

# TryHackMe Task Writeup

## Introduction

Hacking Your First Website (Offensive Security) This document contains my detailed walkthrough and answers for the 'Offensive Security' room on TryHackMe. The room simulates a vulnerable banking website environment to help beginners learn the basics of ethical hacking.

## 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).**

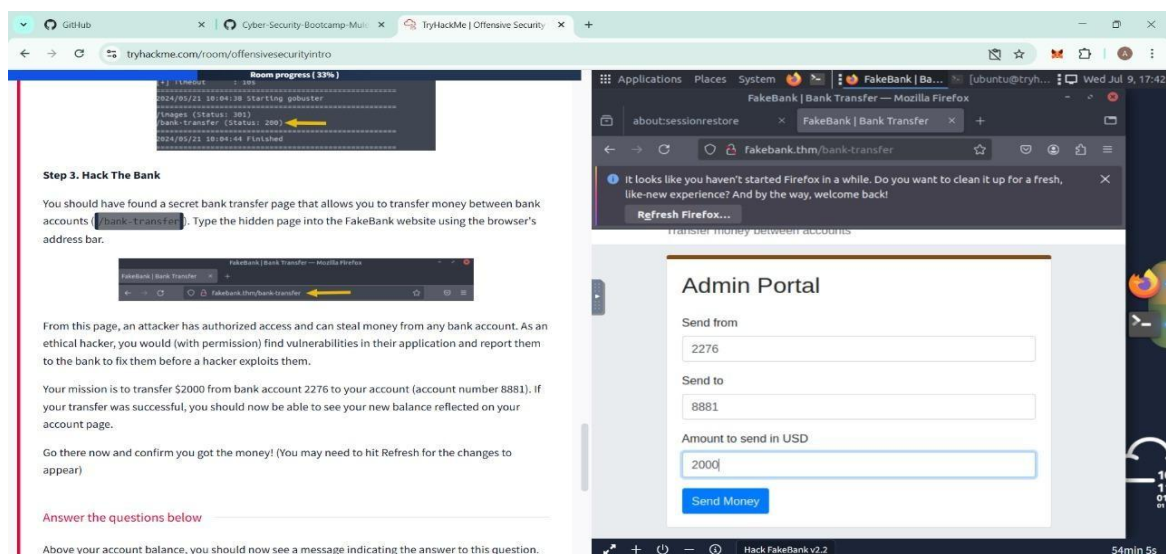
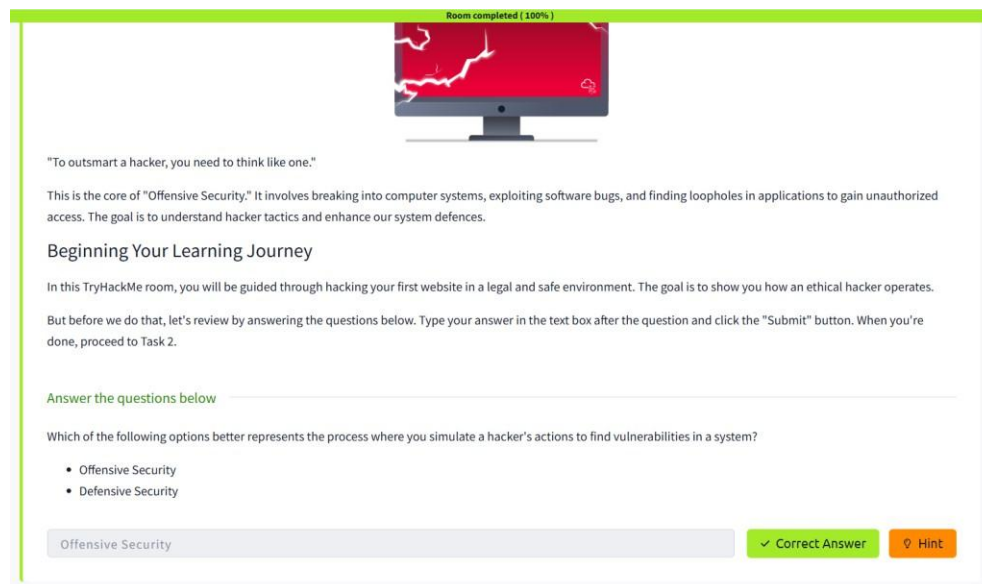
Answer: BANK-HACKED

