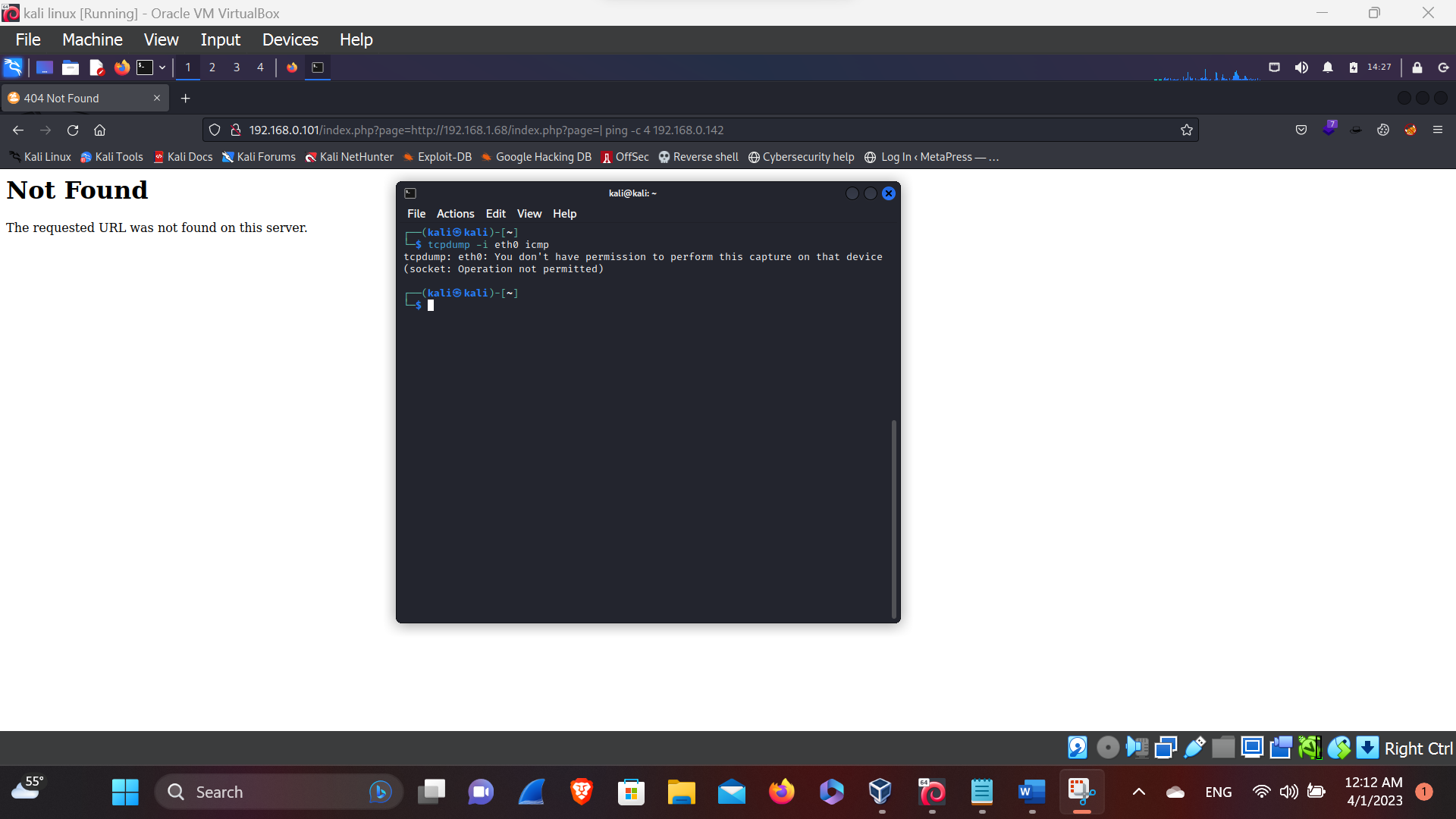
Here, we have tested for the SQL injection by cross checking the parameters (by putting (‘) in the parameters). We’ve found the static page i.e. page not found, it means there is no impact of bug, so let’s try another bug.

 **LFI – Local File Inclusion**

Here, in this above picture while using the LFI payloads (i.e. /etc/passwd), we’ve found that the page could not be found so, let’s try another one, in the URL bar that has been changed through it’s parameter and the value has been also changed.

**XSS (Cross-site Scripting)**

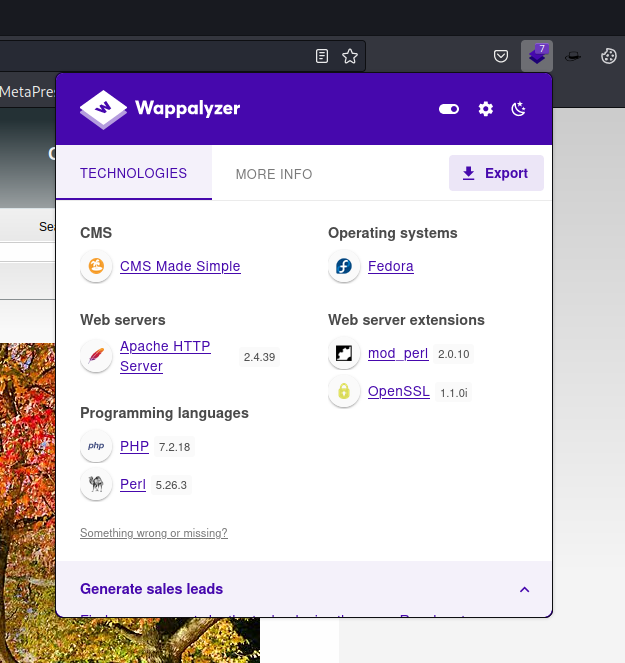
Here, in this above picture while using the XSS payloads (i.e. <script>alert('hi');</script>) we’ve found that the page could not be found so, let’s try another one, in the URL bar that has been changed through it’s parameter and the value has been also changed.

