1. Overall Vulnerability/Risk analysis 0.5p

Business risk (Executive summary)

The vulnerability in the bank's transfer admin portal arises from the lack of authentication. Without authentication anyone, who gains access to the portal can transfer money to and from any account. This creates a high risk of unauthorized transfers which expose the bank to financial losses, data breaches and reputational damage.

Unauthorized access to the bank's servers may give the bad actor access to sensitive information (customers' personal details etc.). This exposes the bank to legal action from regulatory bodies and contributes to the loss of reputation.

Technical risk (Technical summary)

Broken Access Control:

Accesing a hidden webpage gives access to the admin portal. The portal is accesible outside of the banks network and doesn't require the user to authenticate. There is a high likelyhood that other systems are affected by similar mistakes in configuration.

Credential Exposure:

Unauthorized access the banks servers through SSH may be and indication of a larger breach given that login details have been leaked.

2. **Vulnerability impact review 0.5p**

   Risk likelihood

   The risk of the Broken Access Control vulnerability is high given that the page is easily accesible with little technical know-how.

   The risk of the Credential Exposure is also relatively high depending on the sensitivity of the accessed server and if the same credentials are used on other systems.

   Potential impact

   The potential impact of the admin portal vulnerability is extremely high. Since the portal let’s the bad actor transfer funds without any authentication.

   Impact of the Credential Exposure depends on the usecase of the accessed system and if the credentials are used for accessing other systems.

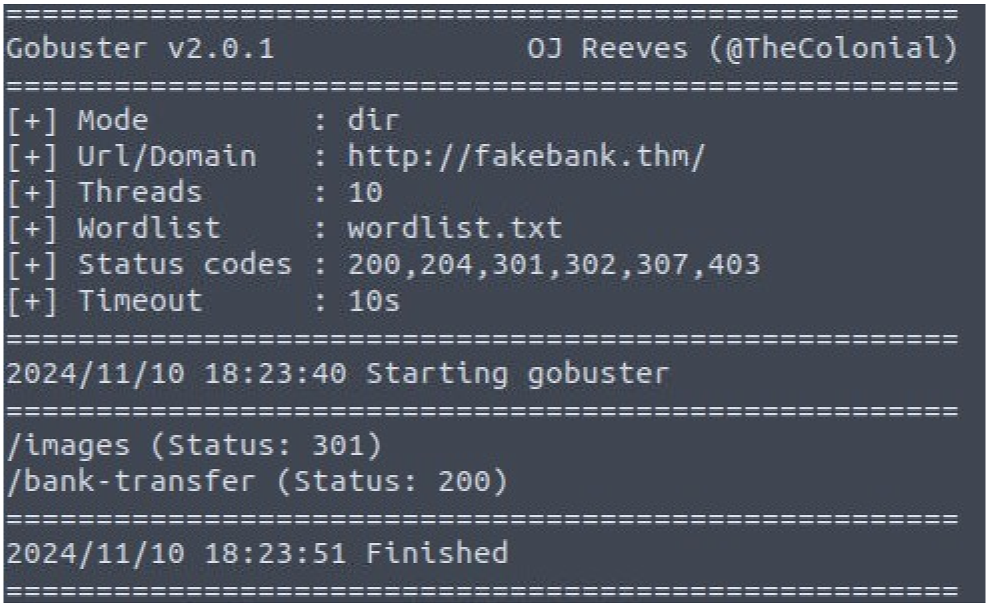
3. **Remediation options 0.5p**
   Vulnerability of the admin portal can be solved by requiring authentication to access the portal. MFA is strongly recommended. Depending on the requirements of the bank making the page only accesible inside the banks network is recommended.

   Unauthorized SSH access can be remedied by using SSH keys and strong passwords. Rotation of keys and passwords is also beneficial. Having the servers SSH port not be open to the internet is recommended.

   Future strategies include auditing software before deployment to find glaring security risks. Stricter monitoring for unknown IP adresses will help with securing the network.

