

TryHackMe Task Writeup

Objectives

- Understand offensive vs. defensive security
- Use dirb to discover hidden web pages
- Exploit a hidden deposit feature to manipulate bank account balance
- Capture the flag from the successful exploit

Questions & Answers

1. Which of the following options better represents the process where you simulate a hacker's actions to find vulnerabilities in a system?

Answer: Offensive Security

2. What is your bank account number in the FakeBank web application?

Answer: 8881

3. Dirb should have found 2 hidden URLs. One of them is <http://fakebank.thm/images>. What is the other one?

Answer: <http://fakebank.thm/bank-deposit>

4. 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).

Answer: BANK-HACKED


Tools Used – TryHackMe Virtual Machine - Terminal / Command Line - dirb (for brute-force scanning of hidden URLs) Step-by-Step Walkthrough

1. Started the FakeBank virtual machine provided by TryHackMe.
2. Opened a terminal inside the VM.
3. Ran the dirb tool using the following command: dirb <http://fakebank.thm>
4. Found two hidden URLs from the dirb scan: - <http://fakebank.thm/images> - <http://fakebank.thm/bank-deposit>
5. Navigated to the /bank-deposit page and added \$2000 to account number 8881.
6. Returned to the account page and confirmed the balance update.
7. Captured the green flag from the pop-up displayed on success.

Screenshots

-Task 1

Room completed (100%)



"To outsmart a hacker, you need to think like one."

This is the core of "Offensive Security." It involves breaking into computer systems, exploiting software bugs, and finding loopholes in applications to gain unauthorized access. The goal is to understand hacker tactics and enhance our system defences.

Beginning Your Learning Journey

In this TryHackMe room, you will be guided through hacking your first website in a legal and safe environment. The goal is to show you how an ethical hacker operates. But before we do that, let's review by answering the questions below. Type your answer in the text box after the question and click the "Submit" button. When you're done, proceed to Task 2.

Answer the questions below

Which of the following options better represents the process where you simulate a hacker's actions to find vulnerabilities in a system?

- Offensive Security
- Defensive Security

✓ Correct Answer

💡 Hint

- Task 2


tryhackme.com/room/offensivesecurityintro

Room progress (33%)

```
024/05/21 10:04:38 Starting gobuster
/ (Status: 200)
/bank-transfer (Status: 200)
024/05/21 10:04:44 Finished
```

Step 3. Hack The Bank

You should have found a secret bank transfer page that allows you to transfer money between bank accounts (`/bank-transfer`). Type the hidden page into the FakeBank website using the browser's address bar.



From this page, an attacker has authorized access and can steal money from any bank account. As an ethical hacker, you would (with permission) find vulnerabilities in their application and report them to the bank to fix them before a hacker exploits them.

Your mission is to transfer \$2000 from bank account 2276 to your account (account number 8881). If your transfer was successful, you should now be able to see your new balance reflected on your account page.

Go there now and confirm you got the money! (You may need to hit Refresh for the changes to appear)

Answer the questions below

Above your account balance, you should now see a message indicating the answer to this question.

FakeBank | Bank Transfer — Mozilla Firefox

about:sessionrestore x FakeBank | Bank Transfer x +

fakebank.thm/bank-transfer

It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back!

Refresh Firefox...

Transfer money between accounts

Admin Portal

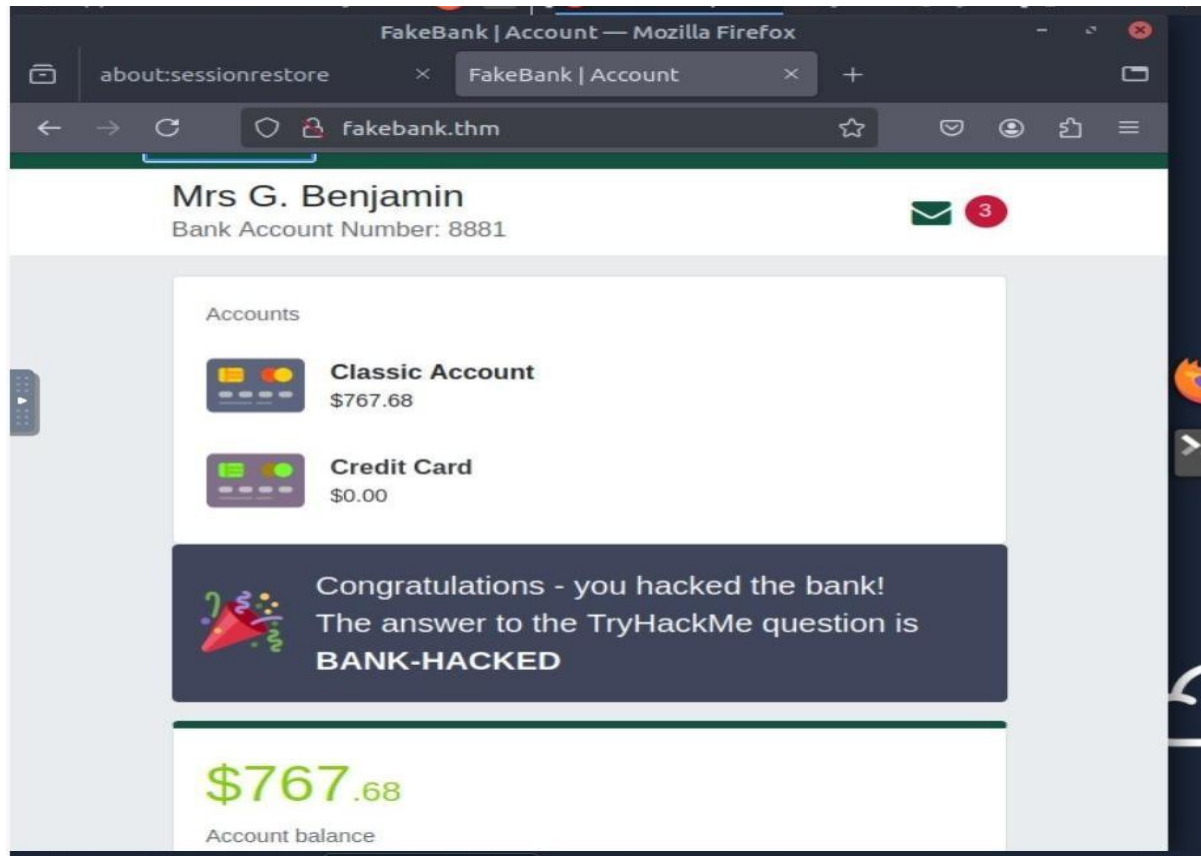
Send from
2276

Send to
8881

Amount to send in USD
2000

Send Money

Hack FakeBank v2.2 54m



Completion