**RCE – Remote Code Execution**

Here, in this above picture we’ve not found anything we have cross checked for the RCE connection ( i.e. <http://192.168.0.101/index.php?page=http://192.168.1.68/index.php?page=|%20ping%20-c%204%20192.168.0.142>) so,

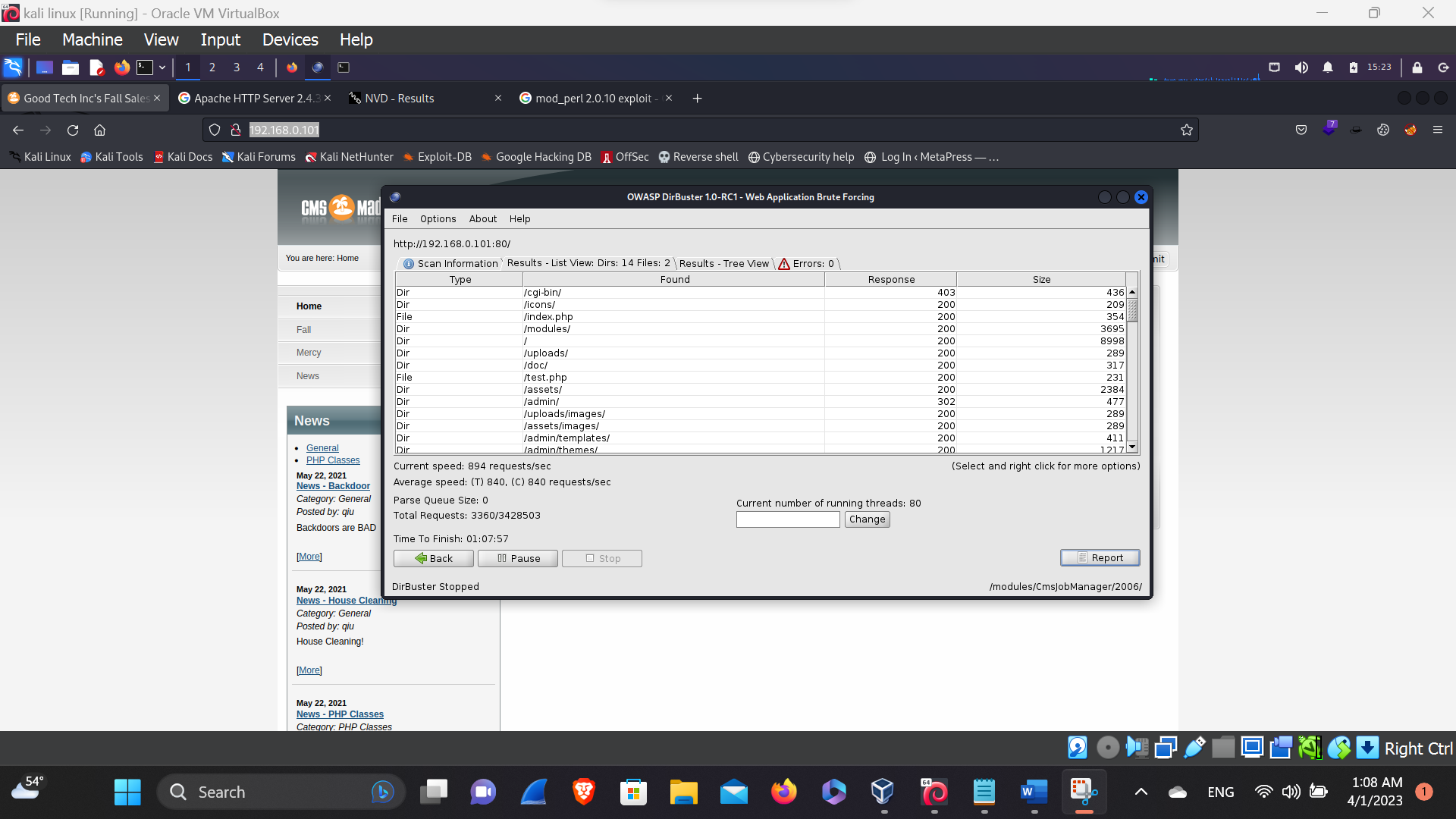
Here we haven’t found anything that really impacts the website so let’s see the version of the Technology through wappalyzer.