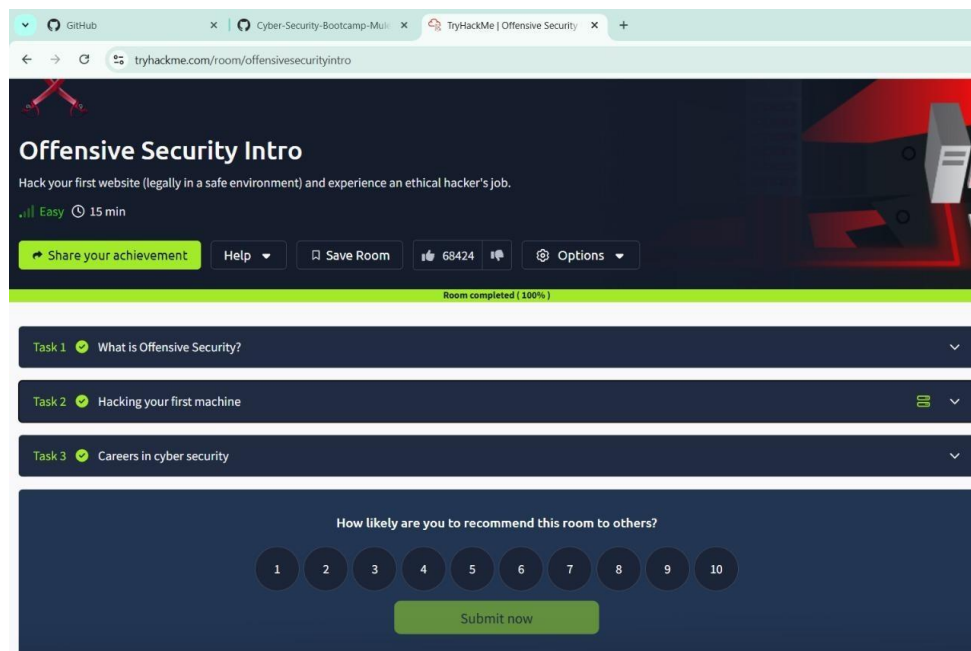
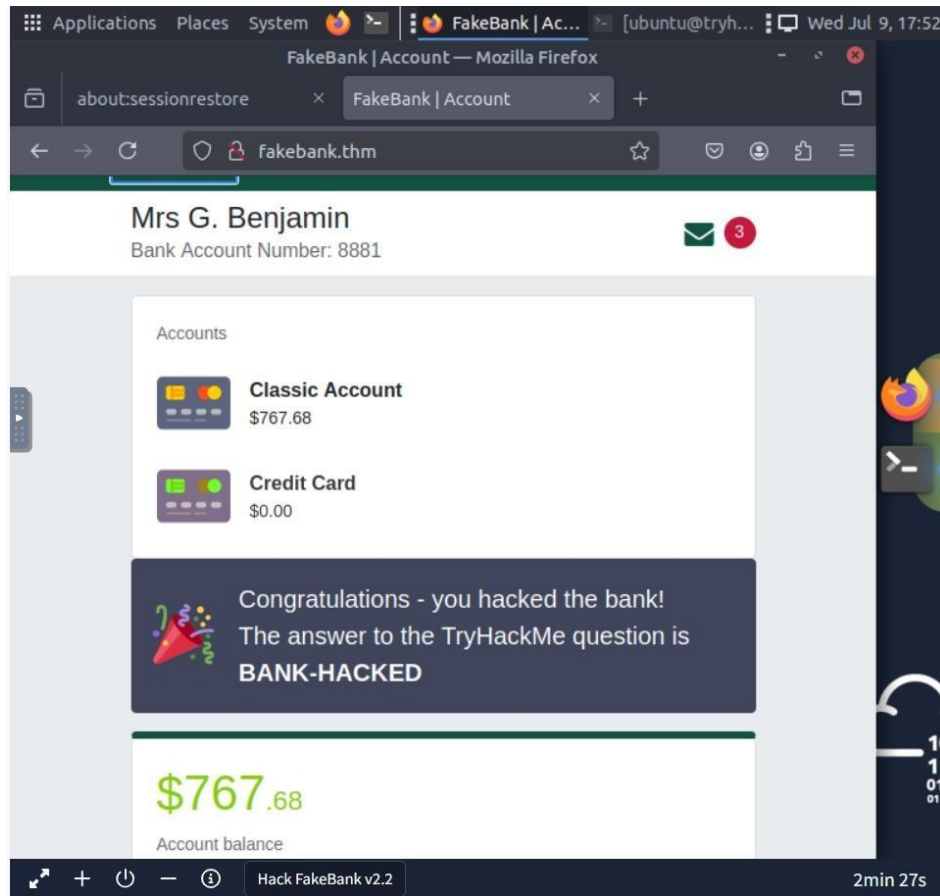
## Tools Used

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.





# TryHackMe - PICKLE RICK CTF

## Overview

In the TryHackMe room **Pickle Rick CTF Walkthrough**, the mission is to help Rick turn himself back into a human by finding three flags.

