Jay's Bank
Security Assessment Findings Report

Confidential

Date: June 1th, 2024

Table of Contents

Table of Contents 2
Confidentiality Statement 3
Disclaimer 3
Contact Information 3
Assessment Overview 4
Assessment Components 4
  Internal Penetration Test 4
Finding Severity Ratings 5
Risk Factors 5
  Likelihood 5
  Impact 5
Scope 6
  Scope Exclusions 6
  Client Allowances 6
Executive Summary 7
  Scoping and Time Limitations 7
  Testing Summary 8
  Tester Notes and Recommendations 8
  Key Strengths and Weaknesses 8
Vulnerability Summary & Report Card 9
  Internal Penetration Test Findings 9
Technical Findings 10
  Internal Penetration Test Findings 10
    Finding IPT-001: CVE-2023-48795 at 10.15.42.7 10
    Finding IPT-002: CVE-2023-48795 at 10.15.42.36 11
    Finding IPT-002: User Enumeration at 10.15.42.7 11
  Additional Scans and Reports 12

Confidentiality Statement

This document is the exclusive property of Jay's Bank and Jay's Bank Security (SafeGuard Solutions). This document contains proprietary and confidential information. Duplication, redistribution, or use, in whole or in part, in any form, requires consent of both Jay's Bank and SafeGuard Solutions.

Jay's Bank may share this document with auditors under non-disclosure agreements to demonstrate penetration test requirement compliance.

Disclaimer

A penetration test is considered a snapshot in time. The findings and recommendations reflect the information gathered during the assessment and not any changes or modifications made outside of that period.

Time-limited engagements do not allow for a full evaluation of all security controls. SafeGuard Solutions prioritized the assessment to identify the weakest security controls an attacker would exploit. SafeGuard Solutions recommends conducting similar assessments on an annual basis by internal or third-party assessors to ensure the continued success of the controls.

Contact Information

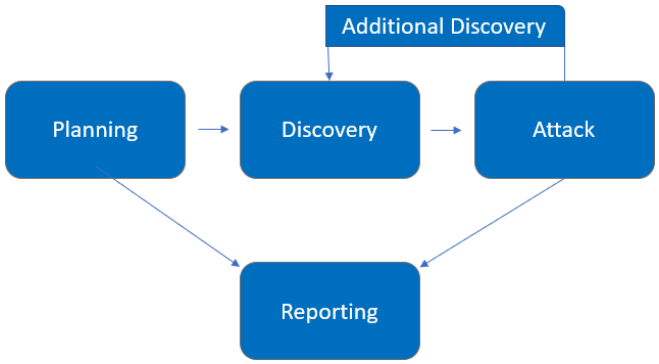
Name	Title	Contact Information
Jay's Bank		
Lab Ethical Hacking	Lab Ethical Hacking	Email: lab@ethicalhack.com
SafeGuard Solutions		
Awang Fraditya	Lead Penetration Tester	Email: ruusack26@gmail.com

Assessment Overview

From May 28th, 2024 to June 1st, 2024, Jay's Bank engaged SafeGuard Solutions to evaluate the security posture of its infrastructure compared to current industry best practices that included an internal network penetration test. All testing performed is based on the NIST *SP 800-115 Technical Guide to Information Security Testing and Assessment, OWASP Testing Guide (v4), and customized testing frameworks*.

Phases of penetration testing activities include the following:

- Planning – Customer goals are gathered and rules of engagement obtained.
- Discovery – Perform scanning and enumeration to identify potential vulnerabilities, weak areas, and exploits.
- Attack – Confirm potential vulnerabilities through exploitation and perform additional discovery upon new access.
- Reporting – Document all found vulnerabilities and exploits, failed attempts, and company strengths and weaknesses.



Assessment Components

Internal Penetration Test

An internal penetration test emulates the role of an attacker from inside the network. An engineer will scan the network to identify potential host vulnerabilities and perform common and advanced internal network attacks, such as: XSS, SQL Injection and Authentication and Authorization Injection. The engineer will seek to gain access to hosts through lateral movement, compromise domain user and admin accounts,and exfiltrate sensitive data.

Finding Severity Ratings

The following table defines levels of severity and corresponding CVSS score range that are used throughout the document to assess vulnerability and risk impact.

Severity	CVSS V3 Score Range	Definition
Critical	9.0-10.0	Exploitation is straightforward and usually results in system-level compromise. It is advised to form a plan of action and patch immediately.
High	7.0-8.9	Exploitation is more difficult but could cause elevated privileges and potentially a loss of data or downtime. It is advised to form a plan of action and patch as soon as possible.
Moderate	4.0-6.9	Vulnerabilities exist but are not exploitable or require extra steps such as social engineering. It is advised to form a plan of action and patch after high-priority issues have been resolved.
Low	0.1-3.9	Vulnerabilities are non-exploitable but would reduce an organization's attack surface. It is advised to form a plan of action and patch during the next maintenance window.
Informational	N/A	No vulnerability exists. Additional information is provided regarding items noticed during testing, strong controls, and additional documentation.