**Wappalyzer**

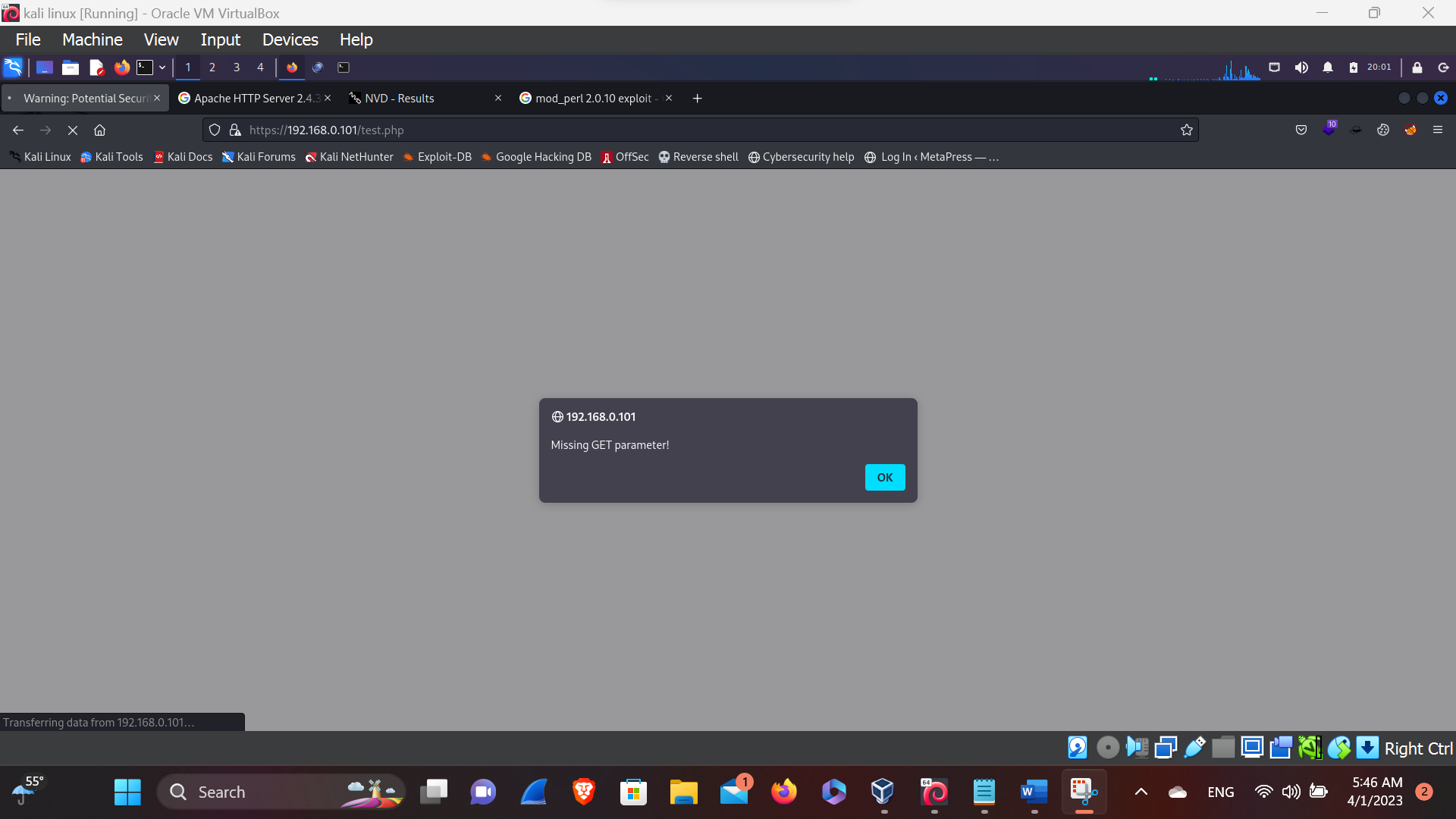


Here, in this above picture we’ve found the Technology version so, let’s

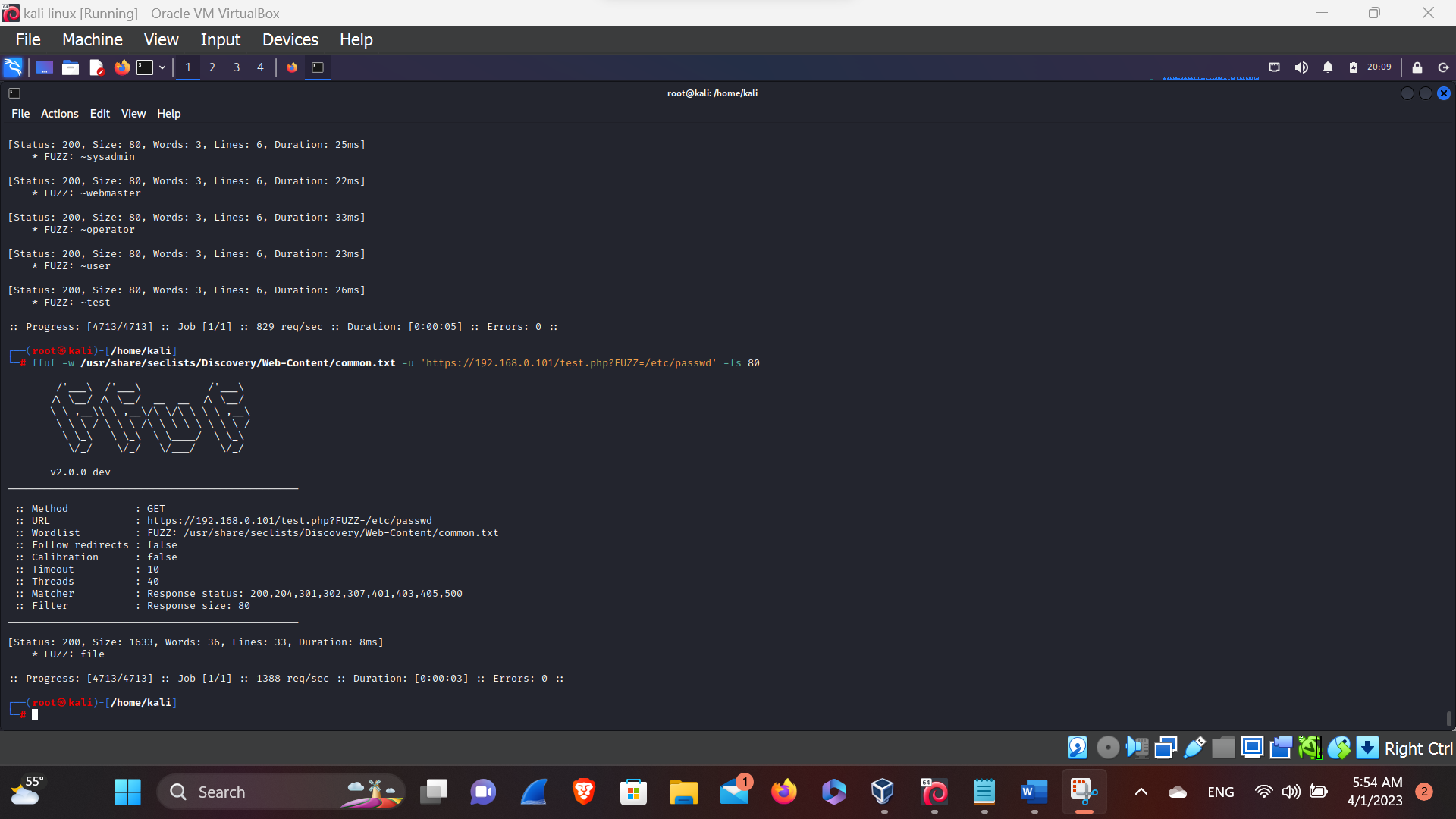
Search for the exploit of the given version of the technology through searching in the google.

**Dirbuster**

Here, in this given picture we’ve searched for the hidden directories and now by searching the hidden directories we’ve found the test page let’s test that page.