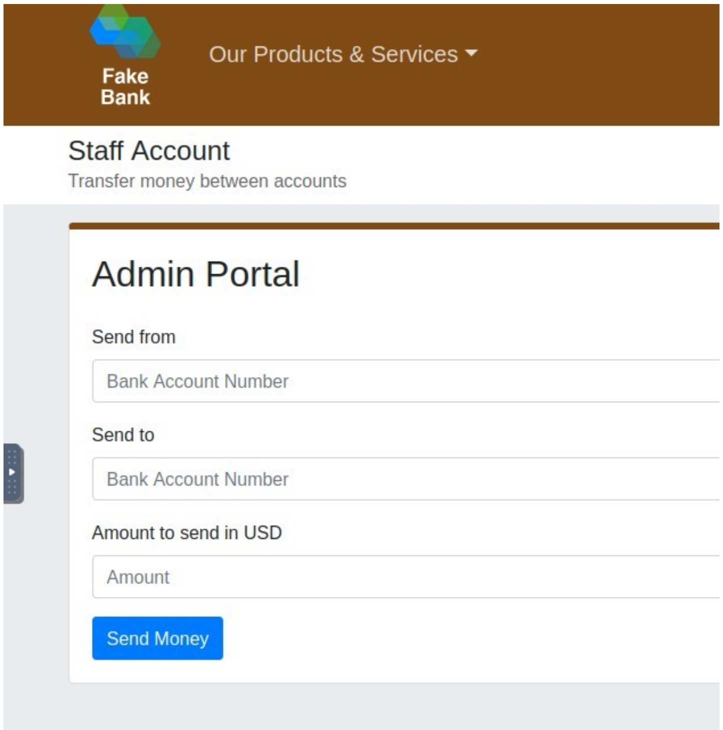
4. Technical findings 2.5p

A hidden unsecured webpage was found using GoBuster.



```
=====================================================
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
=====================================================
2024/11/10 18:23:40 Starting gobuster
=====================================================
/images (Status: 301)
/bank-transfer (Status: 200)
=====================================================
2024/11/10 18:23:51 Finished
=====================================================
```

The hidden page is an admin portal for the bank's staff used to perform transfers between bank accounts. The portal is not secured in any way and is accesible outside of the bank's internal network.



Staff Account

Transfer money between accounts

Admin Portal

Send from

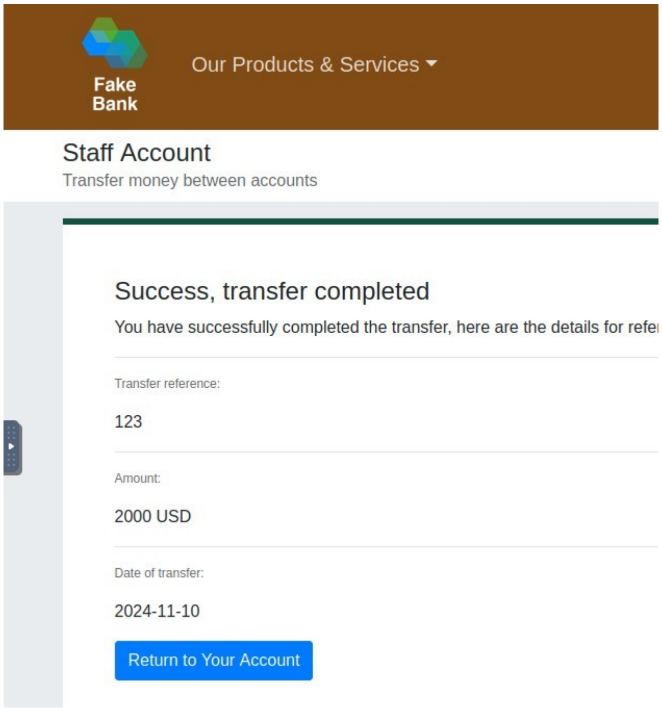
Bank Account Number

Send to

Bank Account Number

Amount to send in USD

Amount



Staff Account

Transfer money between accounts

Success, transfer completed

You have successfully completed the transfer, here are the details for refe

Transfer reference:

123

Amount:

2000 USD

Date of transfer:

2024-11-10

> On the page it is possible to transfer funds from one account to another without authenticating. The test transfer was confirmed to have been succesful.

An unknown actor also gained access to one of the bank’s servers through SSH. The actors IP address has been blocked.

5. **Original cause 0.5p**

The root cause of the admin portal vulnerability is missing authentication and access to the page from outside of the bank’s internal network.

Unknown actors’ access to one of the bank’s servers through SSH is most likely caused by leaked credentials and/or keys.

6. **Conclusions 0.5p**

Most likely compromise scenarios

Broken Access Control:

The vulnerability will most likely be exploited by bank customers since the admin portal is used for internal bank transfers. The exploit would likely happen when a bad actor finds the page and uses it to transfer money.

Credential Exposure:

The vulnerability will most likely be exploited by bad actors looking to gain access to senstive information and/or systems.

Implications

Loss of funds and reputation. Risk of the bank’s systems being compromised with the leaked credentials.

Remedied by implementing authentication to the admin portal and having stricter control of passwords and keys.