Sri Lanka Institute of Information Technology

Web Security – IE2062

TryHackMe Report

Y2S2.WE.CS

S.D.W. GUNARATNE - IT23241978

1. Room Overview:

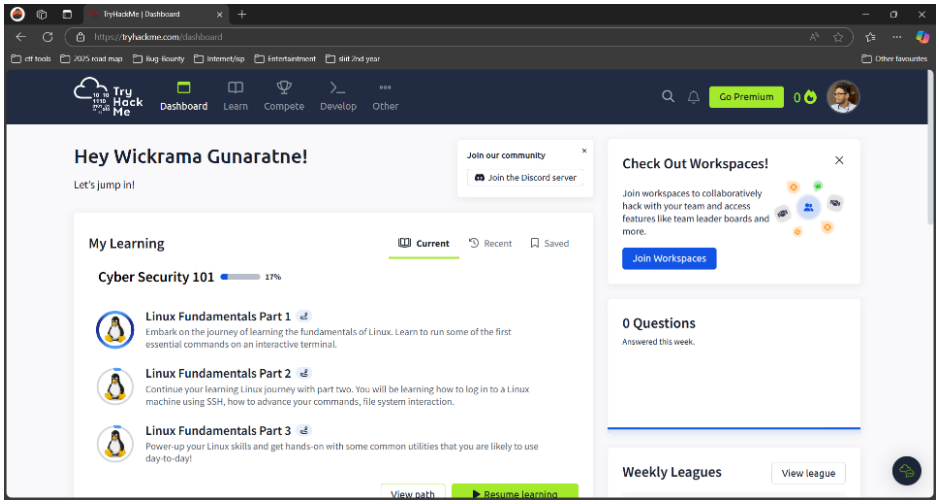
You've logged in as a normal user to your online banking portal. But can you view another user's profile by hacking the URL? Your job is to view another user's account page without logging in as the other user. With these practices and theories help us to understand Broken access control.

2. Learning Objectives:

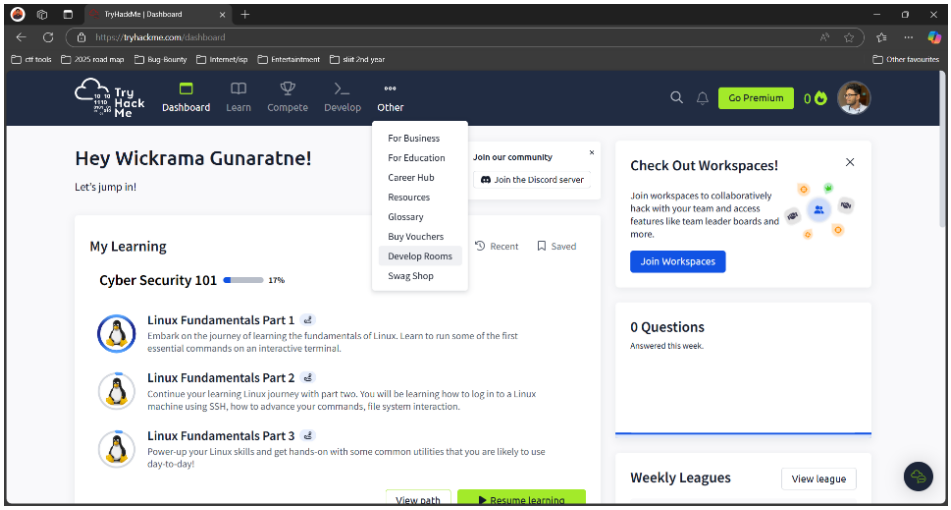
- Understand OWASP top 10 vulnerabilities.
- Understand of Broken access control and its types.
- How to bypass system (use sessions/cookies).
- How to find and mitigate Broken Access Control.
- Practical hands-on experience with Broken Access Control.

3. Room Structure:

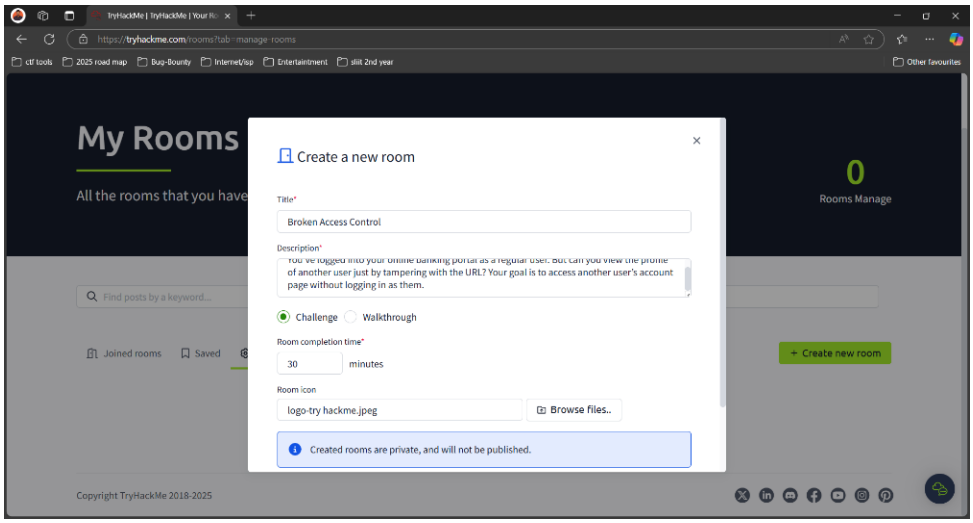
Create a TryHackMe account



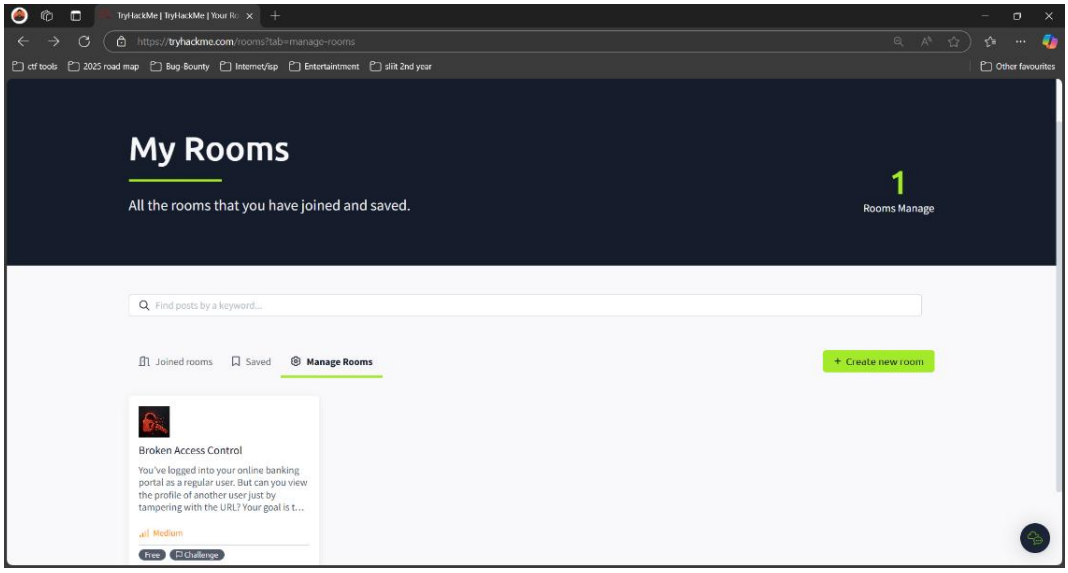
➢ Go to other and select the Develop Rooms



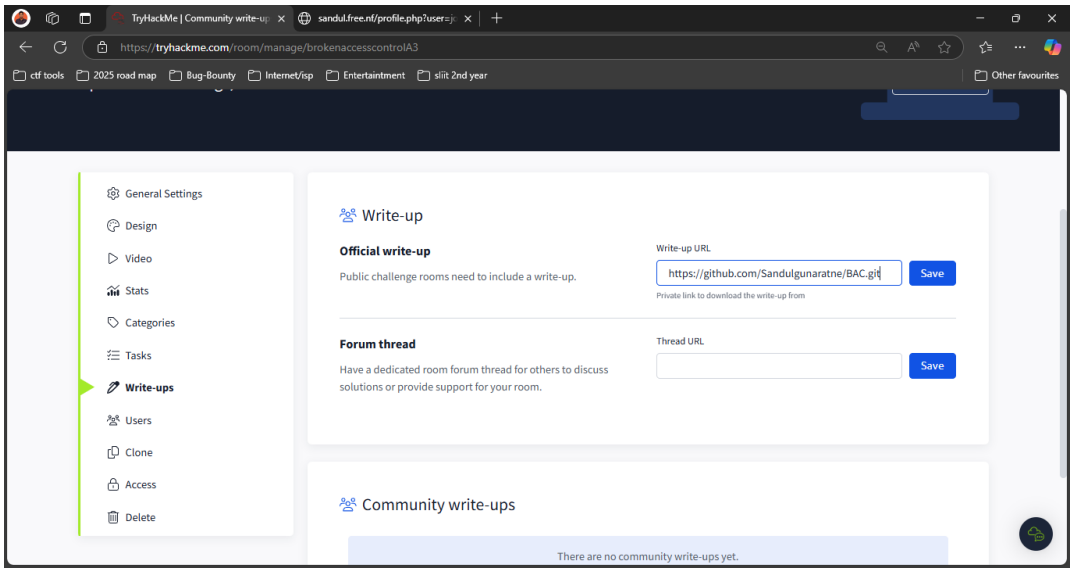
➢ Select Green colour button “create room”

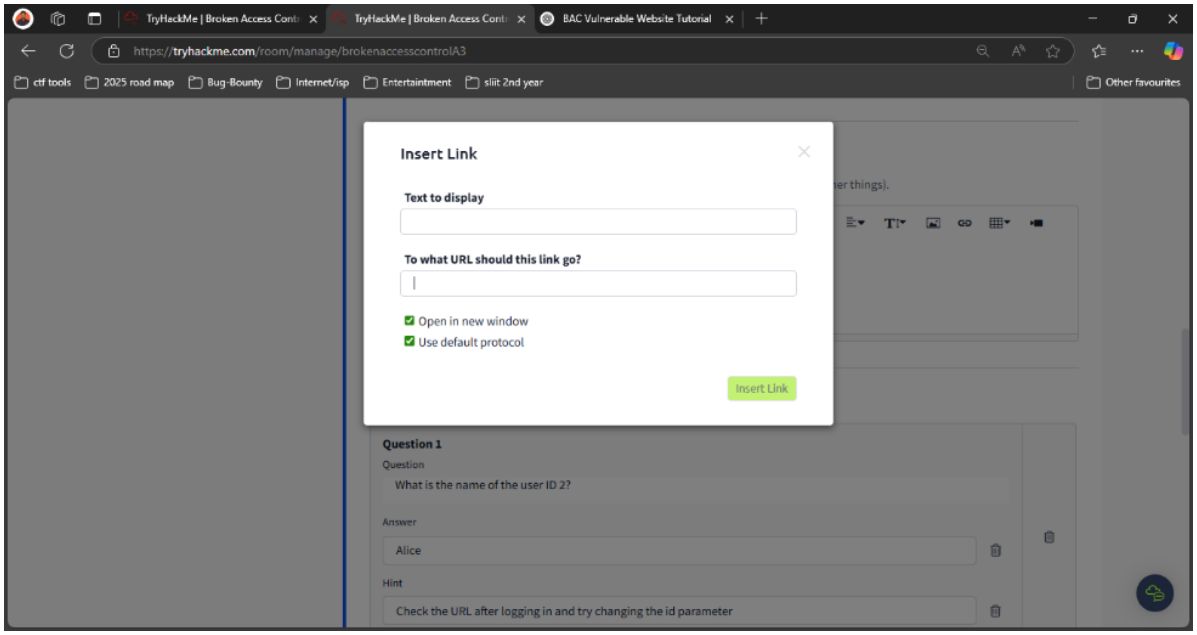


- Select Green colour button “create room”