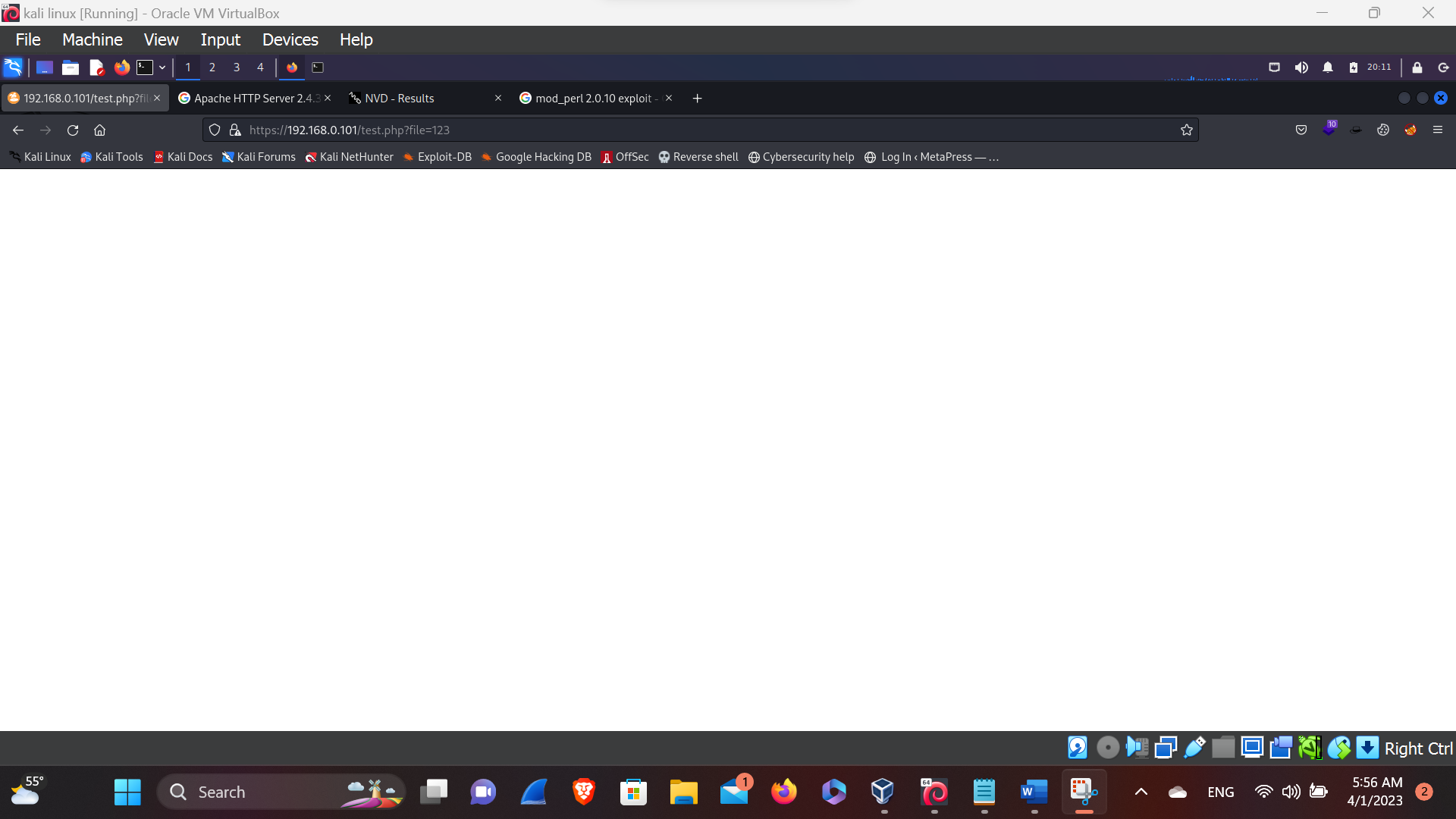
**Test.php**

Here, in the above picture we have found the test page and after putting the test page it shows that this test page is missing his parameters so, let’s try to find out the parameter of the test page.

**FFUF**

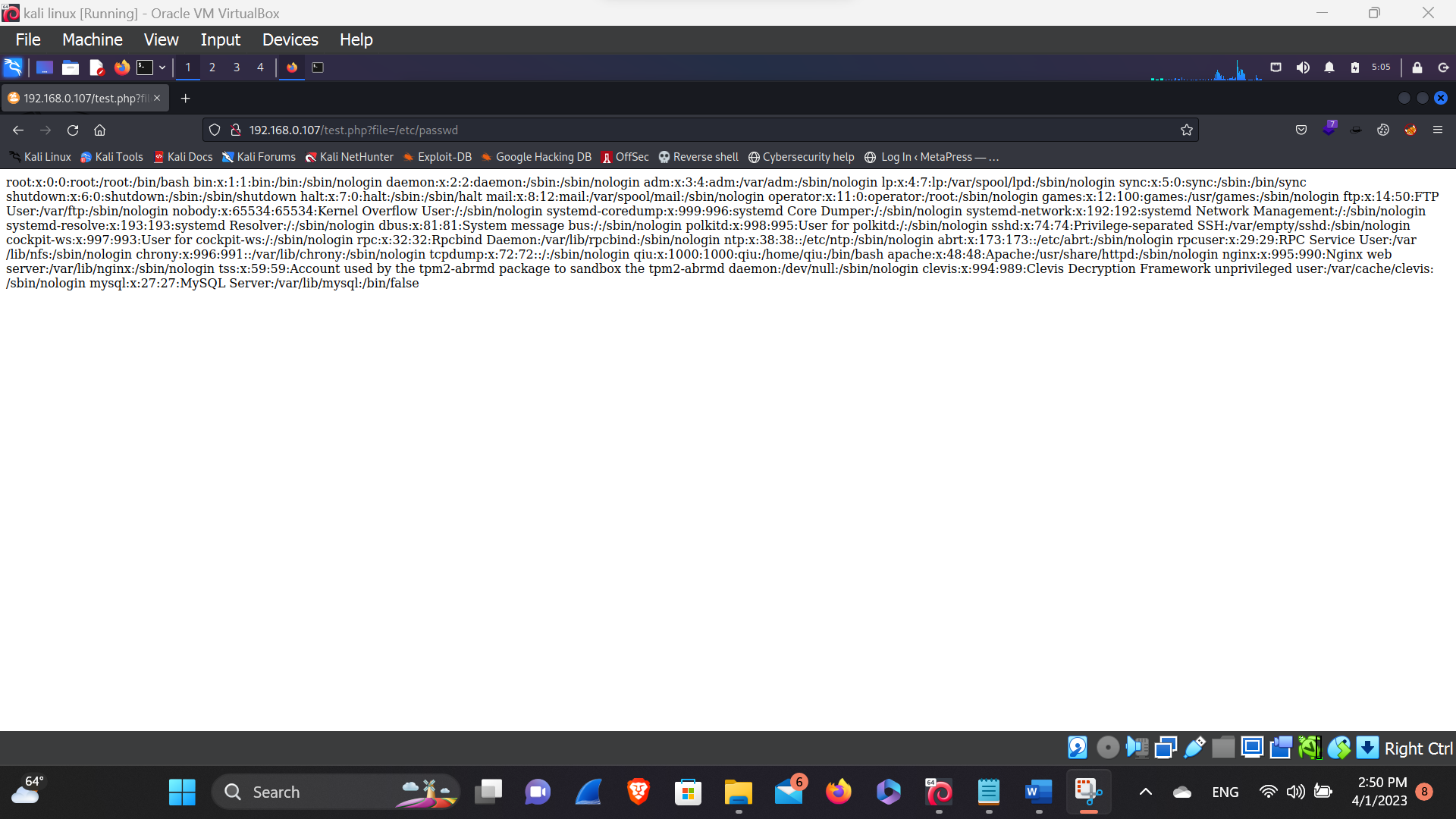
Here, in this above picture we’ve found the parameter i.e. file so, lets go and put in in the browser.

