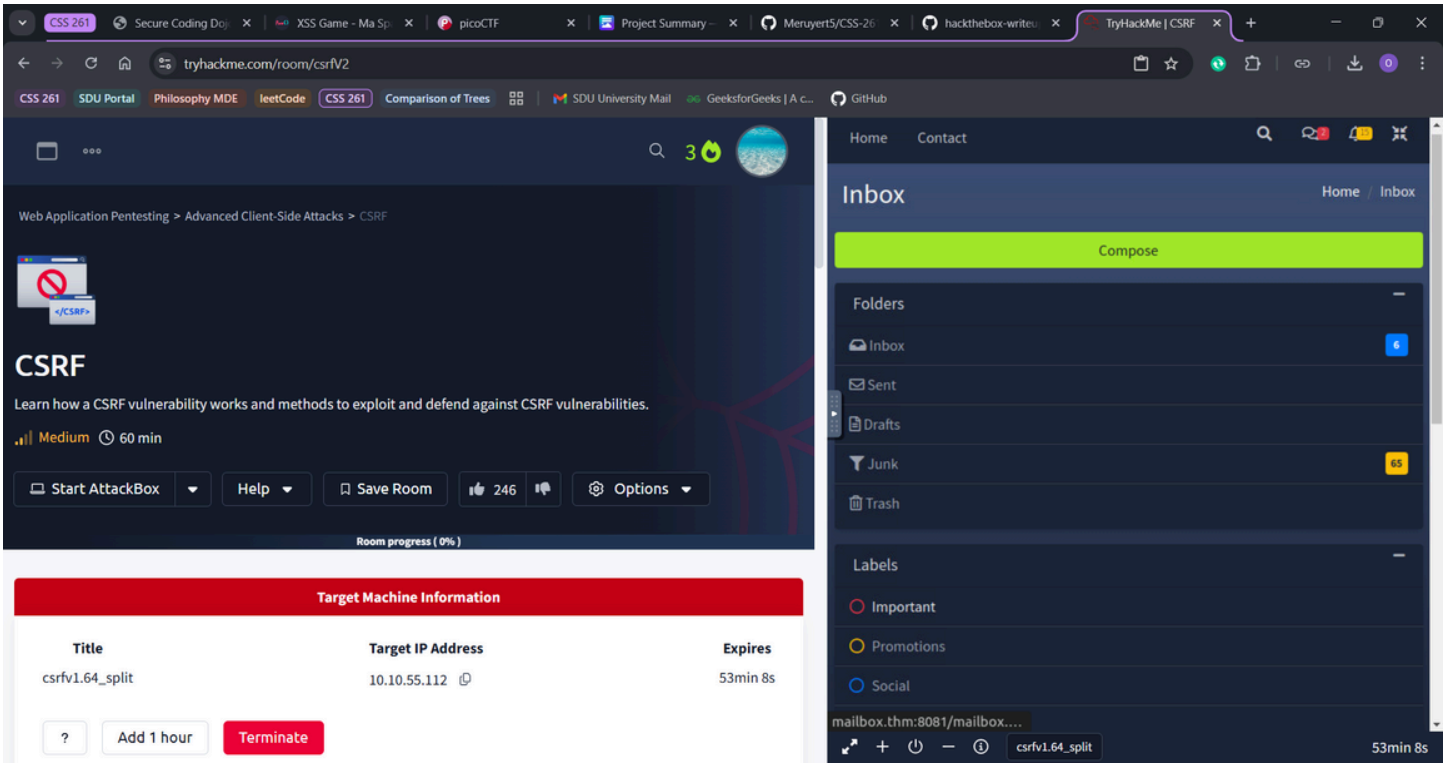
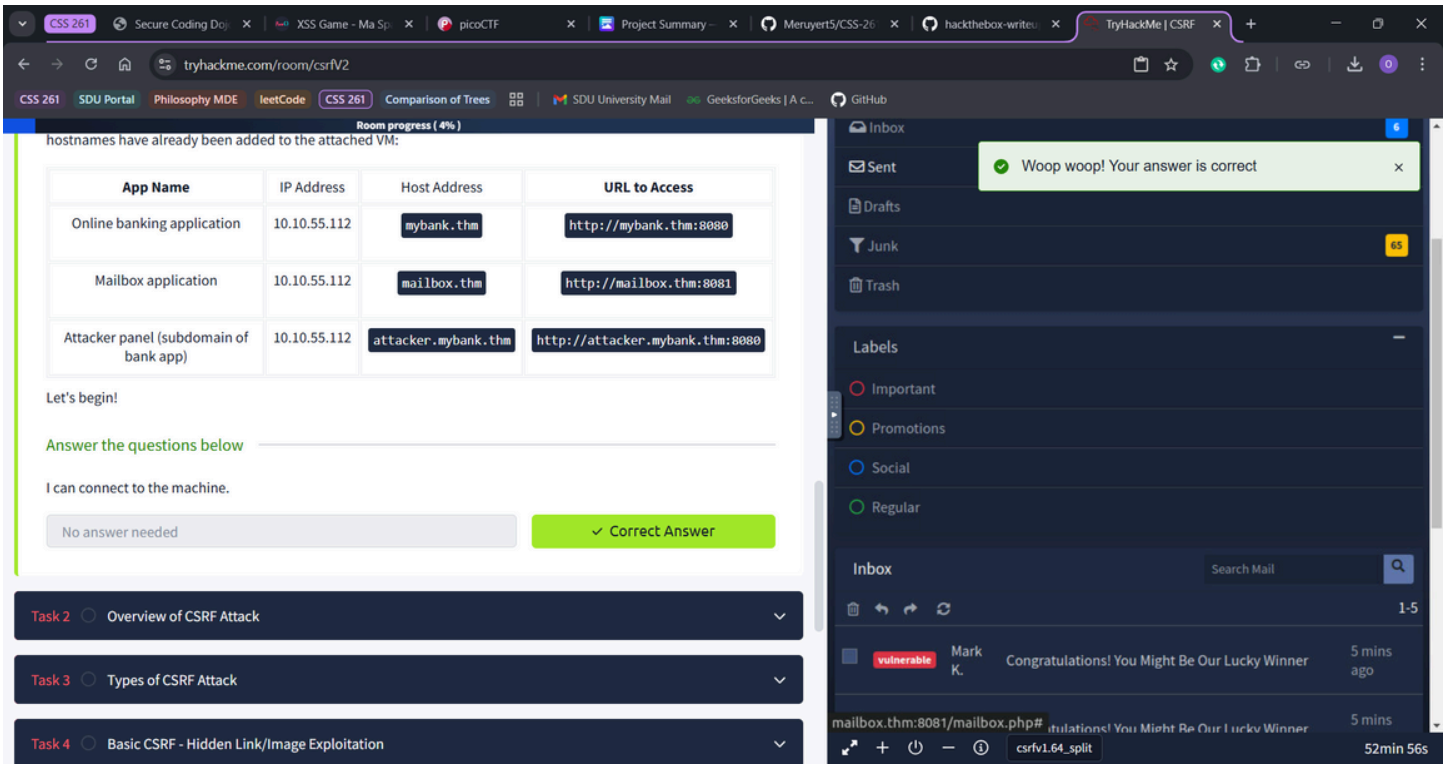
TryHackMe CSRF

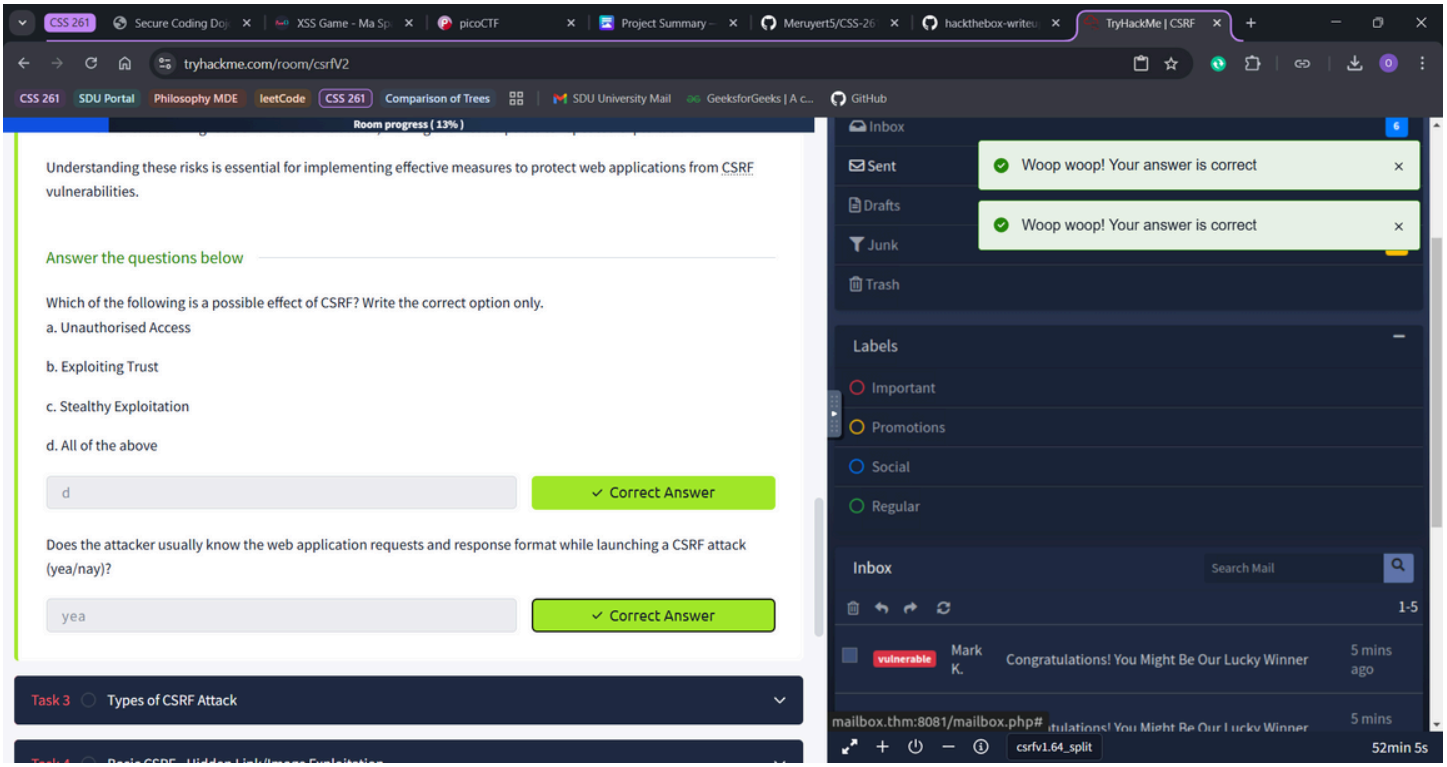
Hi Teacher! This is how I've been able to solve this challenge:

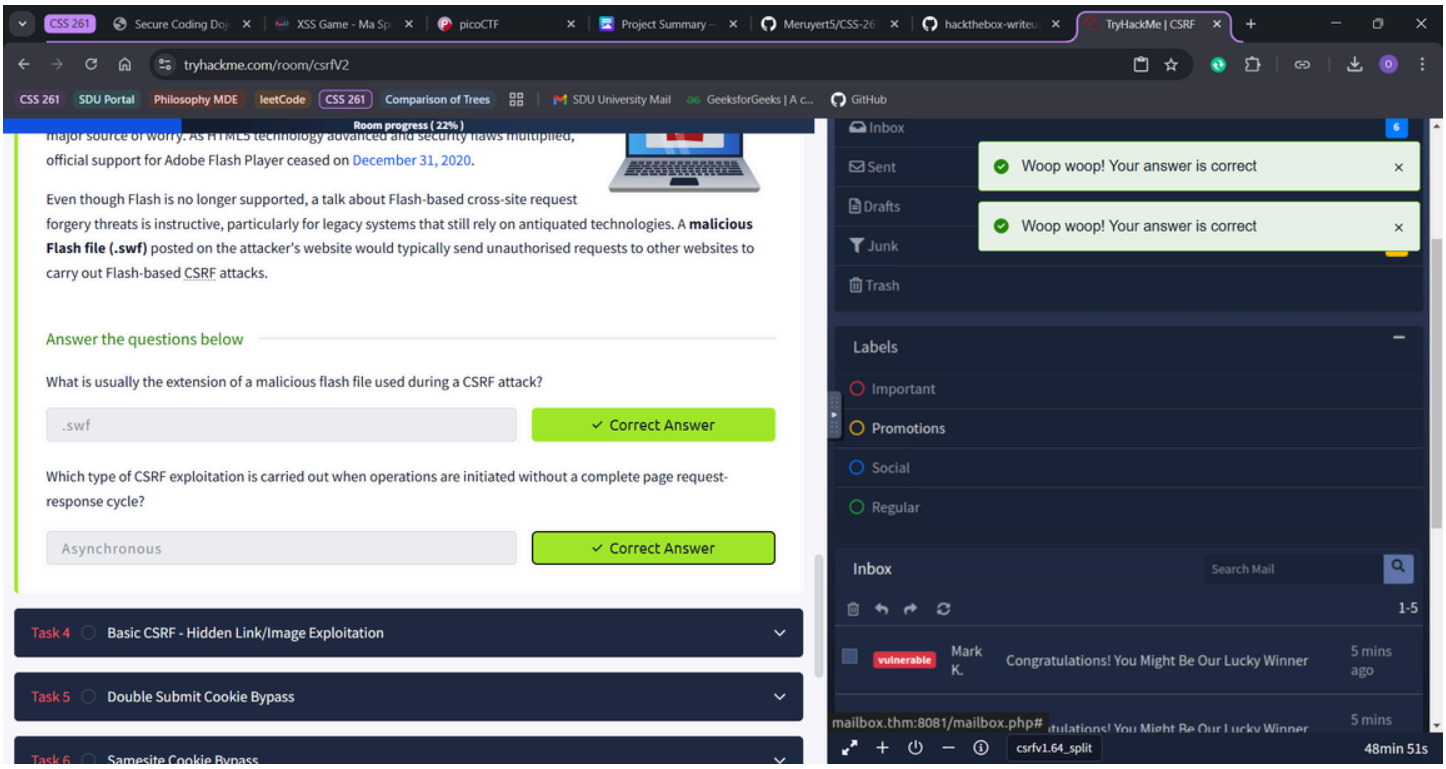
Firstly, we start the machine



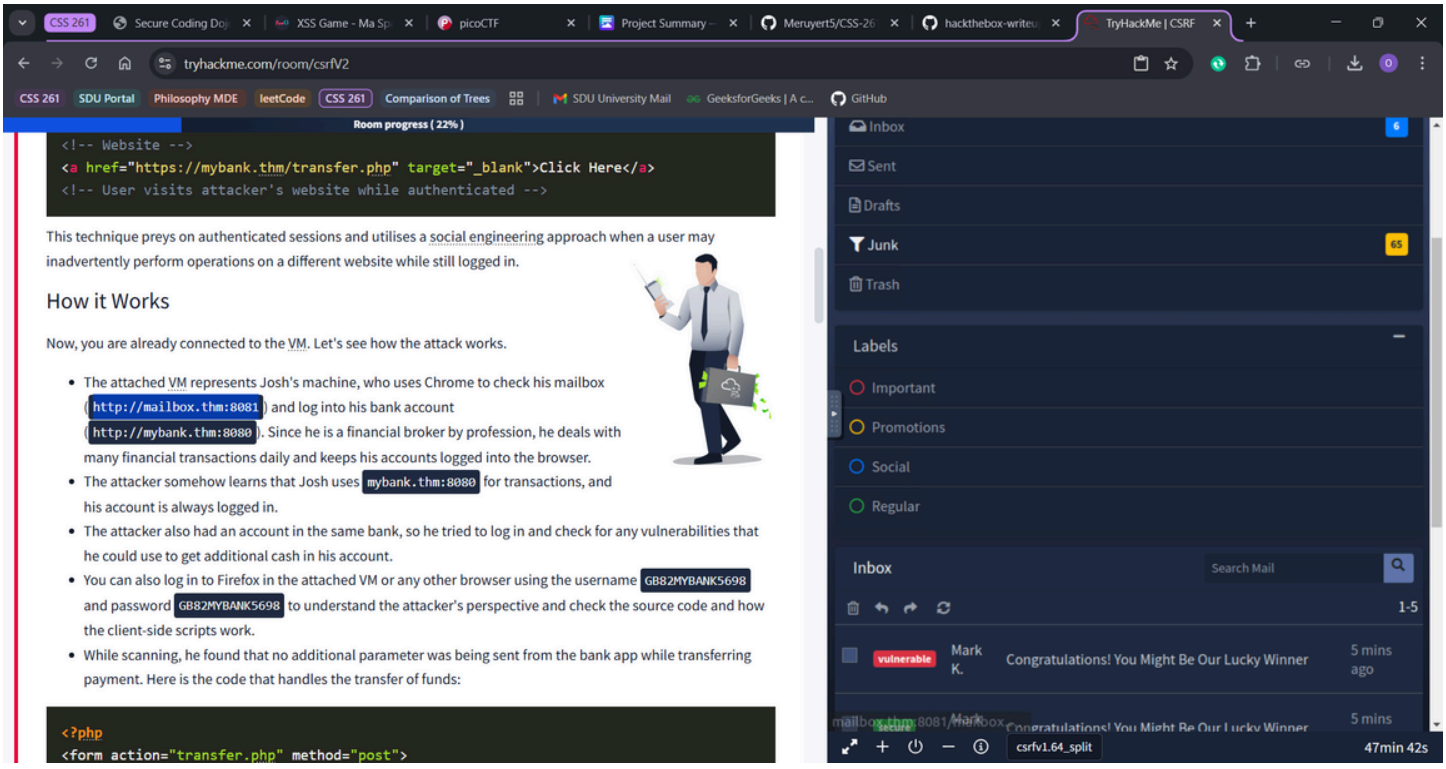
Then, after we read all of that information, we can answer these questions


tryhackme.com/room/csrfV2
Room progress (4%)
hostnames have already been added to the attached VM:
App Name
IP Address
Host Address
URL to Access
Online banking application
10.10.55.112
mybank.thm
http://mybank.thm:8080
Mailbox application
10.10.55.112
mailbox.thm
http://mailbox.thm:8081
Attacker panel (subdomain of bank app)
10.10.55.112
attacker.mybank.thm
http://attacker.mybank.thm:8080
Let's begin!
Answer the questions below
I can connect to the machine.
No answer needed
✓ Correct Answer
Task 2 Overview of CSRF Attack
Task 3 Types of CSRF Attack
Task 4 Basic CSRF - Hidden Link/Image Exploitation
Woop woop! Your answer is correct
Inbox
Sent
Drafts
Junk
Trash
Labels
Important
Promotions
Social
Regular
Search Mail
vulnerable
Mark K.
Congratulations! You Might Be Our Lucky Winner
5 mins ago
mailbox.thm:8081/mailbox.php#
csrfv1.64_split
52min 56s

