

# TryHackMe

## CSRF

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

Firstly, we start the machine

The screenshot shows a Microsoft Edge browser window with multiple tabs open. The active tab is 'tryhackme.com/room/csrfv2'. The page content is a challenge titled 'CSRF' which explains what it is and how to exploit it. It includes a 'Start AttackBox' button, a progress bar at 0%, and a red header 'Target Machine Information' with details: Title 'csrvf1.64\_split', Target IP Address '10.10.55.112', and Expires '53min 8s'. Below this are buttons for '?', 'Add 1 hour', and 'Terminate'. To the right of the browser is an open Gmail inbox window. The inbox shows several messages, with one message from 'mailbox.thm:8081/mailbox....' highlighted. The Gmail interface includes a 'Compose' button, 'Folders' (Inbox, Sent, Drafts, Junk, Trash), and 'Labels' (Important, Promotions, Social).

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

CSS 261 Secure Coding Dojo XSS Game - Ma Sp picoCTF Project Summary Meruyert5/CSS-26 hackthebox-writeup TryHackMe | CSRF

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

Inbox

- Sent: Woop woop! Your answer is correct
- Drafts
- Junk
- Trash

Labels

- Important
- Promotions
- Social
- Regular

Inbox

		Search Mail
	Mark K.	Congratulations! You Might Be Our Lucky Winner
		5 mins ago
	Mark K.	Congratulations! You Might Be Our Lucky Winner
		5 mins ago
		52min 56s

CSS 261 Secure Coding Dojo XSS Game - Ma Sp picoCTF Project Summary Meruyert5/CSS-26 hackthebox-writeup TryHackMe | CSRF

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

Task 4 Basic CSRF - Hidden Link/Image Exploitation

Inbox

- Sent: Woop woop! Your answer is correct
- Sent: Woop woop! Your answer is correct
- Drafts
- Junk
- Trash

Labels

- Important
- Promotions
- Social
- Regular

Inbox

		Search Mail
	Mark K.	Congratulations! You Might Be Our Lucky Winner
		5 mins ago
	Mark K.	Congratulations! You Might Be Our Lucky Winner
		5 mins ago
		52min 5s

tryhackme.com/room/csrfV2

Room progress (22%)

major source of worry. As HTML5 technology advanced and security flaws multiplied, official support for Adobe Flash Player ceased on December 31, 2020.

Even though Flash is no longer supported, a talk about Flash-based cross-site request forgery threats is instructive, particularly for legacy systems that still rely on antiquated technologies. A malicious Flash file (.swf) posted on the attacker's website would typically send unauthorised requests to other websites to carry out Flash-based CSRF attacks.

**Answer the questions below**

What is usually the extension of a malicious flash file used during a CSRF attack?

.swf ✓ Correct Answer

Which type of CSRF exploitation is carried out when operations are initiated without a complete page request-response cycle?

Asynchronous ✓ Correct Answer

**Task 4** Basic CSRF - Hidden Link/Image Exploitation

**Task 5** Double Submit Cookie Bypass

**Task 6** Samesite Cookie Bypass

Inbox

- Sent: Woop woop! Your answer is correct
- Drafts: Woop woop! Your answer is correct
- Trash

Labels

- Important
- Promotions
- Social
- Regular

Inbox

		Search Mail
	Mark K.	Congratulations! You Might Be Our Lucky Winner
		5 mins ago
		mailbox.thm:8081/mailbox.php#
		Congratulations! You Might Be Our Lucky Winner
		5 mins
		48min 51s

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

tryhackme.com/room/csrfV2

Room progress (22%)

```
<!-- Website -->
<a href="https://mybank.thm/transfer.php" target="_blank">Click Here</a>
<!-- User visits attacker's website while authenticated -->
```

This technique preys on authenticated sessions and utilises a social engineering approach when a user may inadvertently perform operations on a different website while still logged in.

**How it Works**

Now, you are already connected to the VM. Let's see how the attack works.

- The attached VM represents Josh's machine, who uses Chrome to check his mailbox (<http://mailbox.thm:8081>) and log into his bank account (<http://mybank.thm:8080>). Since he is a financial broker by profession, he deals with many financial transactions daily and keeps his accounts logged into the browser.
- The attacker somehow learns that Josh uses [mybank.thm:8080](http://mybank.thm:8080) for transactions, and his account is always logged in.
- The attacker also had an account in the same bank, so he tried to log in and check for any vulnerabilities that he could use to get additional cash in his account.
- You can also log in to Firefox in the attached VM or any other browser using the username `GB82MYBANK5698` and password `GB82MYBANK5698` to understand the attacker's perspective and check the source code and how the client-side scripts work.
- While scanning, he found that no additional parameter was being sent from the bank app while transferring payment. Here is the code that handles the transfer of funds:

```
<?php
<form action="transfer.php" method="post">
```

Inbox

		Search Mail
	Mark K.	Congratulations! You Might Be Our Lucky Winner
		5 mins ago
		mailbox.thm:8081/Mark K.
		Congratulations! You Might Be Our Lucky Winner
		5 mins
		47min 42s

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

In our recent promotion, you have been selected as one of our potential winners to receive a free trip to Dubai. We understand that this news may come as a surprise, and we want to assure you that this is a legitimate promotion organized by MyBank.