Website parameters has been updated still, we can test for the bug impact.

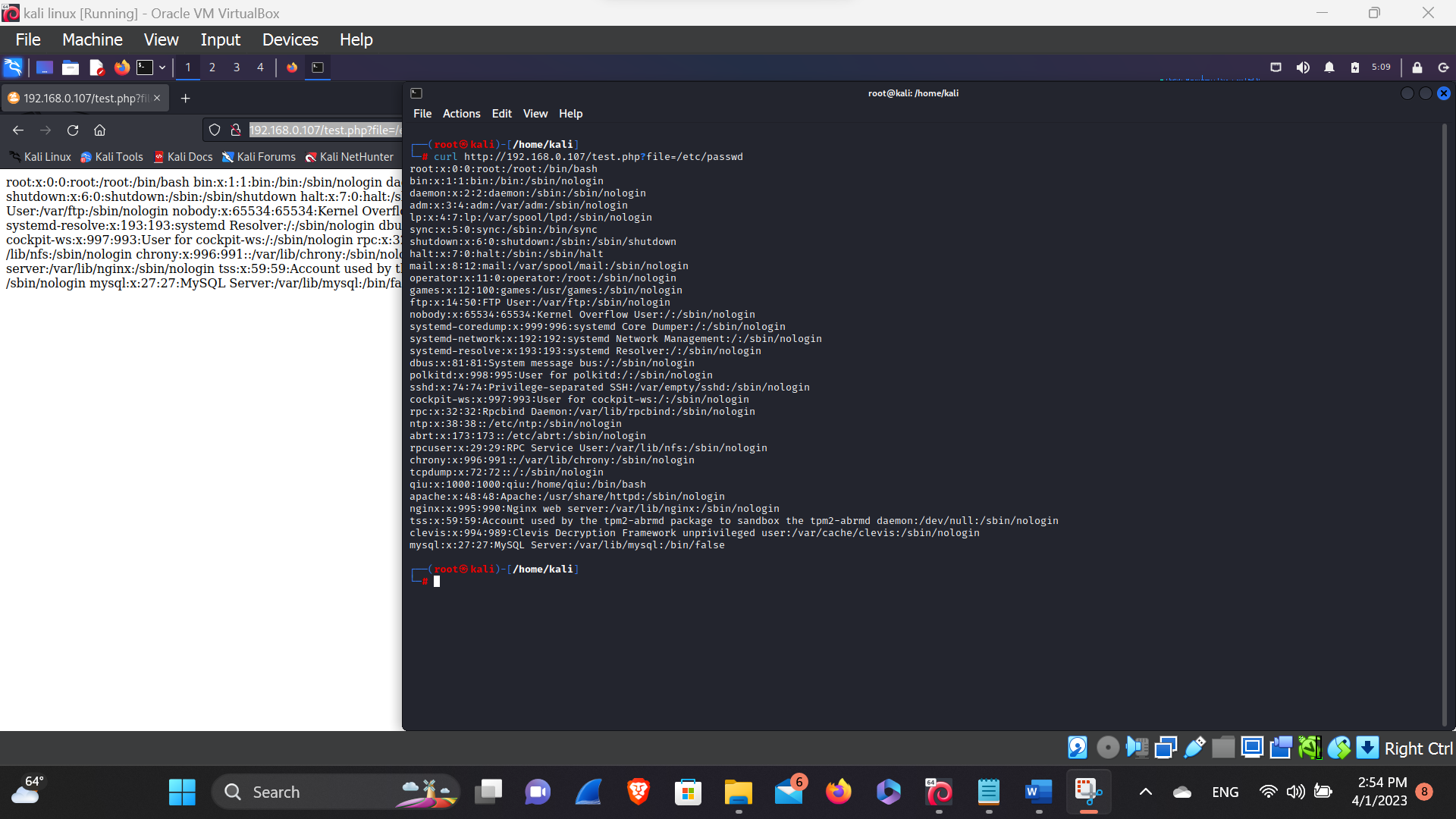


Here in this above picture we can find that the parameters are fine, so lets try for the bug impact, if exist.