## Steps

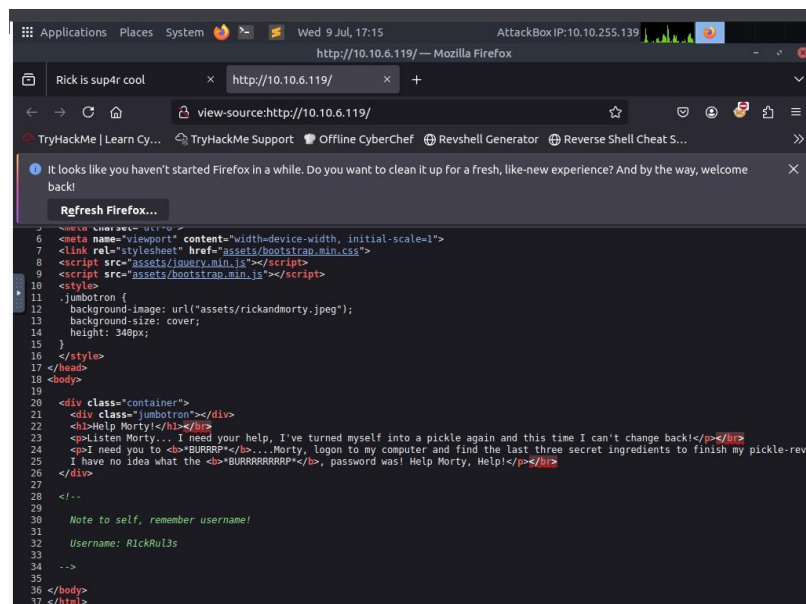
### 1. Initial Reconnaissance

Deploy the machine and once it's up, run the Nmap scan to discover open ports and services.

```
nmap -sC -sV -oN pickle_nmap.txt 10.10.6.119
```

### 2. Explore Website

Visiting the web page on port 80 showed a simple HTML page with Rick's message. View the source code to reveal username.

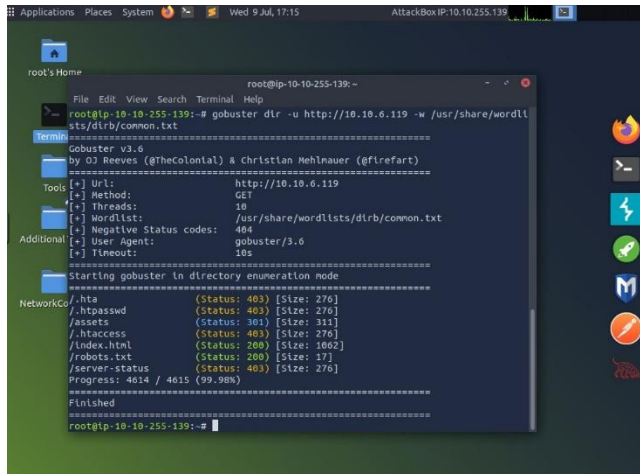


```
1 <meta charset="utf-8">
2 <meta name="viewport" content="width=device-width, initial-scale=1">
3 <link rel="stylesheet" href="assets/bootstrap.min.css">
4 <script src="assets/jquery.min.js"></script>
5 <script src="assets/bootstrap.min.js"></script>
6 <style>
7   .jumbotron {
8     background-image: url("assets/rickandmorty.jpeg");
9     background-size: cover;
10    height: 340px;
11  }
12 </style>
13 </head>
14 <body>
15   <div class="container">
16     <div class="jumbotron"></div>
17     <h1>Help Morty!</h1></div>
18     <p><b>Listen Morty... I need your help, I've turned myself into a pickle again and this time I can't change back!</p></div>
19     <p><b>I need you to <b>BURRRP</b>....Morty, logon to my computer and find the last three secret ingredients to finish my pickle-reve
20     I have no idea what the <b>BURRRRRRRRRP</b>, password was! Help!</p></div>
21   </div>
22 </body>
23 </html>
```

### 3. Directory Bruteforcing

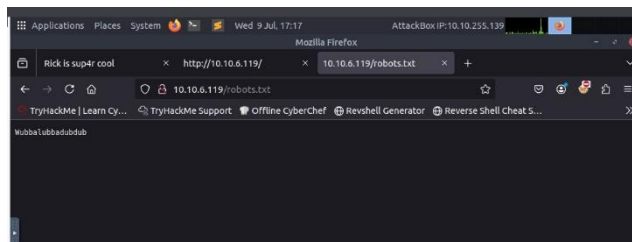
Using the given command lists the hidden files or directories.