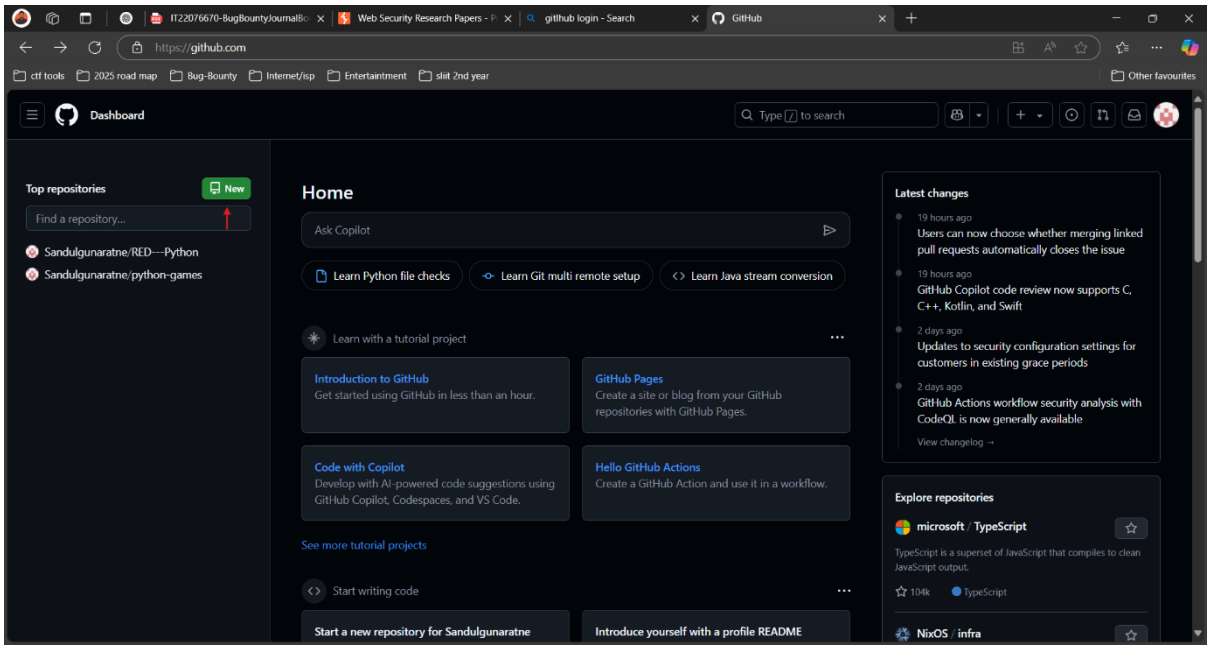


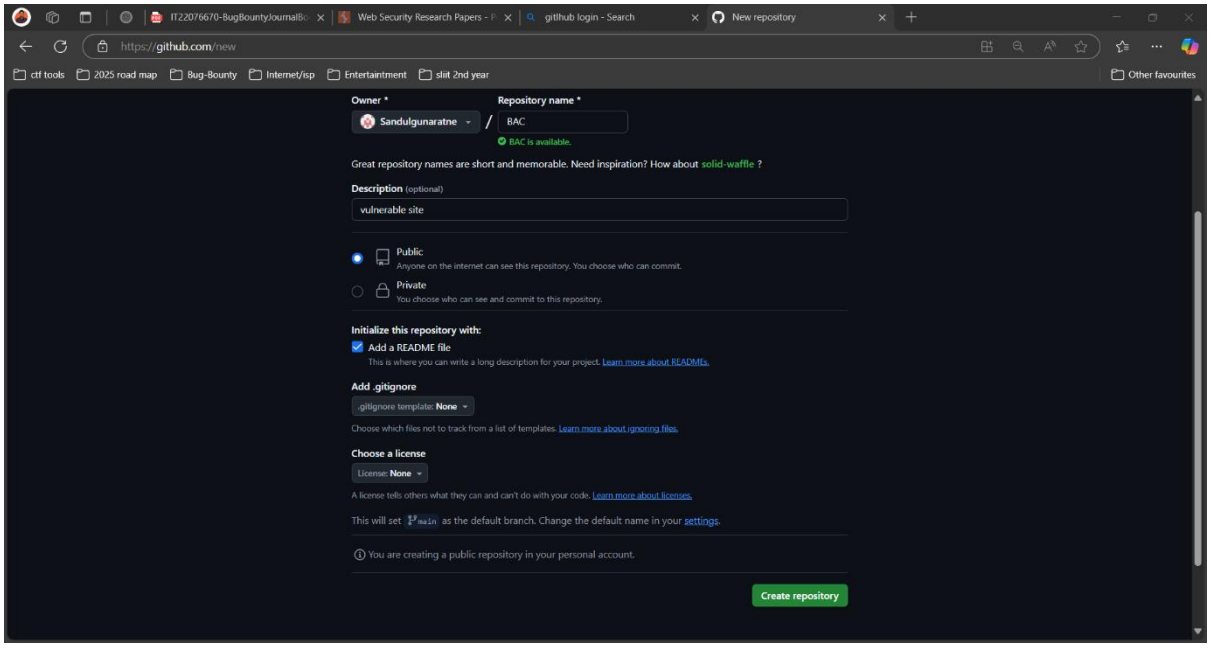
- Define Room Settings as below



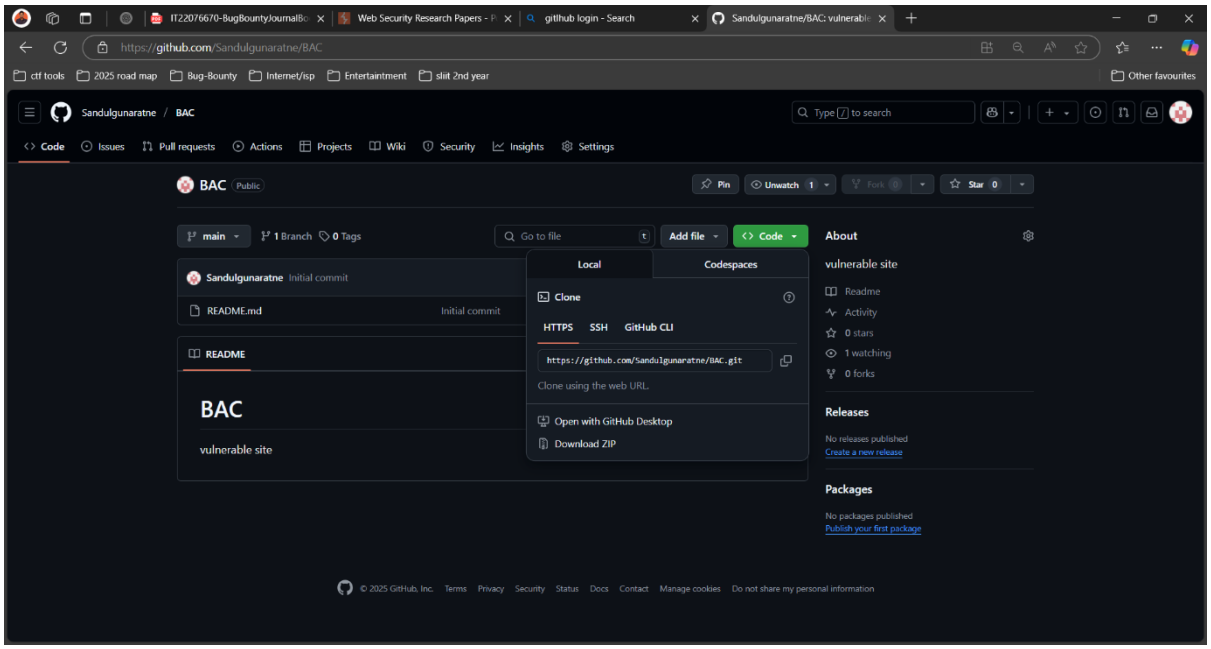


- Go to git and add it to we created vulnerable site.