**LFI -Local file Inclusion**

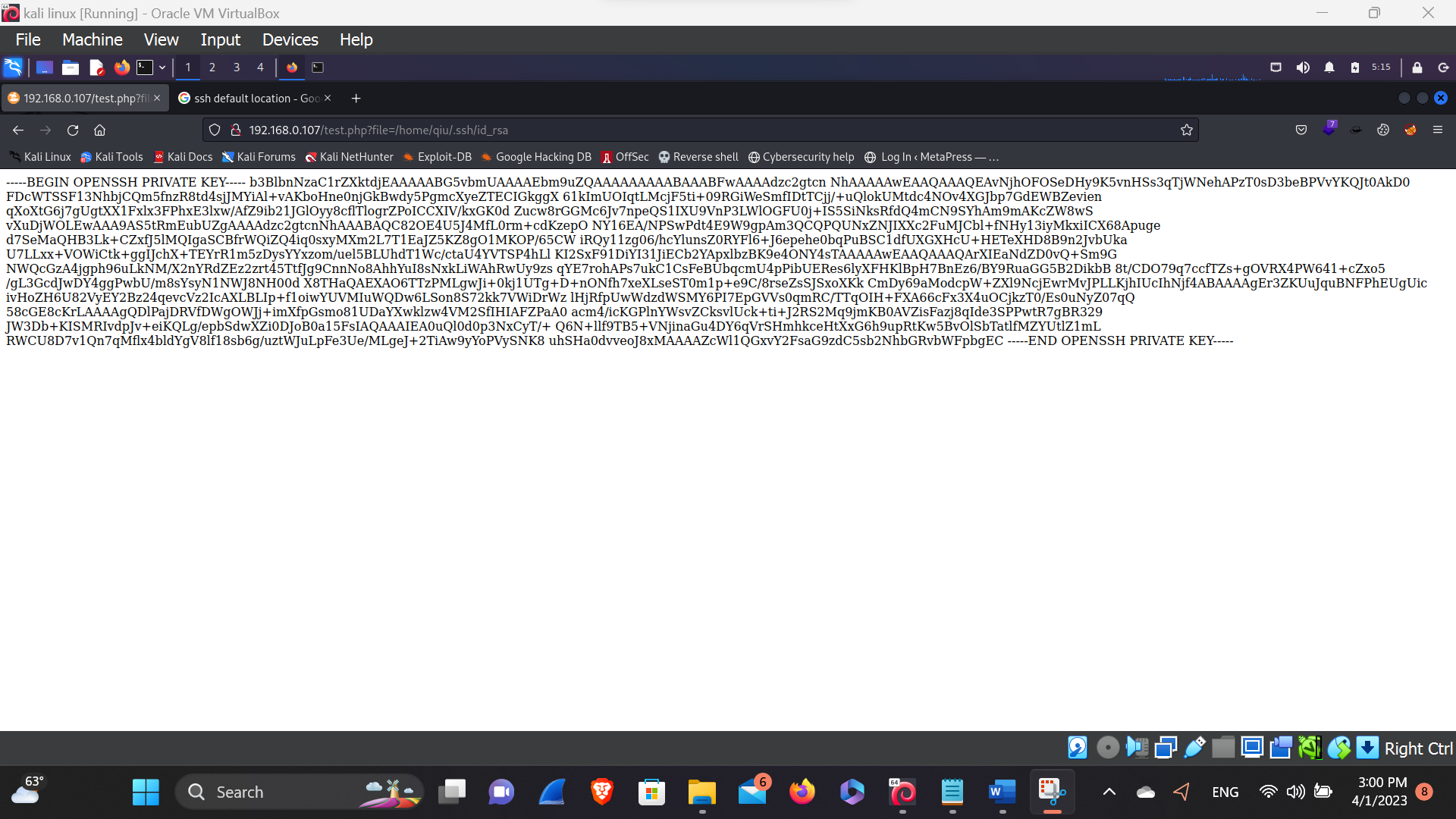


Here, in this above picture we’ve found the LFI bug that we can impact the website, and by getting root privilege we can control the website too. So let’s try



Here, in this above picture we can see that there is system admin qiu let’s find out the default location of the SSH and let’s try to login by using the private key of the qiu.

**Private key of qiu**

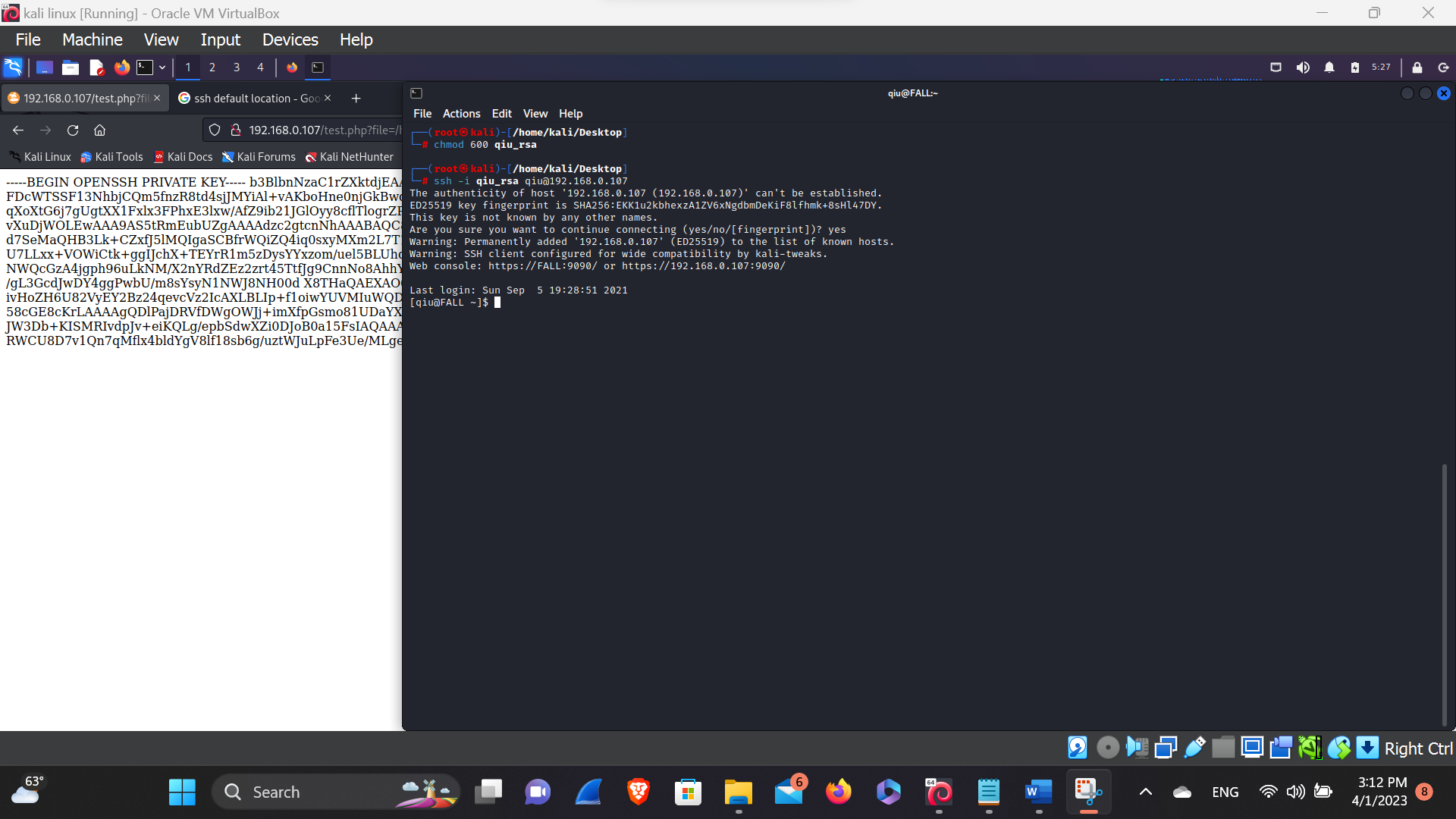


Here, in this above picture we’ve found the private key of the user of qiu that can be directly logged in. we’ve found the private key through the shh default location ( i.e. /home/qiu/.ssh/id\_rsa) so, try to login in the server.

