TRYHACKME

# 2023 Security Assessment Report Prepared For

# FakeBank

Report Issued: 08-26-2023

## Confidentiality Notice

*This report contains sensitive, privileged, and confidential information. Precautions should be taken to protect the confidentiality of the information in this document. Publication of this report may cause reputational damage to FakeBank or facilitate attacks against FakeBank. TryHackMe shall not be held liable for special, incidental, collateral or consequential damages arising out of the use of this information.*

## Disclaimer

*Note that this assessment may not disclose all vulnerabilities that are present on the systems within the scope of the engagement. This report is a summary of the findings from a "point-in-time" assessment made on FakeBank's environment. Any changes made to the environment during the period of testing may affect the results of the assessment.*

# TABLE OF CONTENTS

# EXECUTIVE SUMMARY

TryHackMe performed a security assessment of the internal corporate network of FakeBank on 08-26-2023. TryHackMe's penetration test simulated an attack from an external threat actor attempting to gain access to systems within the FakeBank corporate network. The purpose of this assessment was to discover and identify vulnerabilities in FakeBank's infrastructure and suggest methods to remediate the vulnerabilities. TryHackMe identified a total of 1 vulnerability within the scope of the engagement which are broken down by severity in the table below.

| CRITICAL | HIGH | MEDIUM | LOW |
|---|---|---|---|
| 1 | 0 | 0 | 0 |

The highest severity vulnerabilities give potential attackers the opportunity to transfer money using administrative privileges from any account to any account by accessing an unsecured hidden domain. This domain should not be available to non-credentialed users, and needs some authentication, authorization, and accounting (AAA) measures before allowing administrative access. In order to ensure data confidentiality, integrity, and availability, security remediations should be implemented as described in the security assessment findings.

Note that this assessment may not disclose all vulnerabilities that are present on the systems within the scope. Any changes made to the environment during the period of testing may affect the results of the assessment.

# HIGH LEVEL ASSESSMENT OVERVIEW

## Observed Security Strengths

TryHackMe identified the following strengths in FakeBank's network which greatly increases the security of the network. FakeBank should continue to monitor these controls to ensure they remain effective.

### Webpage Security

- Great thing we saw here that causes us issues (which is a good thing) was the existence of only an account page and a transfer page, greatly limiting the potential attack surface.
- The images page was empty, not giving us any account information.
- The credit card application didn't work, forbidding us from injecting any malicious code into an input form.

## Areas for Improvement

TryHackMe recommends FakeBank takes the following actions to improve the security of the network. Implementing these recommendations will reduce the likelihood that an attacker will be able to successfully attack FakeBank's information systems and/or reduce the impact of a successful attack.

## Short Term Recommendations

TryHackMe recommends FakeBank take the following actions as soon as possible to minimize business risk.

### Immediate

- Require Authentication & Authorization
    - Allowing any user to transfer a bank balance is a recipe for disaster.
    - Implementing 2FA, HTTPS encryption, strong password policies, lease privilege RBAC, time and session policies, logging and monitoring, and alerts will greatly increase all AAA factors.

# SCOPE

All testing was based on the scope as defined in the Request For Proposal (RFP) and official written communications. The items in scope are listed below.

## Networks

| Network | Note |
| --- | --- |
| 10.0.1.0/24 | Network for Corporate HQ |
| 10.0.2.0/24 | Gotham, NY, branch site |