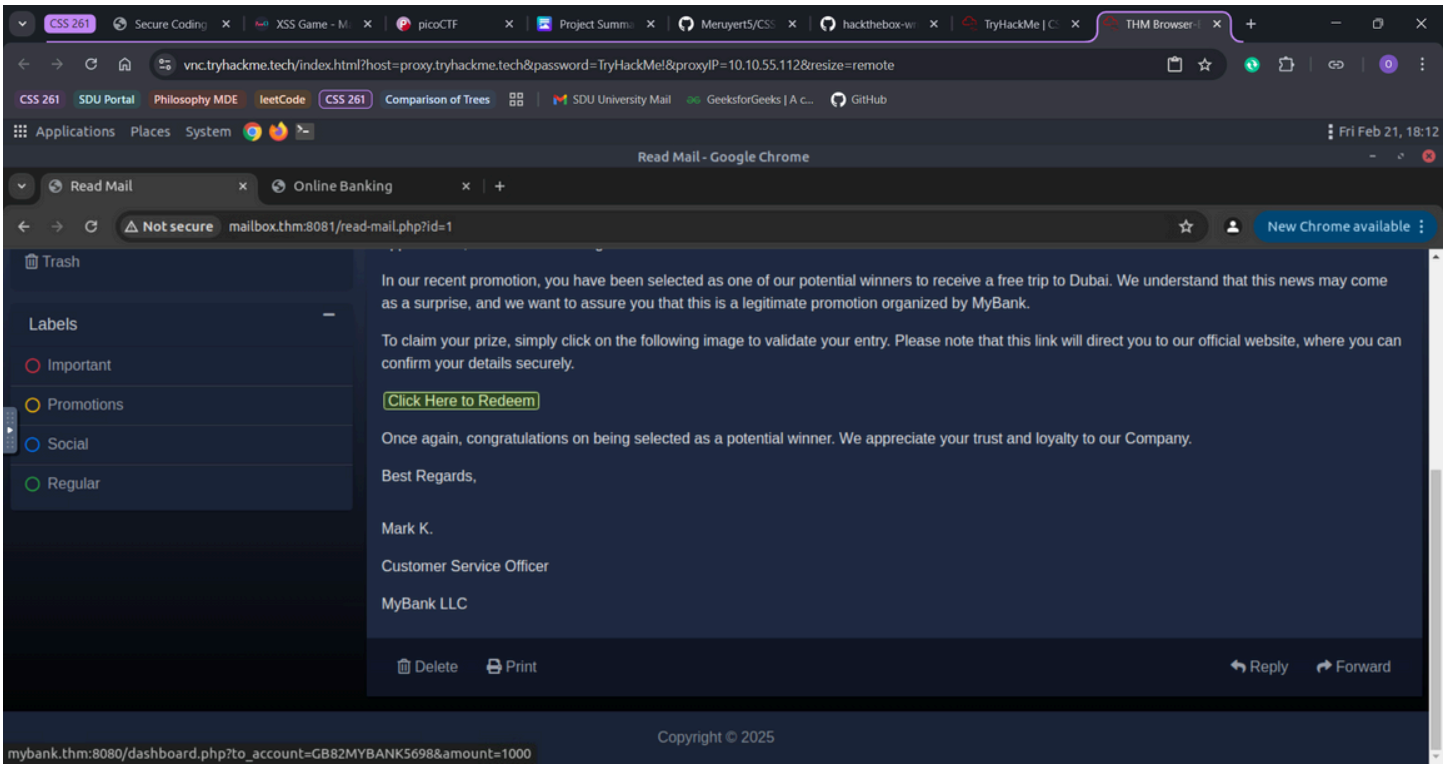

tryhackme.com/room/csrfV2
Room progress (13%)
Understanding these risks is essential for implementing effective measures to protect web applications from CSRF vulnerabilities.
Answer the questions below
Which of the following is a possible effect of CSRF? Write the correct option only.
a. Unauthorised Access
b. Exploiting Trust
c. Stealthy Exploitation
d. All of the above
d
✓ Correct Answer
Does the attacker usually know the web application requests and response format while launching a CSRF attack (yea/nay)?
yea
✓ Correct Answer
Task 3 Types of CSRF Attack
Woop woop! Your answer is correct
Woop woop! Your answer is correct
Inbox
Sent
Drafts
Junk
Trash
Labels
Important
Promotions
Social
Regular
Search Mail
vulnerable
Mark K.
Congratulations! You Might Be Our Lucky Winner
5 mins ago
mailbox.thm:8081/mailbox.php#
csrfv1.64_split
52min 5s



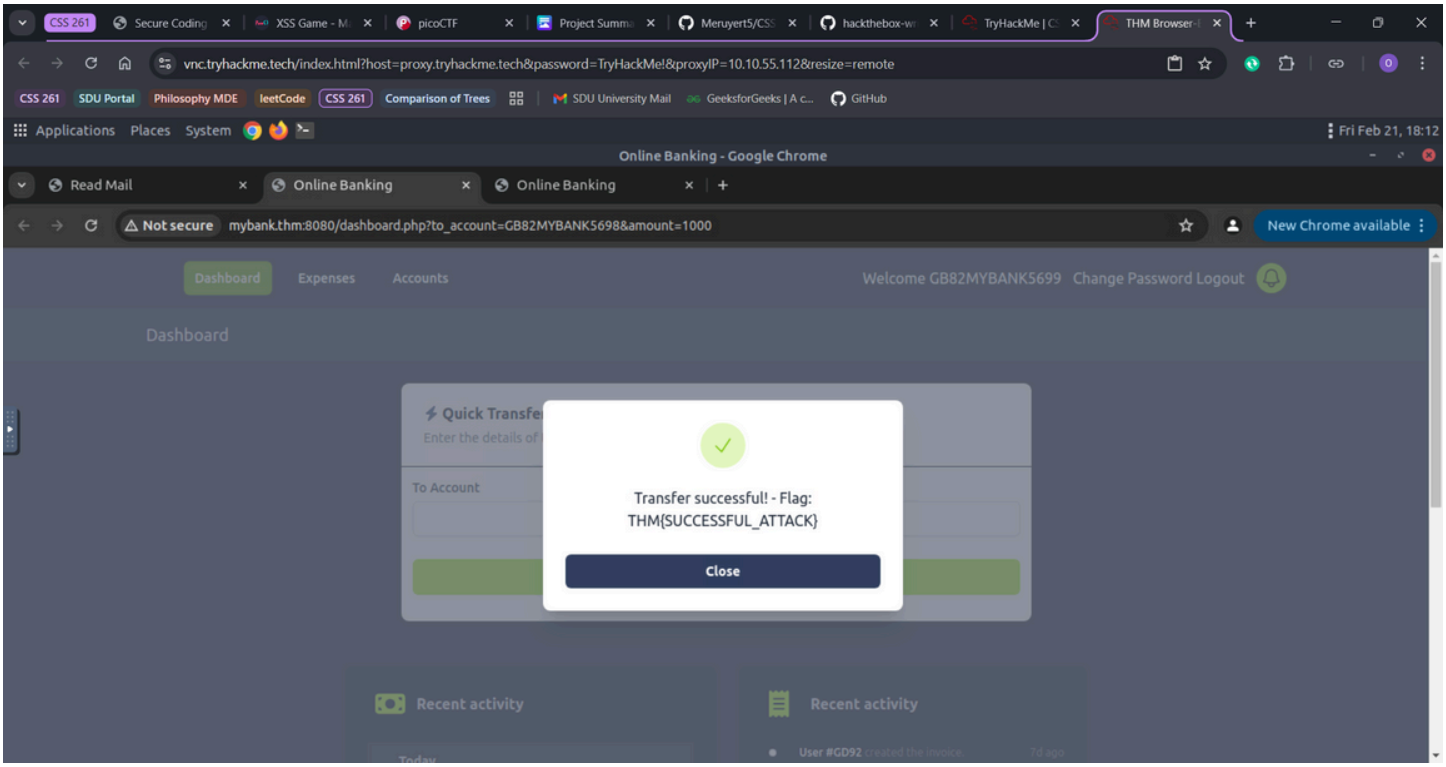
Now for the practical part, we see the victim uses his bank at that address



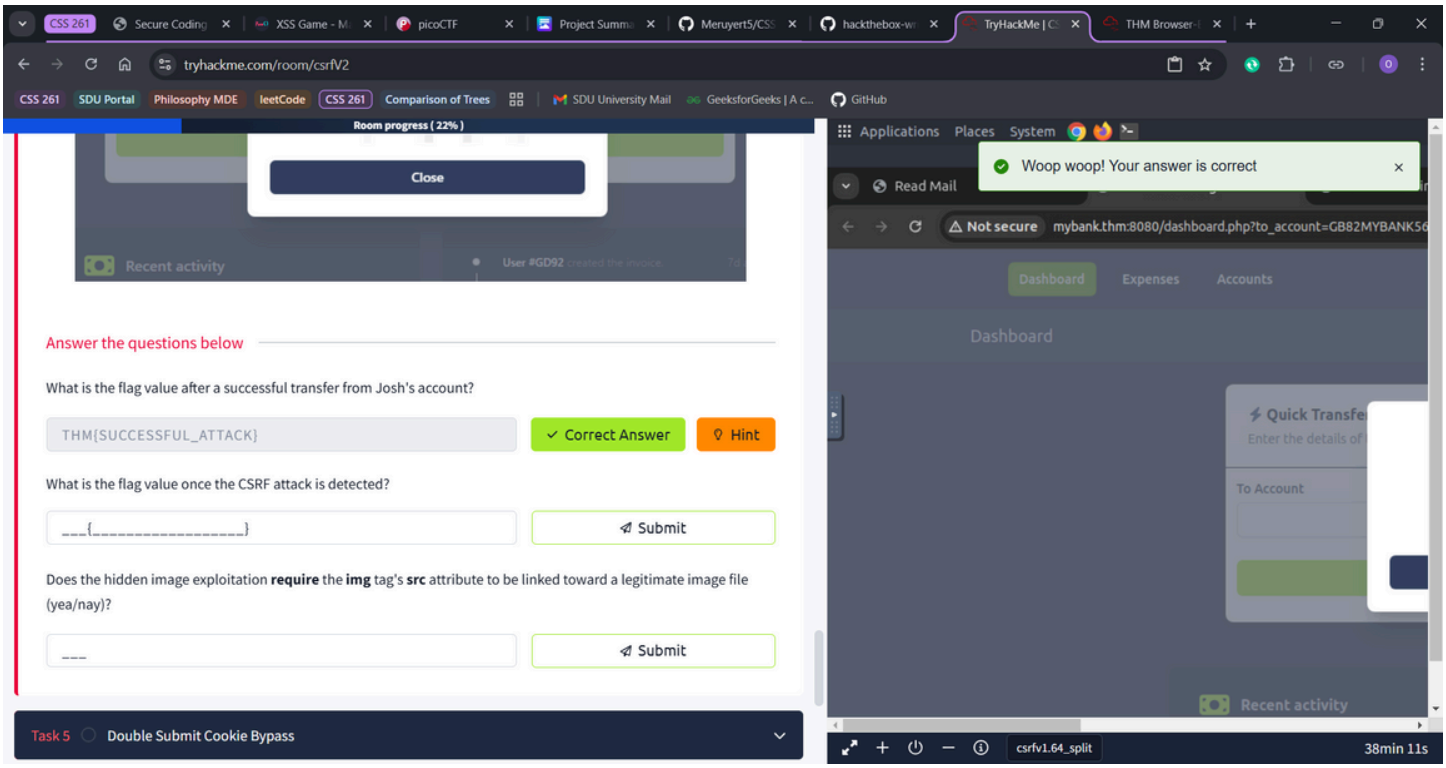
So, as we already logged in his account, we start by checking his mails



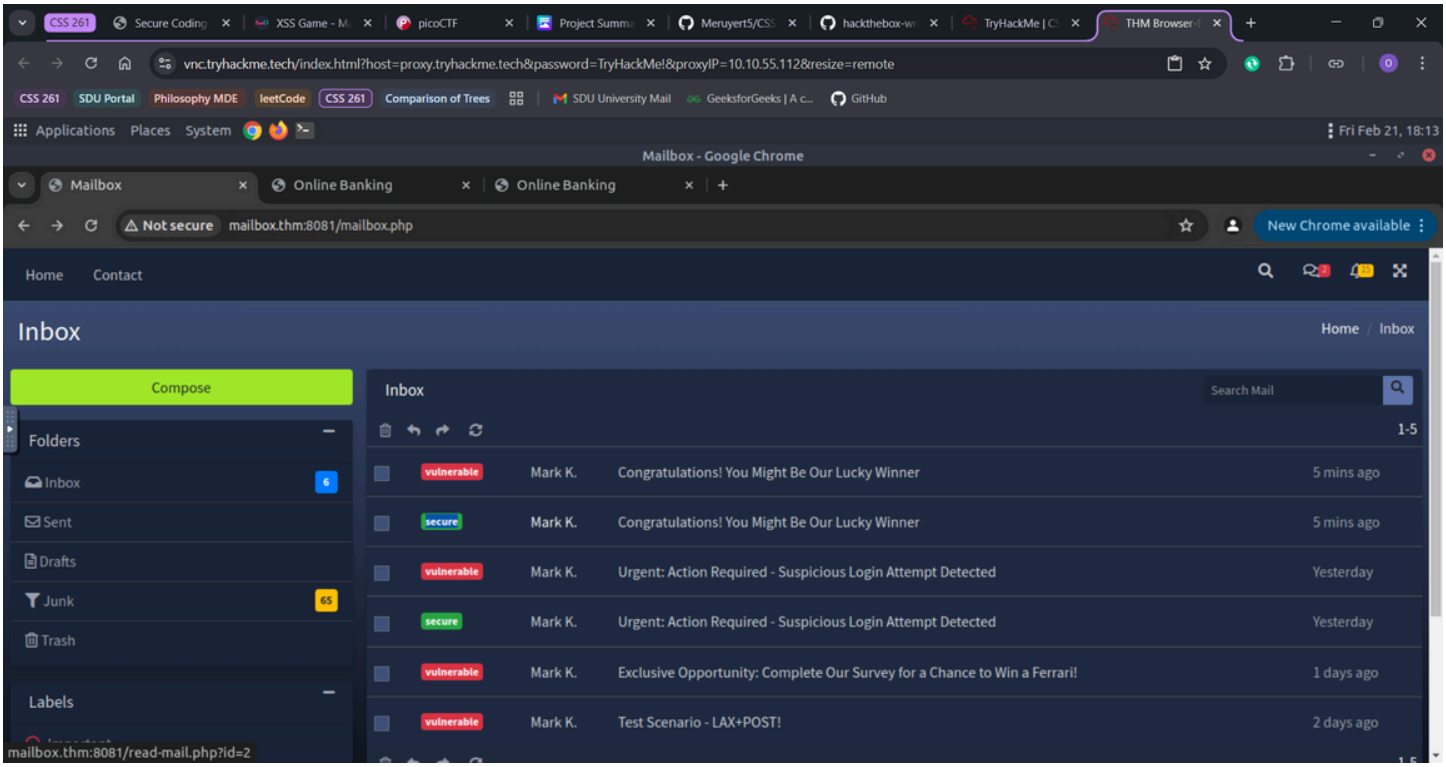
And this what we get when we click on a malicious link