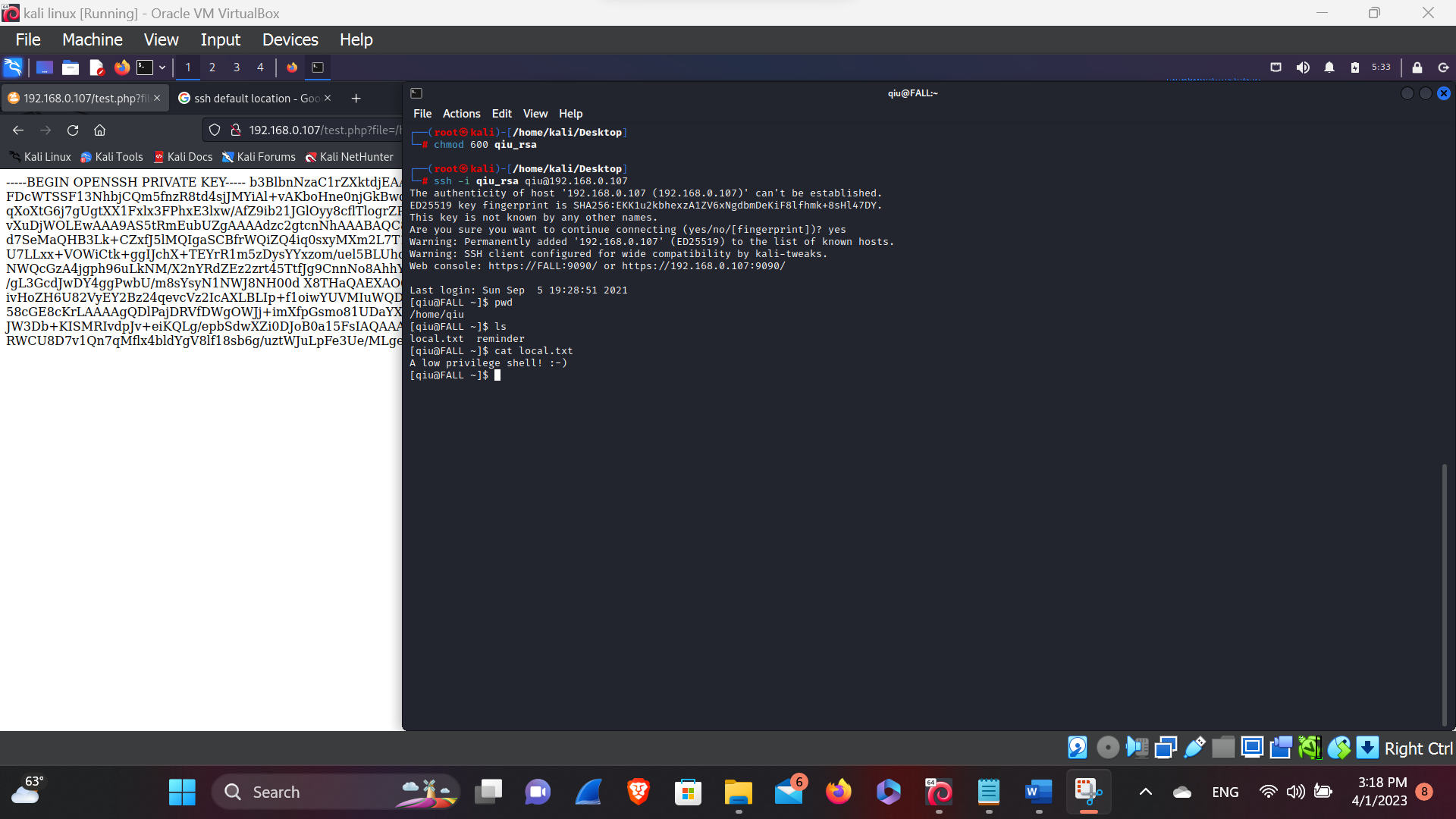
Here, at first we have to download the private key through (curl http://192.168.0.107/test.php?file=/home/qiu/.ssh/id\_rsa > qiu\_rsa

And let them give a permission to read i.e. chmod 600 qiu\_rsa after giving the permission let’s try to login through the private key that we have downloaded.)