## Provided Credentials

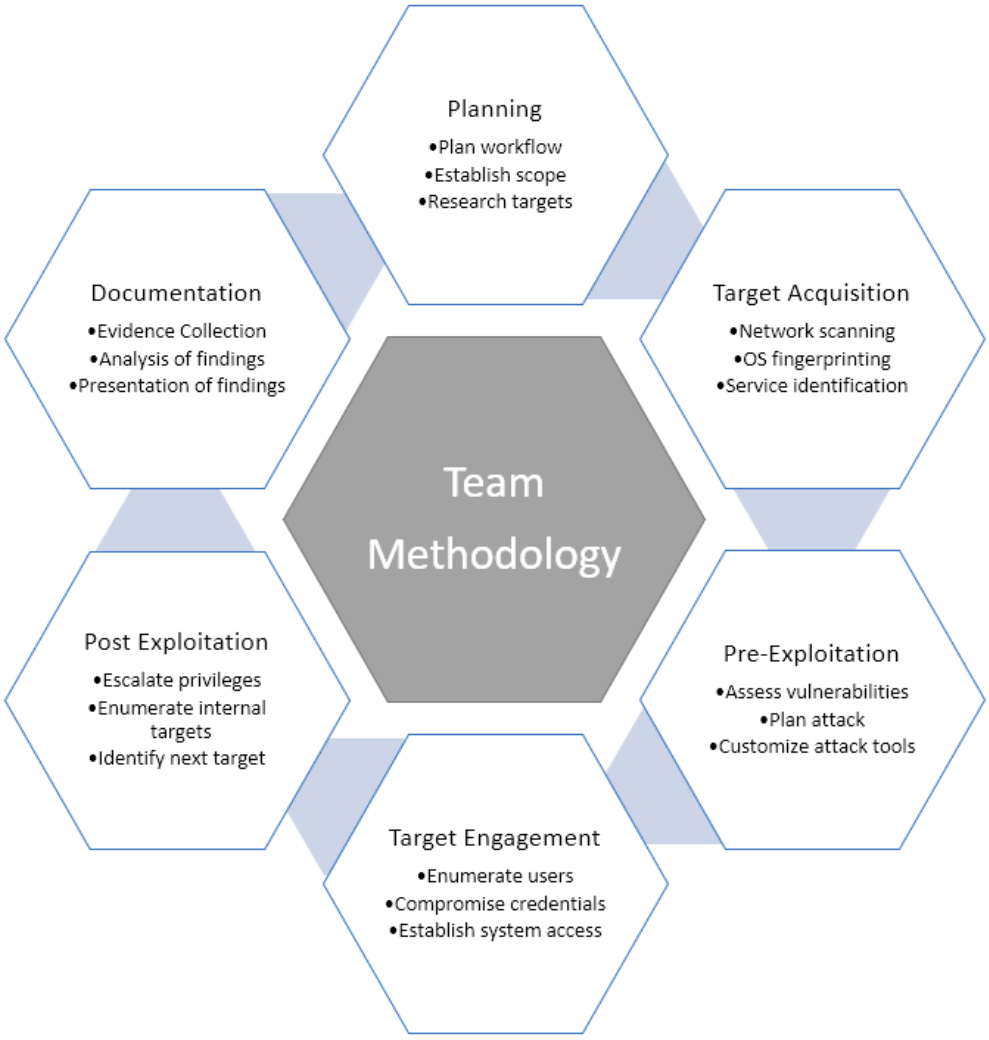
FakeBank provided TryHackMe with the following credentials and access to facilitate the security assessment listed below.

| Item | Note |
| --- | --- |
| Customer Account | (testuser@fakebank.com) A fake customer account in the bank application for testing functionality that requires authentication. |

# TESTING METHODOLOGY

TryHackMe's testing methodology was split into three phases: *Reconnaissance*, *Target Assessment*, and *Execution of Vulnerabilities*. During reconnaissaTryHackMe used gobuster and other enumeration methods to refine target information and assess target values. Next, we conducted our targeted assessment. TryHackMe simulated an attacker exploiting vulnerabilities in the FakeBank network. TryHackMe gathered evidence of vulnerabilities during this phase of the engagement while conducting the simulation in a manner that would not disrupt normal business operations.

The following image is a graphical representation of this methodology.