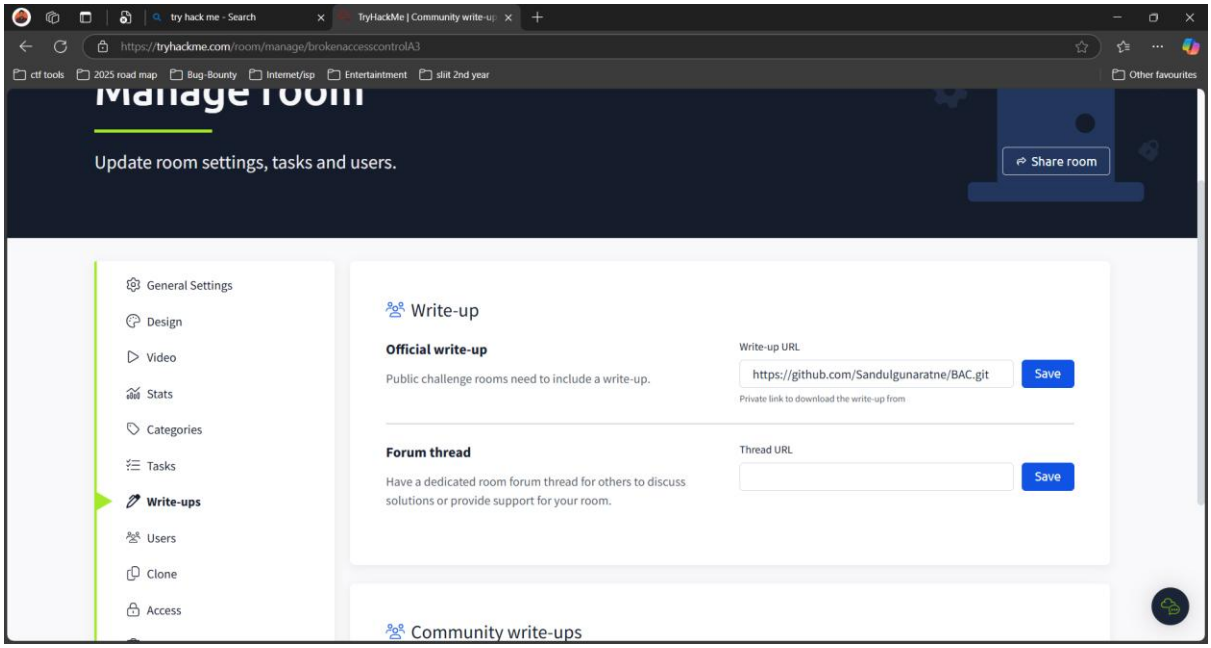


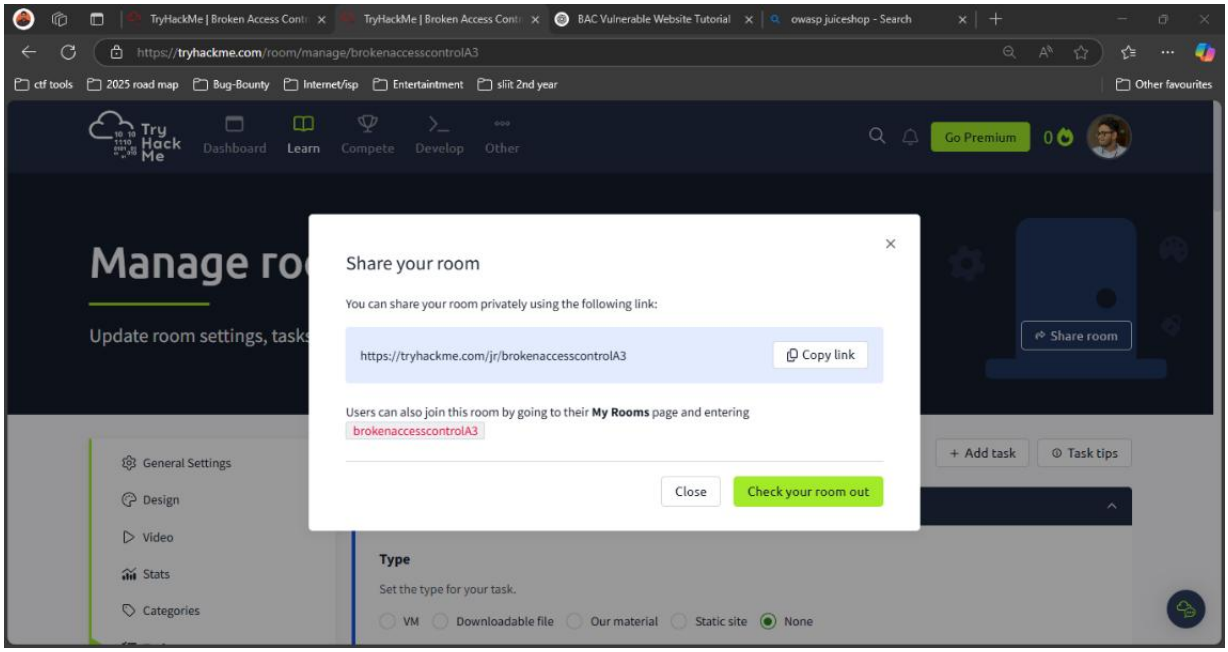


➢ Copy the link on it.



➢ Paste the git link

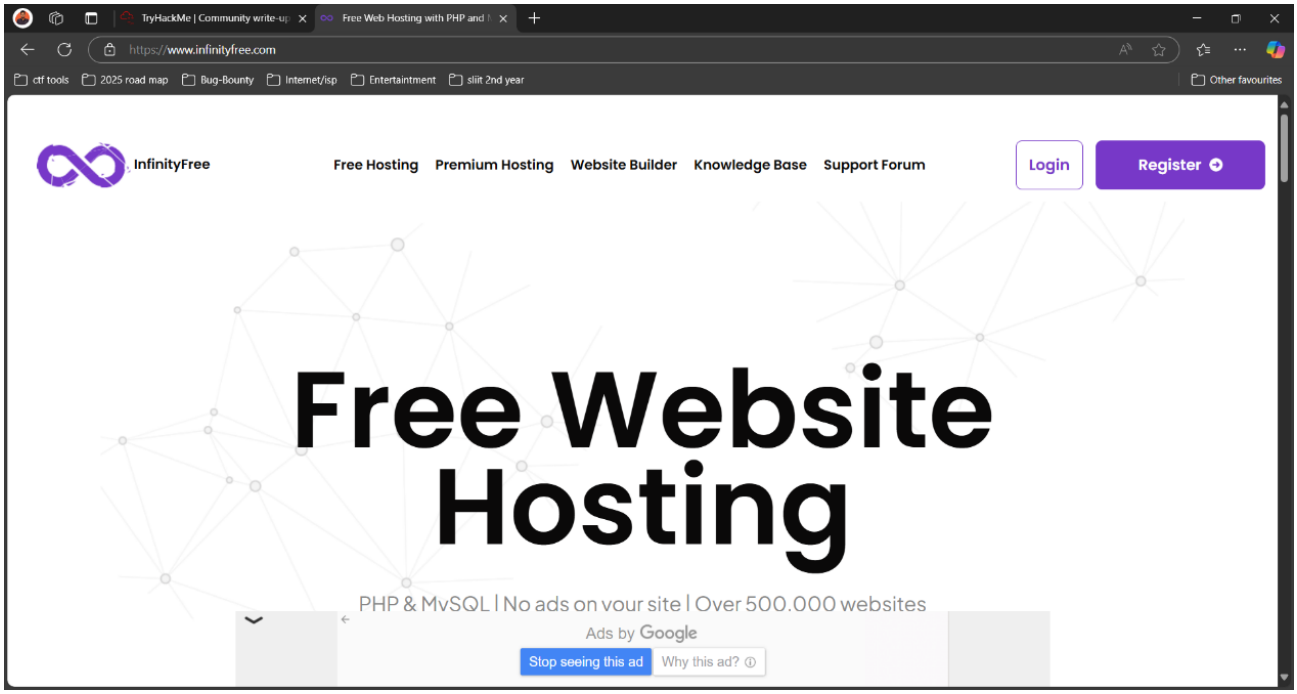




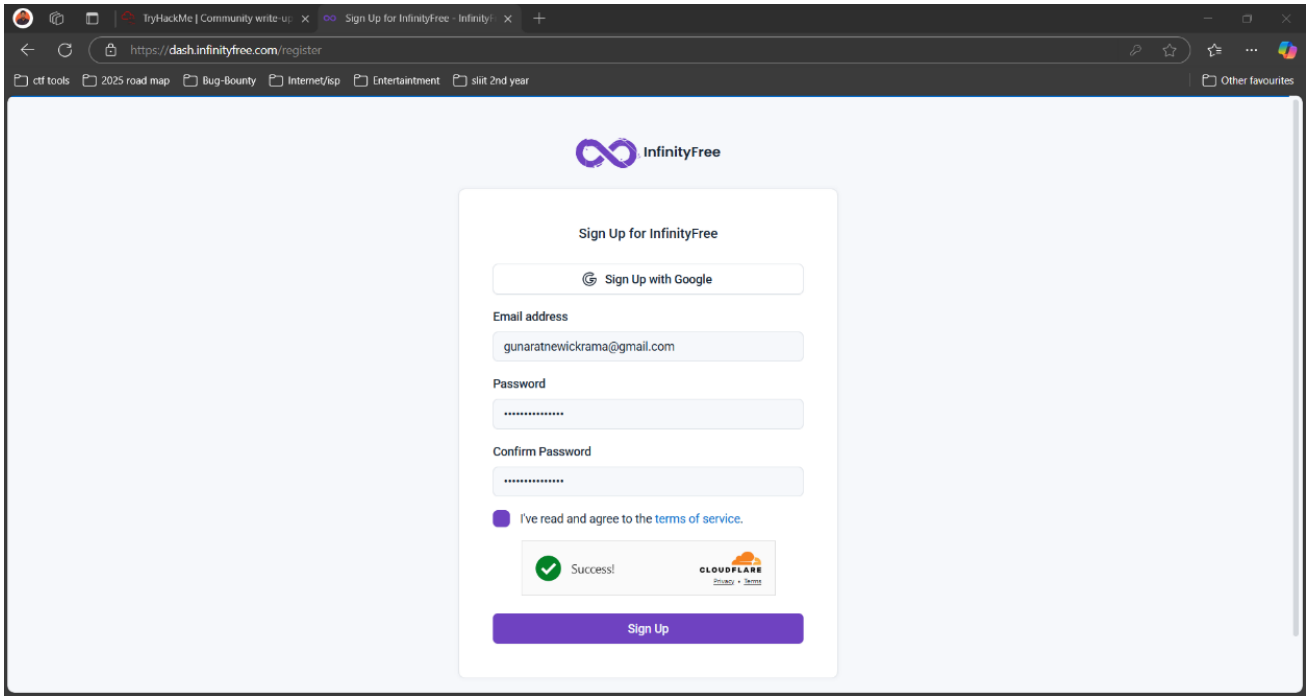
- My link to access TryHackMe room: https://tryhackme.com/jr/brokenaccesscontrolA3

Screenshot of creating webpages and web hosting

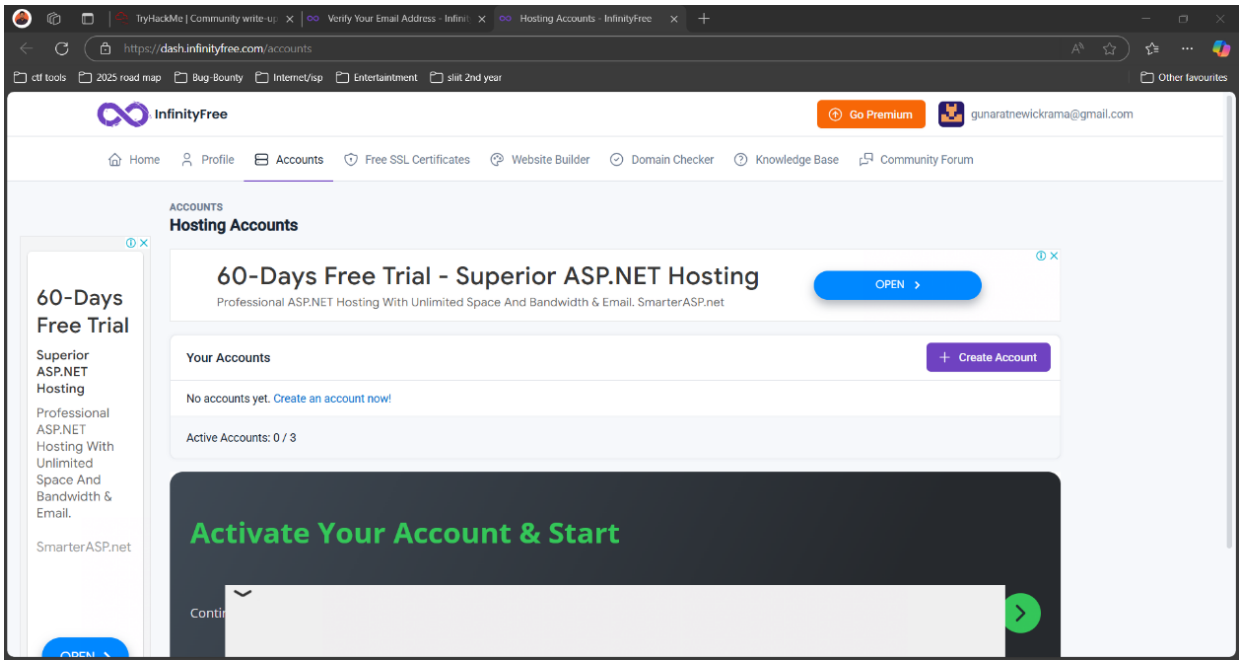
- Go to https://www.infinityfree.com/ site.



