

Intro to Offensive Security - Completed 11-05-24 & Documented 11-07-24

The first lab involves using a tool called 'gobuster' to scan a website for hidden directories, referencing specific words from a wordlist text file.

Target Machine Information

Title	Target IP Address	Expires
Hack FakeBank v2.2	10.10.39.17	56min 9s

Add 1 hour

Terminate

```
[+] Timeout      : 10s
=====
2024/05/21 10:04:38 Starting gobuster
=====
/images (Status: 301)
/bank-transfer (Status: 200)
=====
2024/05/21 10:04:44 Finished
=====
```

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 in the list of page/directory names (indicated by Status: 200).

```
=====
[+] Mode       : dir
[+] Url/Domain  : http://fakebank.thm/
[+] Threads    : 10
[+] Wordlist    : wordlist.txt
[+] Status codes : 200,204,301,302,307,403
[+] Timeout    : 10s
=====
```

```
ubuntu@tryhackme: ~/Desktop
File Edit View Search Terminal Help
ubuntu@tryhackme:~/Desktop$ gobuster -u http://fakebank.thm -w wordlist.txt dir

Gobuster v2.0.1           OJ Reeves (@TheColonial)
=====
[+] Mode       : dir
[+] Url/Domain  : http://fakebank.thm/
[+] Threads    : 10
[+] Wordlist    : wordlist.txt
[+] Status codes : 200,204,301,302,307,403
[+] Timeout    : 10s
=====
2024/11/06 02:48:33 Starting gobuster
=====
/images (Status: 301)
/bank-transfer (Status: 200)
=====
2024/11/06 02:48:42 Finished
=====
ubuntu@tryhackme:~/Desktop$
```

To the right, we ran the following command: `gobuster -u http://www.websitename.xyz -w wordlist.txt dir`

In this command:

`-u` specifies the URL we want gobuster to scan.

`-w` indicates the wordlist file (wordlist.txt) that gobuster will use to identify potential hidden directories.

'dir' is the mode, one of five offered by gobuster, that searches through each directory in the list for matches based on the conditions in our .txt file.

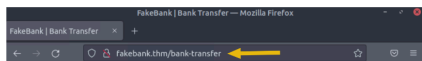
You will see that Gobuster scans the website with each word in the list, finding pages that exist on the site. Gobuster will have told you the pages in the list of page/directory names (indicated by Status: 200).

```
Gobuster v2.0.1           OJ Reeves (@TheColonial)
=====
[+] Mode       : dir
[+] Url/Domain  : http://fakebank.thm/
[+] Threads    : 10
[+] Wordlist    : wordlist.txt
[+] Status codes : 200,204,301,302,307,403
[+] Timeout    : 10s
=====
2024/05/21 10:04:38 Starting gobuster
=====
/images (Status: 301)
/bank-transfer (Status: 200)
=====
2024/05/21 10:04:44 Finished
=====
```

```
[+] Timeout      : 10s
=====
2024/11/06 02:48:33 Starting gobuster
=====
/images (Status: 301)
/bank-transfer (Status: 200)
=====
2024/11/06 02:48:42 Finished
=====
ubuntu@tryhackme:~/Desktop$
```

Between the start and finish messages on the right, we can see that gobuster has found two hidden directories from our wordlist: '/images' and '/bank-transfer.' The 'Status: 301' response indicates a redirection, showing us where the new /images page is located. The 'Status: 200' response indicates that our (GET) request to access the '/bank-transfer' path was successful.

Target Machine Information		
Title	Target IP Address	Expires
Hack FakeBank v2.2	10.10.39.17	52min 23s
<div>Add 1 hour</div> <div>Terminate</div>		