# CLASSIFICATION DEFINITIONS

## Risk Classifications

| Level | Score | Description |
|---|---|---|
| Critical | 10 | The vulnerability poses an immediate threat to the organization. Successful exploitation may permanently affect the organization. Remediation should be immediately performed. |
| High | 7-9 | The vulnerability poses an urgent threat to the organization, and remediation should be prioritized. |
| Medium | 4-6 | Successful exploitation is possible and may result in notable disruption of business functionality. This vulnerability should be remediated when feasible. |
| Low | 1-3 | The vulnerability poses a negligible/minimal threat to the organization. The presence of this vulnerability should be noted and remediated if possible. |
| Informational | 0 | These findings have no clear threat to the organization, but may cause business processes to function differently than desired or reveal sensitive information about the company. |

## Exploitation Likelihood Classifications

| Likelihood | Description |
|---|---|
| **Likely** | Exploitation methods are well-known and can be performed using publicly available tools. Low-skilled attackers and automated tools could successfully exploit the vulnerability with minimal difficulty. |
| **Possible** | Exploitation methods are well-known, may be performed using public tools, but require configuration. Understanding of the underlying system is required for successful exploitation. |
| **Unlikely** | Exploitation requires deep understanding of the underlying systems or advanced technical skills. Precise conditions may be required for successful exploitation. |

## Business Impact Classifications

| Impact | Description |
|---|---|
| **Major** | Successful exploitation may result in large disruptions of critical business functions across the organization and significant financial damage. |
| **Moderate** | Successful exploitation may cause significant disruptions to non-critical business functions. |
| **Minor** | Successful exploitation may affect few users, without causing much disruption to routine business functions. |

## Remediation Difficulty Classifications

| Difficulty | Description |
|---|---|
| **Hard** | Remediation may require extensive reconfiguration of underlying systems that is time consuming. Remediation may require disruption of normal business functions. |
| **Moderate** | Remediation may require minor reconfigurations or additions that may be time-intensive or expensive. |
| **Easy** | Remediation can be accomplished in a short amount of time, with little difficulty. |

# ASSESSMENT FINDINGS

| Number | Finding | Risk Score | Risk | Page |
|---|---|---|---|---|
| 1 | Open Administrative Directory | **10** | **High** | 12 |

TEMPLATE NOTE: (Sorting by descending risk score)

# 1 - Example Vulnerability Finding

| HIGH RISK (8/10) | |
|---|---|
| **Exploitation Likelihood** | **Possible** |
| **Business Impact** | **Severe** |
| **Remediation Difficulty** | **Easy** |

**Security Implications**

Using gobuster we found an exposed administrative bank transfer page and were subsequently able to transfer a large sum of money between accounts. This finding is very important because it can destroy the entire business if left unchecked.

**Analysis**

Upon going through a predetermined list of possible directories we found two open to the internet (see Figure 1). After navigating to the /bank-transfer page, we were shocked to discover administrative controls and subsequently transferred $2000 from account 2276 to account 8881. (see Figures 2 -4)