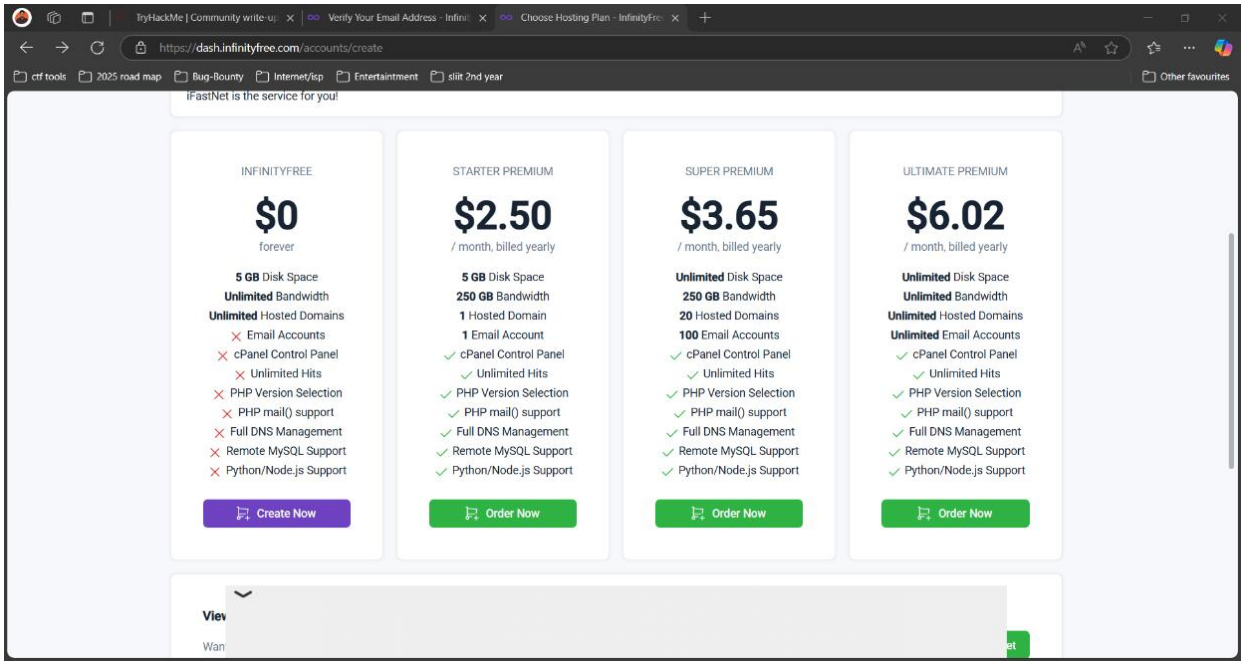
- Register with your details

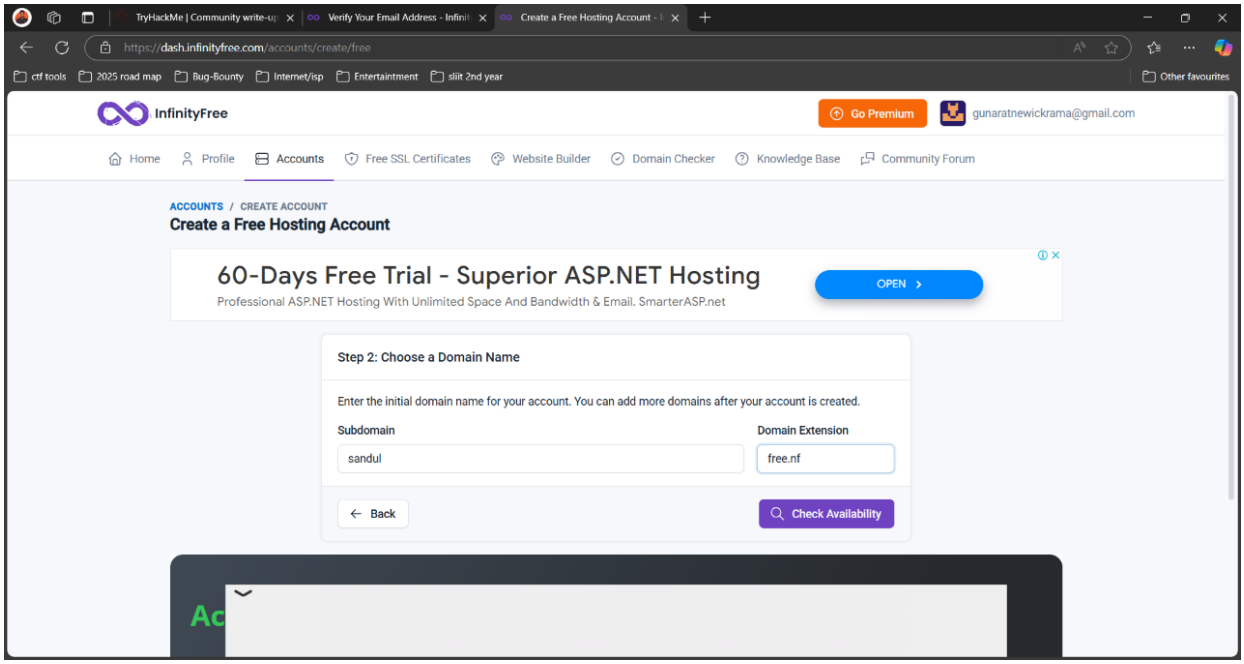


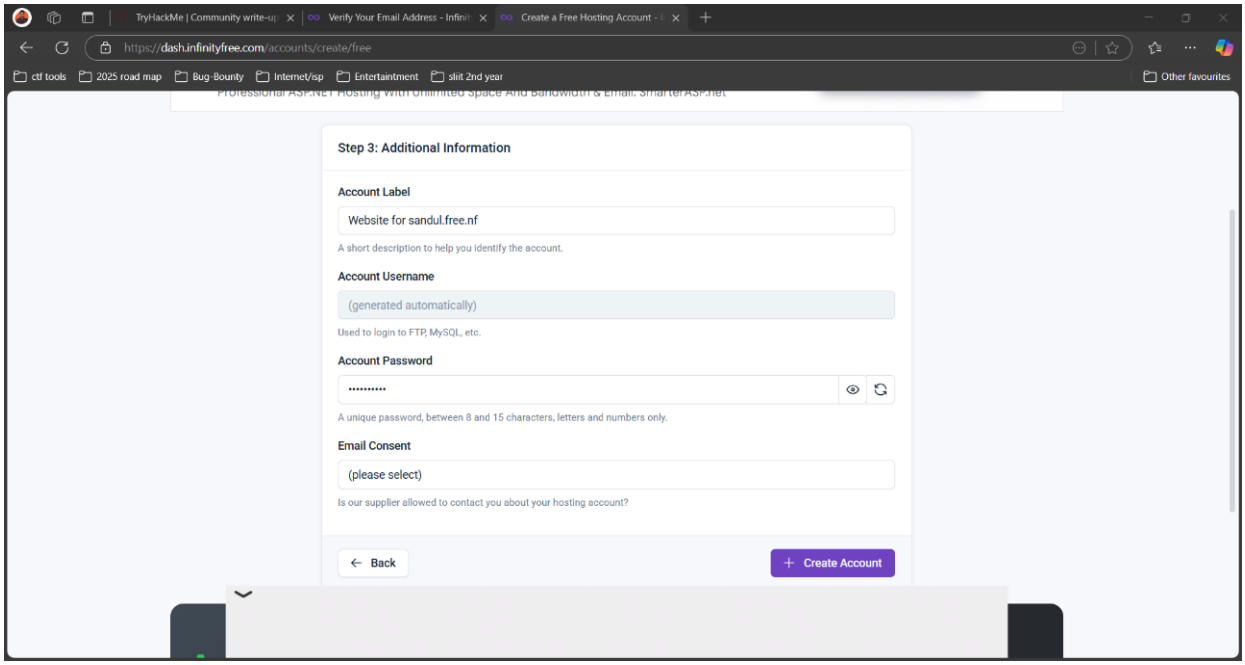
- Select create option button.



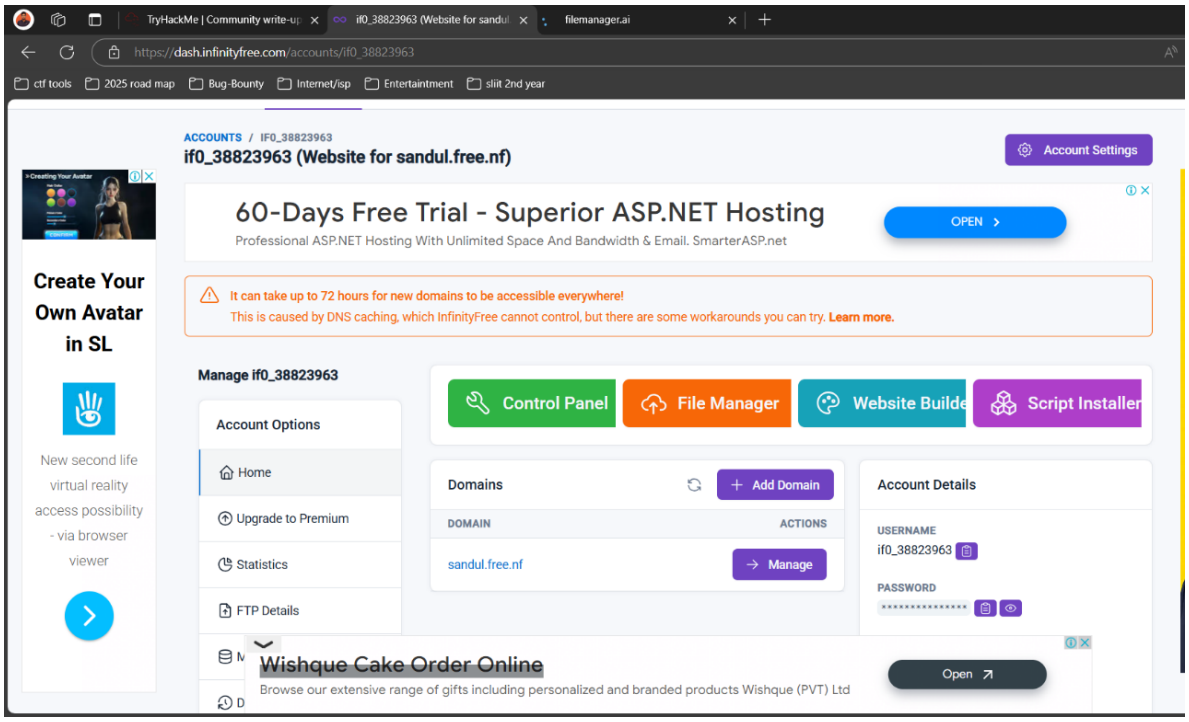
- Select $0 category with clicking purple colour button



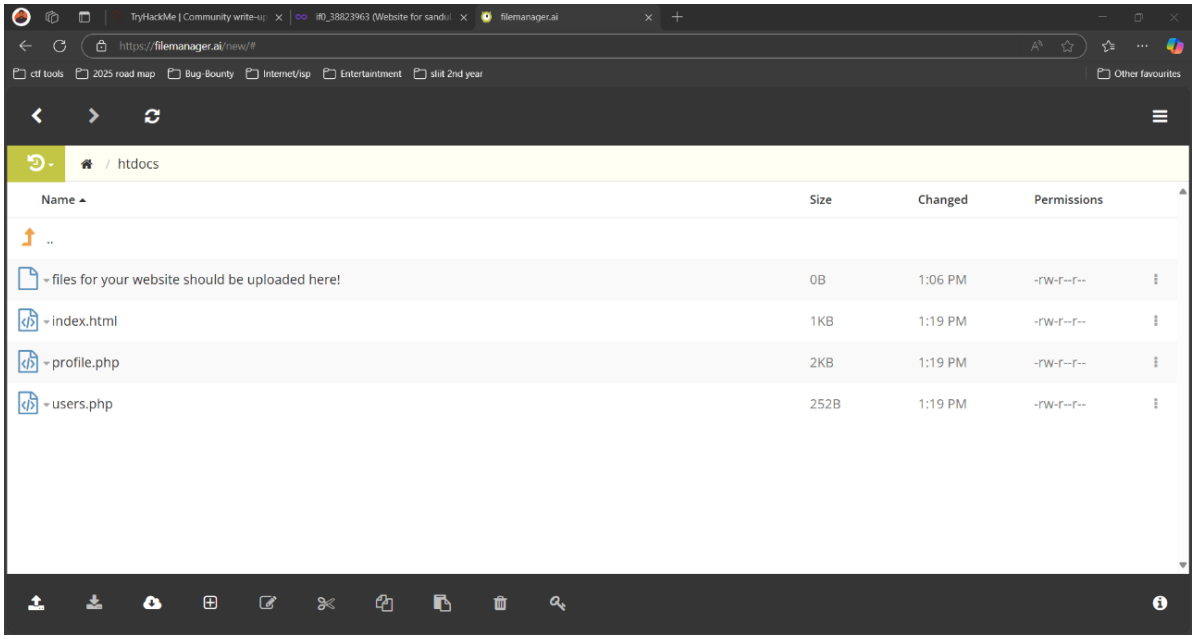

InfinityFree
Go Premium
gunaratnewickrama@gmail.com
Home
Profile
Accounts
Free SSL Certificates
Website Builder
Domain Checker
Knowledge Base
Community Forum
ACCOUNTS / CREATE ACCOUNT
Create a Free Hosting Account
60-Days Free Trial - Superior ASP.NET Hosting
Professional ASP.NET Hosting With Unlimited Space And Bandwidth & Email. SmarterASP.net
OPEN
Step 2: Choose a Domain Name
Enter the initial domain name for your account. You can add more domains after your account is created.
Subdomain
sandul
Domain Extension
free.nf
Back
Check Availability


Step 3: Additional Information
Account Label
Website for sandul.free.nf
A short description to help you identify the account.
Account Username
(generated automatically)
Used to login to FTP, MySQL, etc.
Account Password
A unique password, between 8 and 15 characters, letters and numbers only.
Email Consent
(please select)
Is our supplier allowed to contact you about your hosting account?
Back
Create Account

- Select File manager button.