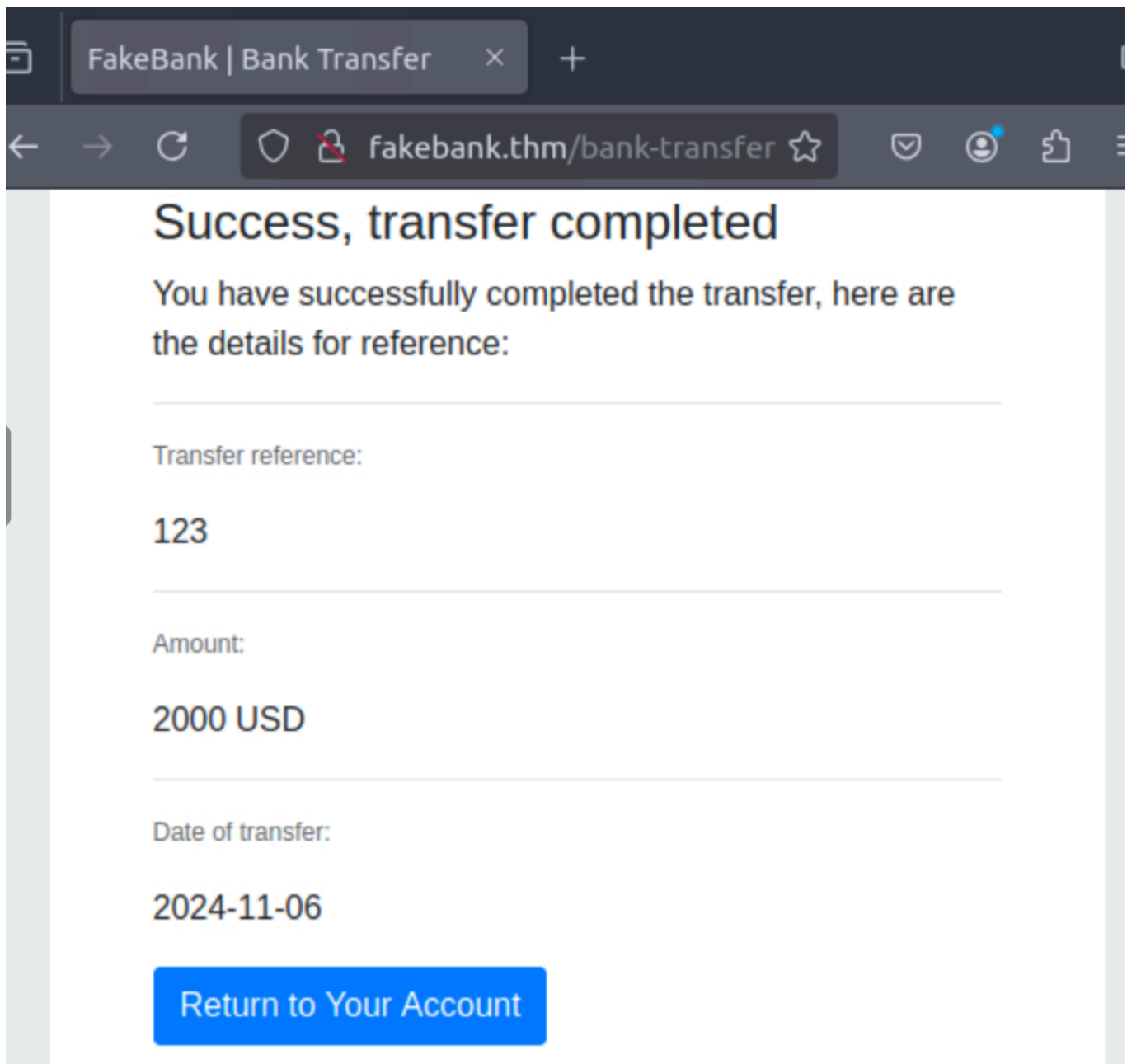
From this page, an attacker has authorized access and can steal money from any bank account. As an ethical hacker, you would (with permission) find vulnerabilities in their application and report them to the bank to fix them before a hacker exploits them.

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)

A screenshot of a web browser window showing the 'FakeBank | Bank Transfer' page. The browser's address bar shows 'fakebank.lhmy/bank-transfer'. The page has a title 'FakeBank | Bank Transfer' and a subtitle 'Transfer money between accounts'. The main content area is titled 'Admin Portal' and contains three input fields: 'Send from' with the value '2276', 'Send to' with the value '8881', and 'Amount to send in USD' with the value '2000'. A blue button labeled 'Send Money' is at the bottom of the form. The browser's status bar at the bottom shows 'Wed Nov 6, 0'.

After receiving the successful response, we navigated to the page by appending the path to the site's URL. Our next task was to transfer funds from the victim's account to our own.



Shortly after submitting the transfer request, we received a confirmation message.

(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

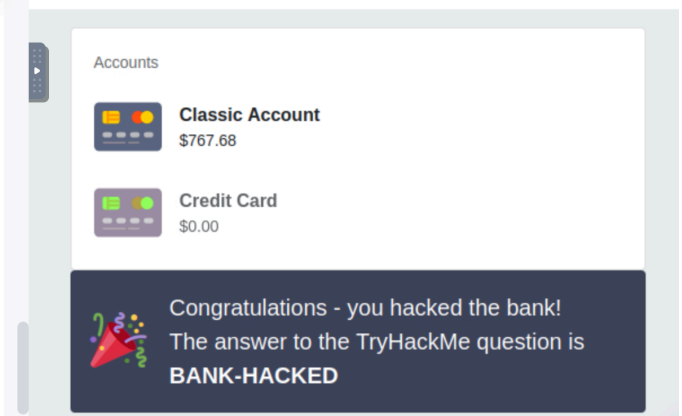
Above your account balance, you should now see a message indicating the answer to this question. Can you find the answer you need?

BANK-HACKED

Submit

Hint

If you were a penetration tester or security consultant, this is an exercise you'd



Finally, we unlocked a message confirming the completion of our first TryHackMe learning path!

Additional resources:

<https://www.freecodecamp.org/news/gobuster-tutorial-find-hidden-directories-sub-domains-and-s3-buckets/>