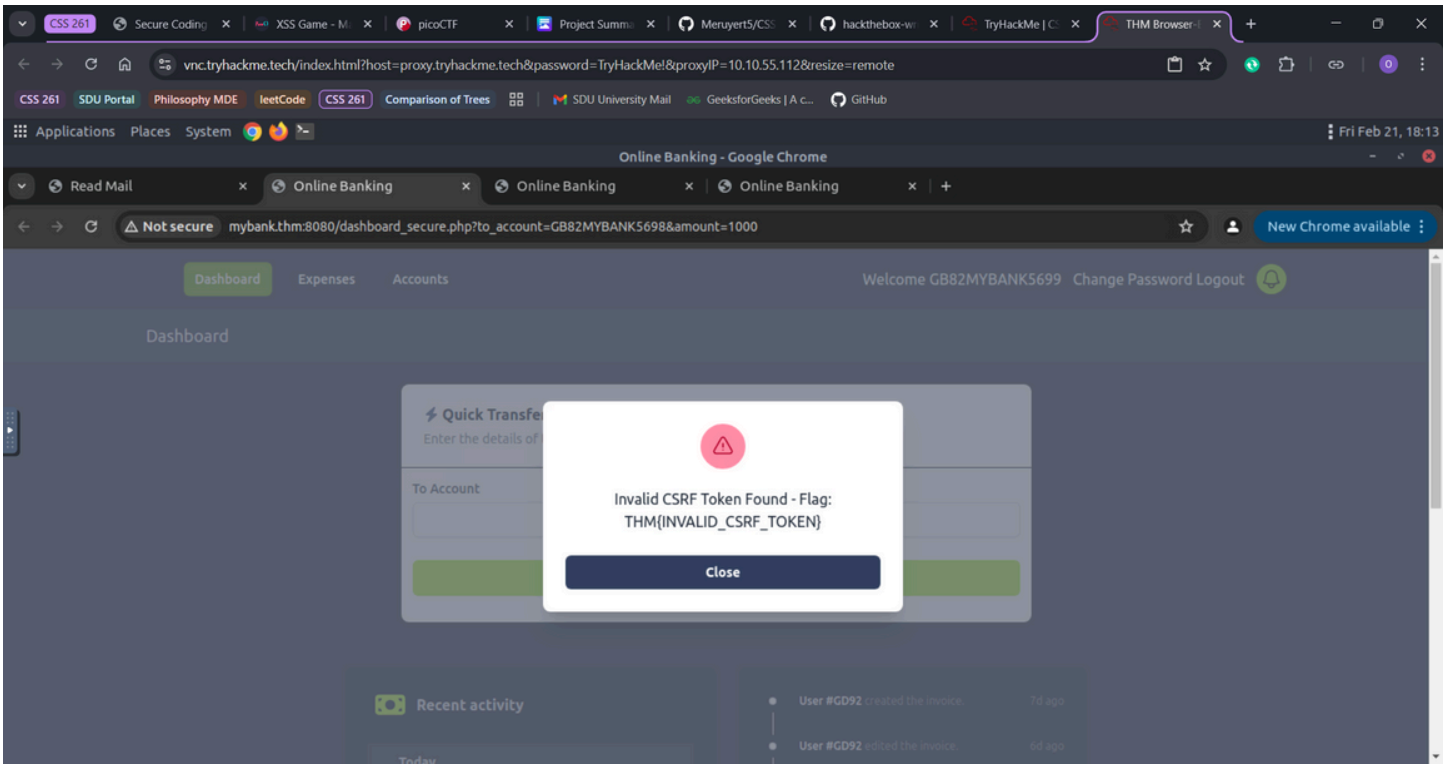
Our first flag



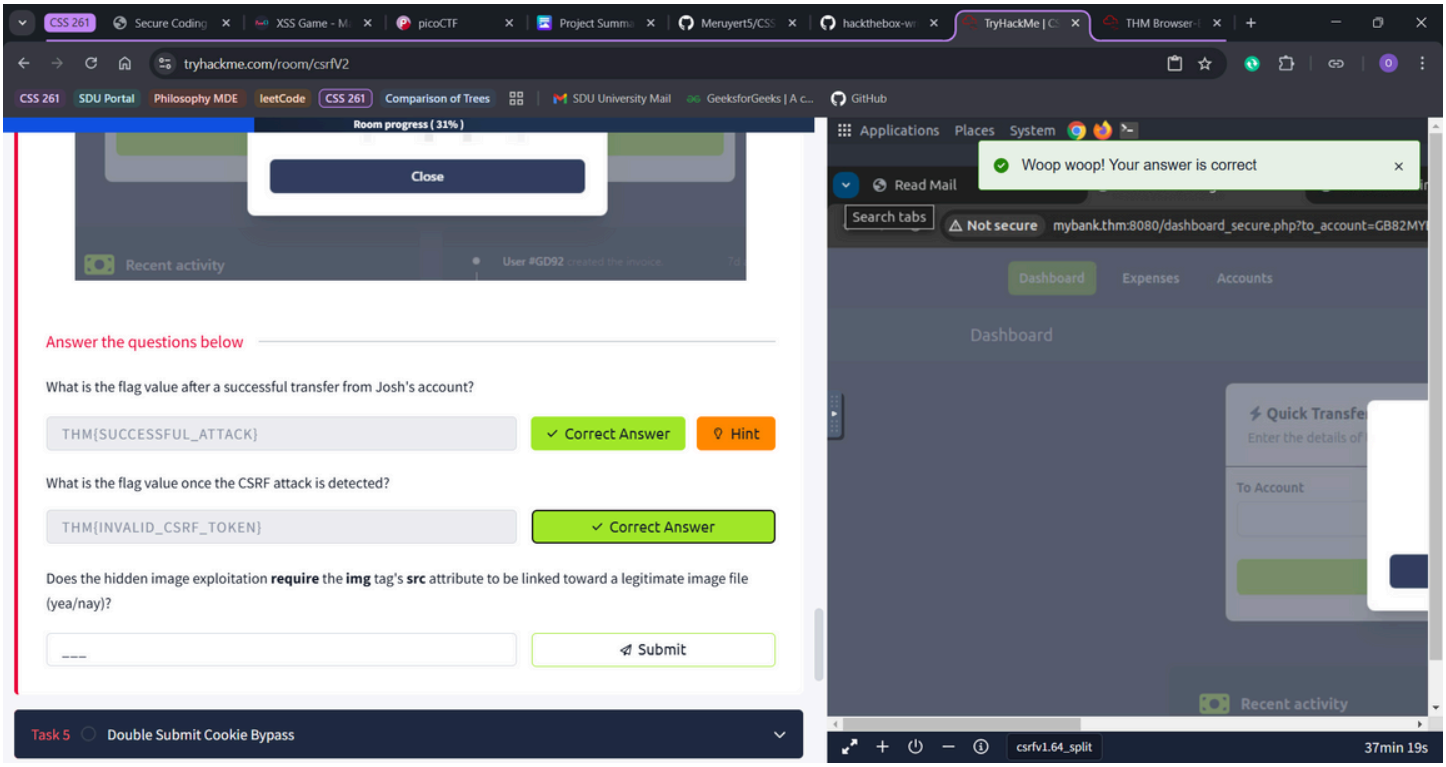
Now if we try to click on a safe(secure) link

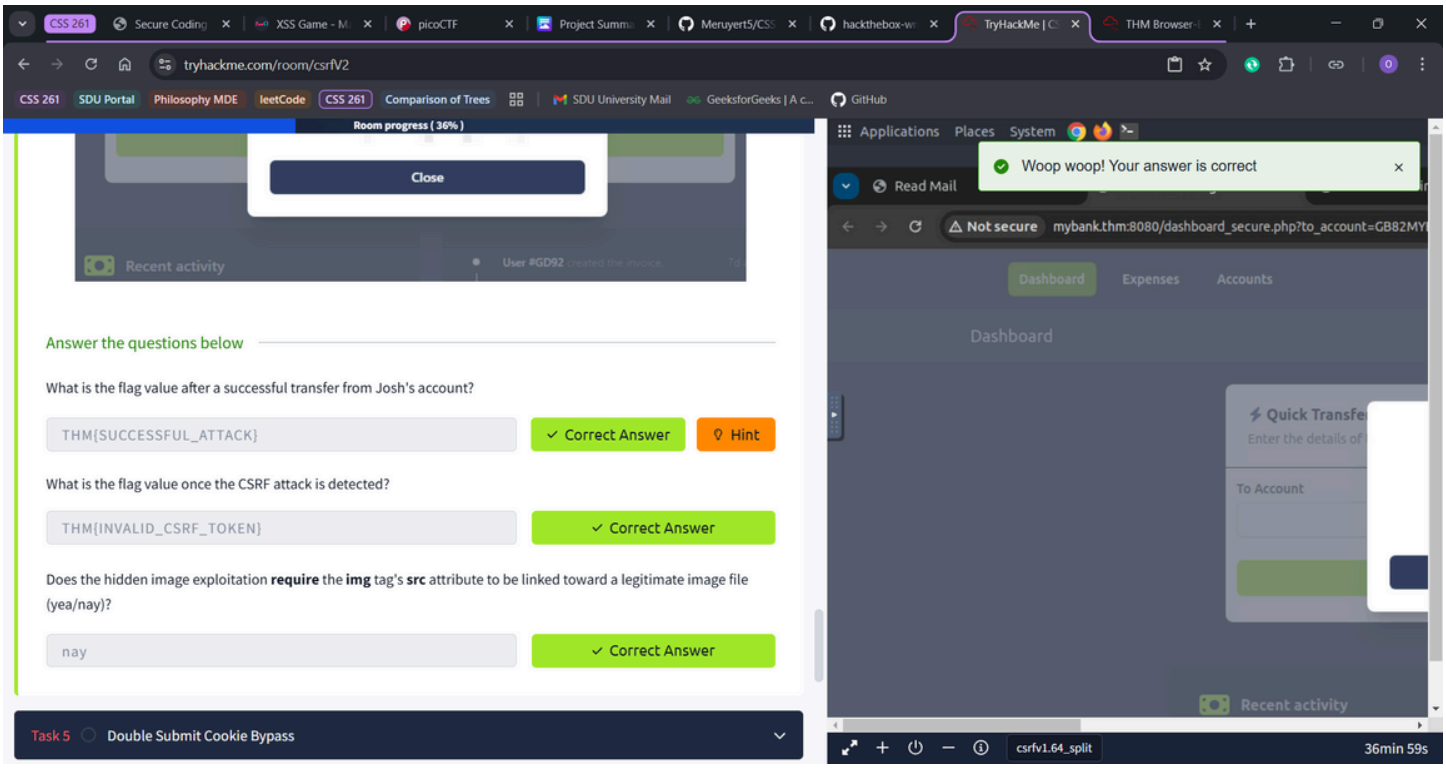


We see that it was blocked by our system

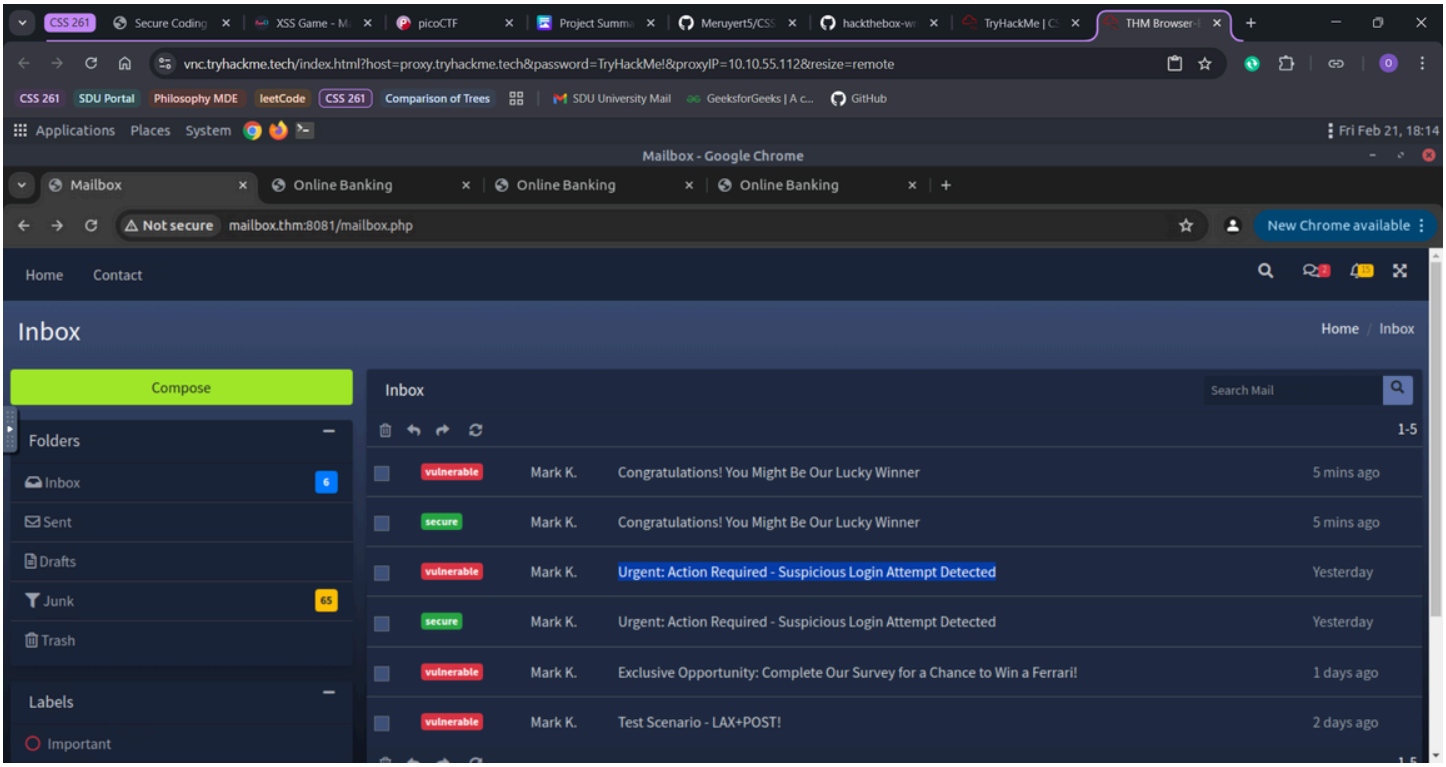


This is our second flag

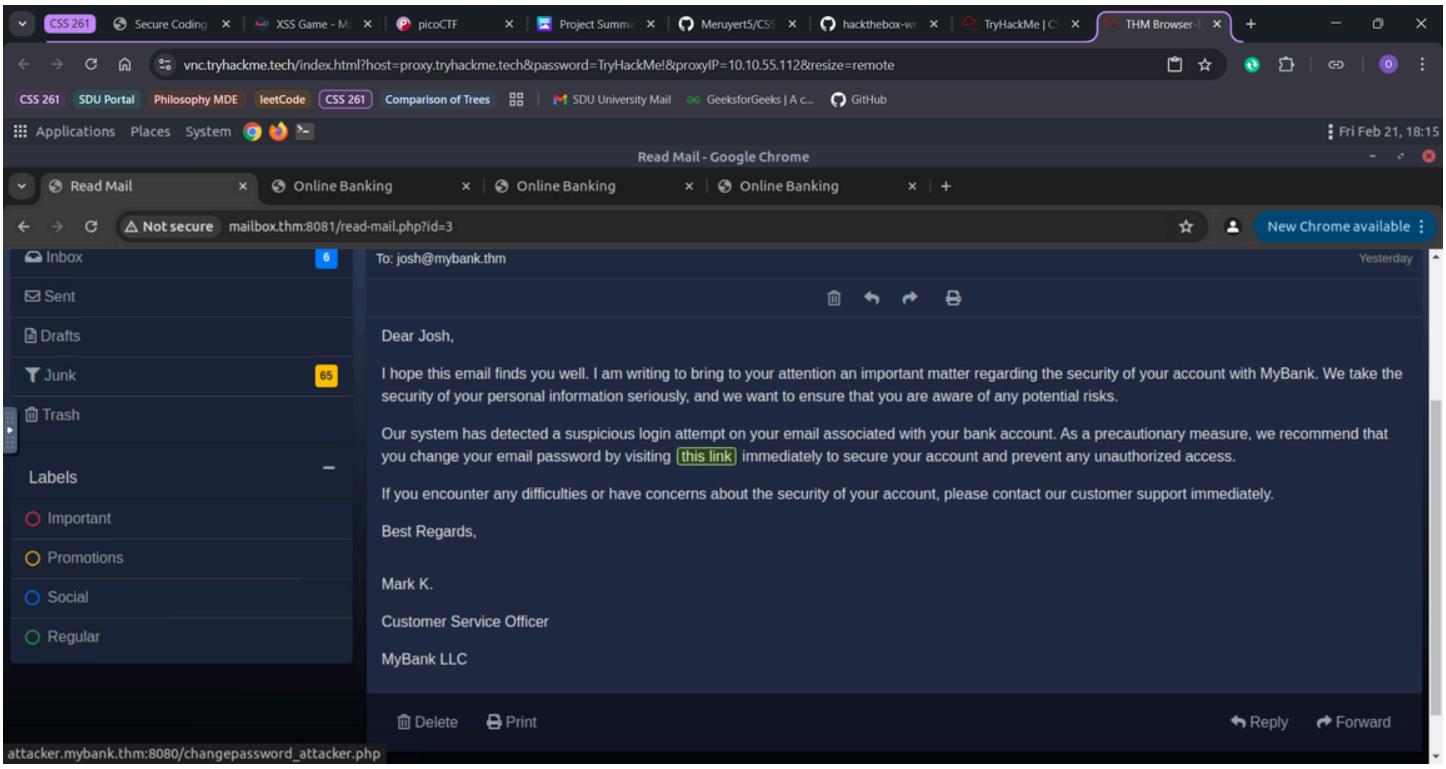




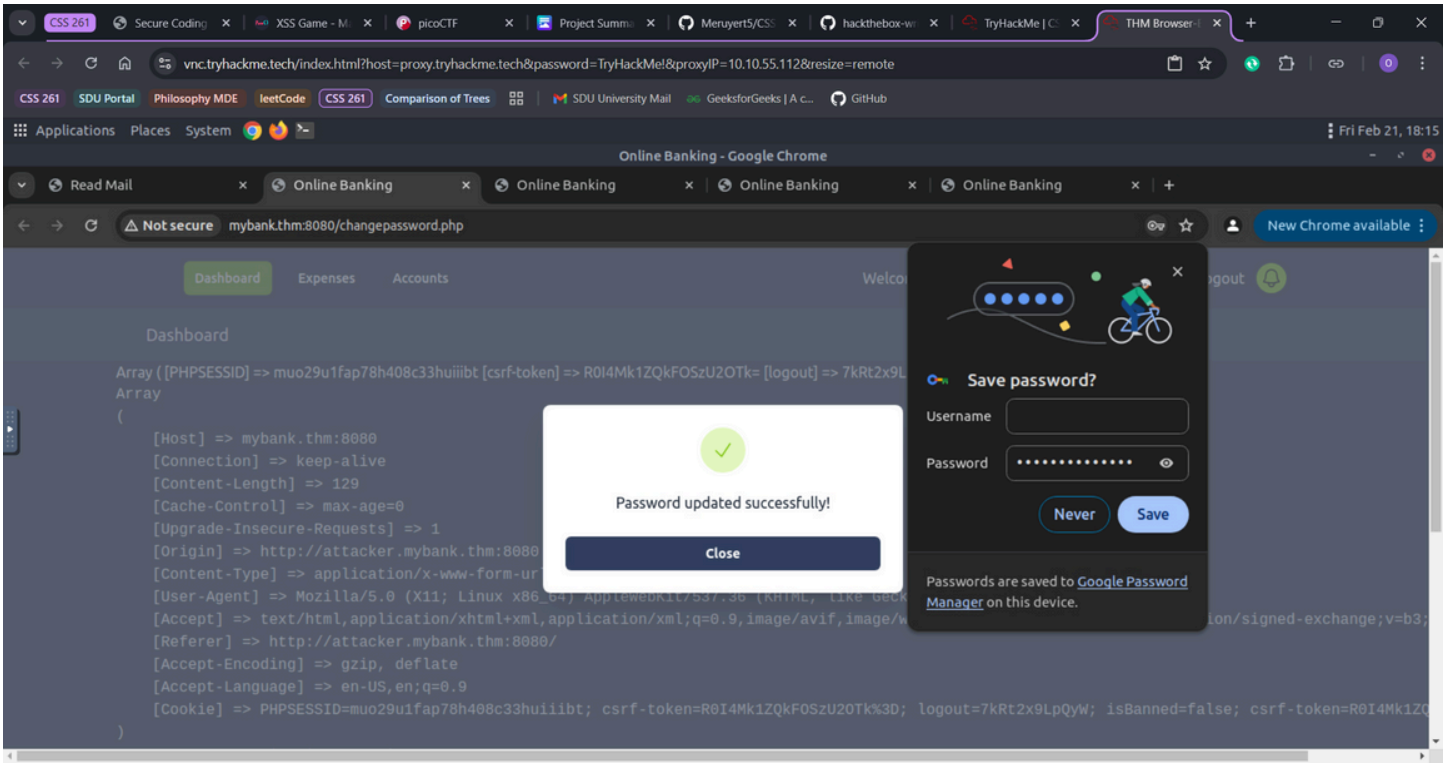
In this part, we look into that type of mails



