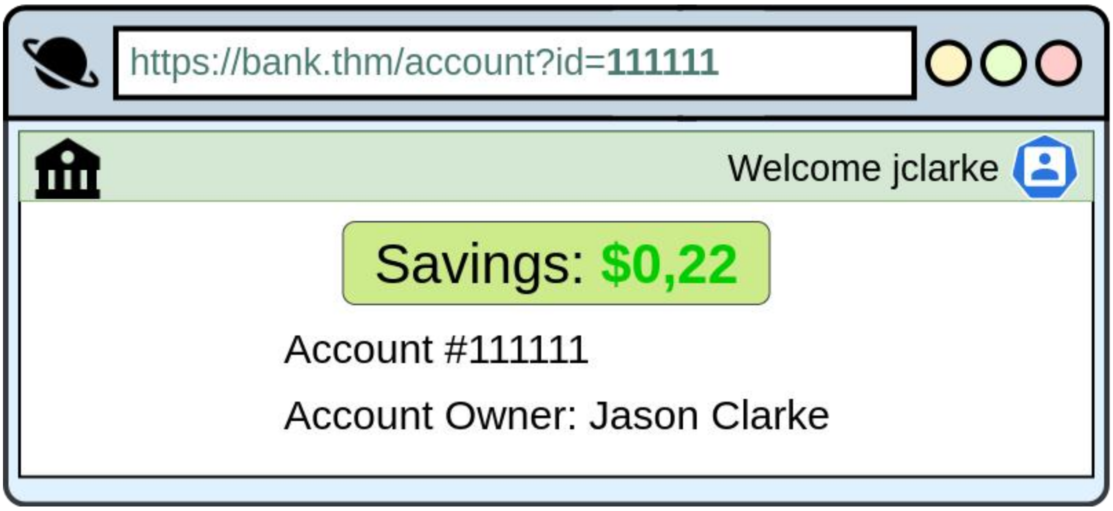
Task 4 : Broken Access Control (IDOR Challenge)

Insecure Direct Object Reference

IDOR or **Insecure Direct Object Reference** refers to an access control vulnerability where you can access resources you wouldn't ordinarily be able to see. This occurs when the programmer exposes a Direct Object Reference, which is just an identifier that refers to specific objects within the server. By object, we could mean a file, a user, a bank account in a banking application, or anything really.

For example, let's say we're logging into our bank account, and after correctly authenticating ourselves, we get taken to a URL like this `https://bank.thm/account?id=111111`. On that page, we can see all our important bank details, and a user would do whatever they need to do and move along their way, thinking nothing is wrong.



