1 Executive Security Assessment Report

1.1 Introduction

This report presents the findings from a comprehensive security assessment conducted on the domain **ofx1.secureinternetbank.com**. The analysis was initiated on **June 27th** at **01:45** and completed in **00h:10m:29s**. The assessment, identified by tracking ID **0303d95a74e9**, was executed using a Basic scan type. The evaluation focused on identifying potential vulnerabilities within the web application and its infrastructure, adhering to OWASP and OSCP methodologies.

1.2 Short Summary of Main Issues

The security assessment identified a total of **18** issues, categorized as **0** high-risk, **1** medium-risk, **2** low-risk, and **15** informational. The most significant finding is a medium-risk issue related to open port **80**, which lacks encryption and poses potential security risks if not redirected to HTTPS or if HSTS is not enabled. This could expose sensitive data to interception, impacting business confidentiality. Additionally, the SSL/TLS assessment revealed that while TLS **1.2** is in use, there is no support for the more secure TLS **1.3**, which is recommended for enhanced security. The analysis also confirmed that no services are vulnerable to brute force attacks, and there are no shared hosting risks. It is crucial to address the medium-risk port issue promptly and consider upgrading to TLS **1.3** to mitigate potential vulnerabilities.

1.3 Key Security Issues

Title	Risk
Nmap Port Scan Results Analysis	Medium
SSL/TLS Protocols Security Assessment	Low
Login Form Detection Analysis	Low

1.3.1 Nmap Port Scan Results Analysis

Description:

The assessment identified an open port **80** running an HTTP service without encryption. This poses a medium risk as it could allow sensitive data to be intercepted if not properly redirected to HTTPS or if HSTS (HTTP Strict Transport Security) is not enabled.

Affected Assets:

- **IP Address:** 6[illegible].22.21.172 - **Ports:** 80/tcp (http), 443/tcp (ssl/https)

Recommendations:

Immediate action should be taken to ensure that all HTTP traffic is redirected to HTTPS. Implementing HSTS will further enhance security by ensuring that browsers only interact with the server over a secure connection. Regularly review and update security configurations to adhere to best practices.

1.3.2 SSL/TLS Protocols Security Assessment

Description:

The SSL/TLS assessment revealed that while TLS **1.2** is currently in use, there is no support for TLS **1.3**, which is considered the best practice for enhanced security and performance.

Affected Assets:

- **Endpoints using TLS 1.2: 1**

Recommendations:
It is recommended to upgrade to TLS **1.3** to leverage its improved security features and performance benefits. Regularly review cryptographic protocols and ensure that deprecated versions are disabled.

1.3.3 Login Form Detection Analysis

Description:
A login form was detected on the application, which requires security validation to ensure that authentication mechanisms are robust against potential threats.

Affected Assets:
- **URLs associated with the detected login form:** - `https://ofx1.secureinternetbank.com:443` - `http://66.22.21.172:443`

Recommendations:
Conduct thorough security testing on the login form to ensure it is protected against common vulnerabilities such as SQL injection, cross-site scripting (XSS), and brute force attacks. Implement multi-factor authentication (MFA) where feasible to enhance security.

1.4 General Recommendations

To enhance the overall security posture, it is recommended to implement a continuous monitoring strategy that includes regular vulnerability assessments and penetration testing. Keeping software and systems updated with the latest security patches is crucial. Additionally, adopting a defense-in-depth approach will provide multiple layers of security controls, reducing the risk of successful attacks.