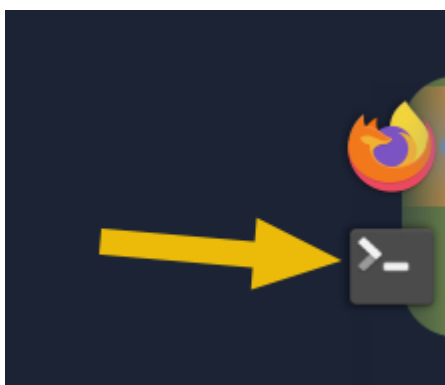


Using Gobuster Tool for files search and taking access of a bank app in TryHackMe Labs

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 try 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 by clicking on the Terminal icon on the right of the screen.



Step 2. Use Gobuster To Find Hidden Website Pages

Most companies 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. Due to human error or negligence, there may be instances when these pages are not made private, allowing attackers to find hidden pages that show or give access to admin controls or sensitive data.

To begin, type the following command into the terminal to find potentially hidden pages on FakeBank's website using Gobuster (a command-line security application).

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

The command will run and show you an output similar to this:

Gobuster command to brute-force website pages

```
ubuntu@tryhackme:~/Desktop$ gobuster -u http://fakebank.thm -w wordlist.txt dir
```

```
=====
```

```
Gobuster v2.0.1      OJ Reeves (@TheColonial)
```

© Anushka Sinha | <https://github.com/rikusmiles/> | Original work

=====

[+] 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

© Anushka Sinha | github.com/rikusmiles/

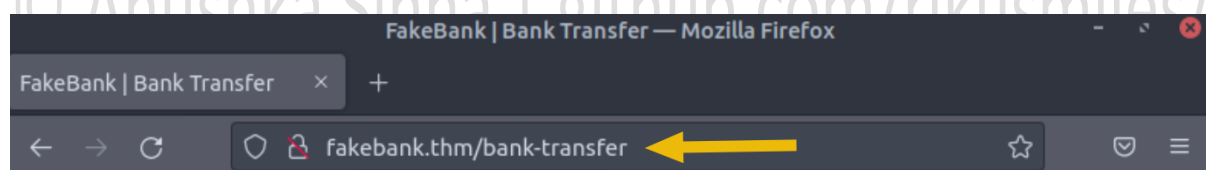
In the command above, -u is used to state the website we're scanning, -w takes a list of words to iterate through to find hidden pages.

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).

```
=====
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
=====
```

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)

References:

TryHackMe Labs