- Go inside the htdocs file and uploaded needed files.

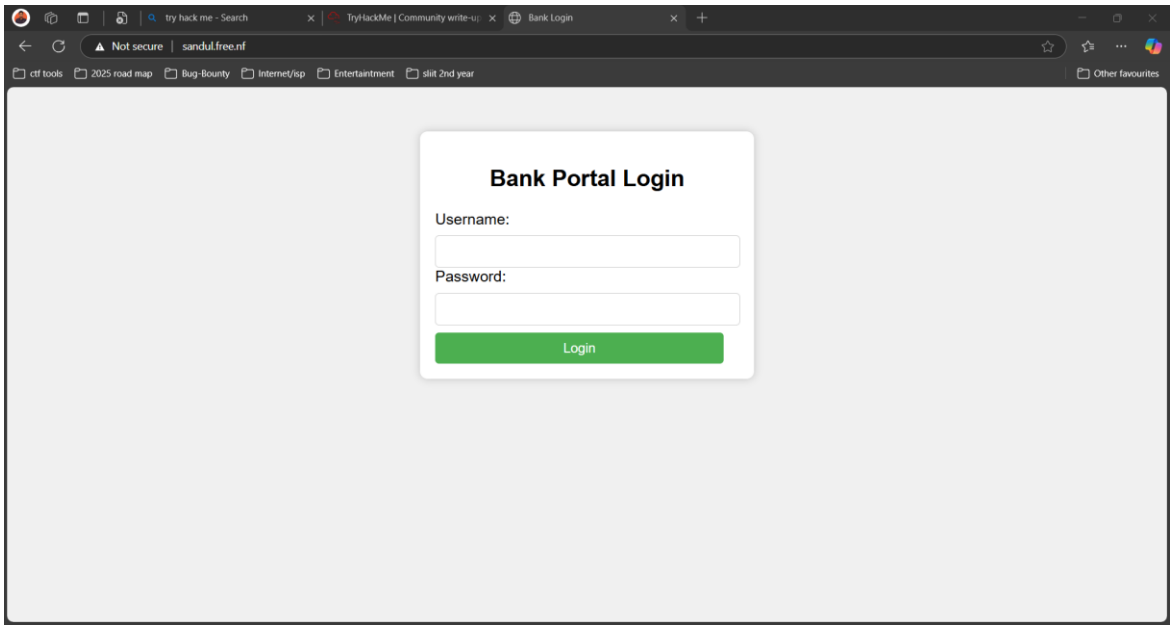


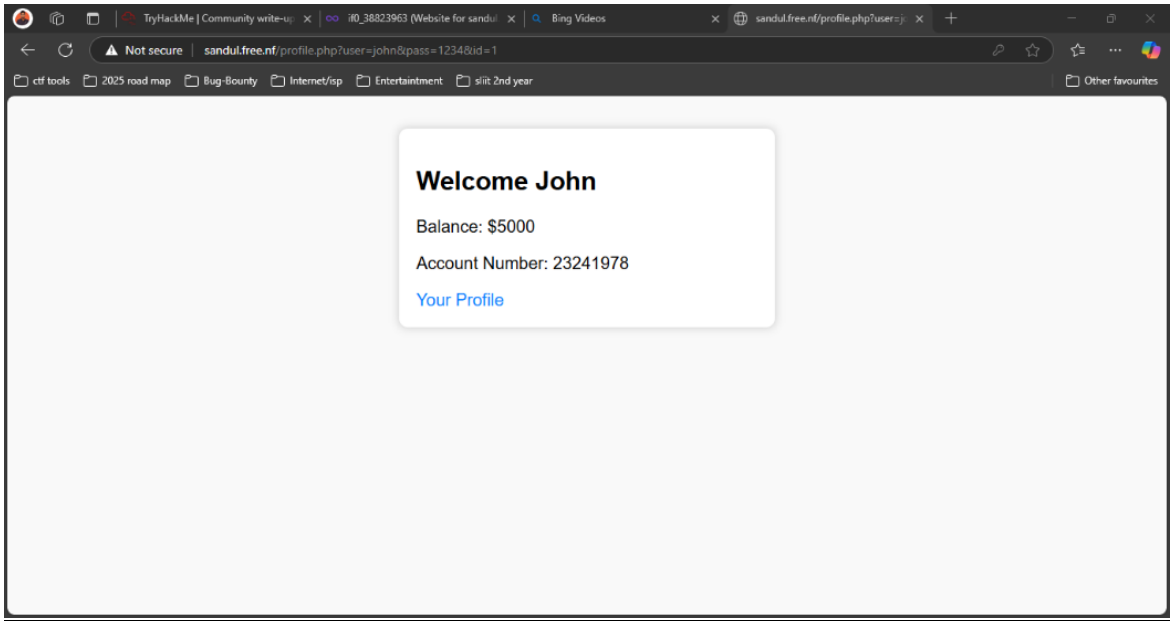
This is how the webpage looks like

Lab 01 (BAC - Insecure Direct Object Reference)

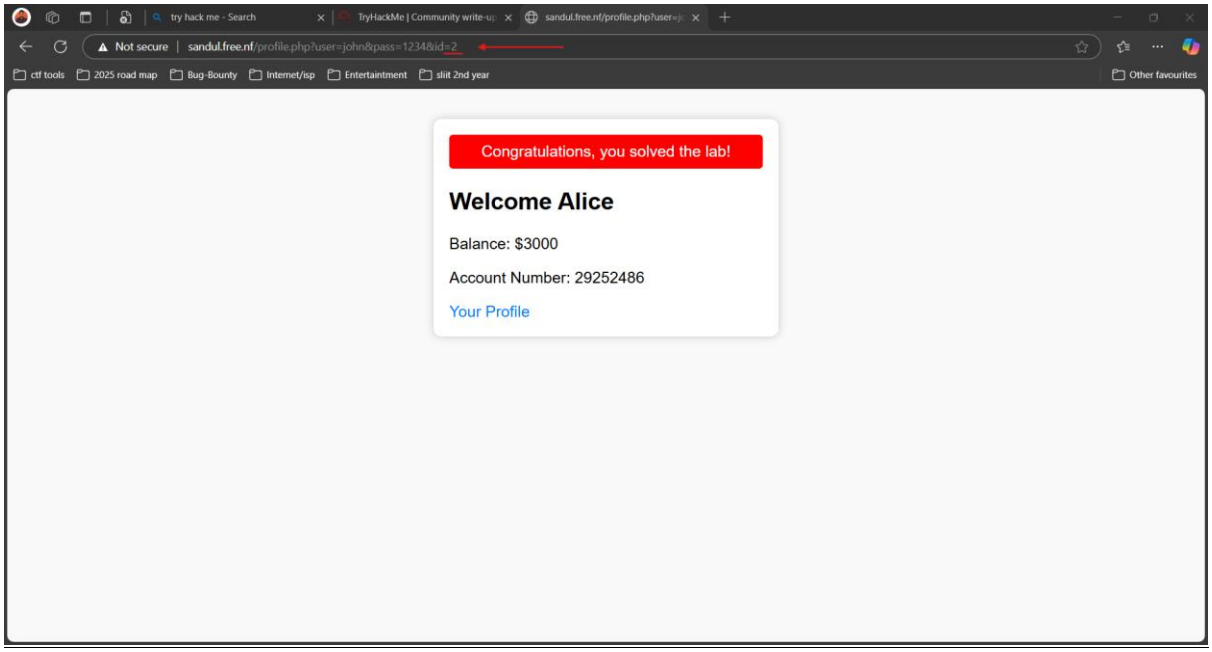
Security Mistake is - Trusting user-supplied URL parameters

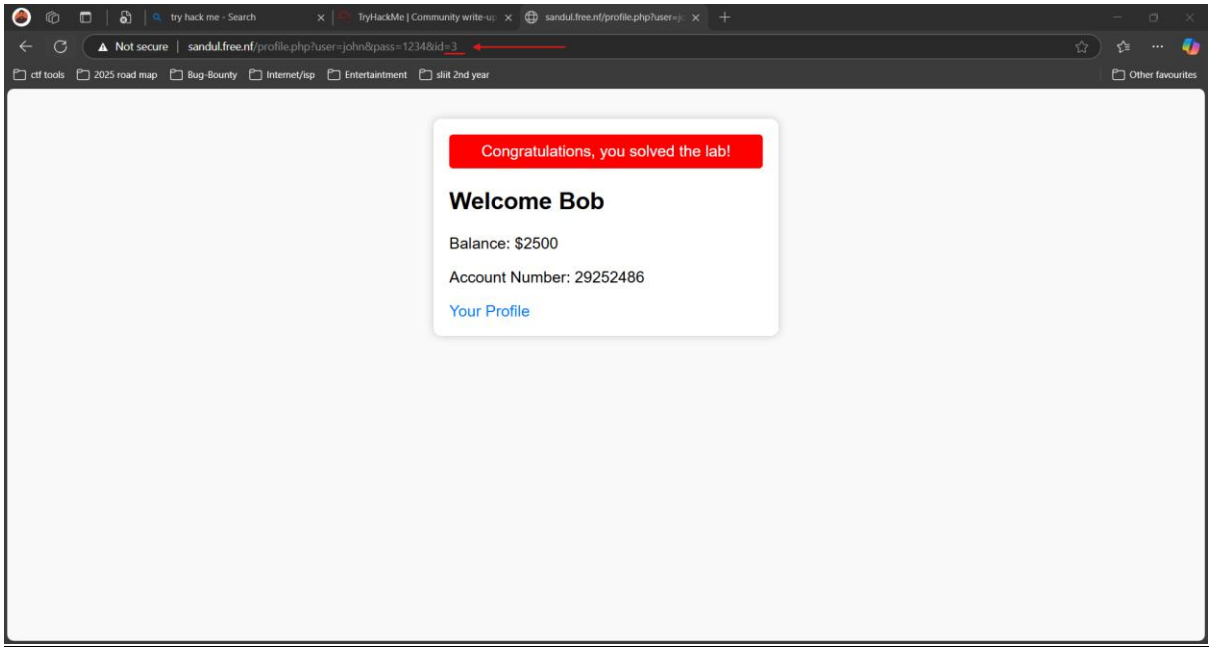
1. Give credentials as username: john / password:1234