https://bank.thm/account?id=**111111**

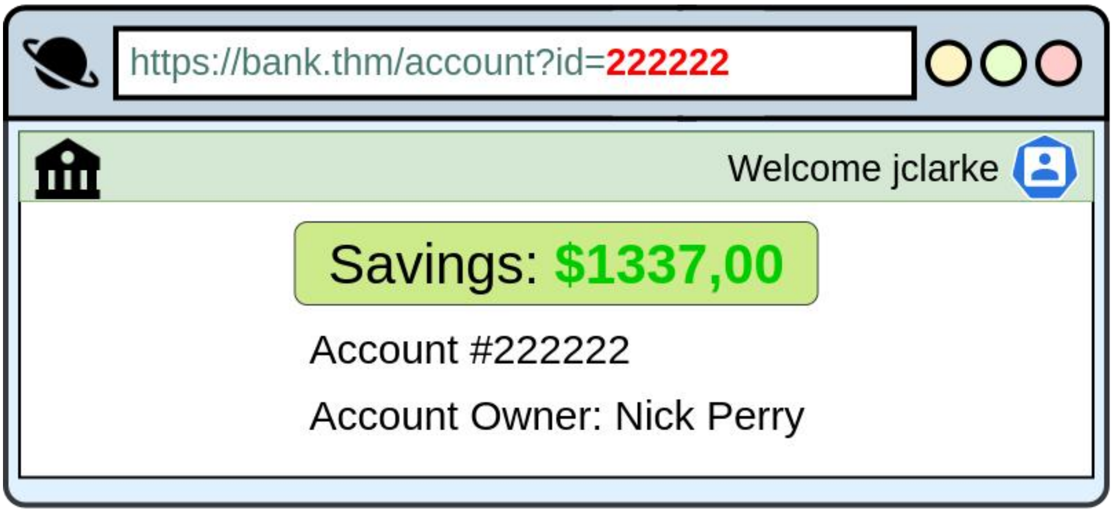
Welcome jclarke

Savings: $0,22

Account #111111

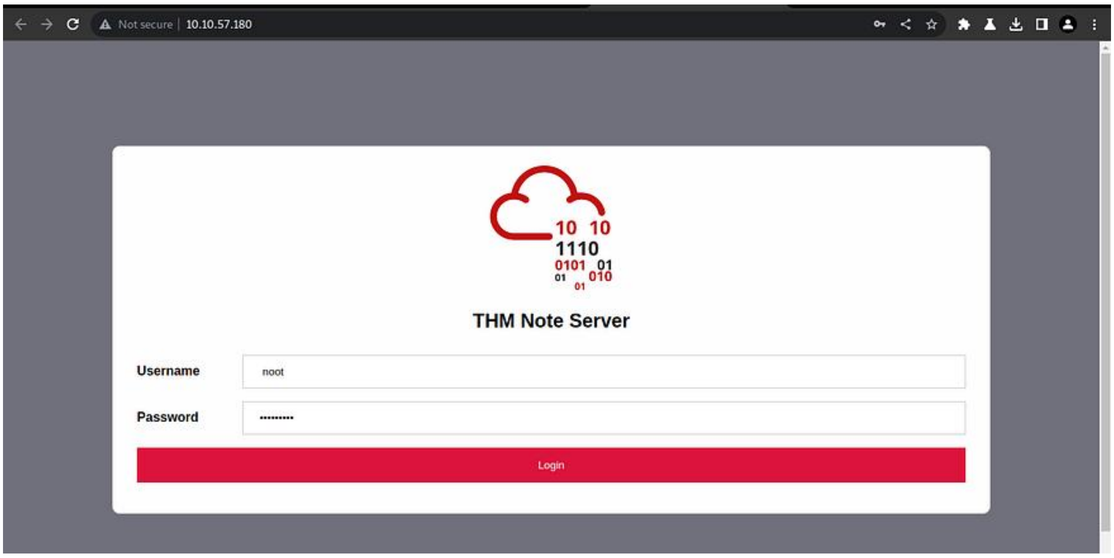
Account Owner: Jason Clarke

There is, however, a potentially huge problem here, anyone may be able to change the `id` parameter to something else like `222222`, and if the site is incorrectly configured, then he would have access to someone else's bank information.



The application exposes a direct object reference through the id parameter in the URL, which points to specific accounts. Since the application isn't checking if the logged-in user owns the referenced account, an attacker can get sensitive information from other users because of the IDOR vulnerability. Notice that direct object references aren't the problem, but rather that the application doesn't validate if the logged-in user should have access to the requested account.

First of all login :

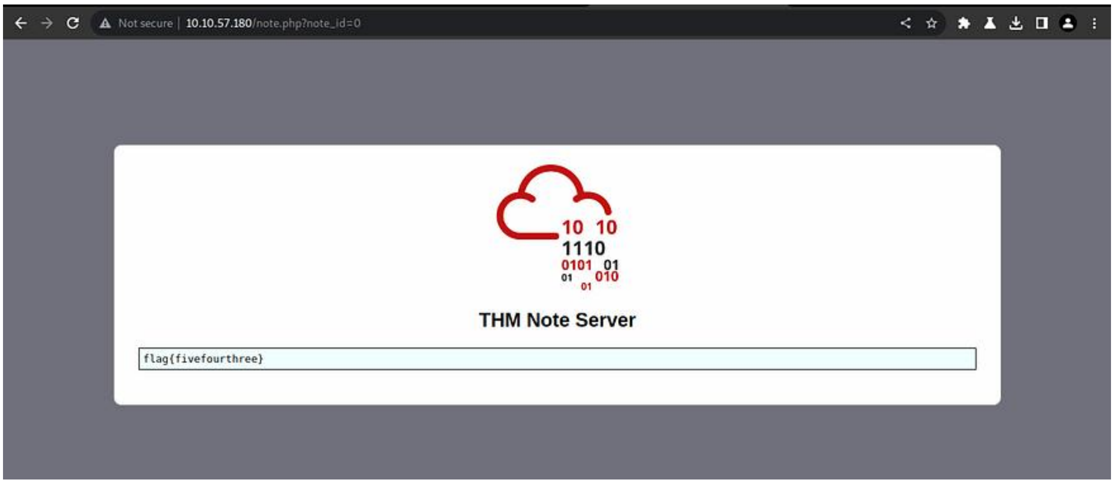

Not secure | 10.10.57.180

THM Note Server

Username: noot

Password: ••••••••••

Put id=0 (http://machine-ip/note.php?note_id=0) and you will get the flag



THM Note Server

flag{fivefourthree}

Answer the questions below :

1. Read and understand how IDOR works.
A. No answer needed

2. Deploy the machine and go to http://MACHINE_IP - Login with the username noot and the password test1234.
A. No answer needed

3. Look at other users' notes. What is the flag?
A. flag{fivefourthree}