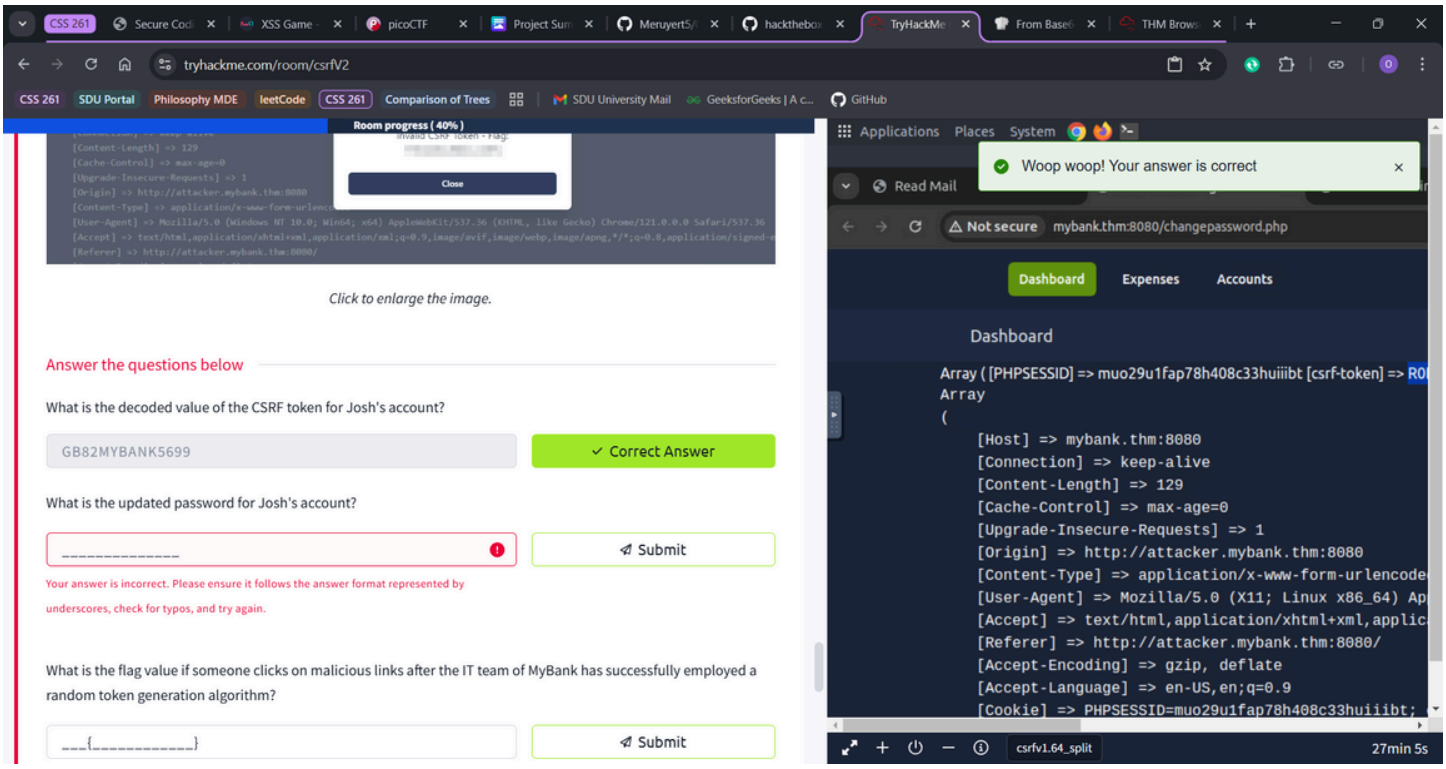
As we click on the link



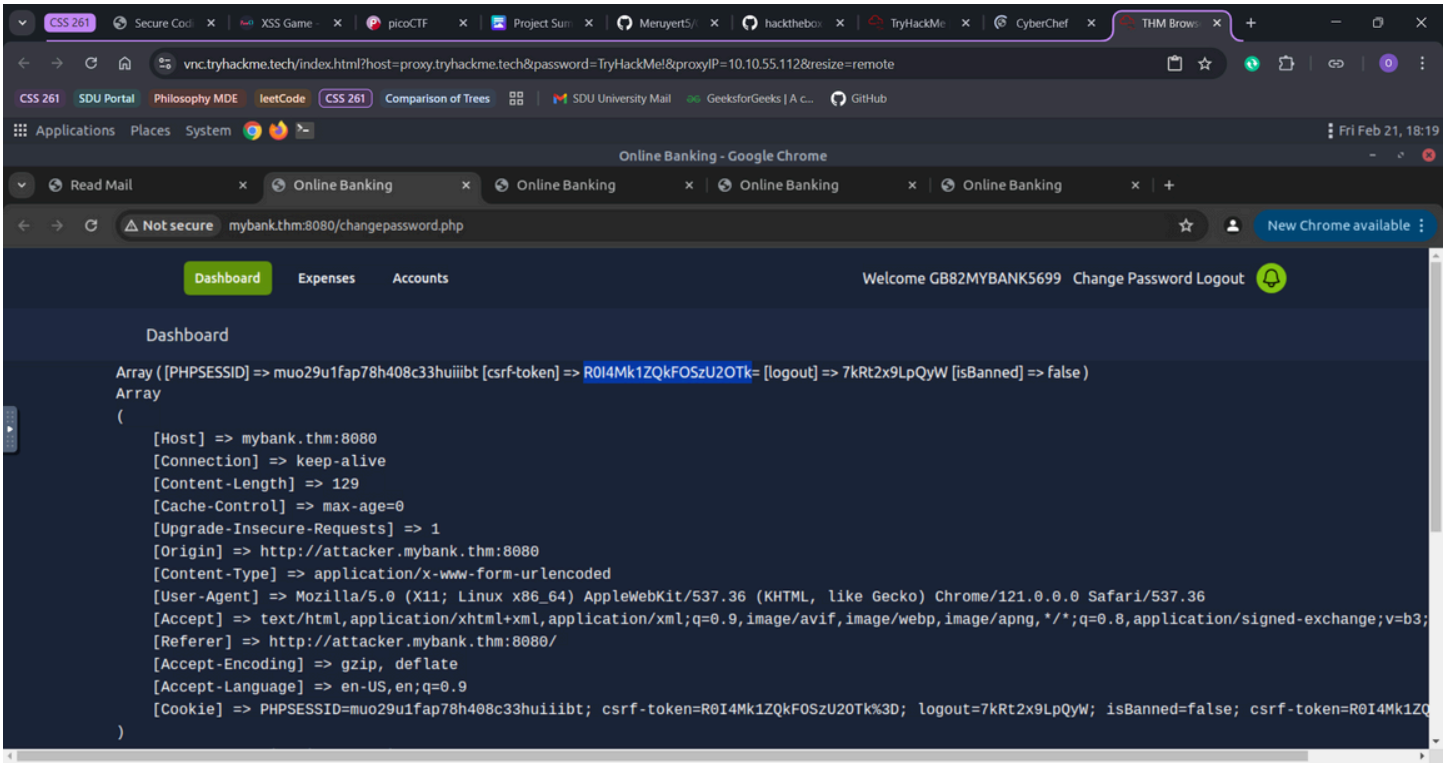
Our password was updated



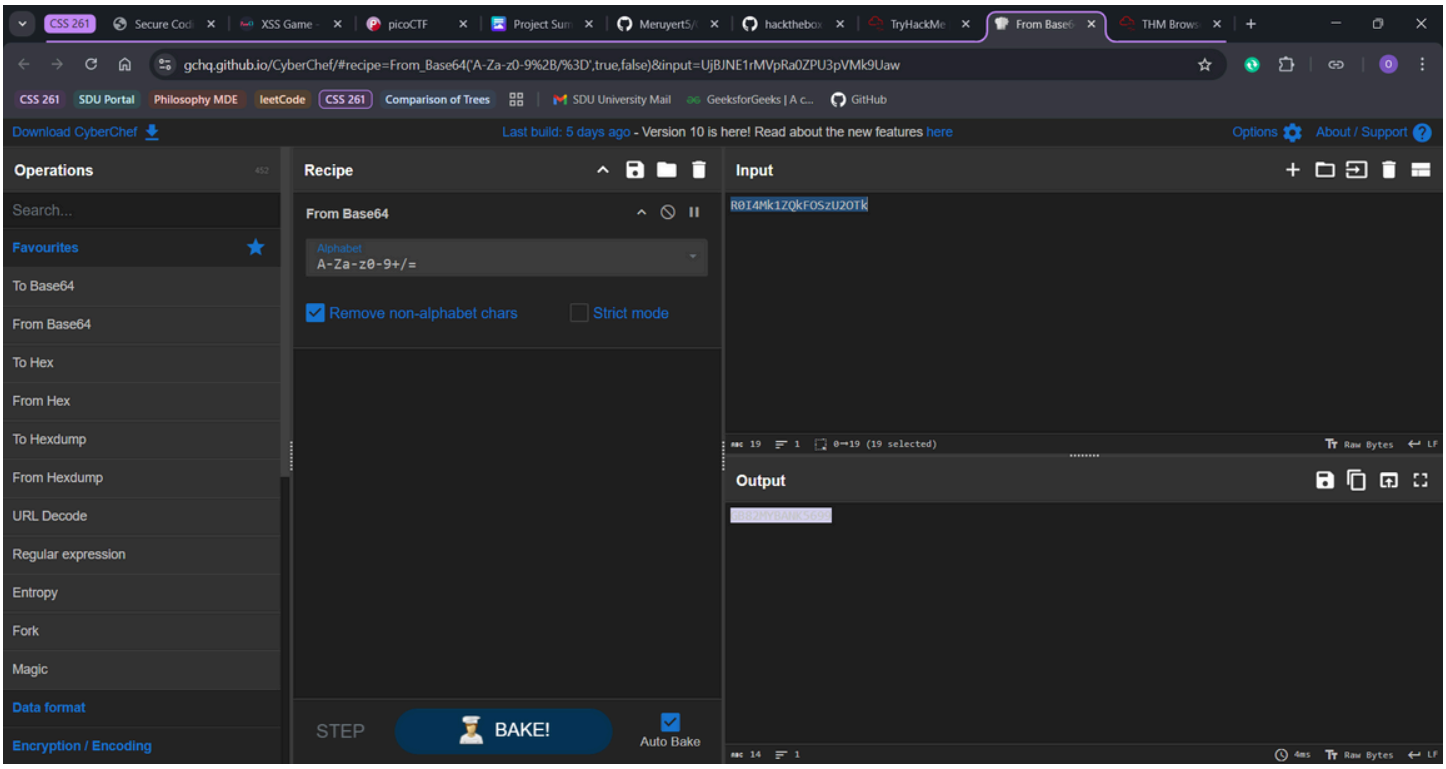
Our next flag



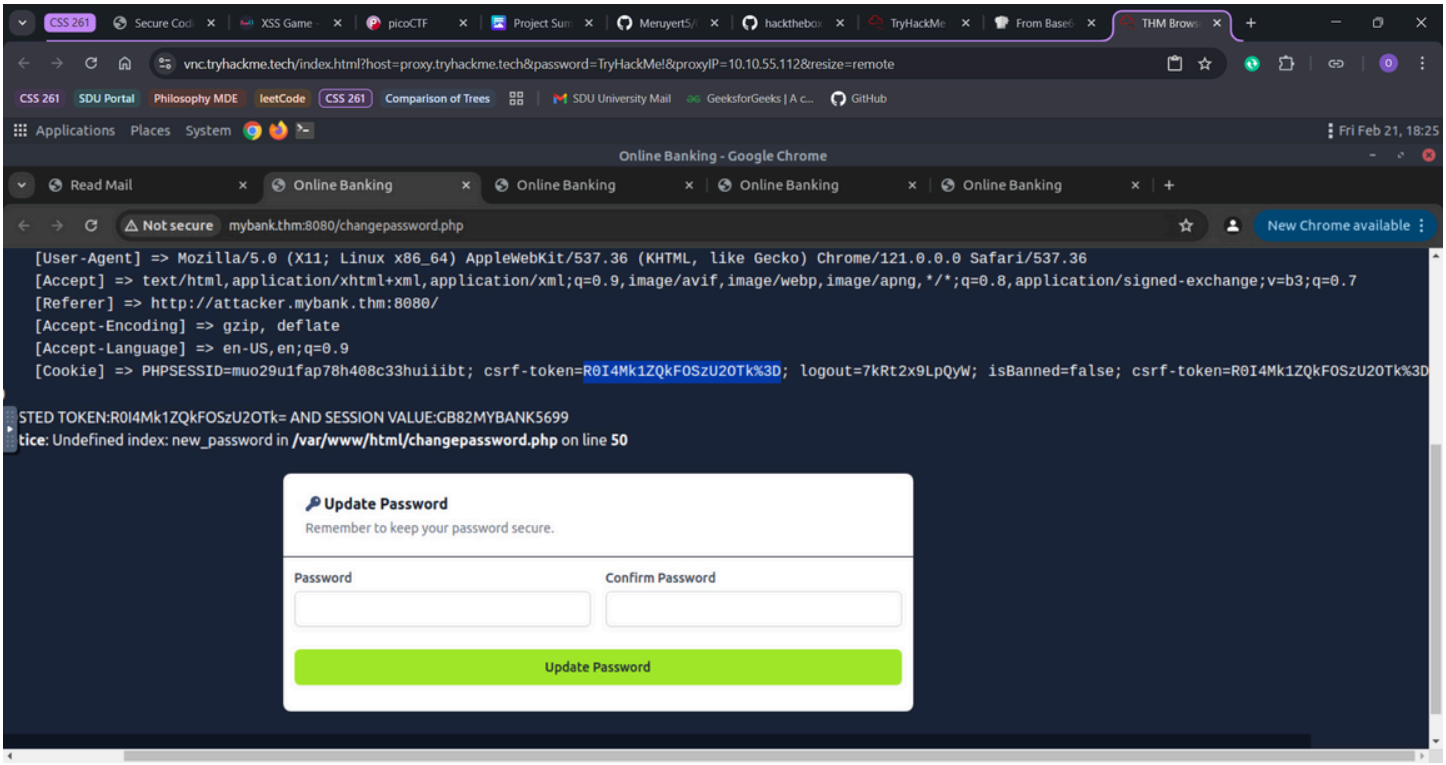
In here we got the inside of the request, also this is victim's CSRF-token



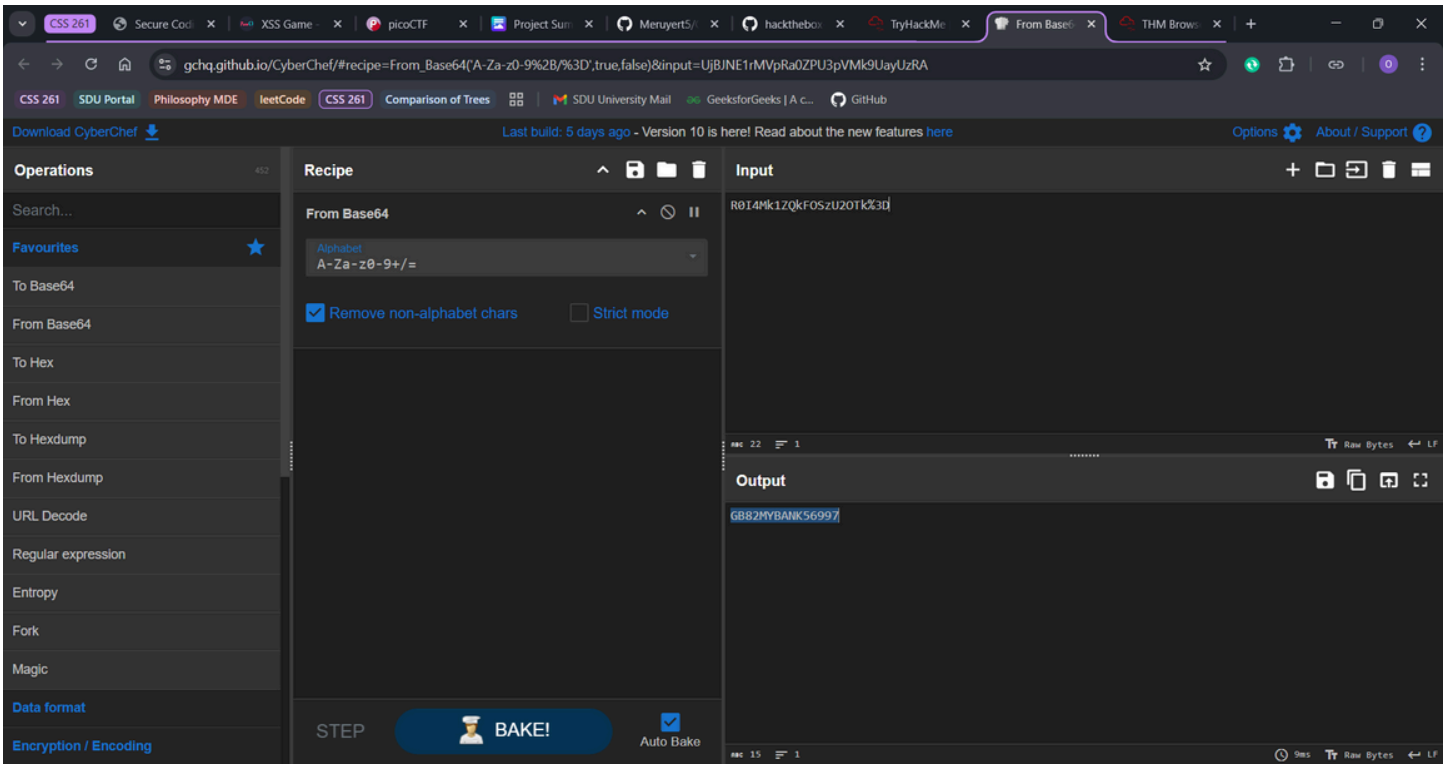
By decoding it at CyberChef we get this text, which is Josh's password