To claim your prize, simply click on the following image to validate your entry. Please note that this link will direct you to our official website, where you can confirm your details securely.

[Click Here to Redeem](#)

Once again, congratulations on being selected as a potential winner. We appreciate your trust and loyalty to our Company.

Best Regards,

Mark K.  
Customer Service Officer  
MyBank LLC

Delete Print Reply Forward

Copyright © 2025  
mybank.thm:8080/dashboard.php?to\_account=GB82MYBANK5698&amount=1000

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

Welcome GB82MYBANK5699 Change Password Logout

Quick Transfer

Enter the details of the transfer

To Account

Transfer successful! - Flag:  
THM{SUCCESSFUL\_ATTACK}

Close

Recent activity

Today

User #GD92 created the invoice. 7d ago

Our first flag

Recent activity

User #GD92 created the invoice.

Answer the questions below

What is the flag value after a successful transfer from Josh's account?

THM{SUCCESSFUL\_ATTACK}

✓ Correct Answer

✗ Hint

What is the flag value once the CSRF attack is detected?

\_\_\_\_\_

✗ Submit

Does the hidden image exploitation require the img tag's src attribute to be linked toward a legitimate image file (yea/nay)?

---

✗ Submit

Task 5 Double Submit Cookie Bypass

38min 11s

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

Compose

Inbox

Sent

Drafts

Junk

Trash

Labels

vulnerable

secure

Mark K.

Congratulations! You Might Be Our Lucky Winner

5 mins ago

Mark K.

Congratulations! You Might Be Our Lucky Winner

5 mins ago

Mark K.

Urgent: Action Required - Suspicious Login Attempt Detected

Yesterday

Mark K.

Urgent: Action Required - Suspicious Login Attempt Detected

Yesterday

Mark K.

Exclusive Opportunity: Complete Our Survey for a Chance to Win a Ferrari!

1 days ago

Mark K.

Test Scenario - LAX+POST!

2 days ago

We see that it was blocked by our system

A screenshot of a web browser window titled "Online Banking - Google Chrome". The URL in the address bar is "mybank.thm:8080/dashboard\_secure.php?to\_account=GB82MYBANK5698&amount=1000". The page displays a "Quick Transfer" form with a red warning box overlaid. The warning box contains the text "Invalid CSRF Token Found - Flag: THM{INVALID\_CSRF\_TOKEN}" and a "Close" button. The background shows a "Recent activity" section with two entries: "User #GD92 created the invoice." (7d ago) and "User #GD92 edited the invoice." (6d ago). The top of the browser window has a tab bar with various open tabs.

This is our second flag

A screenshot of a web browser window. On the left, there is a sidebar for "tryhackme.com/room/csrfV2" showing "Room progress (31%)". The main content area displays a challenge titled "Answer the questions below". It asks: "What is the flag value after a successful transfer from Josh's account?" with input field "THM{SUCCESSFUL\_ATTACK}" and buttons "Correct Answer" and "Hint". Another question asks: "What is the flag value once the CSRF attack is detected?" with input field "THM{INVALID\_CSRF\_TOKEN}" and button "Correct Answer". A third question asks: "Does the hidden image exploitation require the img tag's src attribute to be linked toward a legitimate image file (yea/nay)?". Below these questions is a "Submit" button. At the bottom, a task bar shows "Task 5" and "Double Submit Cookie Bypass". On the right side of the browser, another tab is visible with the message "Woop woop! Your answer is correct". The top of the browser window has a tab bar with various open tabs.

The screenshot shows a web browser with multiple tabs open. On the left, a TryHackMe challenge titled 'Task 5 Double Submit Cookie Bypass' is displayed. It contains three questions with answer fields and 'Correct Answer' buttons:

- What is the flag value after a successful transfer from Josh's account? (Answer: THM{SUCCESSFUL\_ATTACK})
- What is the flag value once the CSRF attack is detected? (Answer: THM{INVALID\_CSRF\_TOKEN})
- Does the hidden image exploitation require the img tag's src attribute to be linked toward a legitimate image file (yea/nay)? (Answer: nay)

The right side of the screen shows a THM (TryHackMe) dashboard with a 'Recent activity' section and a 'Dashboard' section containing a 'Quick Transfer' form.