2. Change the URL's id as id 2 or id 3

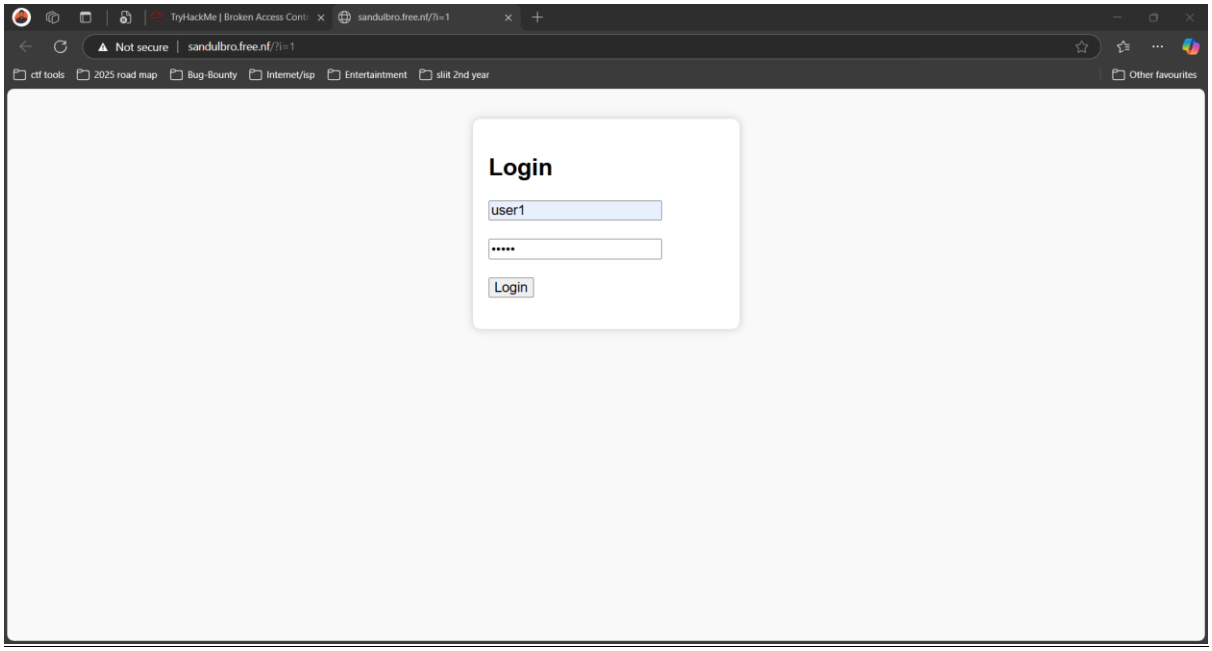


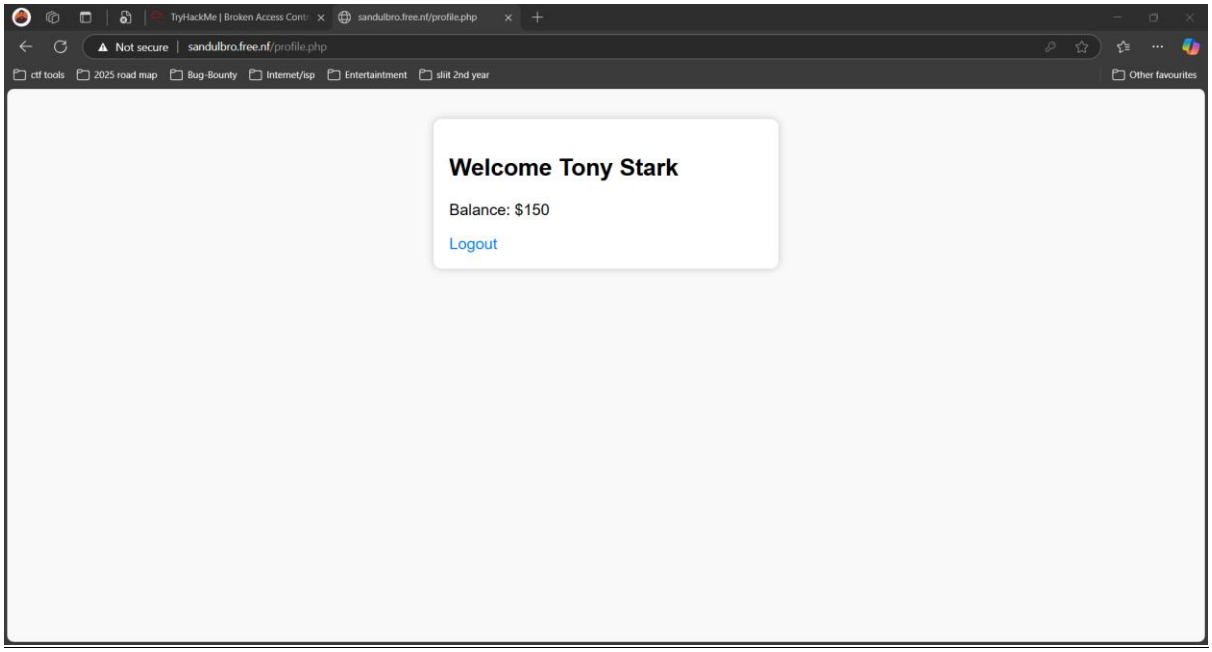


Lab 02 (BAC - Insecure Session Management)

Security Mistake is - Trusting client-side cookie without server validation

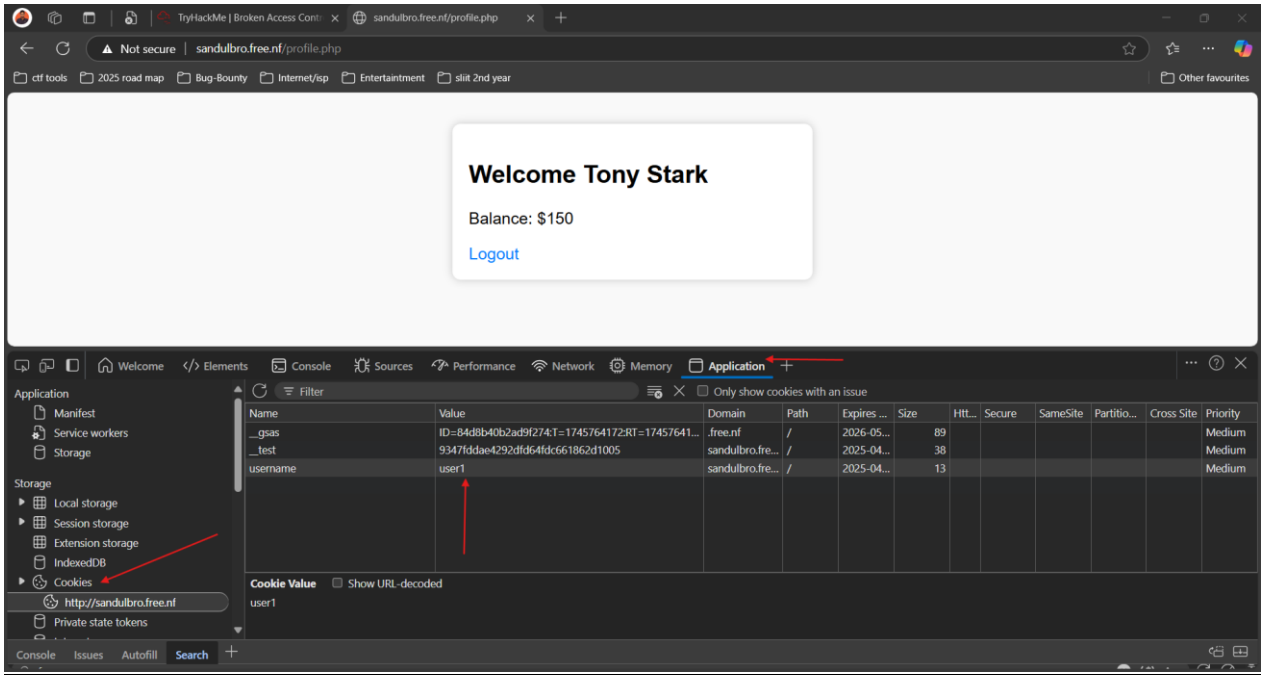
1. Give credentials as username: user1/ password: pass1