Risk Factors

Risk is measured by two factors: Likelihood and Impact:

Likelihood

Likelihood measures the potential of a vulnerability being exploited. Ratings are given based on the difficulty of the attack, the available tools, attacker skill level, and client environment.

Impact

Impact measures the potential vulnerability's effect on operations, including confidentiality, integrity, and availability of client systems and/or data, reputational harm, and financial loss.

Scope

Assessment	Details
XSS Vulnerability Findings	167.172.75.216/register
HTTP Intercept	167.172.75.216

Scope Exclusions

Per client request, SafeGuard Solutions did not perform any of the following attacks during testing:

- Data Breach
- RCE and Privilege Escalation
- DOS/DDOS

All other attacks not specified above were permitted by Jay's Bank.

Client Allowances

Jay's Bank provided SafeGuard Solutions the following allowances:

- Internal access to network via web and external penetration software

Executive Summary

SafeGuard Solutions evaluated Jay's Bank's internal security posture through Vulnerability Finding from May 28th, 2024 to June 1st, 2024. The following sections provide a high-level overview of vulnerabilities discovered, successful and unsuccessful attempts, and strengths and weaknesses.

Scoping and Time Limitations

Scoping during the engagement did not permit denial of service or social engineering across all testing components.

Time limitations were in place for testing. Internal network penetration testing was permitted for 4 days.

Testing Summary

The application assessment evaluated Jay's Bank internal application security posture. From an internal perspective, the SafeGuard Solutions team performed XSS Scripting, HTTP intercept and SQL Injection. SafeGuard Solutions team discovered XSS Scripting can be used to exploit the web through the `/register` endpoint. Furthermore, HTTP Intercept can be used to change other users password.

Tester Notes and Recommendations

Testing results of the Jay's Bank network are in a critical state here. Basic XSS Scripting can be performed which will lead to worst security issues. Furthermore, HTTP Intercept can be used to change other user password if we know the username.

Key Strengths and Weaknesses

The following identifies the key strengths identified during the assessment:

1. Dynamic Values in Web

Each device The following identifies the key weaknesses identified during the

assessment:

1. Vulnerable to XSS Scripting
2. Vulnerable to HTTP Intercept

Vulnerability Summary & Report Card

The following tables illustrate the vulnerabilities found by impact and recommended remediations:

Internal Penetration Test Findings

1	1	0	0	0
Critical	High	Moderate	Low	Informational

Finding	Severity	Recommendation
Internal Penetration Test		
IPT-001: XSS Scripting	Critical	Use Input Validation, use HTTP-only and server cookies, and Content Security Policy
IPT-002: MITM Through BurpSuite HTTP Intercept	High	Use HTTPS, ensure proper certificate validation, and secure DNS

Technical Findings

Internal Penetration Test Findings

Finding IPT-001: XSS Scripting

Description:	Jay's Bank allows user to register with javascript script and execute the script it while logging in
Risk:	Credential theft, unauthorized actions, malware spreading, defacement and reputation damage
System:	All
Tools Used:	Arc Browser