In this part, we look into that type of mails

The screenshot shows a web browser displaying a THM mailbox interface. The URL is `mailto.thm:8081/mailbox.php`. The inbox contains several emails:

Label	To	Subject	Time
vulnerable	Mark K.	Congratulations! You Might Be Our Lucky Winner	5 mins ago
secure	Mark K.	Congratulations! You Might Be Our Lucky Winner	5 mins ago
vulnerable	Mark K.	Urgent: Action Required - Suspicious Login Attempt Detected	Yesterday
secure	Mark K.	Urgent: Action Required - Suspicious Login Attempt Detected	Yesterday
vulnerable	Mark K.	Exclusive Opportunity: Complete Our Survey for a Chance to Win a Ferrari!	1 days ago
vulnerable	Mark K.	Test Scenario - LAX+POST!	2 days ago

As we click on the link

To: josh@mybank.thm

Dear Josh,

I hope this email finds you well. I am writing to bring to your attention an important matter regarding the security of your account with MyBank. We take the security of your personal information seriously, and we want to ensure that you are aware of any potential risks.

Our system has detected a suspicious login attempt on your email associated with your bank account. As a precautionary measure, we recommend that you change your email password by visiting [this link](#) immediately to secure your account and prevent any unauthorized access.

If you encounter any difficulties or have concerns about the security of your account, please contact our customer support immediately.

Best Regards,

Mark K.  
Customer Service Officer  
MyBank LLC

[Delete](#) [Print](#)

## Our password was updated

Dashboard Expenses Accounts

Welcome

Logout

Save password?

Username

Password  ⚡

Never Save

Passwords are saved to [Google Password Manager](#) on this device.

Array ([PHPSESSID] => muo29u1fafp78h408c33huillbt [csrf-token] => R0I4Mk1ZQkFOSzU2OTk= [logout] => 7kRt2x9L Array ( [Host] => mybank.thm:8080 [Connection] => keep-alive [Content-Length] => 129 [Cache-Control] => max-age=0 [Upgrade-Insecure-Requests] => 1 [Origin] => http://attacker.mybank.thm:8080 [Content-Type] => application/x-www-form-urlencoded [User-Agent] => Mozilla/5.0 (X11; Linux x86\_64) AppleWebKit/537.36 (KHTML, like Gecko) [Accept] => text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/w [Referer] => http://attacker.mybank.thm:8080 [Accept-Encoding] => gzip, deflate [Accept-Language] => en-US,en;q=0.9 [Cookie] => PHPSESSID=muo29u1fafp78h408c33huillbt; csrf-token=R0I4Mk1ZQkFOSzU2OTk%3D; logout=7kRt2x9LpQyW; isBanned=false; csrf-token=R0I4Mk1ZQ

## Our next flag

tryhackme.com/room/csrfV2

Room progress (40%)

```
[Content-Length] => 129
[Cache-Control] => max-age=0
[Upgrade-Insecure-Requests] => 1
[Origin] => http://attacker.mybank.thm:8080
[Content-Type] => application/x-www-form-urlencoded
[User-Agent] => Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.0.0 Safari/537.36
[Accept] => text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3
[Referer] => http://attacker.mybank.thm:8080/
```

Click to enlarge the image.

Answer the questions below

What is the decoded value of the CSRF token for Josh's account?

✓ Correct Answer

What is the updated password for Josh's account?

ⓘ

Your answer is incorrect. Please ensure it follows the answer format represented by underscores, check for typos, and try again.

What is the flag value if someone clicks on malicious links after the IT team of MyBank has successfully employed a random token generation algorithm?

ⓘ

Dashboard

```
Array ([PHPSESSID] => muo29u1fap78h408c33huiibt [csrf-token] => R0I4Mk1ZQkFOSzU2OTk= [logout] => 7kRt2x9LpQyW [isBanned] => false )
Array
(
    [Host] => mybank.thm:8080
    [Connection] => keep-alive
    [Content-Length] => 129
    [Cache-Control] => max-age=0
    [Upgrade-Insecure-Requests] => 1
    [Origin] => http://attacker.mybank.thm:8080
    [Content-Type] => application/x-www-form-urlencoded
    [User-Agent] => Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.0.0 Safari/537.36
    [Accept] => text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3
    [Referer] => http://attacker.mybank.thm:8080/
    [Accept-Encoding] => gzip, deflate
    [Accept-Language] => en-US,en;q=0.9
    [Cookie] => PHPSESSID=muo29u1fap78h408c33huiibt; csrf-token=R0I4Mk1ZQkFOSzU2OTk%3D; logout=7kRt2x9LpQyW; isBanned=false; csrf-token=R0I4Mk1ZQ
```

27min 5s

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

vnc.tryhackme.tech/index.html?host=proxy.tryhackme.tech&password=TryHackMe&proxyIP=10.10.55.112&resize=remote