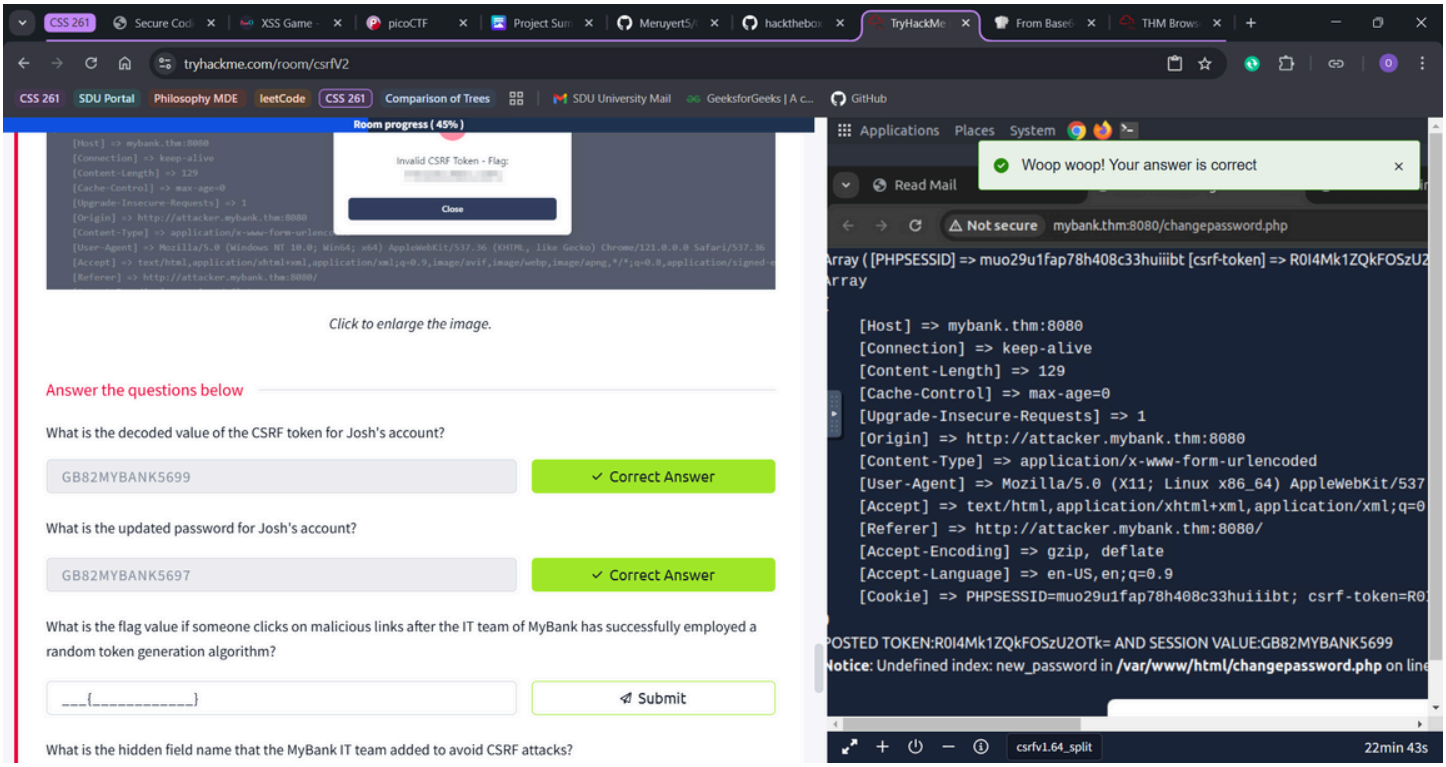


Next is the CSRF-token the attacker updated

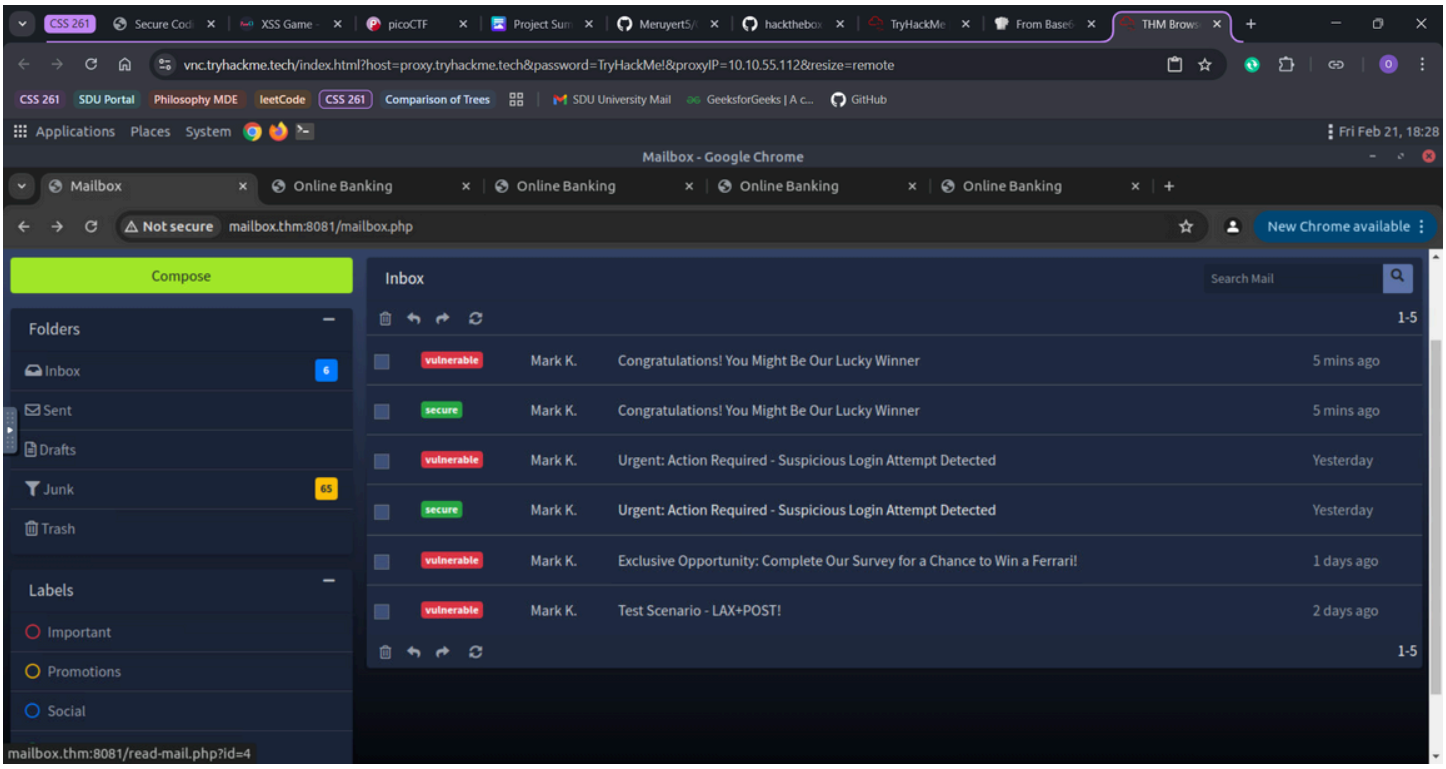


This is the password he changed to

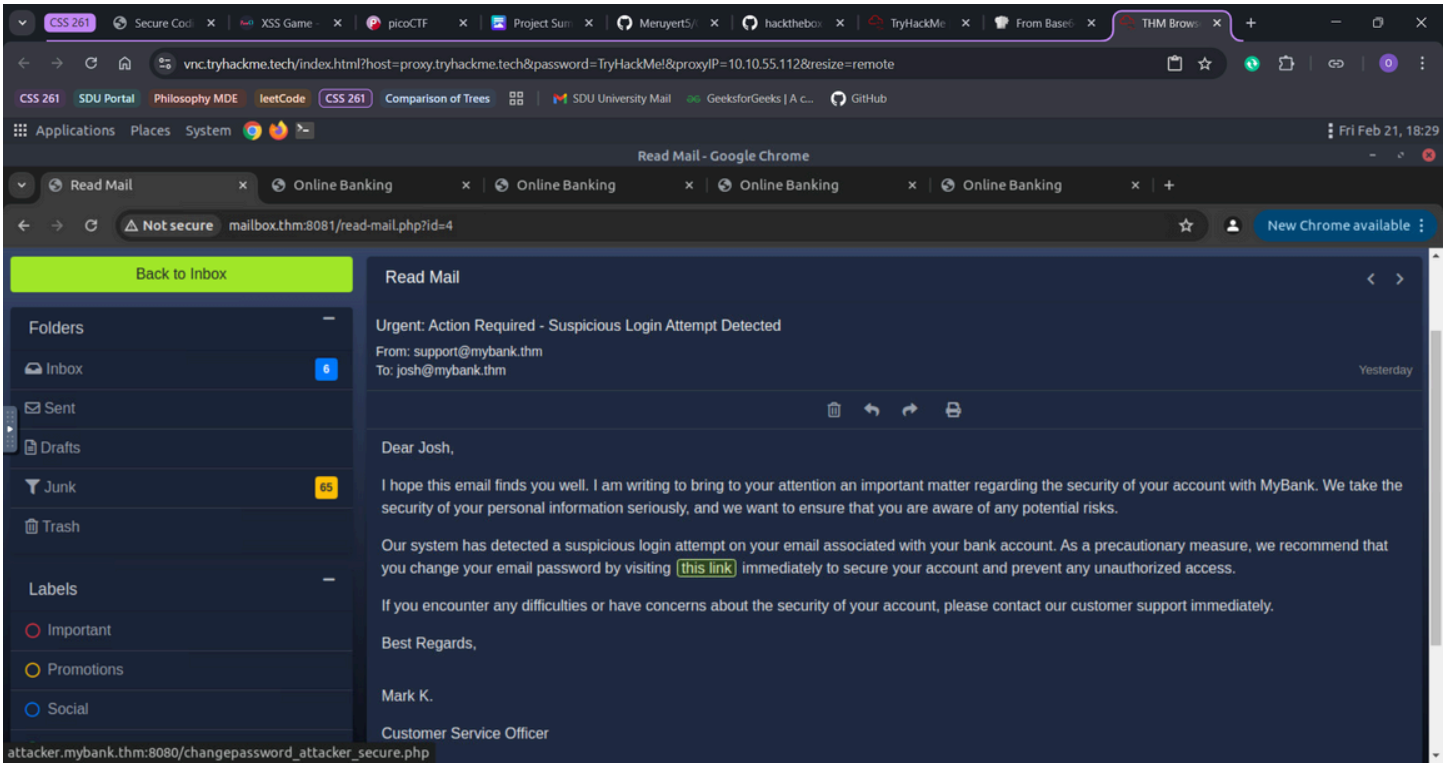




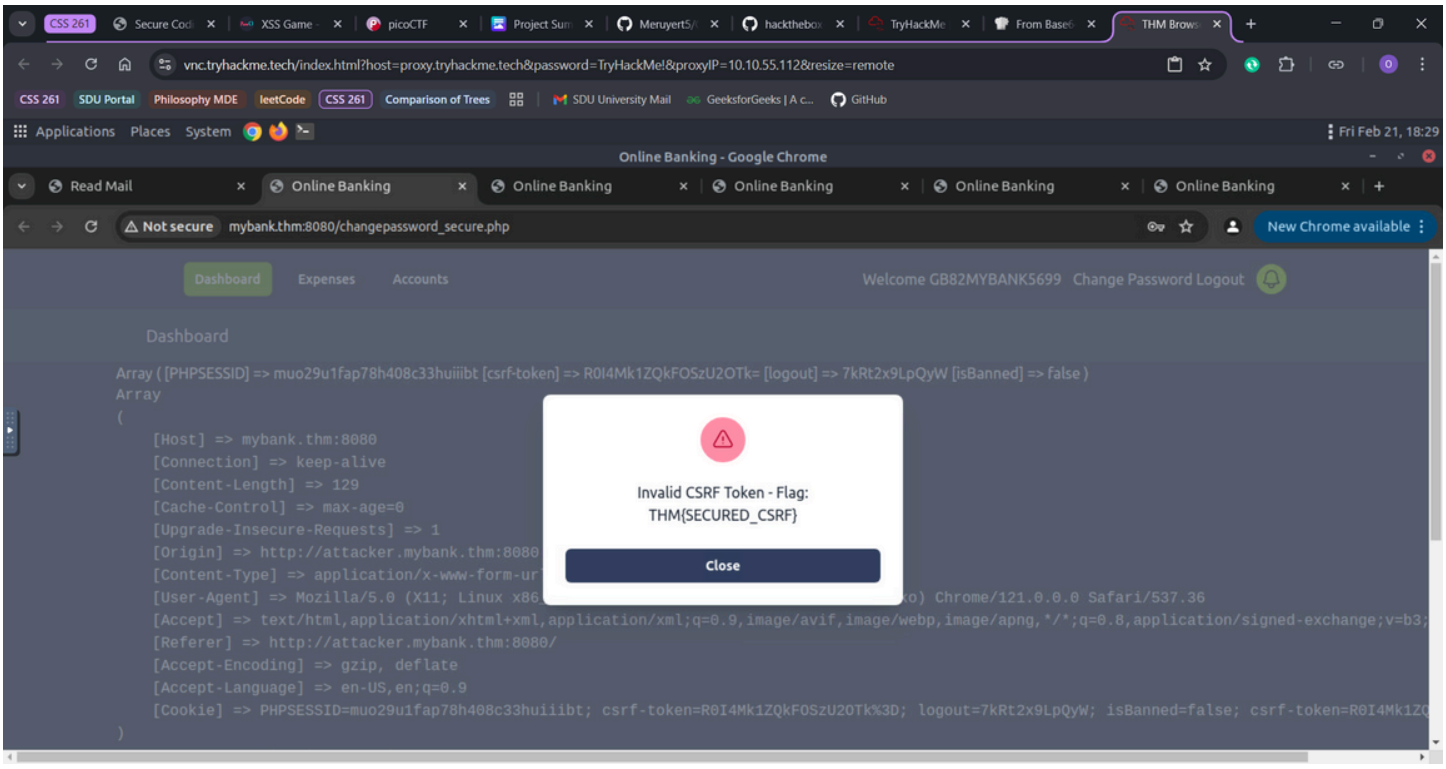
Now we click on a secure mail

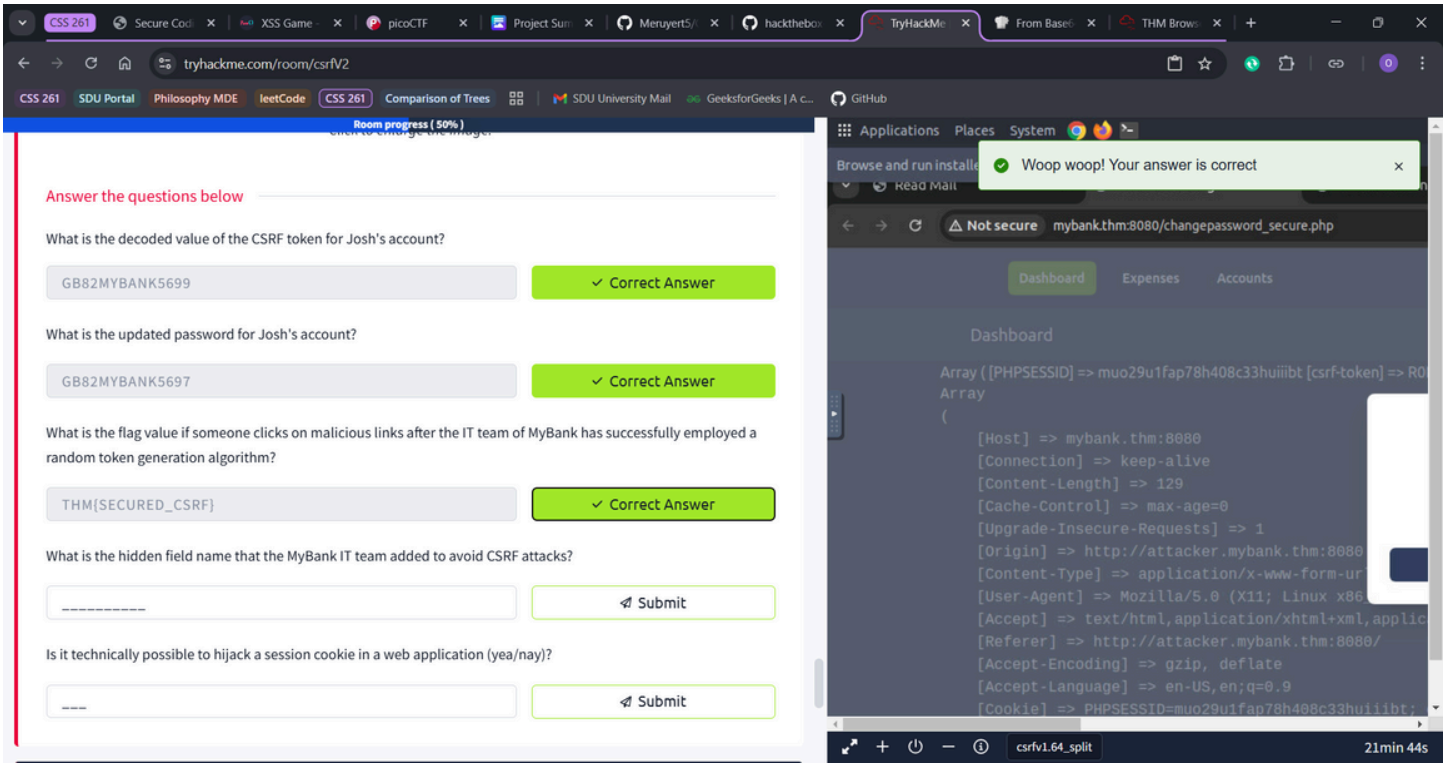


In here we also see a suspicious link

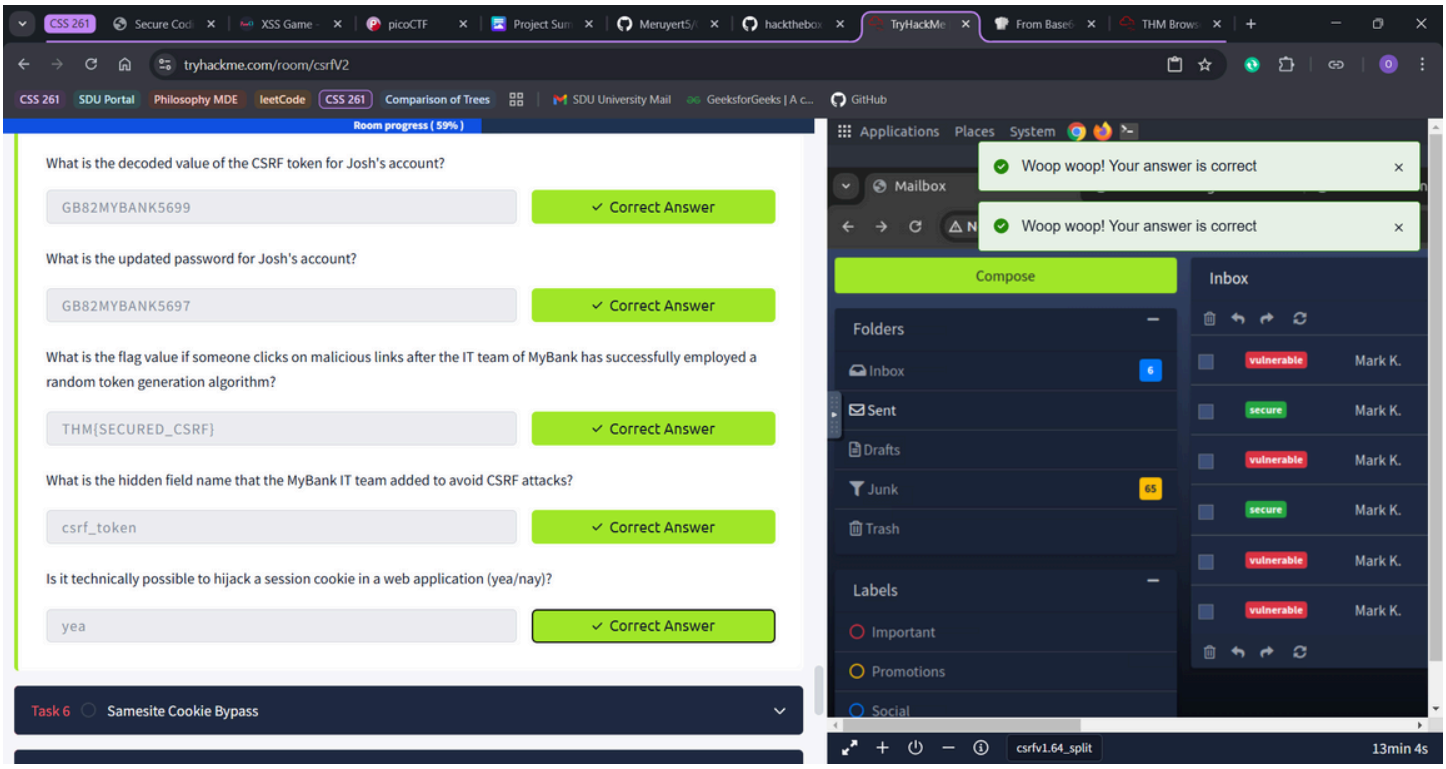