***Figure 1**: A terminal showing the exposed web directory*

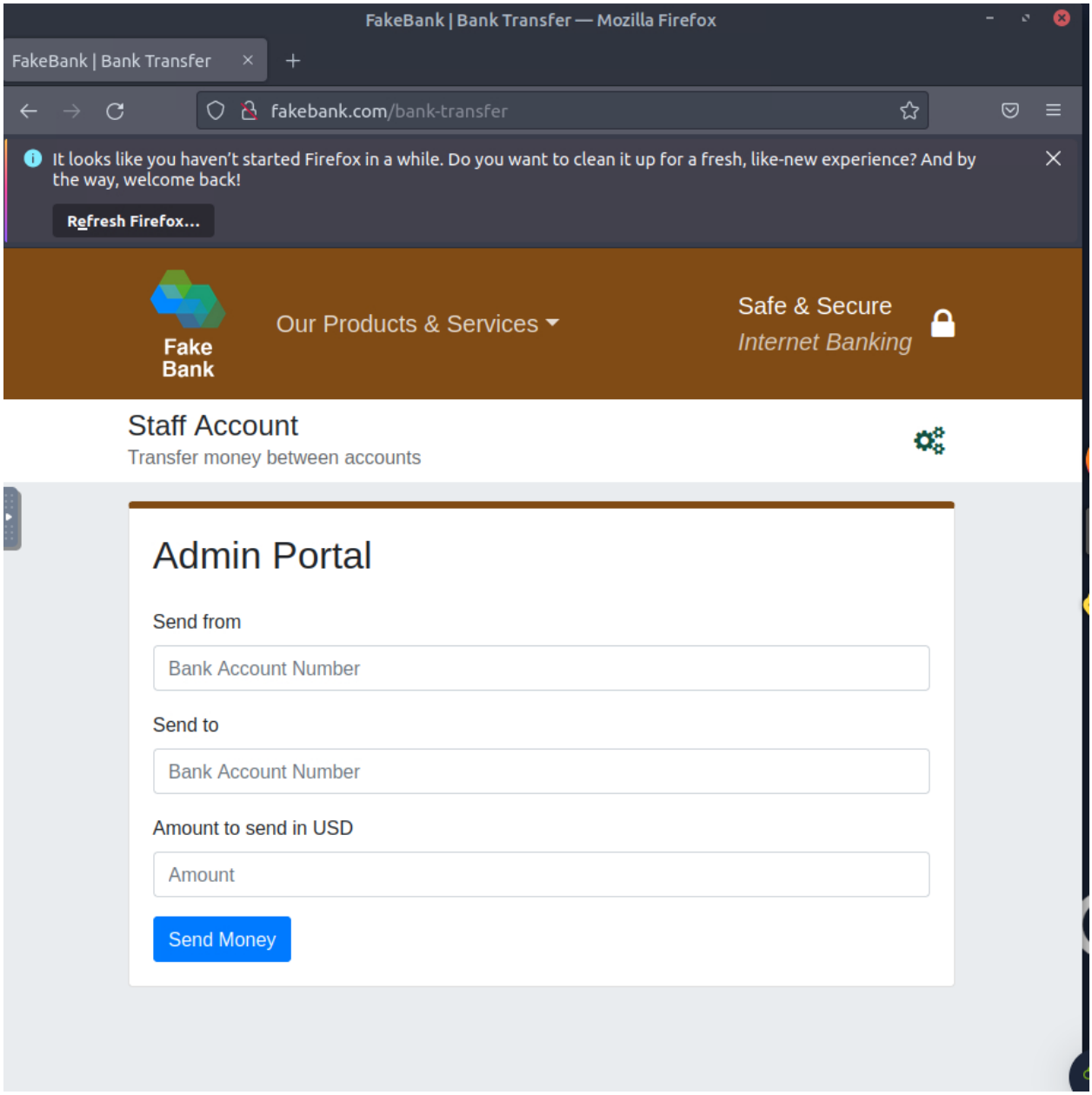



***Figure 2**: The exposed controls*

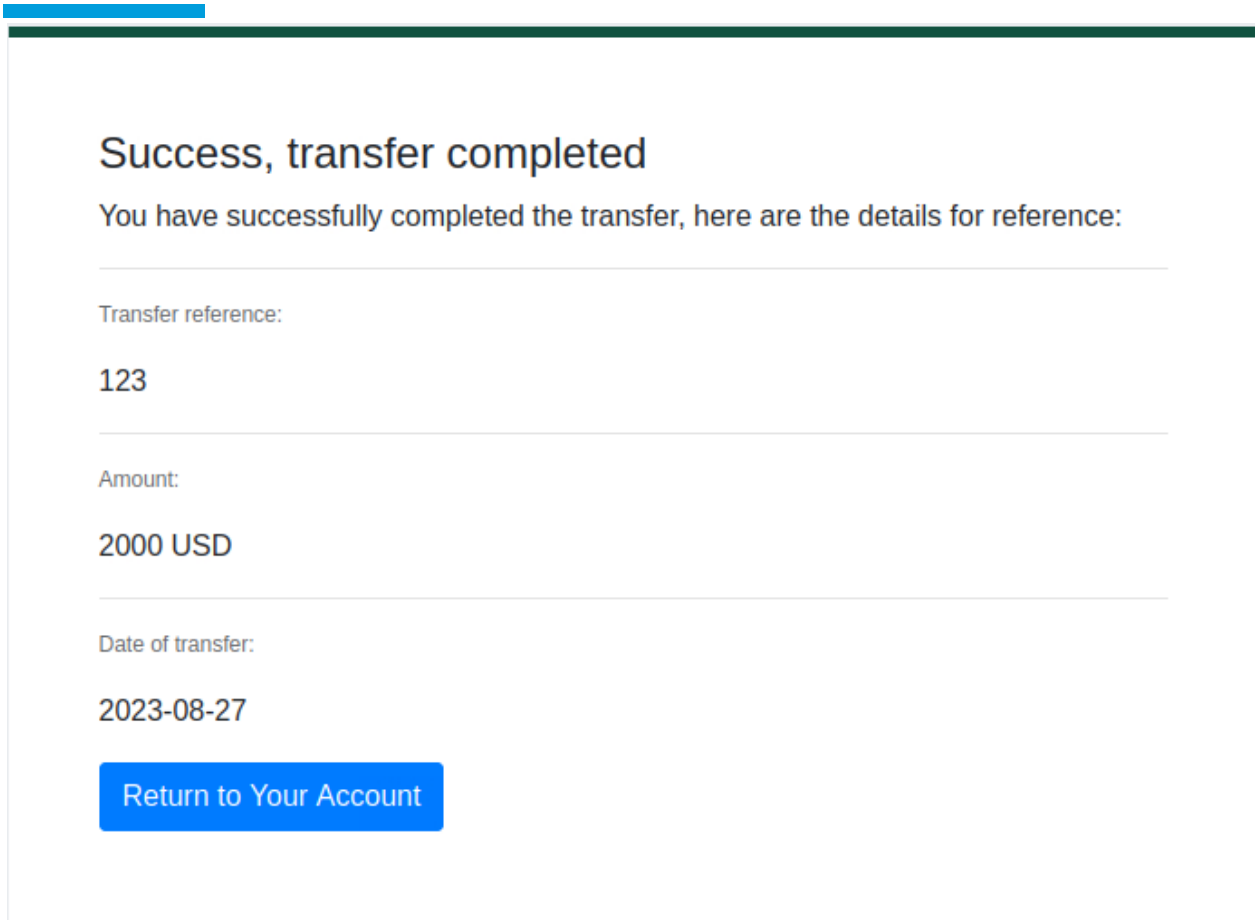



***Figure 3**: The transfer confirmation*

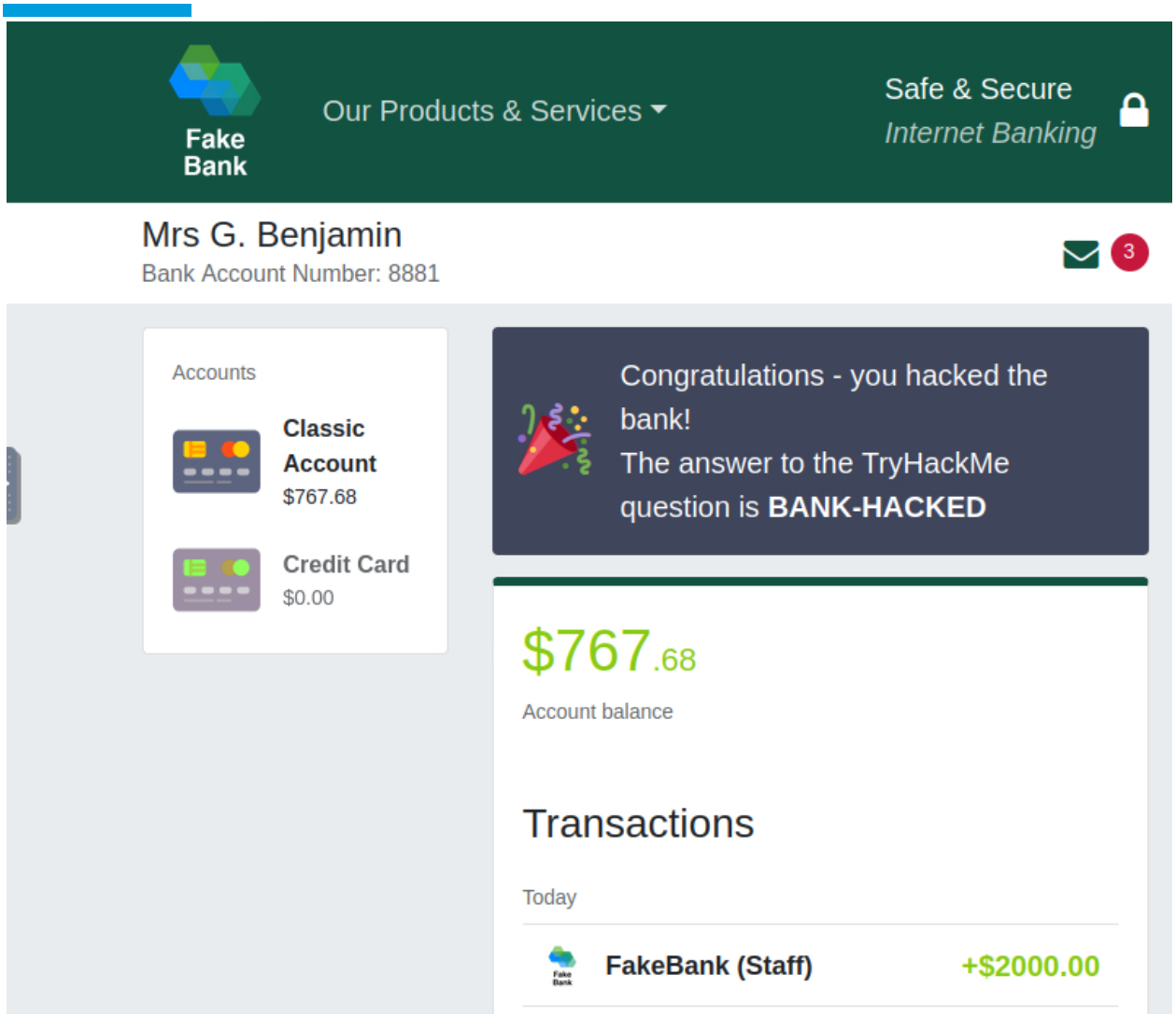



***Figure 4**: The transfer confirmation*

**Recommendations**

- Remove insecure access to the directory
- Implement strong AAA measures

**References (opt)**

- https://github.com/Sevaarcen/RADAR/tree/master/radar/playbooks
- https://owasp.org/www-project-top-ten/

# APPENDIX A - TOOLS USED

| TOOL | DESCRIPTION |
|---|---|
| **gobuster** | Used for testing of web directories. |
| **Firefox** | Used for connecting to various servers. |

***Table A.1:*** *Tools used during assessment*

# APPENDIX B - ENGAGEMENT INFORMATION

## Client Information

| | |
|---|---|
| **Client** | FakeBank |
| **Primary Contact** | John Doe,<br>CSO |
| **Approvers** | The following people are authorized to change the scope of engagement and modify the terms of the engagement<br>● Janet Doe<br>● Marco Polo |

## Version Information

| Version | Date | Description |
|---|---|---|
| 1.0 | 08-26-2023 | Initial report to client |

## Contact Information

| | |
|---|---|
| **Name** | TryHackMe Consulting |
| **Address** | 1001 Fake Street, Gotham, NY 11201 |
| **Phone** | 555-185-1782 |
| **Email** | email@example.com |