Online Banking - Google Chrome

Online Banking

Welcome GB82MYBANK5699 Change Password Logout

Dashboard Expenses Accounts

```
Array ([PHPSESSID] => muo29u1fap78h408c33huiibt [csrf-token] => R0I4Mk1ZQkFOSzU2OTk= [logout] => 7kRt2x9LpQyW [isBanned] => false )
Array
(
    [Host] => mybank.thm:8080
    [Connection] => keep-alive
    [Content-Length] => 129
    [Cache-Control] => max-age=0
    [Upgrade-Insecure-Requests] => 1
    [Origin] => http://attacker.mybank.thm:8080
    [Content-Type] => application/x-www-form-urlencoded
    [User-Agent] => Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.0.0 Safari/537.36
    [Accept] => text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3
    [Referer] => http://attacker.mybank.thm:8080/
    [Accept-Encoding] => gzip, deflate
    [Accept-Language] => en-US,en;q=0.9
    [Cookie] => PHPSESSID=muo29u1fap78h408c33huiibt; csrf-token=R0I4Mk1ZQkFOSzU2OTk%3D; logout=7kRt2x9LpQyW; isBanned=false; csrf-token=R0I4Mk1ZQ
```

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

The screenshot shows the CyberChef interface. On the left sidebar under 'Operations', there are various tools like To Base64, From Base64, To Hex, From Hex, To Hexdump, From Hexdump, URL Decode, Regular expression, Entropy, Fork, Magic, Data format, and Encryption / Encoding. The main area has tabs for 'Recipe' (set to 'From Base64') and 'Input'. The input field contains the Base64 string 'R0I4Mk1ZQkF0SzU20Tk'. The output section shows the resulting ASCII characters: 'R0I4Mk1ZQkF0SzU20Tk'. Below the input field are options: 'Alphabet' (set to 'A-Za-z0-9%2B%3D'), 'Remove non-alphabet chars' (checked), and 'Strict mode' (unchecked). At the bottom are buttons for 'STEP', 'BAKE!' (with a chef icon), and 'Auto Bake'.

Next is the CSRF-token the attacker updated

The screenshot shows a browser window with multiple tabs open, all titled 'Online Banking - Google Chrome'. The active tab is 'Not secure mybank.thm:8080/changedpassword.php'. The page displays a warning about the connection being not secure. The URL bar shows the full URL: 'vnc.tryhackme.tech/index.html?host=proxy.tryhackme.tech&password=TryHackMe!&proxyIP=10.10.55.112&resize=remote'. The page content includes a user agent dump and a notice about undefined indices. Below this, a form titled 'Update Password' is shown with fields for 'Password' and 'Confirm Password', and a large green 'Update Password' button.

This is the password he changed to

CSS 261 Secure Cod... XSS Game picoCTF Project Sum... Meruyert5/... hackthebox TryHackMe From Base64 THM Browser

Last build: 5 days ago - Version 10 is here! Read about the new features here

Download CyberChef

Operations 452

Recipe Input

**From Base64**

Alphabet: A-Za-zA-Z0-9+=  
Remove non-alphabet chars Strict mode

Input: R0I4Mk1ZQkFOSzU2OTk%3D

Output: GB82MYBANK56997

STEP BAKE! Auto Bake

CSS 261 Secure Cod... XSS Game picoCTF Project Sum... Meruyert5/... hackthebox TryHackMe From Base64 THM Browser

tryhackme.com/room/csrfV2

Room progress (45%)

Invalid CSRF Token - Flag: [REDACTED]

Close

Click to enlarge the image.

Answer the questions below

What is the decoded value of the CSRF token for Josh's account?

GB82MYBANK5699

What is the updated password for Josh's account?

GB82MYBANK5697

What is the flag value if someone clicks on malicious links after the IT team of MyBank has successfully employed a random token generation algorithm?

\_\_\_\_\_

What is the hidden field name that the MyBank IT team added to avoid CSRF attacks?

POSTED TOKEN:R0I4Mk1ZQkFOSzU2OTk= AND SESSION VALUE:GB82MYBANK5699  
Notice: Undefined index: new\_password in /var/www/html/changepassword.php on line 1

22min 43s

Now we click on a secure mail

The screenshot shows a web browser window with multiple tabs open. The active tab is titled "Mailbox - Google Chrome" and displays an inbox with six messages. The messages are as follows:

- vulnerable Mark K. Congratulations! You Might Be Our Lucky Winner 5 mins ago
- secure Mark K. Congratulations! You Might Be Our Lucky Winner 5 mins ago
- vulnerable Mark K. Urgent: Action Required - Suspicious Login Attempt Detected Yesterday
- secure Mark K. Urgent: Action Required - Suspicious Login Attempt Detected Yesterday
- vulnerable Mark K. Exclusive Opportunity: Complete Our Survey for a Chance to Win a Ferrari! 1 days ago
- vulnerable Mark K. Test Scenario - LAX+POST! 2 days ago

The left sidebar shows "Folders" (Inbox, Sent, Drafts, Junk, Trash) and "Labels" (Important, Promotions, Social). The URL in the address bar is `mailto:thm:8081/read-mail.php?id=4`.