Evidence

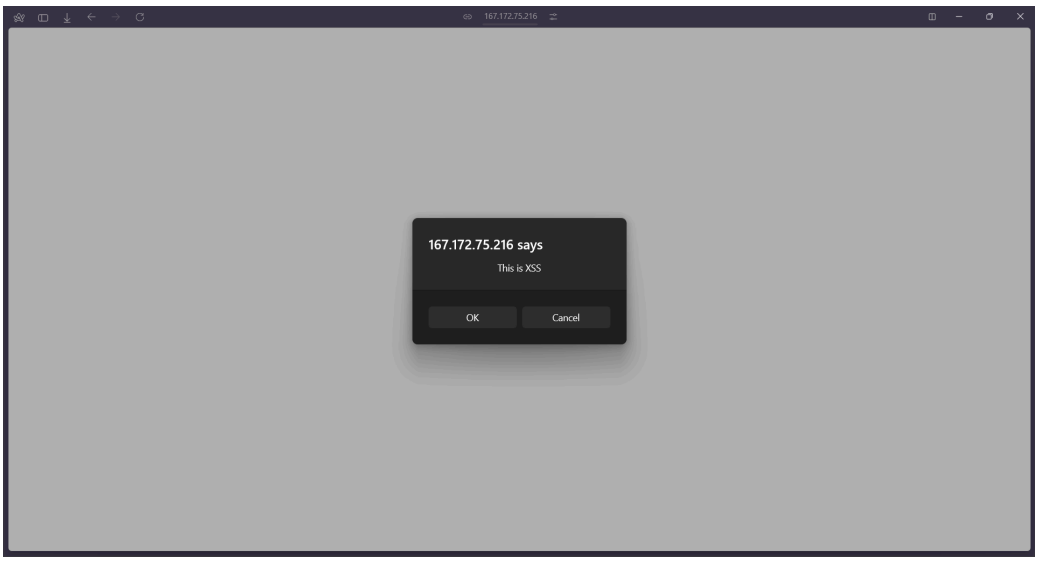


Figure 1: Captured XSS Scripting at 167.172.75.216

Remediation

Update the web with input validation in every endpoint that has input form with input validation, in example not allowing an entry with `<script>` in the entry. Use Secure Cookies and HTTP-only.

Finding IPT-002: MITM Through BurpSuite HTTP Intercept

Description:	Jay's Bank allows user to intercept other user data in BurpSuite HTTP intercept while updating in /dashboard endpoint
Risk:	The vulnerability allows remote attackers to bypass integrity checks and change other users password and steal credentials, which can lead into data manipulation and impersonation.
System:	All
Tools Used:	BurpSuite

Evidence

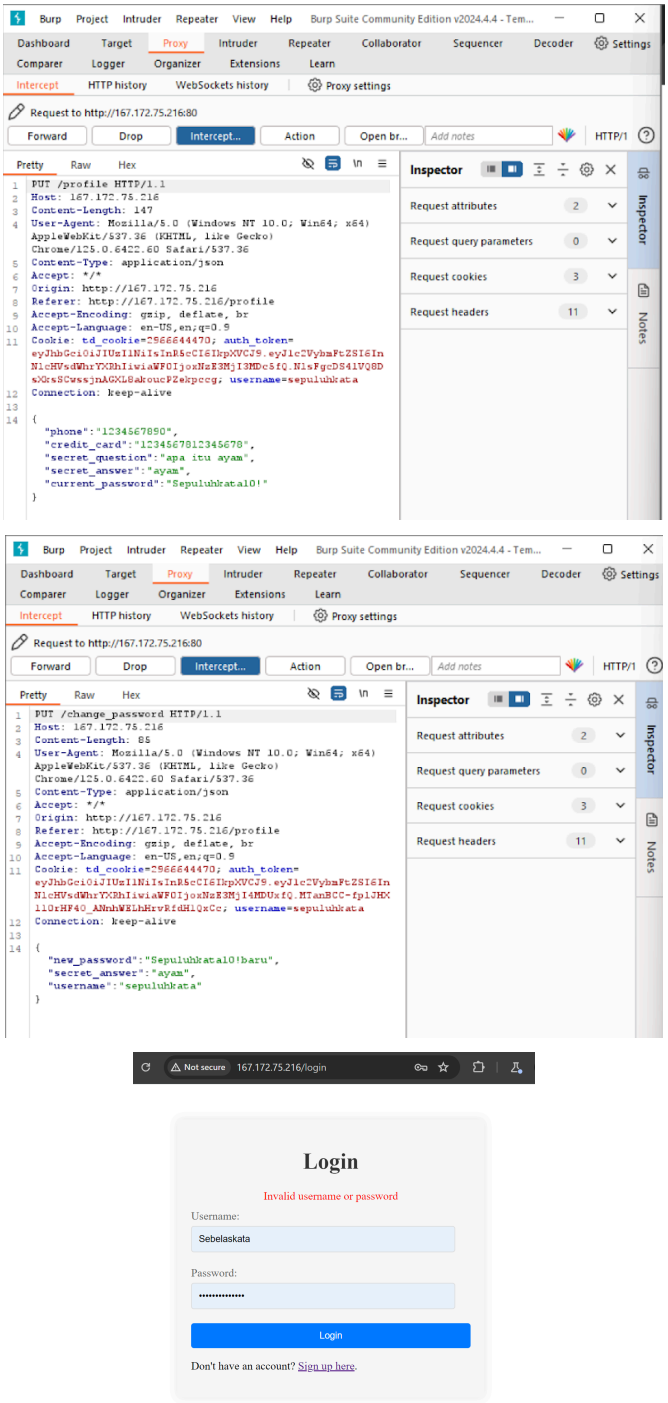


Figure 2: Captured MITM

Remediation

Update the web by using HTTPS like SSL/TLS. Use Multi-Factor Authentication,

Certificate Validation, and Session security like Cookies.

Last Page