Intro to Offensive Security

Hack your first website (legally in a safe environment) and experience an ethical hacker's job.
https://tryhackme.com/room/introtooffensivesecurity

Task 1 Hacking your first machine

Before going into cyber security careers and what offensive security is, let's get you hacking (and yes, its legal, all exercises are fake simulations)

Your first hack

Click the "Start Machine" button. Once loaded in Split View in your browser, you will have access to a machine you'll use to hack a fake bank application called FakeBank. If you don't see the machine appear, use the blue Show Split View button on the top-right of this page.

We will use a command-line application called "GoBuster" to brute-force FakeBank's website to find hidden directories and pages. GoBuster will take a list of potential page or directory names and tries accessing a website with each of them; if the page exists, it tells you.

Step 1) Open a terminal

A terminal, also known as the command-line, allows us to interact with a computer without using a graphical user interface. On the machine, open the terminal using the Terminal icon:

Stuck? See video

https://assets.tryhackme.com/additional/introtooffensivesecurity/open-terminal.mp4

Step 2) Find hidden website pages

Most companies will have an admin portal page, giving their staff access to basic admin controls for day-to-day operations. For a bank, an employee might need to transfer money to and from client accounts. Often these pages are not made private, allowing attackers to find hidden pages that show, or give access to, admin controls or sensitive data.

Type the following command into the terminal to find potentially hidden pages on FakeBank's website using GoBuster (a command-line security application).

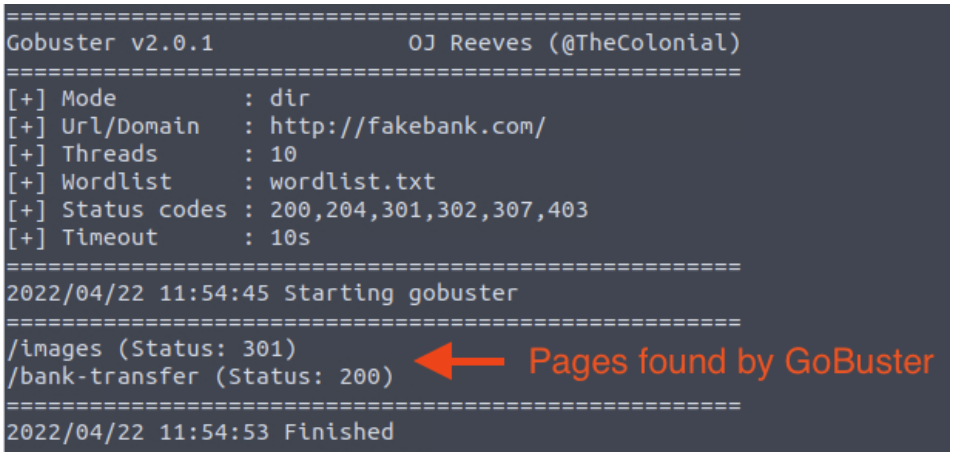
GoBuster command to brute-force website pages

```
ubuntu@tryhackme:~/Desktop$ gobuster -u http://fakebank.com -w wordlist.txt dir
===============================================================
Gobuster v2.0.1
===============================================================
[+] Mode         : dir
[+] Url/Domain   : http://fakebank.com/
[+] Threads      : 10
[+] Wordlist     : wordlist.txt
[+] Status codes : 200,204,301,302,307,403
[+] Timeout      : 10s
===============================================================
2022/04/11 18:23:28 Starting gobuster
===============================================================
/images (Status: 301)
/DIRECTORY_NAME_OUTPUT (Status: 200)
===============================================================
2022/04/11 18:23:38 Finished
===============================================================
```

Don't worry if you have not used a terminal before - TryHackMe walks you through everything!

In the command above, `-u` is used to state the website we're scanning, `-w` takes a list of words to iterate through to find hidden pages.

You will see that GoBuster scans the website with each word in the list, finding pages that exist on the site. GoBuster will have told you the pages it found in the list of page/directory names (indicated by Status: 200).