In here we also see a suspicious link

The screenshot shows a web browser window with multiple tabs open. The active tab is titled "Read Mail - Google Chrome" and displays a single email message. The message content is as follows:

Urgent: Action Required - Suspicious Login Attempt Detected  
From: support@mybank.thm  
To: josh@mybank.thm  
Yesterday

Dear Josh,

I hope this email finds you well. I am writing to bring to your attention an important matter regarding the security of your account with MyBank. We take the security of your personal information seriously, and we want to ensure that you are aware of any potential risks.

Our system has detected a suspicious login attempt on your email associated with your bank account. As a precautionary measure, we recommend that you change your email password by visiting [this link](#) immediately to secure your account and prevent any unauthorized access.

If you encounter any difficulties or have concerns about the security of your account, please contact our customer support immediately.

Best Regards,

Mark K.  
Customer Service Officer

The left sidebar shows "Folders" (Inbox, Sent, Drafts, Junk, Trash) and "Labels" (Important, Promotions, Social). The URL in the address bar is `attacker.mybank.thm:8080/changepassword_attacker_secure.php`.

But it has been detected by out system

The screenshot shows a Google Chrome window with multiple tabs open. The active tab is titled "Online Banking - Google Chrome" and displays a login page for "mybank.thm:8080/changedpassword\_secure.php". The URL bar shows the full path: "vnc.tryhackme.tech/index.html?host=proxy.tryhackme.tech&password=TryHackMe&proxyIP=10.10.55.112&resize=remote". The page content includes a dashboard with "Read Mail", "Online Banking", and "Online Banking" links. A modal dialog box is centered, displaying an error message: "Invalid CSRF Token - Flag: THM{SECURED\_CSRF}" with a red exclamation mark icon. The background page shows a PHP session dump with various headers and a cookie line containing the flag.

The screenshot shows a browser window for "tryhackme.com/room/csrfV2". The left panel displays a challenge room with progress at 50%. It contains several questions with input fields and "Correct Answer" buttons:

- What is the decoded value of the CSRF token for Josh's account? Answer: GB82MYBANK5699
- What is the updated password for Josh's account? Answer: GB82MYBANK5697
- What is the flag value if someone clicks on malicious links after the IT team of MyBank has successfully employed a random token generation algorithm? Answer: THM{SECURED\_CSRF}
- What is the hidden field name that the MyBank IT team added to avoid CSRF attacks? Answer: -----
- Is it technically possible to hijack a session cookie in a web application (yea/nay)? Answer: ---

The right panel shows a terminal window with the message "Woop woop! Your answer is correct". Below it is another browser window showing a similar banking application interface with a session dump and a modal dialog about an invalid CSRF token.

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

The screenshot shows a browser window with multiple tabs open. The active tab is 'tryhackme.com/room/csrfV2'. The page displays several questions related to CSRF attacks:

- What is the decoded value of the CSRF token for Josh's account? Answer: GB82MYBANK5699 (Correct Answer)
- What is the updated password for Josh's account? Answer: GB82MYBANK5697 (Correct Answer)
- What is the flag value if someone clicks on malicious links after the IT team of MyBank has successfully employed a random token generation algorithm? Answer: THM[SECURED\_CSRF] (Correct Answer)
- What is the hidden field name that the MyBank IT team added to avoid CSRF attacks? Answer: csrf\_token (Correct Answer)
- Is it technically possible to hijack a session cookie in a web application (yea/nay)? Answer: yea (Correct Answer)

Below the questions, there is a section titled "Task 6" with the sub-task "Samesite Cookie Bypass".

On the right side of the browser, a Gmail inbox window is open, showing several messages from "Mark K." with labels like "vulnerable" and "secure". The inbox also includes sections for Sent, Drafts, Junk, and Trash.

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

The screenshot shows a browser window with multiple tabs open. The active tab is 'vnc.tryhackme.tech/index.html?host=proxy.tryhackme.tech&password=TryHackMe!&proxyIP=10.10.55.112&resize=remote'. The page title is 'Mailbox - Google Chrome'.

The inbox contains the following messages:

- vulnerable Mark K. Congratulations! You Might Be Our Lucky Winner 5 mins ago
- secure Mark K. Congratulations! You Might Be Our Lucky Winner 5 mins ago
- vulnerable Mark K. Urgent: Action Required - Suspicious Login Attempt Detected Yesterday
- secure Mark K. Urgent: Action Required - Suspicious Login Attempt Detected Yesterday
- vulnerable Mark K. Exclusive Opportunity: Complete Our Survey for a Chance to Win a Ferrari! 1 days ago
- vulnerable Mark K. Test Scenario - LAX+POST! 2 days ago

In here we see new link called Survey link

The screenshot shows a web browser window with multiple tabs open. The active tab is titled "Read Mail - Google Chrome" and displays an email from "josh@mybank.thm". The email subject is "To: josh@mybank.thm". The message content is as follows:

Dear Josh,

We hope this message finds you well and thriving. At MyBank LLC, we highly value your opinion and are continually striving to enhance your experience with our products and services.