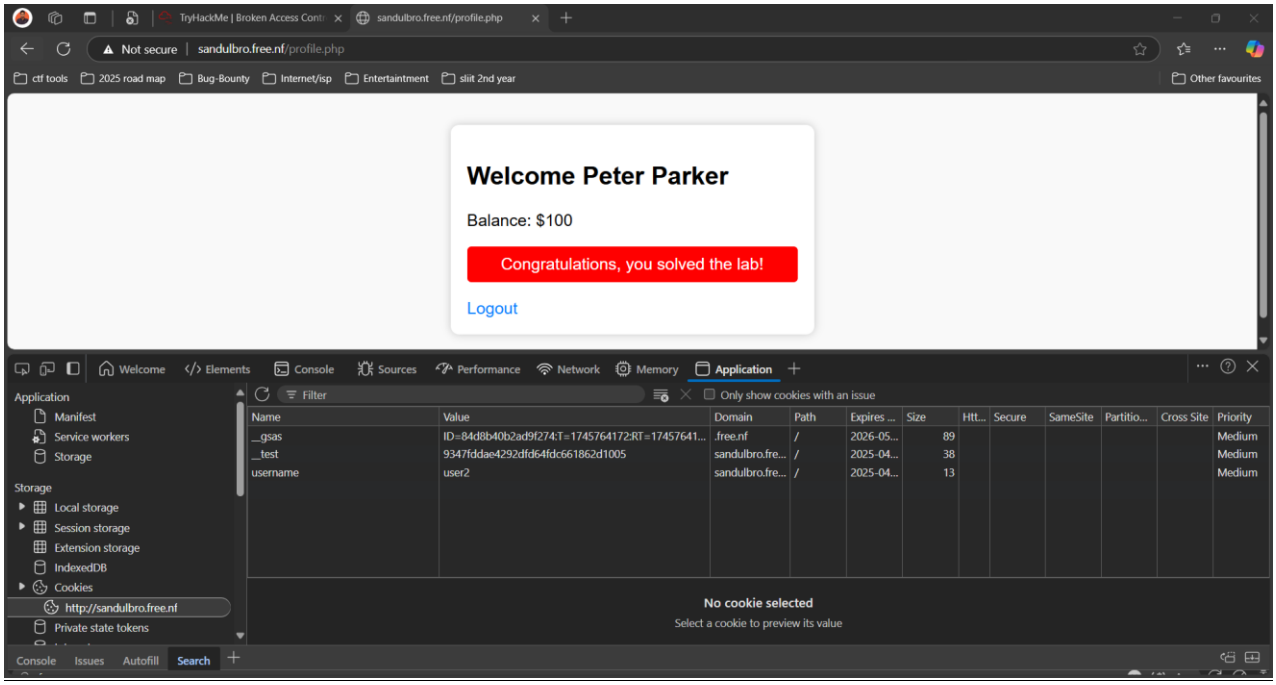




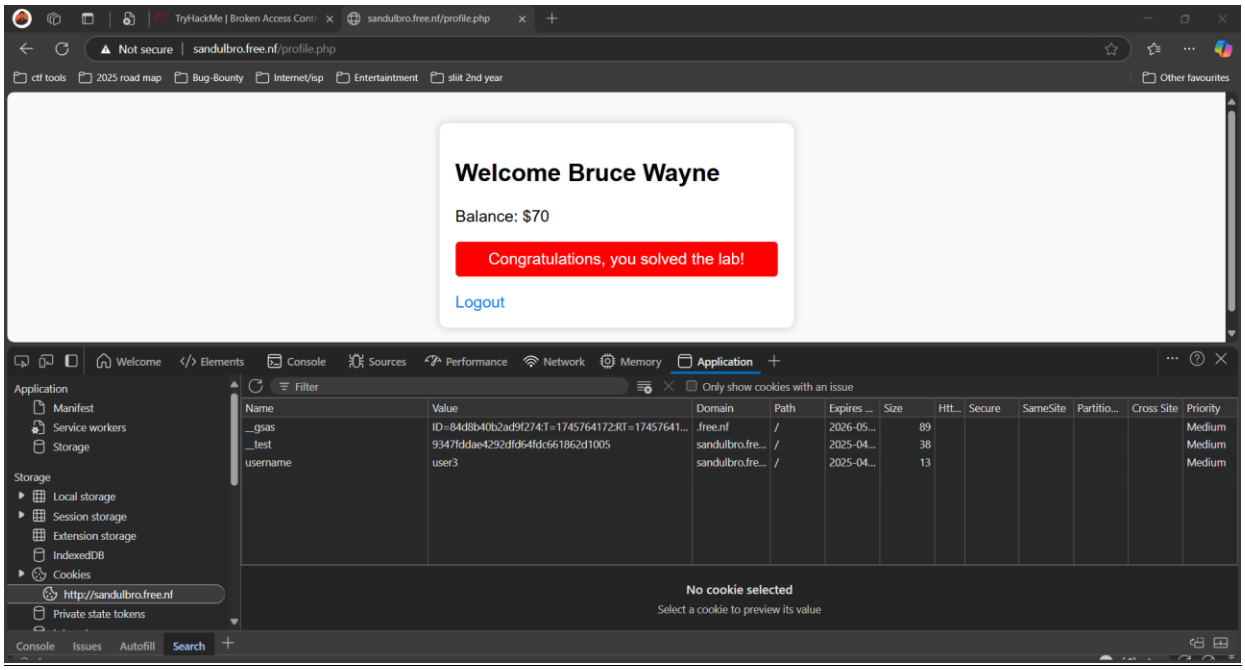
2. Go to developer tools > applications >cookies

3. Change the cookies value “user2” and break the system (Access Peter’s account).

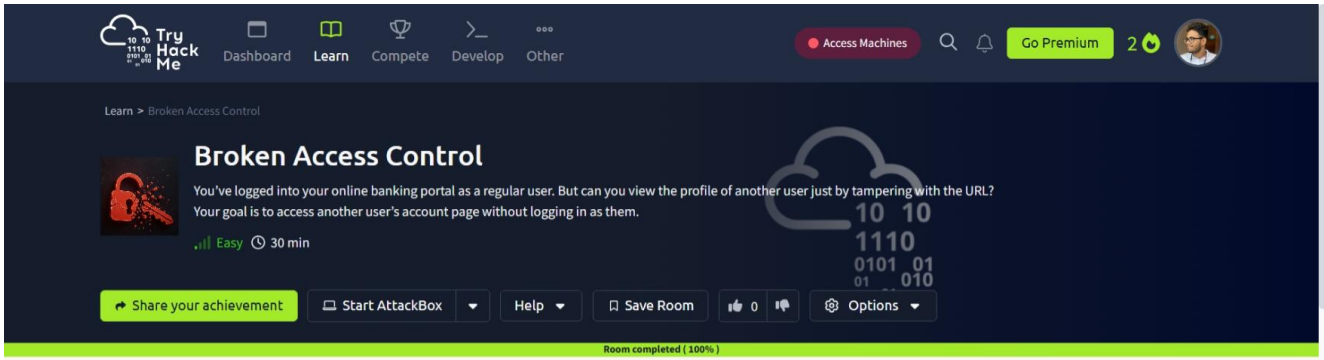


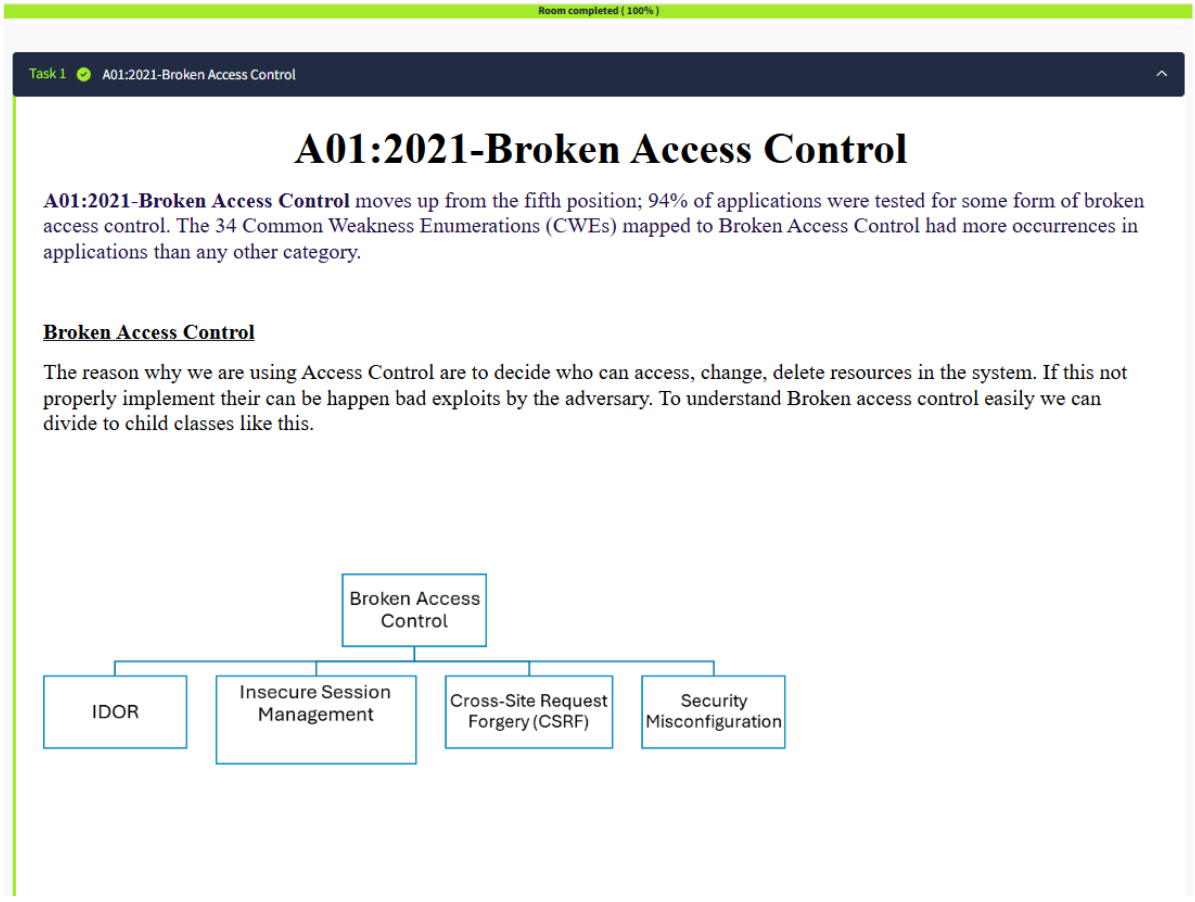


1. Change the cookies value “user3” and break the system (Access Bruce’s account).



Final output or the assignment



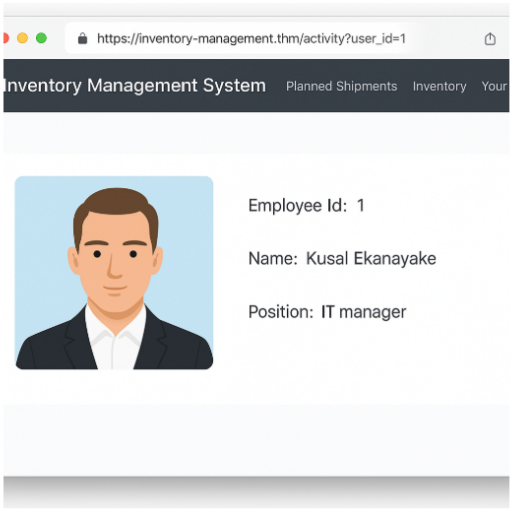


1) Insecure Direct Object References (IDOR)

This happens without having proper authorization checks, if app allows direct access to files, database records or other system resources. So that attackers can changing id and URL and get access, modify or terminate data. This can lead informational to business-critical risk level.

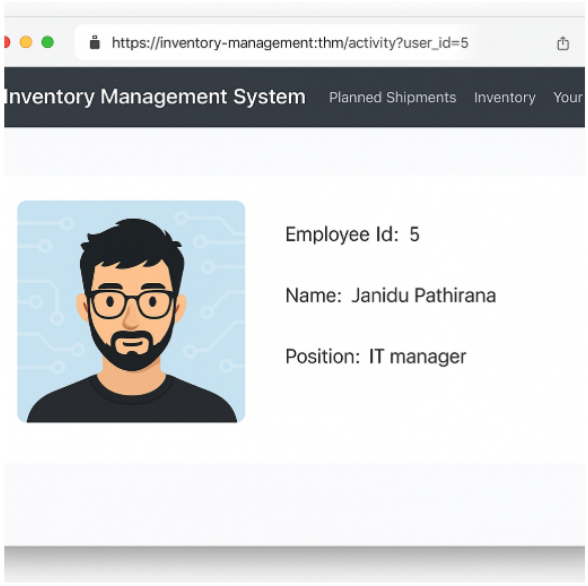
Example scenario: If user (attacker) accesses his page and would try other possible ids and can access another user's sensitive data.

Login as employee id 1.



Room completed (100%)

Edit the URL as "5" and access the other user.



2) Insecure Session Management

Usually, every session has unique session token to identify it uniquely. Insecure Session Management happens, because of week session token generates, lack of session timeouts, effective session termination and tokens are not properly storing and sharing. Because of this kind of scenario gains many problems, such as session hijack, unauthorize access and security breaches. To mitigate this, we can do use https, use secure session token algorithms for token generation, implementing secure cookie attributes, and frequently validating and expiring session token.

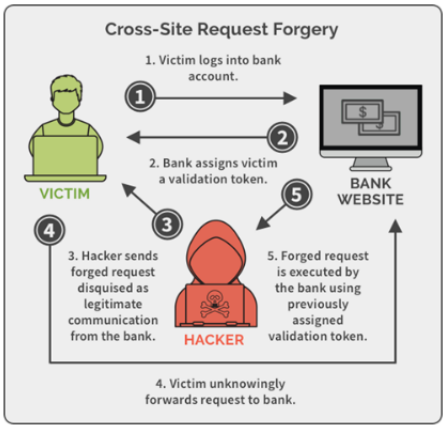
Room completed (100%)

2) Insecure Session Management

Usually, every session has unique session token to identify it uniquely. Insecure Session Management happens, because of week session token generates, lack of session timeouts, effective session termination and tokens are not properly storing and sharing. Because of this kind of scenario gains many problems, such as session hijack, unauthorize access and security breaches. To mitigate this, we can do use https, use secure session token algorithms for token generation, implementing secure cookie attributes, and frequently validating and expiring session token.

3) Cross-Site Request Forgery (CSRF)

Hacker tricks a user into performing an unwanted activity on website they are already logging.



4) Security Misconfiguration

Security misconfiguration happens when security settings are not configured correctly. Reason for happening these are outdated software, unused features being enabled.

Answer the questions below

What security flaw category does this scenario belong to in OWASP Top 10?