Step 3) Hack the bank

You should have found a secret bank transfer page that allows you to transfer money between accounts at the bank (/bank-transfer). Type the hidden page into the FakeBank website on the machine.

Stuck? See video

This page allows an attacker to steal money from any bank account, which is a critical risk for the bank. As an ethical hacker, you would (with permission) find vulnerabilities in their application and report them to the bank to fix before a hacker exploits them.

Transfer $2000 from the bank account 2276, to your account (account number 8881).

Answer the questions below

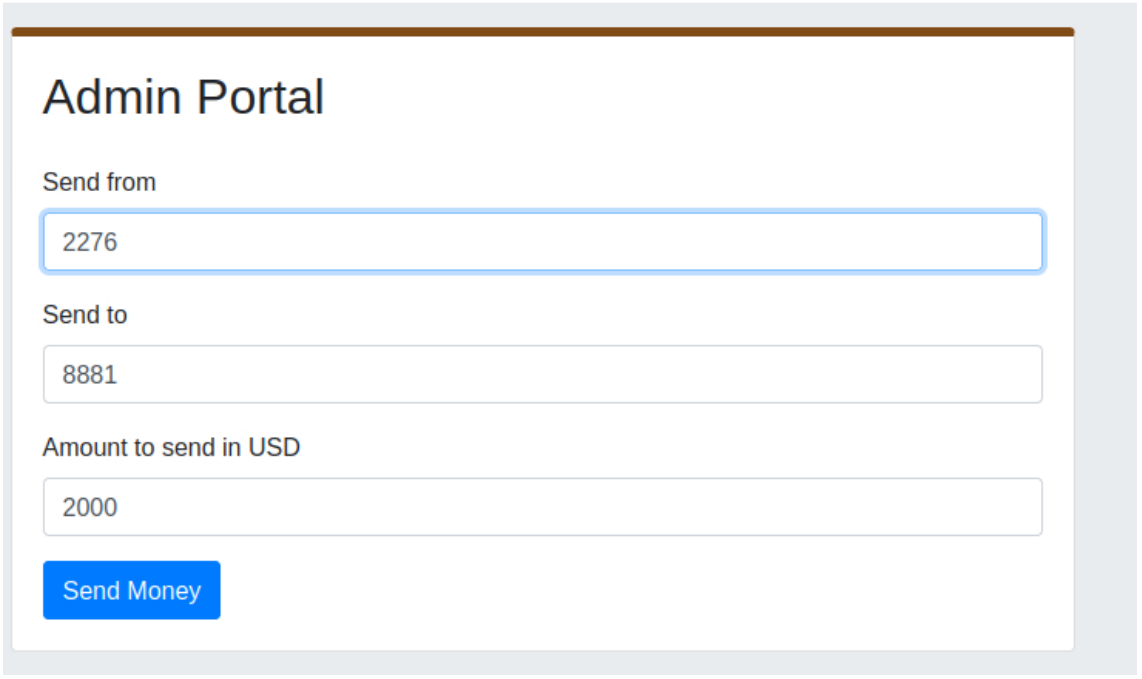
When you've transferred money to your account, go back to your bank account page. What is the answer shown on your bank balance page?