**gobuster dir -u <http://10.10.6.119> -w /usr/share/wordlists/dirb/common.txt**



```
root@ip-10-10-255-139:~# gobuster dir -u http://10.10.6.119 -w /usr/share/wordlists/dirb/common.txt
=====
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlner (@firefart)
=====
[+] Url: http://10.10.6.119
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Timeout: 10s
=====
Starting gobuster in directory enumeration mode
=====
NetworkCo /_hta (Status: 403) [Size: 276]
           /_htpasswd (Status: 403) [Size: 276]
           /assets (Status: 301) [Size: 311]
           /.htaccess (Status: 403) [Size: 276]
           /index.html (Status: 200) [Size: 1862]
           /robots.txt (Status: 200) [Size: 17]
           /server-status (Status: 403) [Size: 276]
Progress: 4014 / 4615 (99.98%)
Finished
=====
root@ip-10-10-255-139:~#
```

Get the password from **10.10.6.119/robots.txt**.



### 4. Logging In

Head over to **10.10.6.119/login.php**. Using the username **R1ckRul3s** and password

**Wubbalubbadubdub**, login to the page.

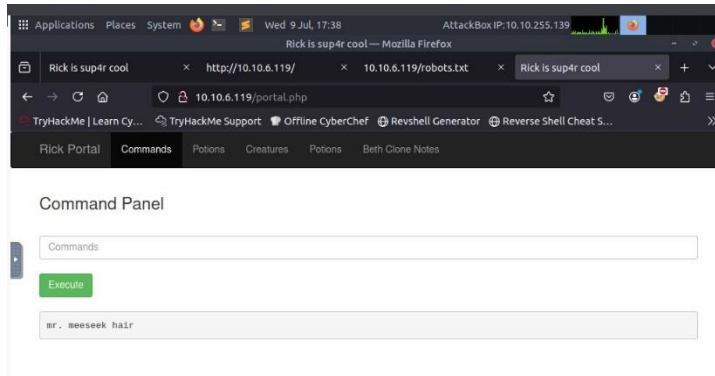
### 5. Finding the Ingredients

i) Ingredient 1:

Running **ls** in the command panel showed a file named

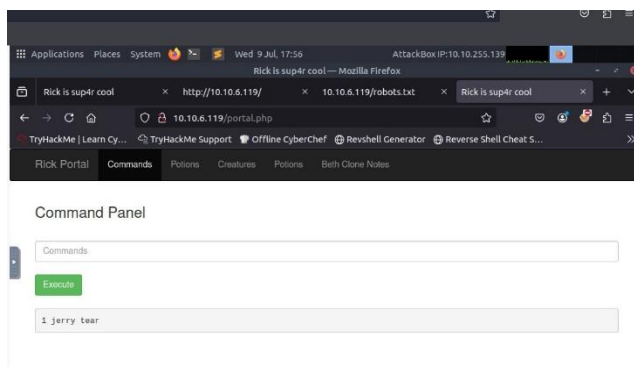
**Sup3rS3cretPickl3Ingred.txt**

Used **less Sup3rS3cretPickl3Ingred.txt** to reveal the first ingredient.



ii) Ingredient 2:

Checked Rick's home directory **ls /home/rick** which showed the second

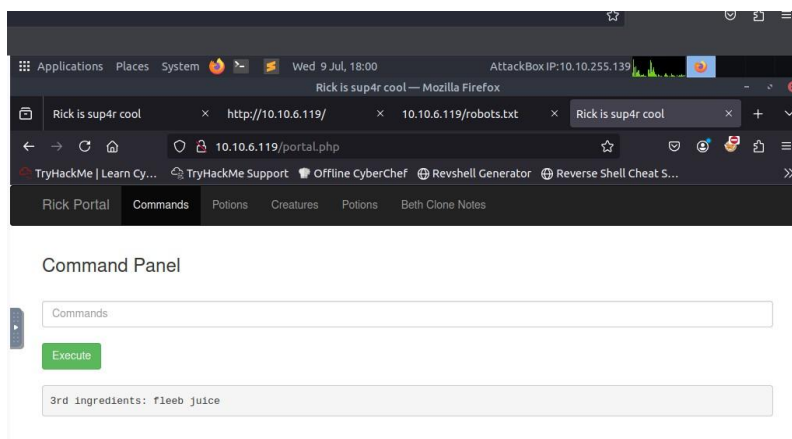


ingredient. The command **less /home/rick/"second ingredients"** revealed the second ingredient.

iii) Ingredient 3:


Checked **sudo ls /root** which showed **3rd.txt**.

The command **sudo less /root/3rd.txt** revealed the third ingredient.




All three ingredients were found!!

kali NetHunter Exploit-DB Google Hacking DB OffSec



**Congratulations on completing Pickle Rick!!! 🎉**

Points earned 🎯 90	Completed tasks ✅ 1	Room type 🚩 Challenge	Difficulty 📶 Easy	Streak 🔥 1
-----------------------	------------------------	--------------------------	----------------------	---------------

 This room counted toward joining the league 🎯

[🗉 Leave Feedback](#) [Continu](#)