To express our appreciation for your valuable feedback, we invite you to participate in our customer satisfaction survey. By taking a few minutes to share your thoughts, you not only help us improve, but you also stand a chance to win an incredible prize—a brand-new Ferrari!

To participate and enter the draw for the Ferrari giveaway, simply click on the survey link below.

[Survey Link](#)

We appreciate your time and commitment to helping us serve you better. The winner of the Ferrari will be selected randomly from all completed survey entries, and the results will be announced in one month.

Best Regards,

Mark K.  
Customer Service Officer  
MyBank LLC

It was also detected by the bank

The screenshot shows a web browser window with multiple tabs open. The active tab is titled "Online Banking - Google Chrome" and displays a modal dialog box. The dialog box contains the following text:

⚠️

CSRF log out detected. Flag:  
THM{LOGGED\_OUT}

[Close](#)

At the bottom of the page, there is a footer bar with the text "© 2025 mybank.thm All rights reserved."

This is the logout cookie the attacker added in here

Online Banking - Google Chrome

Not secure mybank.thm:8080/changepassword\_secure.php

```
Array
(
    [Host] => mybank.thm:8080
    [Connection] => keep-alive
    [Content-Length] => 129
    [Cache-Control] => max-age=0
    [Upgrade-Insecure-Requests] => 1
    [Origin] => http://attacker.mybank.thm:8080
    [Content-Type] => application/x-www-form-urlencoded
    [User-Agent] => Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.0.0 Safari/537.36
    [Accept] => text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3
    [Referer] => http://attacker.mybank.thm:8080/
    [Accept-Encoding] => gzip, deflate
    [Accept-Language] => en-US,en;q=0.9
    [Cookie] => PHPSESSID=muo29u1fafp78h408c33huiibt; csrf-token=R0I4Mk1ZQkF0SzU2OTk%3D; logout=7kRt2x9LpQyW; isBanned=false; csrf-token=R0I4Mk1ZQkF0SzU2OTk%3D
)
```

POSTED TOKEN:R0I4Mk1ZQkF0SzU2OTk= AND SESSION VALUE:GB82MYBANK5699

**Update Password**

Remember to keep your password secure.

Your Account number

Room progress ( 68% )

User Banned - Flag: [REDACTED]

Close

Answer the questions below

What is the logout cookie value?

7kRt2x9LpQyW

Correct Answer

What is the flag value after successfully logging out Josh from the **mybank.thm** application?

THM{LOGGED\_OUT}

Correct Answer

Once logged into the **mybank.thm:8080** application, change the logout cookie value to **hellothm**, and try to click on the malicious link. What is the flag value after detecting a CSRF attack?

[REDACTED]

Submit

Woop woop! Your answer is correct

Woop woop! Your answer is correct

```
Array
(
    [Host] => mybank.thm:8080
    [Connection] => keep-alive
    [Content-Length] => 129
    [Cache-Control] => max-age=0
    [Upgrade-Insecure-Requests] => 1
    [Origin] => http://attacker.mybank.thm:8080
    [Content-Type] => application/x-www-form-urlencoded
    [User-Agent] => Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.0.0 Safari/537.36
    [Accept] => text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3
    [Referer] => http://attacker.mybank.thm:8080/
    [Accept-Encoding] => gzip, deflate
    [Accept-Language] => en-US,en;q=0.9
    [Cookie] => PHPSESSID=muo29u1fafp78h408c33huiibt; csrf-token=R0I4Mk1ZQkF0SzU2OTk%3D
)
```

POSTED TOKEN:R0I4Mk1ZQkF0SzU2OTk= AND SESSION VALUE:GB82MYBANK5699

**Update Password**

Remember to keep your password secure.

Next, we'll change the cookie values to **hellothm**

The screenshot shows a browser window with multiple tabs open. The main tab displays a challenge room with several questions and input fields. One question asks for the logout cookie value, which is correctly answered as '7kRt2x9LpQyW'. Another question asks for the flag after logging out, also correctly answered as 'THM{LOGGED\_OUT}'. A third question involves changing the logout cookie to 'hellothm' and detecting a CSRF attack, with the answer being '...{\_\_\_\_\_}'.

