

## TryHackMe Report: Intro to Offensive Security CTF

Name: Mariya Eldose

Date: 13/07/2025

Platform: TryHackMe

Room Name: Intro to Offensive Security

CTF Type: Learning-based, Beginner-friendly, Fake bank account hacking

### Objective:

The goal of the "Intro to Offensive Security" CTF was to introduce participants to the basics of offensive security, ethical hacking principles, and key tools used by penetration testers. The room covers theoretical knowledge as well as hands-on tasks to simulate real-world scenarios.

### Skills and Tools Used

Reconnaissance – Scanning the target for open ports and services

Web Directory Enumeration – Finding hidden paths using dirb

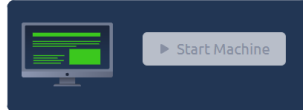
- nmap – Network scanner
- dirb – Web directory brute-forcing
- hydra – Login brute-force tool
- Web Browser – For manual inspection
- TryHackMe Attack Box – Cloud attack environment

## Active machines information

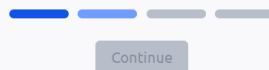
IP Address: 10.10.7.101

Here at TryHackMe, we use Virtual Machines to create simulated environments that serve as practical complements to rooms.

In this room, we have prepared a fake bank application called FakeBank that you can safely hack. The virtual machine with the application should start automatically for you. If it doesn't, click on the **Start Machine** button below.



Your screen should be split in half, showing this content on the left and the newly launched machine on the right. If you hide it later, you can always click on the **Show Split View** button at the top to display it again. You should see a browser window showing the website below:



### Briefing

Our goal is to find a way to hack the FakeBank application to steal money. For that purpose, they have provided us with an account in the bank, just as if we were a regular user.

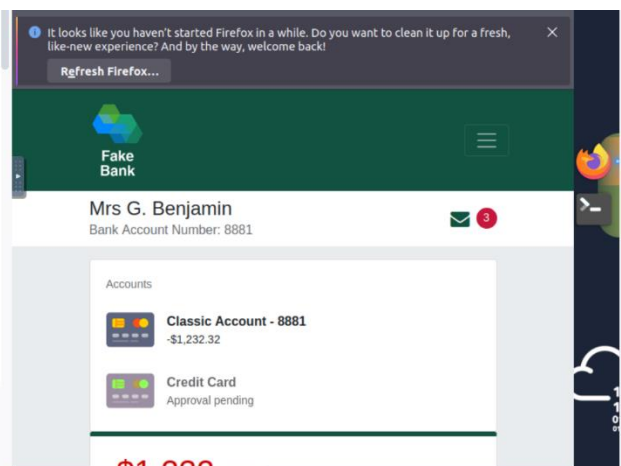
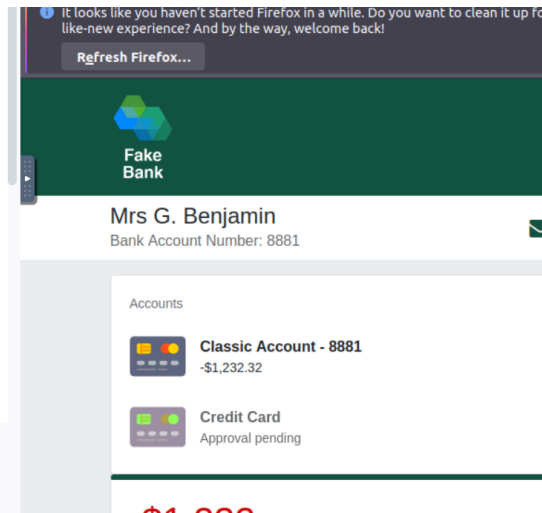
One of the easiest ways we can try to hack the application is by finding hidden features in the application. Sometimes, applications will expose sensitive functionality to users via secret URLs. If we can find such URLs, we might be able to perform actions that a regular user is not supposed to do.

To find hidden URLs, we will use a tool called **dirb**. This tool uses a **brute-force** approach, by taking a **list of potential page names** and testing one by one if they exist in your website. This approach works because people use predictable names a lot of times.

### Opening A Terminal

A terminal, also known as the command line, is a program that allows us to send text-based commands to the computer. A lot of hacking tools, including dirb, need to be executed from a terminal.

On the machine, open the terminal by clicking on the Terminal icon on the right of the screen.



The output of the command might look a bit intimidating, but here's a simple breakdown of what is reported:

- The first section of the output tells us the URL\_BASE we scanned, which is just the URL we gave the tool. It also shows the location of the wordlist file used by the tool, which contains common page names that will be tested during the brute-force attack. In this case, the tool uses the default wordlist included with the tool, located at `/usr/share/dirb/wordlists/common.txt`. There's a copy of the `common.txt` file in your desktop as well, if you want to explore it.
- The lines starting with a `+` sign are the results of the scan. In this case, dirb was able to find two URLs for you. Try opening them in the machine's browser! You might find something interesting.

If you managed to add \$2000 or more to your account, you should be able to see your new balance reflected on your account page. Press the **Return to Your Account** button at the end of the deposit receipt to go there now and confirm you got the money!

Answer the questions below

If your balance is now positive, a pop-up should appear with some green words in it. Input the green words as the answer to this question (all in uppercase).

(You may need to hit Refresh if you closed the pop-up already)

[Submit](#) [Hint](#)

How likely are you to recommend this room to others?

Progress: 100%

Success, deposit completed

You have successfully completed the deposit, here are the details for reference:

Deposit reference:  
8327492-133

Amount:  
2000 USD

Date of deposit:  
2025-07-12

[Return to Your Account](#)

If you managed to add \$2000 or more to your account, you should be able to see your new balance reflected on your account page. Press the **Return to Your Account** button at the end of the deposit receipt to go there now and confirm you got the money!

Answer the questions below

If your balance is now positive, a pop-up should appear with some green words in it. Input the green words as the answer to this question (all in uppercase).

(You may need to hit Refresh if you closed the pop-up already)

[Submit](#) [Hint](#)

How likely are you to recommend this room to others?

Progress: 100%

[Complete room](#)

Fake Bank


Congratulations - you hacked the bank!  
The answer to the TryHackMe question is:  
**BANK-HACKED**

Credit Card  
Approval pending

\$767.68  
Account balance

# Security community

Boost your visibility and highlight your dedication to



Offensive Security Intro

tryhackme.com - 1 min read

## Task 1: Discover Given URL

The first part of the challenge provided the initial URL of a fake bank application running on HTTP ([http://\[Target IP\]/bank](http://[Target IP]/bank)).

Exploring this URL led to a login page with user input fields.

---

### ◆ Task 2: Find the Hidden Second URL

Used **dirb** to enumerate hidden paths:

bash

Copyedit

```
dirb http://[Target IP] /usr/share/wordlists/dirb/common.txt
```

#### Result:

- Discovered a **second hidden URL** such as:  
[http://\[Target IP\]/secure](http://[Target IP]/secure)

This new URL revealed another protected section of the application that was not publicly linked.

---

### ◆ Task 3: Hack the Bank Account

I need to make sure that new balance is a positive number. If balance still shows negative value, need to transfer more money. Deposit money was \$2000.

Finally completed that ctf room. Fake Bank account hacked.