But it has been detected by out system

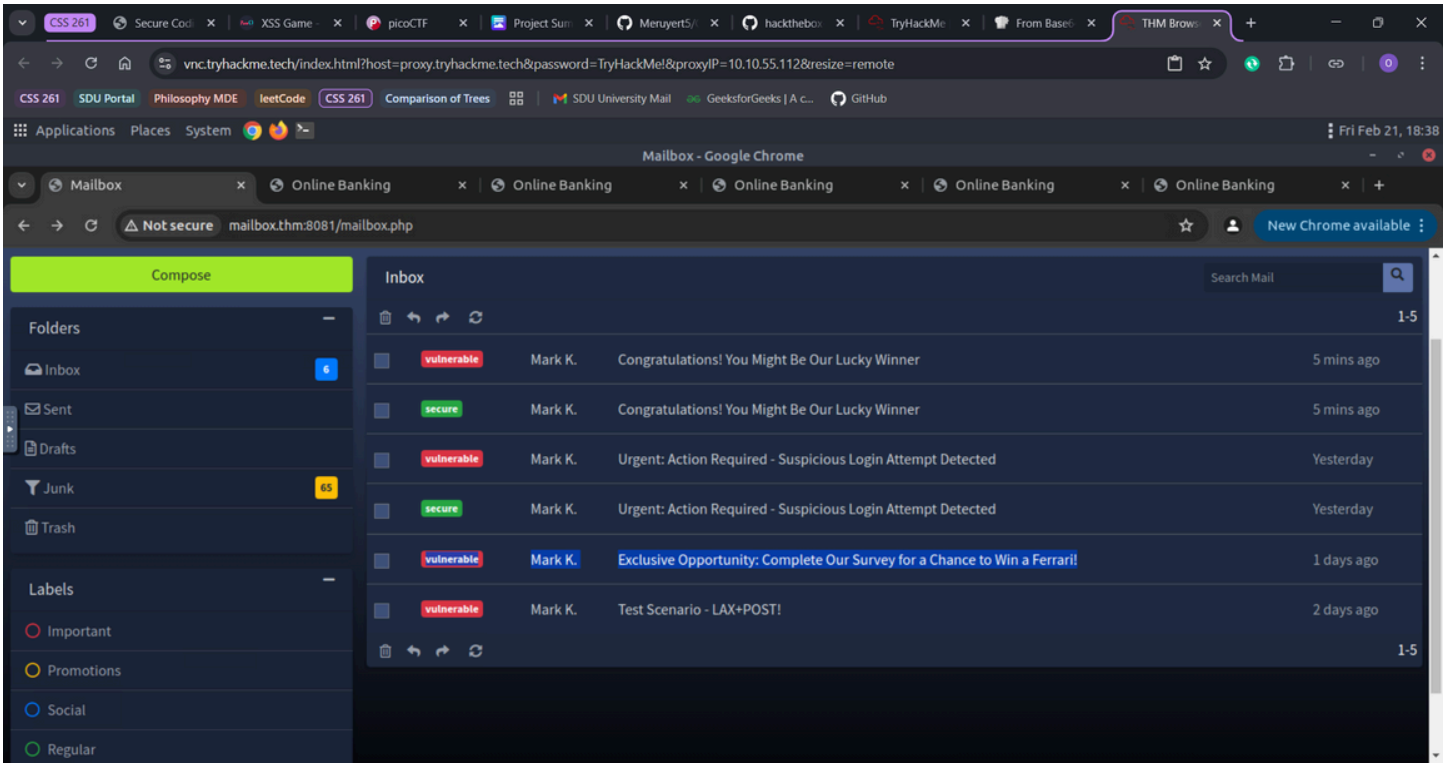




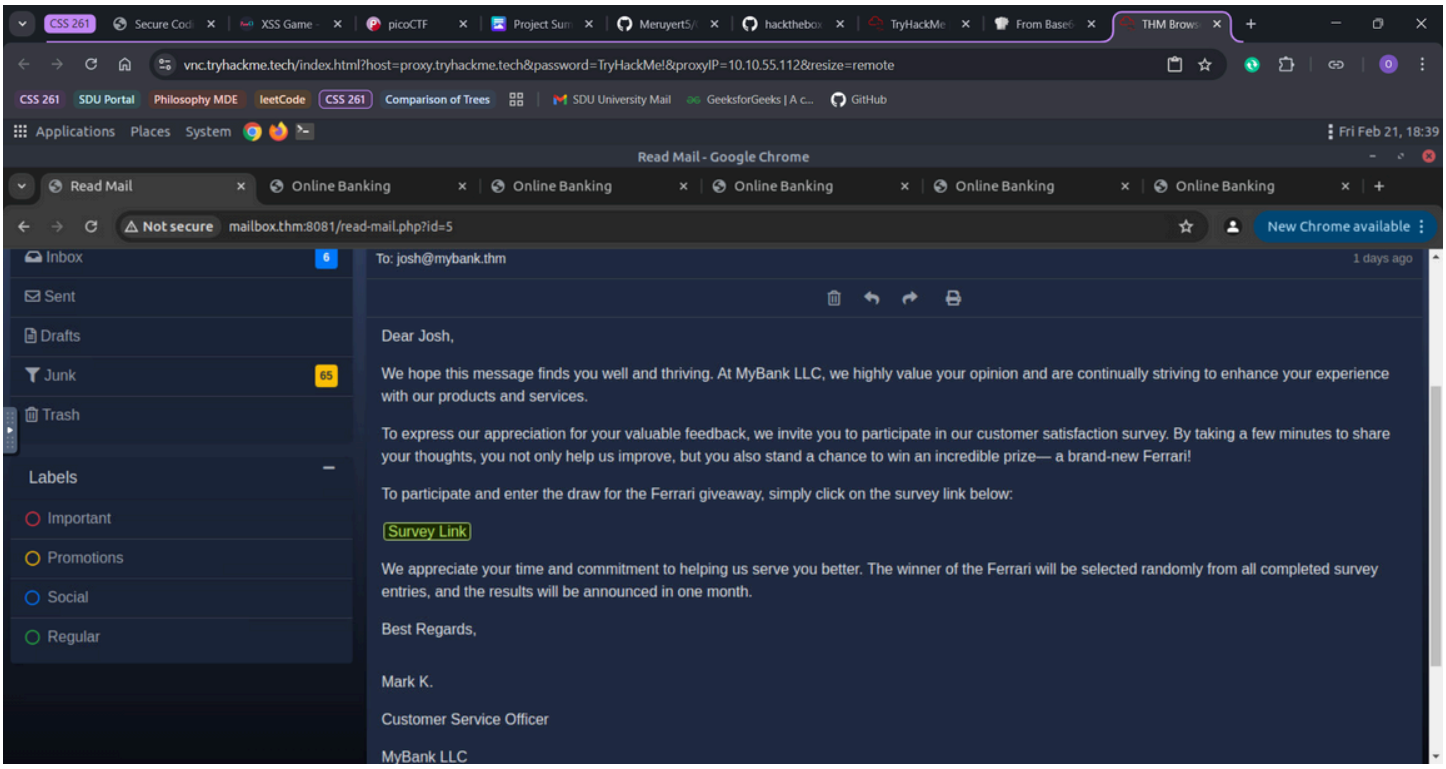
Our system detected it by adding another field named CSRF-token



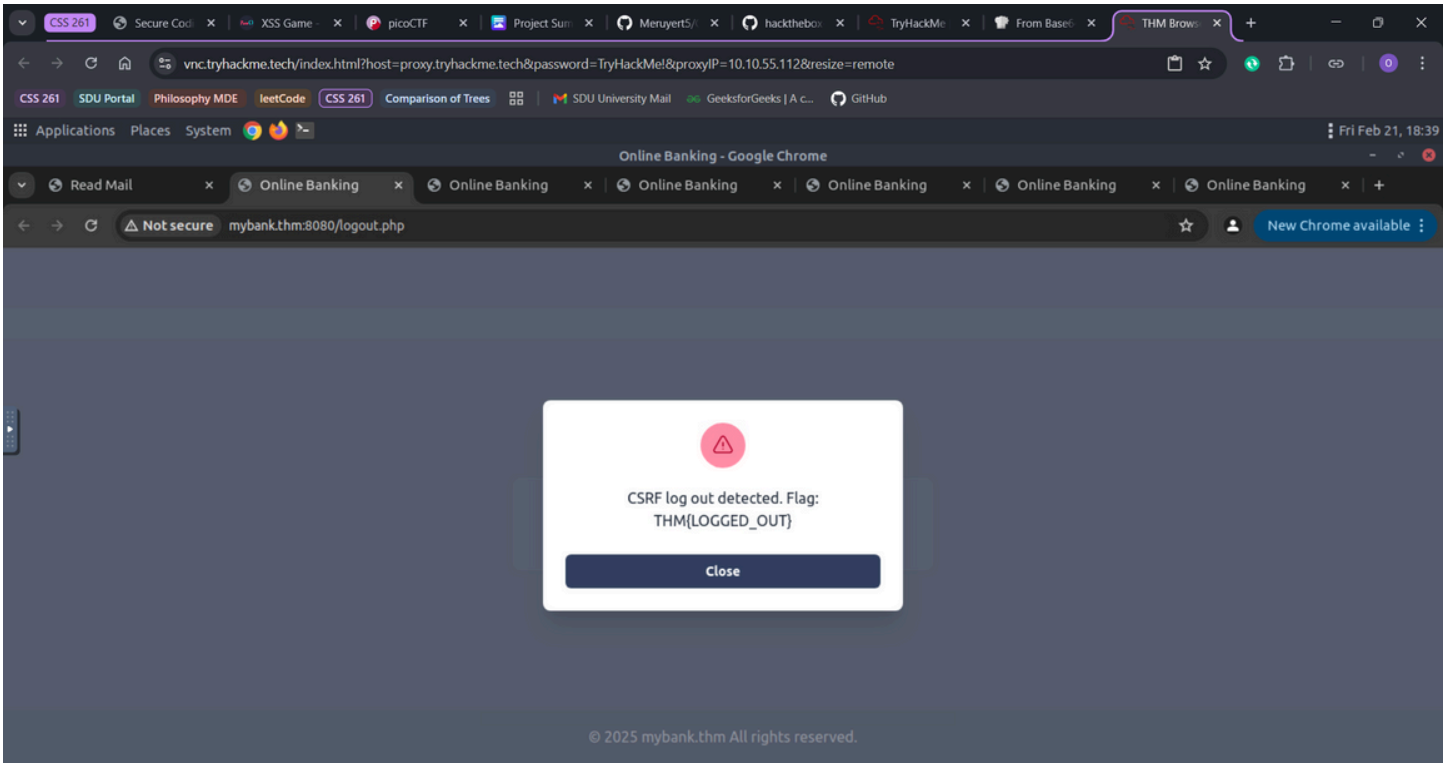
Next, we'll look at the mail received 1 day ago



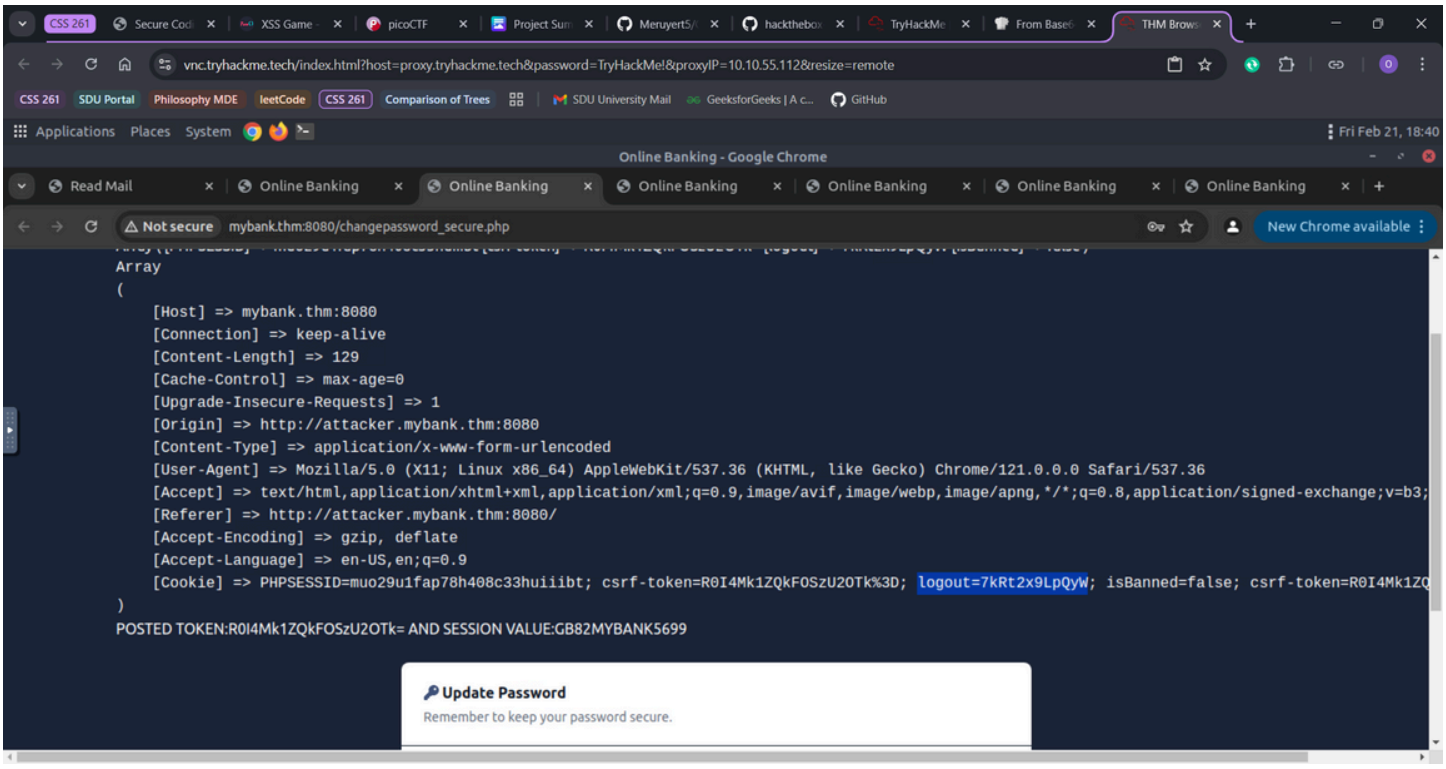
In here we see new link called Survey link