On the right side of the screen, a terminal window is running a command to capture network traffic. The command is:

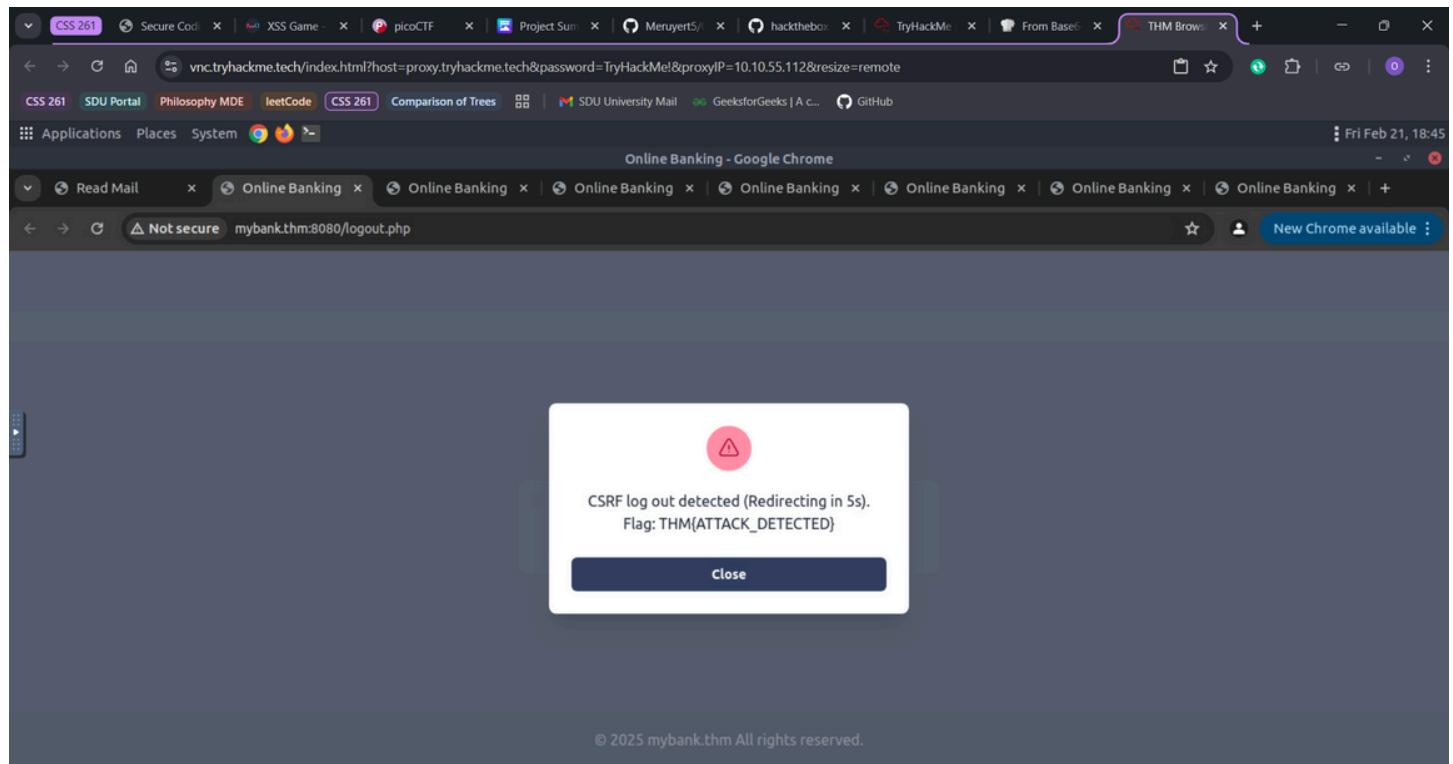
```
curl -H "Host: mybank.thm:8080" -H "Connection: keep-alive" -H "Upgrade-Insecure-Requests: 1" -H "User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.0.0 Safari/537.36" -H "Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9" -H "Referer: http://mybank.thm:8080/dashboard.php" -H "Accept-Encoding: gzip, deflate" -H "Accept-Language: en-US,en;q=0.9" -H "Cookie: csrf-token=R0I4Mk1ZQkF0SzU20Tk%3D; PHPSESSID=ki9qk8o7b1eelcc3gju895on92; csrf-t... R0I4Mk1ZQkF0SzU20Tk%3D; PHPSESSID=ki9qk8o7b1eelcc3gju895on92; csrf-t..." http://mybank.thm:8080/changepassword.php
```

The terminal output shows the captured request and response, including the CSRF token and session ID.

This is how it performed in the page code

The screenshot shows a password update form on the left and the Chrome DevTools Application tab on the right. The Application tab displays the browser's internal state, specifically the cookies. The 'isBanned' cookie is set to 'False'. Other visible cookies include 'logout' (value 'hellothm'), 'csrf-t...' (value 'R0I4Mk1ZQkF0SzU20Tk%3D'), and 'PHPSESSID' (value 'ki9qk8o7b1eelcc3gju895on92').

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



A screenshot of a browser window titled "tryhackme.com/room/csrfV2". The address bar shows "tryhackme.com/room/csrfV2". A progress bar at the top indicates "Room progress (72%)". Below it, there is a "Close" button. On the left, there is a section titled "Answer the questions below" with several questions and their answers:

- What is the logout cookie value? Answer: 7kRt2x9LpQyW
- What is the flag value after successfully logging out Josh from the mybank.thm application? Answer: THM{LOGGED\_OUT}
- Once logged into the mybank.thm:8080 application, change the logout cookie value to hellothm, and try to click on the malicious link. What is the flag value after detecting a CSRF attack? Answer: THM{ATTACK\_DETECTIED}
- After updating the isBanned cookie value to true through a CSRF attack, what is the flag value? Answer: \_\_\_\_\_

To the right of the main window, a smaller window shows a message: "Woop woop! Your answer is correct".