Broken Access Control — ✓ Correct Answer

Read and understand how IDOR (Insecure Direct Object References) works.

No answer needed — ✓ Correct Answer

Go to http://sandul.free.nf/ Login with the username **john** and the password **1234**.

No answer needed — ✓ Correct Answer

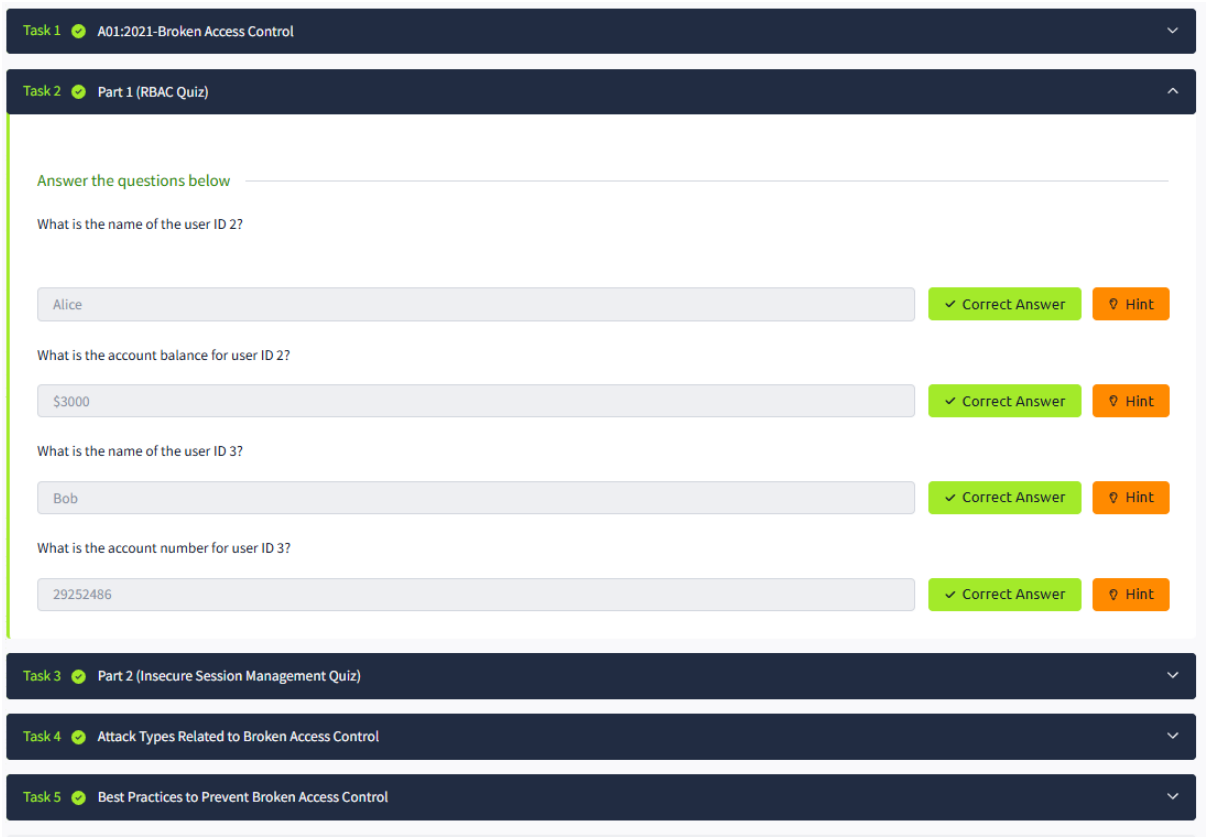
Task 2 Part 1 (RBAC Quiz)

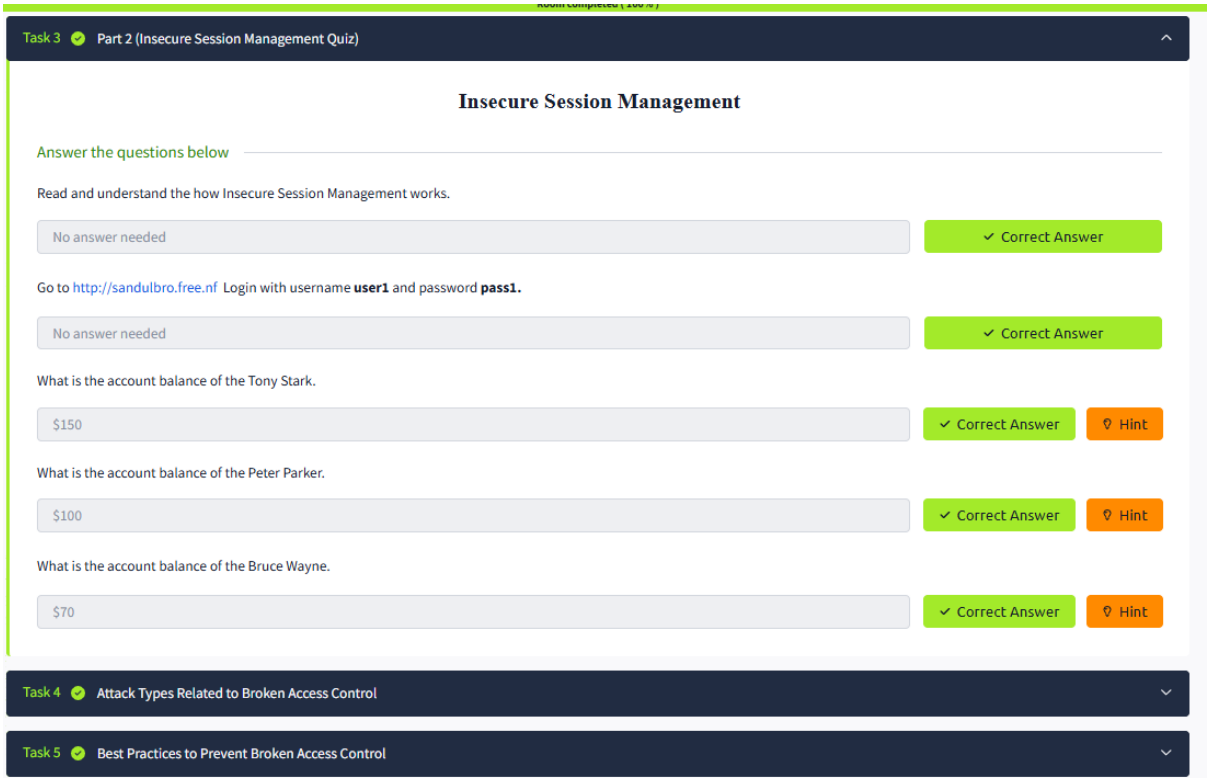
Task 3 Part 2 (Insecure Session Management Quiz)

Task 4 Attack Types Related to Broken Access Control

Task 5 Best Practices to Prevent Broken Access Control

Created by	Room Type	Users in Room	Created
ApolloCipher	Free Room. Anyone can deploy virtual machines in the room (without being subscribed)!	2	8 days ago


Task 1 A01:2021-Broken Access Control
Task 2 Part 1 (RBAC Quiz)
Answer the questions below
What is the name of the user ID 2?
Alice
Correct Answer
Hint
What is the account balance for user ID 2?
$3000
Correct Answer
Hint
What is the name of the user ID 3?
Bob
Correct Answer
Hint
What is the account number for user ID 3?
29252486
Correct Answer
Hint
Task 3 Part 2 (Insecure Session Management Quiz)
Task 4 Attack Types Related to Broken Access Control
Task 5 Best Practices to Prevent Broken Access Control


Task 3 Part 2 (Insecure Session Management Quiz)
Insecure Session Management
Answer the questions below
Read and understand the how Insecure Session Management works.
No answer needed
Correct Answer
Go to http://sandulbro.free.nf Login with username user1 and password pass1.
No answer needed
Correct Answer
What is the account balance of the Tony Stark.
$150
Correct Answer
Hint
What is the account balance of the Peter Parker.
$100
Correct Answer
Hint
What is the account balance of the Bruce Wayne.
$70
Correct Answer
Hint
Task 4 Attack Types Related to Broken Access Control
Task 5 Best Practices to Prevent Broken Access Control

Task 3 Part 2 (Insecure Session Management Quiz)

Task 4 Attack Types Related to Broken Access Control

Attack Types Related to Broken Access Control

Attack Type	Description
IDOR Attack	Exploiting object references in URLs to access other users' data.
Privilege Escalation	Gaining more permissions than allowed.
Vertical Privilege Escalation	Moving from a low privilege user to an admin.
Horizontal Privilege Escalation	Accessing another user's data at the same privilege level.
Function Access Without Auth	Calling endpoints not meant for your role.
Forced Browsing	Accessing unlinked or hidden URLs directly without permission.

Answer the questions below

No answer needed ✓ Correct Answer

Task 5 Best Practices to Prevent Broken Access Control

Room completed (100%)

Impact of Broken Access Control on Organizations

1. Financial Loss:

- Attackers can access sensitive data (like customer info, payment details).
- Leads to fraud, data breaches, or ransom demands.
- Example: Fines under laws like GDPR can cost millions.

2. Reputational Damage:

- Customers lose trust after a breach.
- Negative media coverage affects brand image.
- It can lead to customer loss and reduced business.

3. Legal Consequences:

- Organizations may be sued by affected users.
- Government regulations (like HIPAA, GDPR, CCPA) require strict data control.
- Non-compliance due to broken access control can lead to penalties or shutdowns.

Answer the questions below

Room completed (100%)

Tools for Detecting Broken Access Control

1. Burp Suite (Pro & Community Edition):

- Intercept requests to check for IDOR, forced browsing, or role tampering.
- Repeater and Intruder tools help test access to unauthorized endpoints.

2. OWASP ZAP:

- Open-source alternative to Burp Suite.
- Can automatically scan for access control issues.
- Ideal for testing during development.

3. Manual Testing:

- Change user IDs in URLs or switch tokens to test unauthorized access.
- Try performing admin actions as a normal user.
- Check response codes and role-based behavior.

4. Authorization Testing Plugins:

- Tools like **AuthMatrix** (Burp plugin) help map and test access control rules.

5. Automated Scanners:

- Tools like **Acunetix** or **Netsparker** can detect broken access patterns.

Room completed (100%)

Task 2 Part 1 (RBAC Quiz)

Task 3 Part 2 (Insecure Session Management Quiz)

Task 4 Attack Types Related to Broken Access Control

Task 5 Best Practices to Prevent Broken Access Control

Best Practices to Prevent BAC

- Enforce access checks **on the server-side** (never trust frontend controls).
- Use a consistent **access control mechanism** across all endpoints.
- Avoid exposing direct object references (use tokens or UUIDs).
- Deny by default — allow only explicitly authorized actions.
- Test thoroughly for role-based and object-level access control.

Answer the questions below

No answer needed

✓ Correct Answer

Created by	Room Type	Users in Room	Created
ApolloCipher	Free Room. Anyone can deploy virtual machines in the room (without being subscribed)!	2	8 days ago

4. Room Link:

- My link to access TryHackMe room: https://tryhackme.com/jr/brokenaccesscontrolA3

5. Reflection:

- Our THM room is a practical, So in the practical environment for learners/THM players to engage with real-world scenario about BAC.
- It helps players to understand the impact of these system weakness and how to attack.
- Once finishing this room, player/learner can understand the Broken Access Control.

References sites and courses

Course I follows:

Understanding the OWASP® Top 10 Security Threats (SKF100) - The Linux Foundation

Learning platforms:

TryHackMe | OWASP Broken Access Control

TryHackMe | OWASP Top 10 - 2021

All labs | Web Security Academy

Website:

OWASP Top 10:2021

*** The End ***