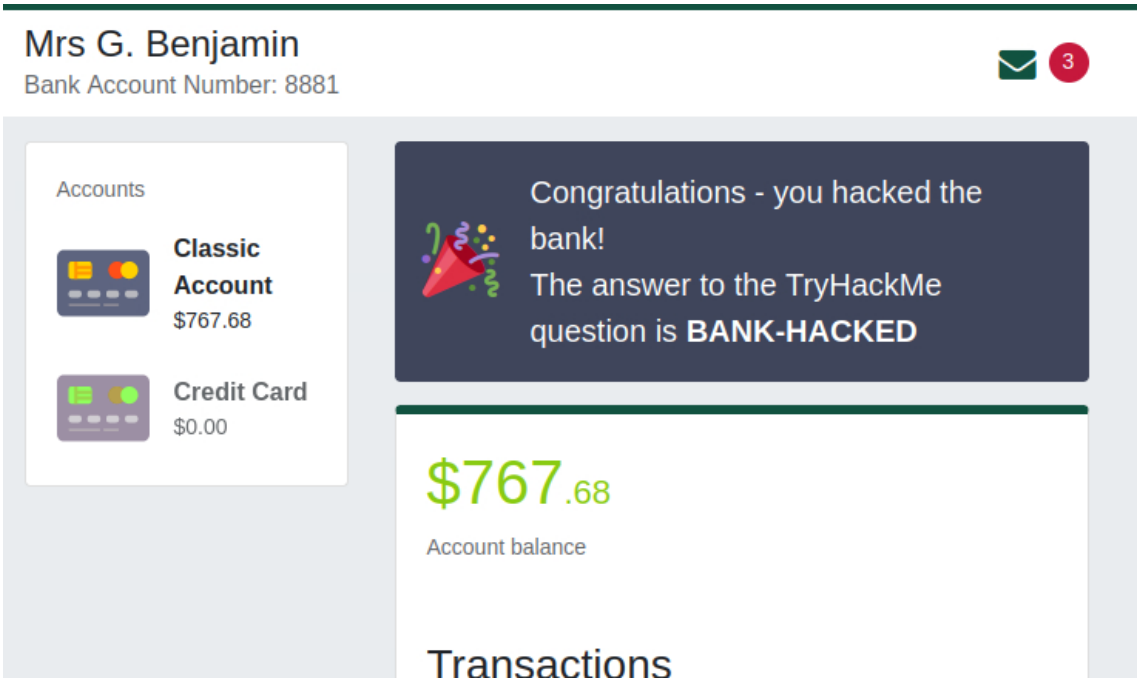
```
Bank-Hacked
```

If you were a penetration tester or security consultant, this is an exercise you'd perform for companies to test for vulnerabilities in their web applications; find hidden pages to investigate for vulnerabilities.

Terminate the machine by clicking the red "Terminate" button at the top of the page.

```
gobuster -u http://fakebank.com -w wordlist.txt dir
```





Task 2 What is Offensive Security?

In short, offensive security is the process of breaking into computer systems, exploiting software bugs, and finding loopholes in applications to gain unauthorized access to them.

To beat a hacker, you need to behave like a hacker, finding vulnerabilities and recommending patches before a cybercriminal does, as you did in this room!

On the flip side, there is also defensive security, which is the process of protecting an organization's network and computer systems by analyzing and securing any potential digital threats; learn more in the digital forensics room.

In a defensive cyber role, you could be investigating infected computers or devices to understand how it was hacked, tracking down cybercriminals, or monitoring infrastructure for malicious activity.

Answer the questions below

Read the above.

Task 3 Careers in cyber security

How can I start learning?

People often wonder how others become hackers (security consultants) or defenders (security analysts fighting cybercrime), and the answer is simple. Break it down, learn an area of cyber security you're interested in, and regularly practice using hands-on exercises. Build a habit of learning a little bit each day on TryHackMe, and you'll acquire the knowledge to get your first job in the industry.

Trust us; you can do it! Just take a look at some people who have used TryHackMe to get their first security job:

- Paul went from a construction worker to a security engineer. Read more.
- Kassandra went from a music teacher to a security professional. Read more.
- Brandon used TryHackMe while at school to get his first job in cyber. Read more.

What careers are there?

The cyber careers room goes into more depth about the different careers in cyber. However, here is a short description of a few offensive security roles:

- Penetration Tester - Responsible for testing technology products for finding exploitable security vulnerabilities.
- Red Teamer - Plays the role of an adversary, attacking an organization and providing feedback from an enemy's perspective.
- Security Engineer - Design, monitor, and maintain security controls, networks, and systems to help prevent cyberattacks.

Answer the questions below

Read the above, and continue with the next room!