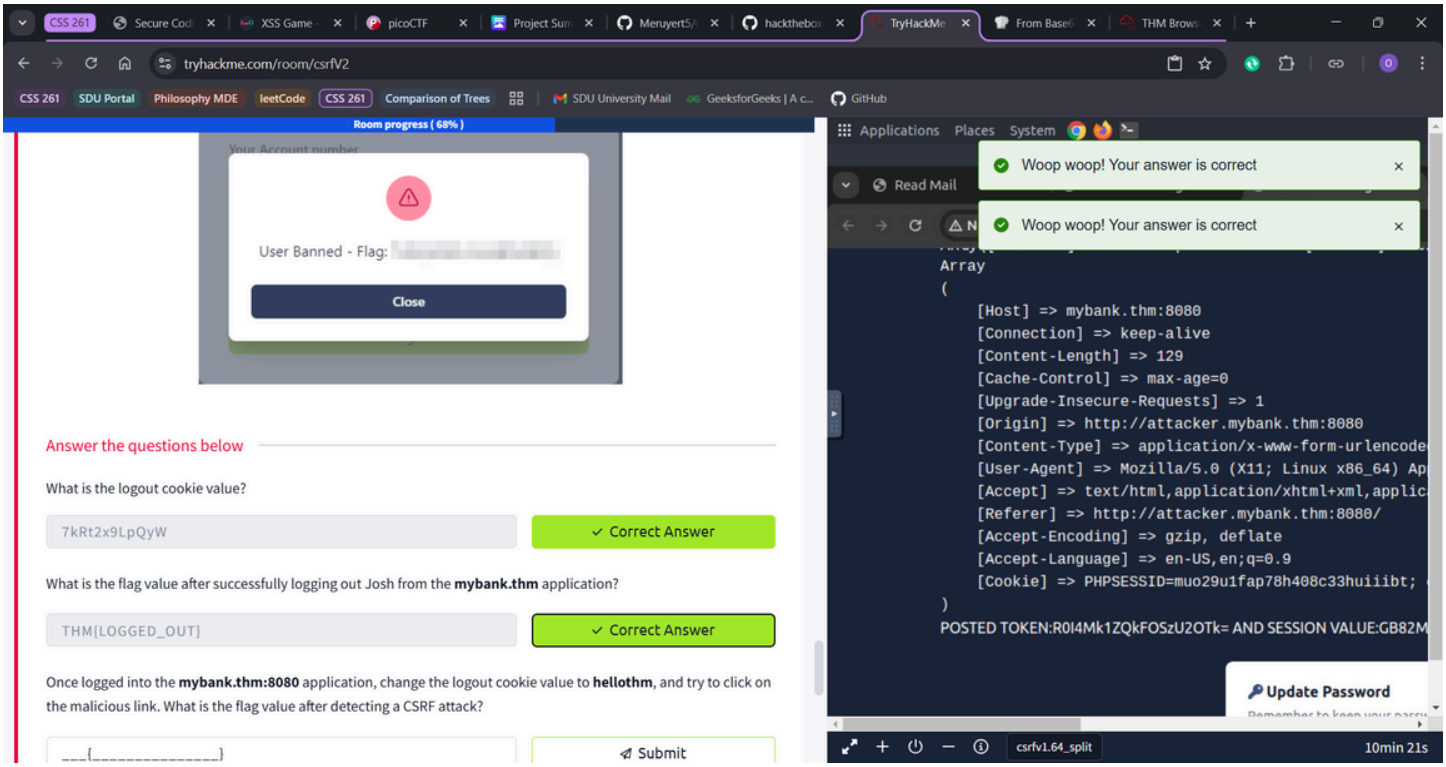


It was also detected by the bank

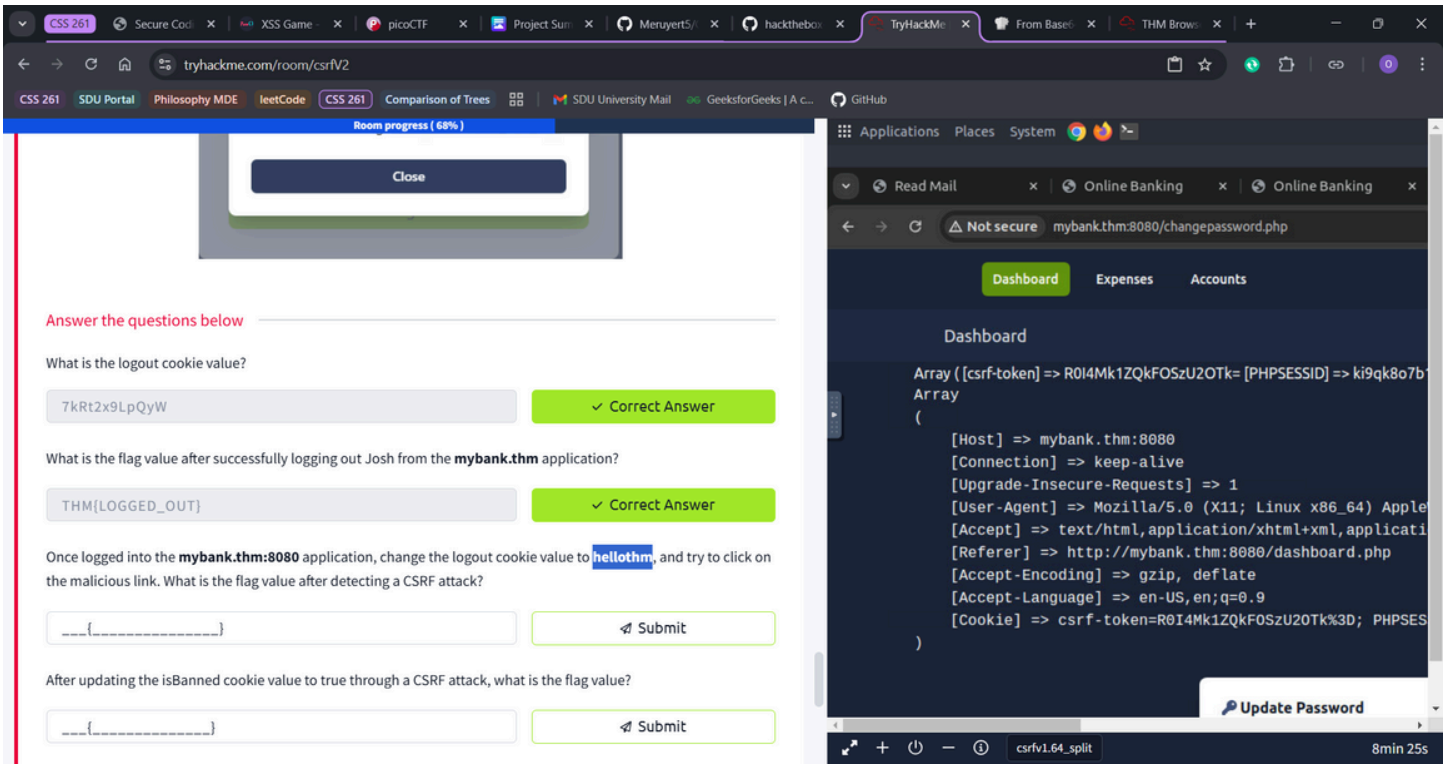


This is the logout cookie the attacker added in here

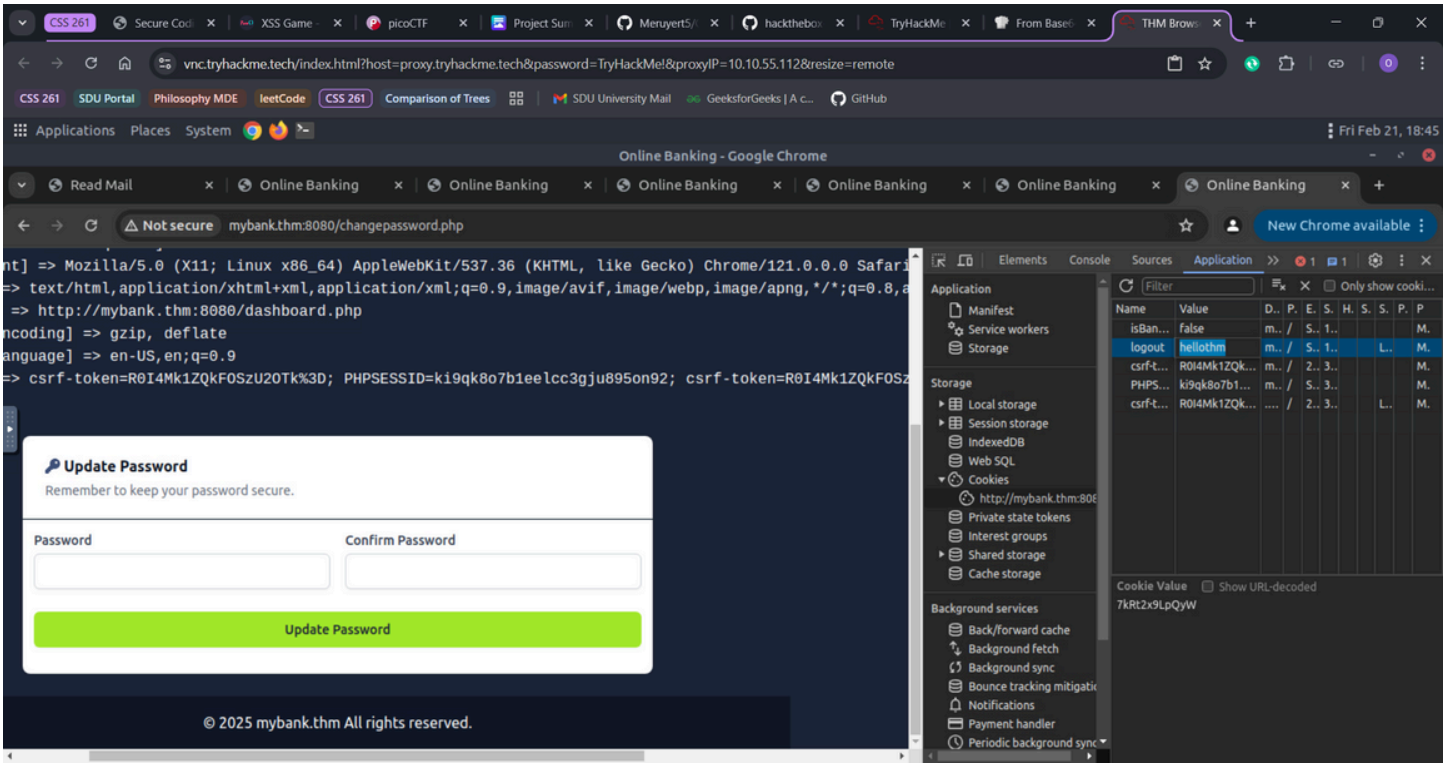




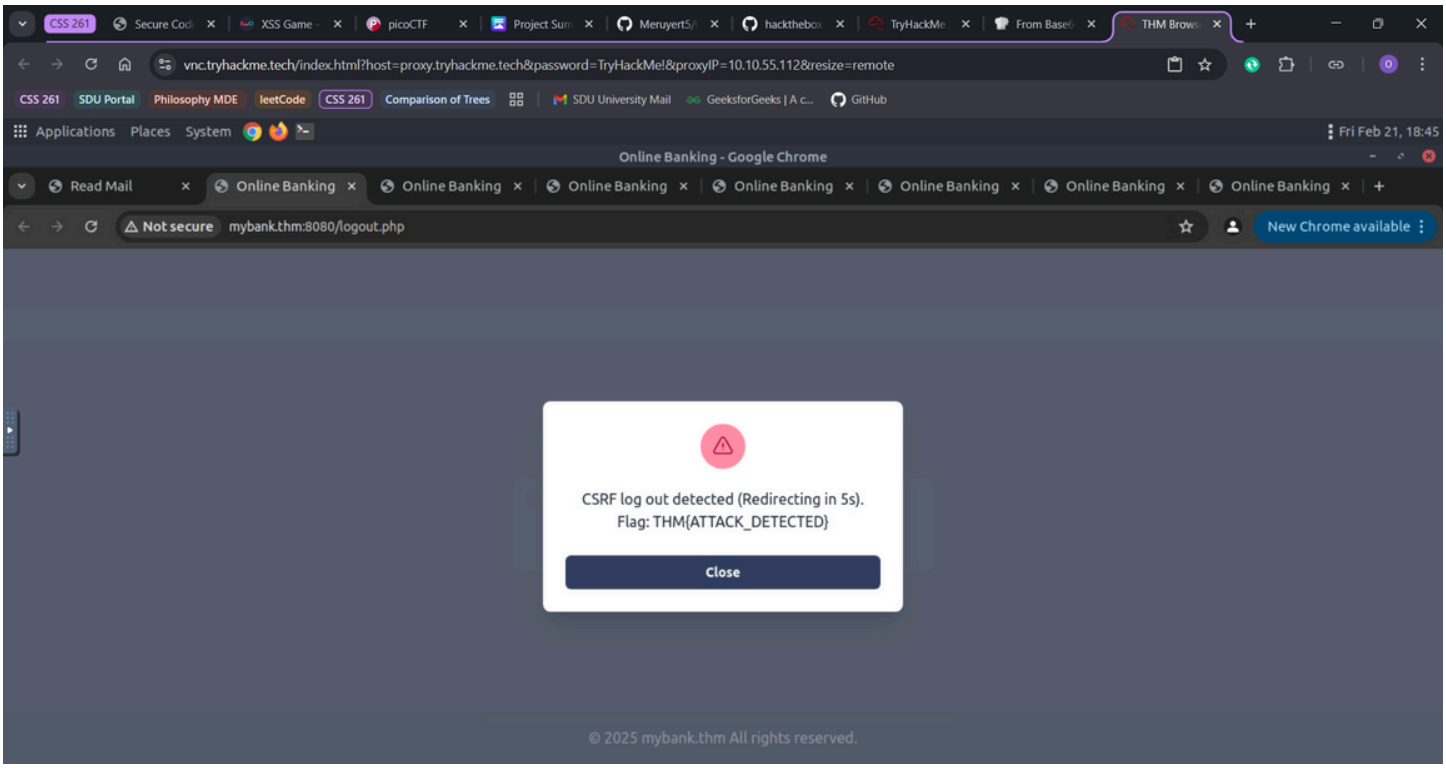
Next, we'll change the cookie valuese to `hellothm`