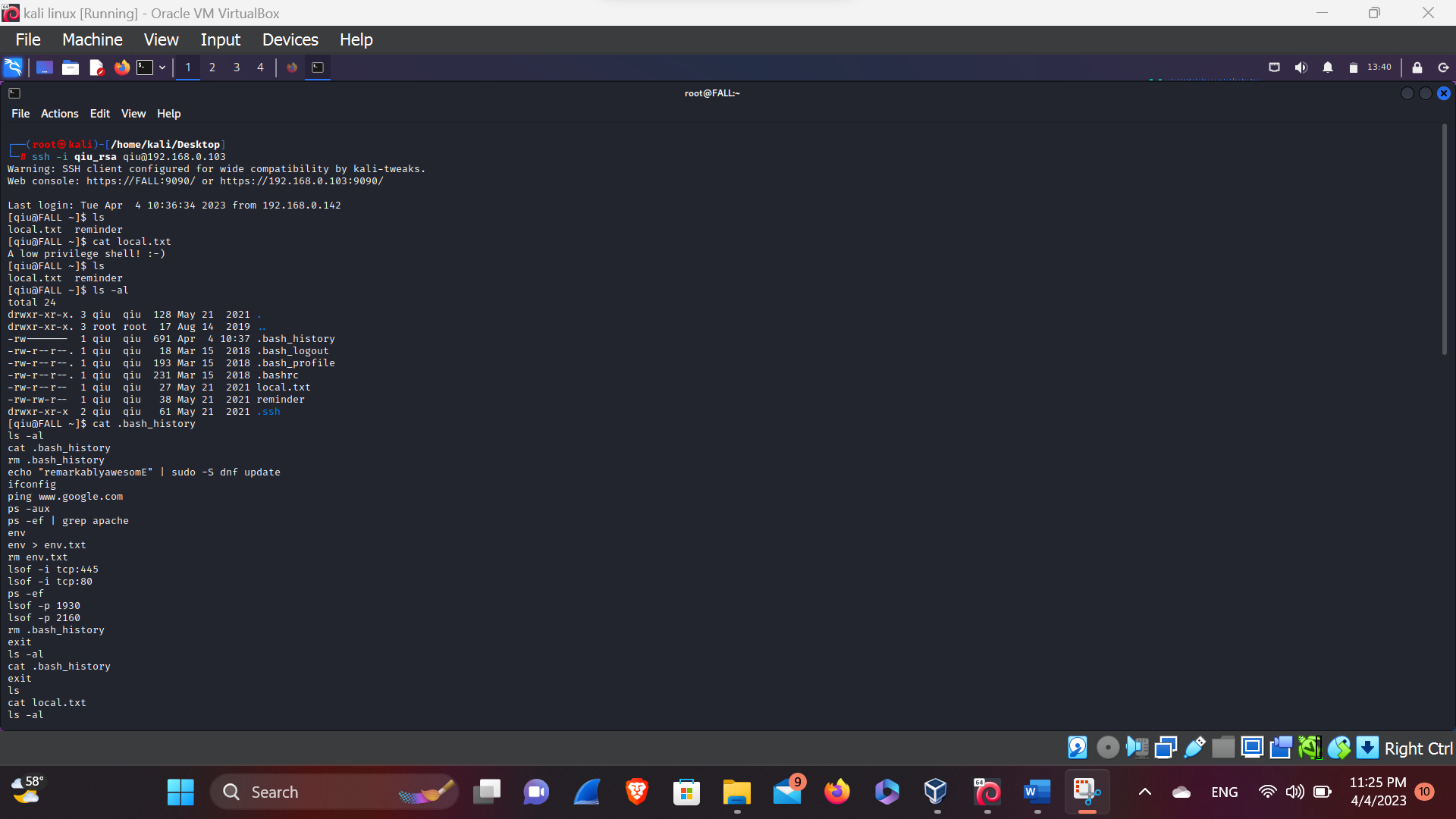
**SSH private key Login**



Here, as we can see that we’re logged in a qiu account through small mistake of the system admin. So, let’s try to be root and get a privilege escalation.

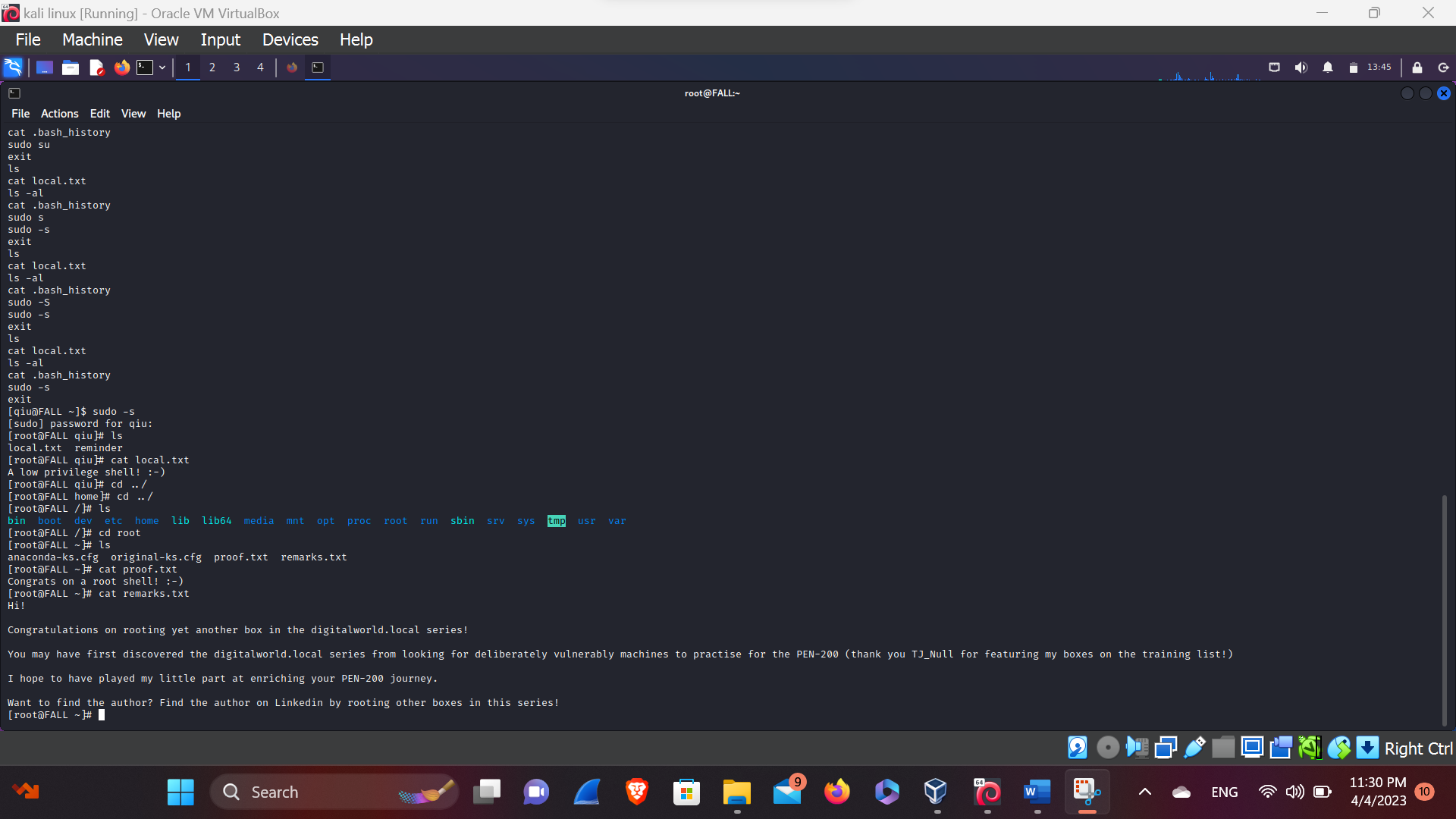


Here, in this picture we can see the qiu account and there is local.txt file by opening the local. Txt file we have got the low privilege escalation.

**Privilege Escalation**

Here, in this above picture we’ve found the hidden files and the directory with the help of command ( I.e. ls -al), so let’s check the file we’ve found during the qiu user. And after doing cat of the .bash\_history we, found the password.

And here, above we’ve seen that there is a Guessable password of the root user so let’s try to login with the guessable password of the root.

**Root Login**

Here, in this above picture we’ve found the Guessable password of the root user, we’ve tried to login and now we can see that we’ve logged in the root user as a super user that we can delete anything from the file. And we’ve found some file in the root directory and we’ve checked the root directory and now the root directory explains that we are now super user.