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

The screenshot shows a web browser window with multiple tabs open. The active tab is titled "Read Mail - Google Chrome" and displays an email inbox. On the left, there's a sidebar with "Folders" (Inbox, Sent, Drafts, Junk, Trash) and "Labels" (Important). The main area shows an email from "support@mybank.thm" to "josh@mybank.thm" with the subject "Test Scenario - LAX+POST!". Below the message, there are two red and green buttons labeled "Test Attack - No isBanned Cookie" and "Test Attack - Successful". At the bottom of the email view are standard controls: Delete, Print, Reply, and Forward.

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

The screenshot shows a web browser window with multiple tabs open. The active tab is titled "Online Banking - Google Chrome" and displays a user login interface. At the top right, it says "Welcome GB82MYBANK5699 Change Password Logout". A central modal dialog box is displayed, showing a red triangle icon and the text "User Banned - Flag: THM{USER\_IS\_B@NNED}" with a "Close" button. In the background, there are navigation links for "Dashboard", "Expenses", and "Accounts".

What is the logout cookie value?

7kRt2x9LpQyW

✓ Correct Answer

What is the flag value after successfully logging out Josh from the **mybank.thm** application?

THM[LOGGED\_OUT]

✓ Correct Answer

Once logged into the **mybank.thm:8080** application, change the logout cookie value to **hellothm**, and try to click on the malicious link. What is the flag value after detecting a CSRF attack?

THM[ATTACK\_DETECTED]

✓ Correct Answer

After updating the isBanned cookie value to true through a CSRF attack, what is the flag value?

THM[USER\_IS\_B@NNED]

✓ Correct Answer

**Task 7** ○ Few Additional Exploitation Techniques

**Task 8** ○ Defence Mechanisms

**Task 9** ○ Conclusion

Woop woop! Your answer is correct

Dashboard Expenses Accounts

Your streak has increased. You're 3 streaks away from a badge!

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

CSRF attacks.

- **SameSite Cookie Attribute:** Set the SameSite attribute on cookies to 'Strict' or 'Lax' to control when cookies are sent with cross-site requests, minimising the risk of CSRF by restricting cookie behaviour.
- **Referrer Policy:** Implement a strict referrer policy, limiting the information disclosed in the referer header and ensuring that requests come from trusted sources, thereby preventing unauthorised cross-site requests.
- **Content Security Policy (CSP):** Utilise CSP to define and enforce a policy that specifies the trusted sources of content, mitigating the risk of injecting malicious scripts into web pages.
- **Double-Submit Cookie Pattern:** Implement a secure double-submit cookie pattern, where an anti-CSRF token is stored both in a cookie and as a request parameter. The server then compares both values to authenticate requests.
- **Implement CAPTCHAS:** Secure developers can incorporate CAPTCHA challenges as an additional layer of defense against CSRF attacks especially in user authentication, form submissions, and account creation processes.



Woop woop! Your answer is correct

Dashboard

Client Login

Your Account number: GBP1001

Password: .....  
.....

Is it a good practice to keep the anti-CSRF token predictable so that secure coders can quickly implement them? (yea/nay)

nay

✓ Correct Answer

**Task 9** ○ Conclusion

55min 1s

The screenshot shows a web browser with multiple tabs open. The main tab displays the TryHackMe CSRF room completion page. The page shows a green progress bar at 100% completion. Below it, two sections are listed: 'Task 8 Defence Mechanisms' and 'Task 9 Conclusion'. The 'Conclusion' section contains a message about advanced security techniques and CSRF vulnerabilities, followed by a call to action to share thoughts on a Discord channel or account. A note says 'I have successfully completed the room.' with a 'Correct Answer' button. A satisfaction survey asks 'How likely are you to recommend this room to others?' with a scale from 1 to 10. A sidebar on the right shows a 'Client Login' interface with fields for account number (GBP1001) and password, and a 'Dashboard' section.

And that's how we can complete the CSRF room

The screenshot shows the TryHackMe CSRF room completion summary page. It features a large circular icon with a computer monitor and a 'No' symbol, with the text '</CSRF>' below it. A green success message box says 'Woop woop! Your answer is correct'. Below the icon, a congratulatory message reads 'Congratulations on completing CSRF!!!' with a small emoji. At the bottom, five summary statistics are displayed in cards: 'Points earned' (160), 'Completed tasks' (9), 'Room type' (Walkthrough), 'Difficulty' (Medium), and 'Streak' (4). Buttons for 'Leave Feedback' and 'Next' are at the bottom.