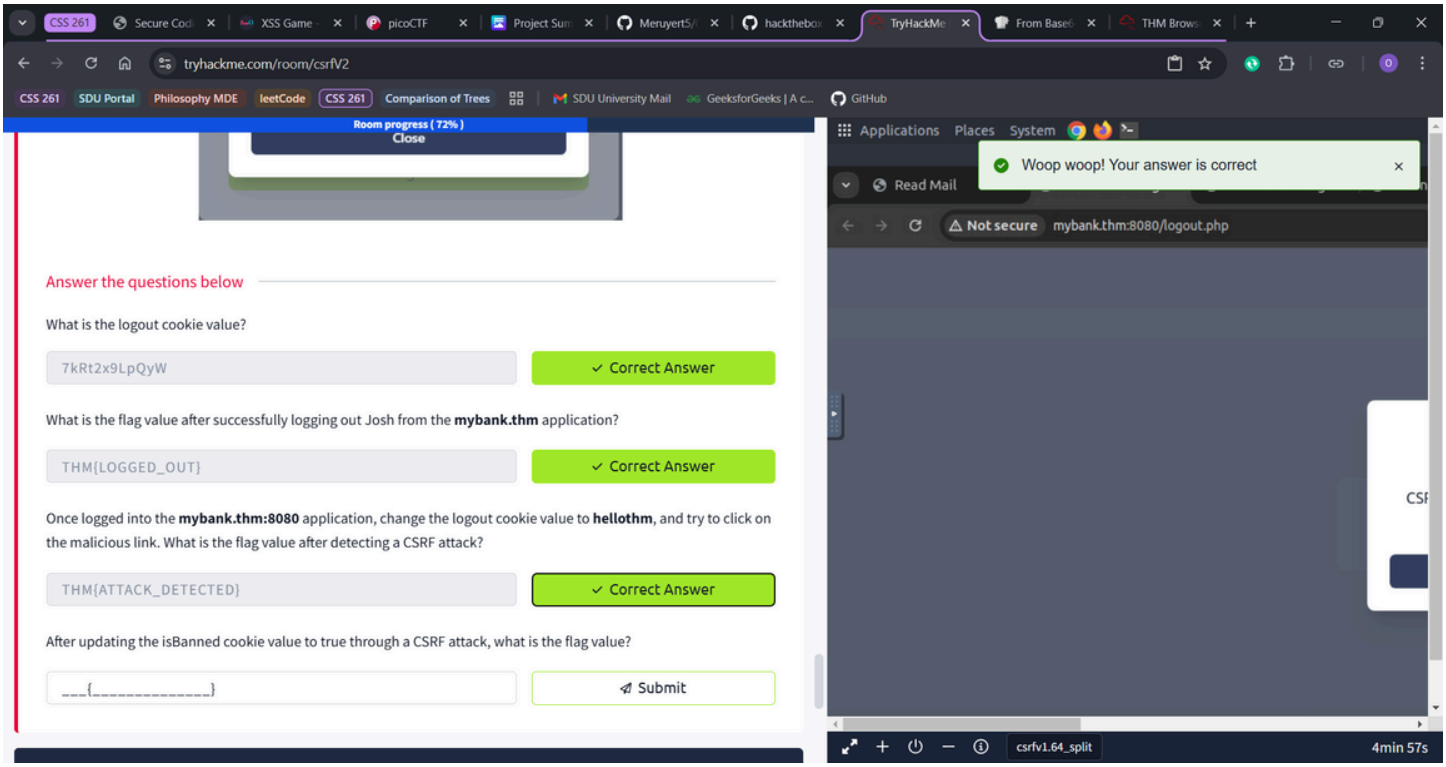


This is how it performed in the page code

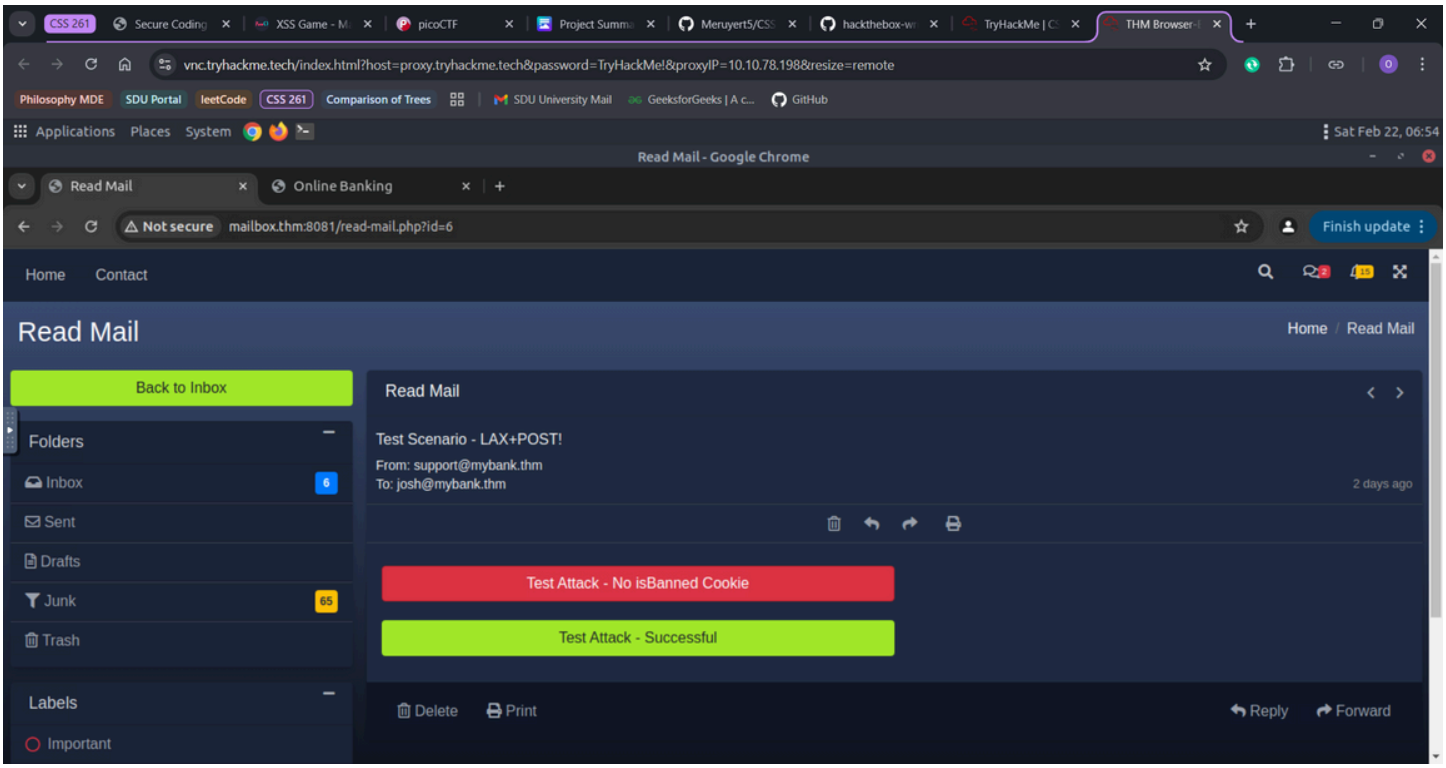


And after clicking the link again, we see our next flag

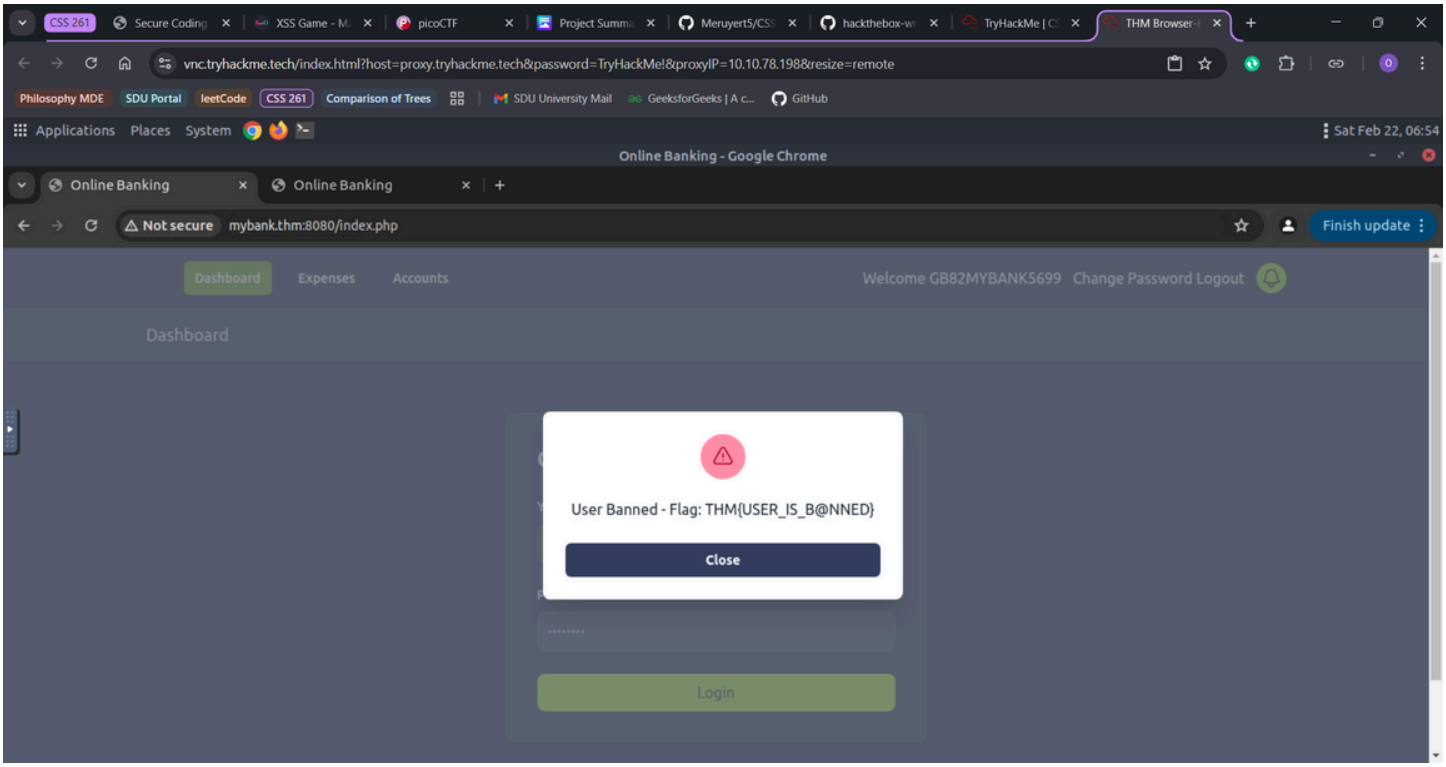


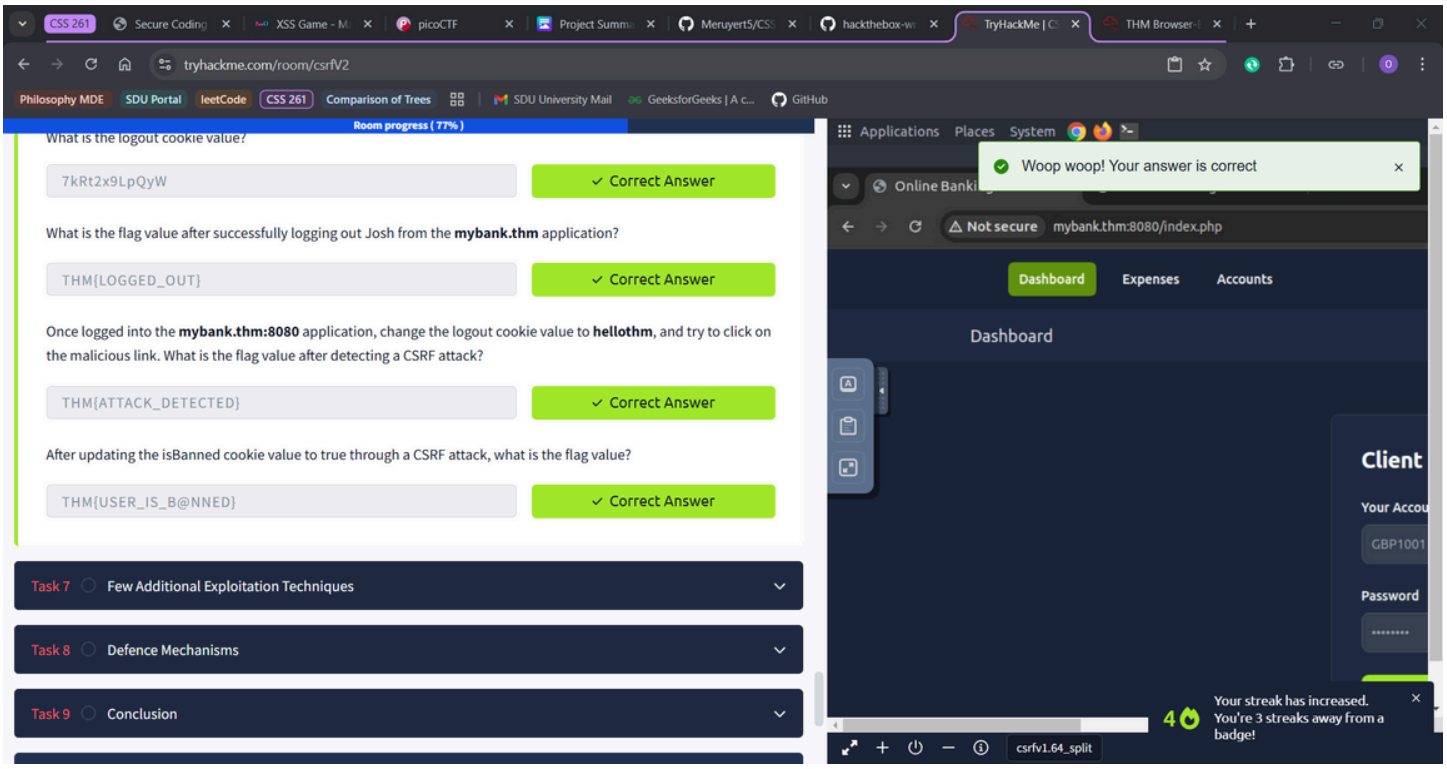


And lastly, this is the oldest mail, what we see here is two buttons

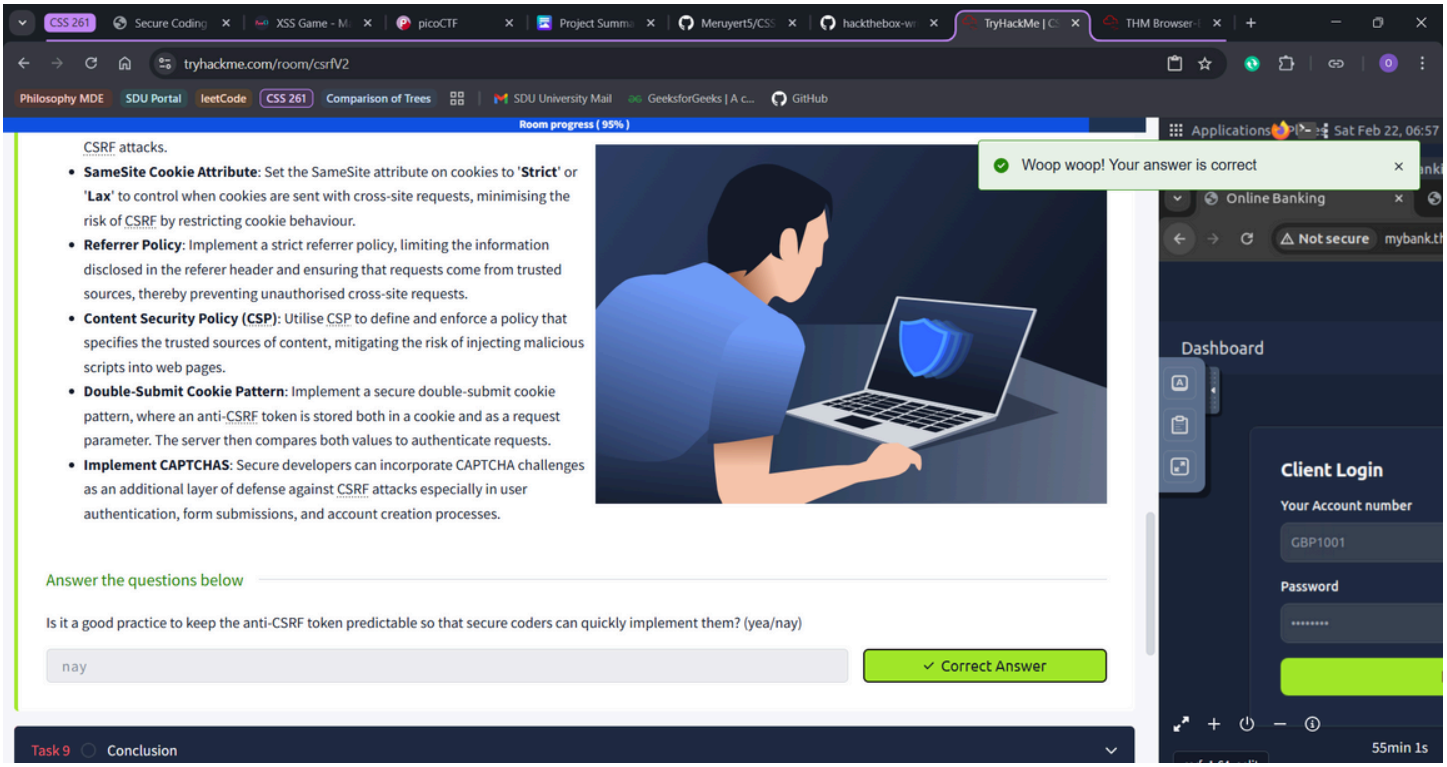


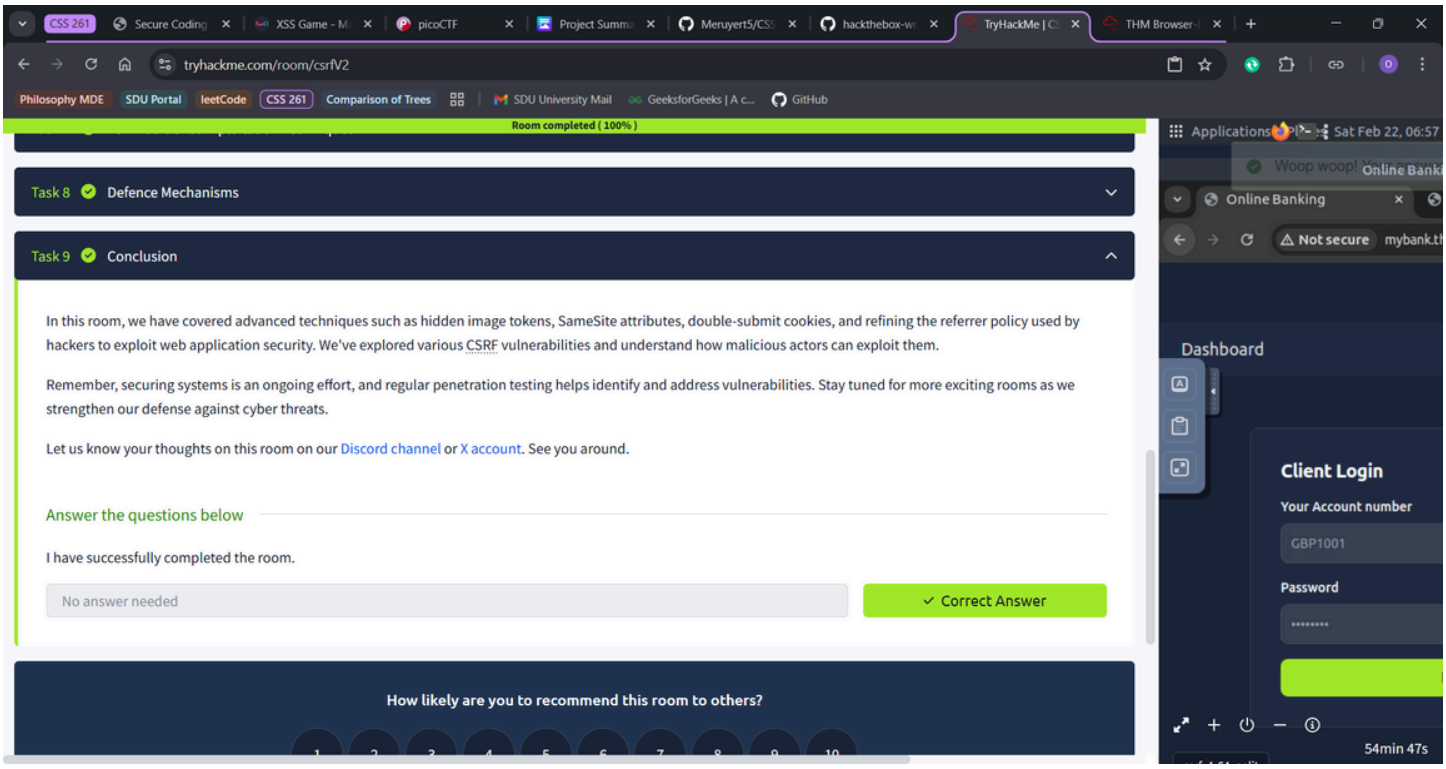
And this is the result of clicking the Test Attack, it changed the isBanned to true





So, in the end we'll just have to answer two more questions like that:





And that's how we can complete the CSRF room