JAY'S BANK
Security Assessment Findings Report

Business Confidential

Date: June 1st, 2024
Project: Praktikum 3
Version 1.0

Table of Contents

Confidentiality Statement

This document is the exclusive property of Jay's Bank and 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

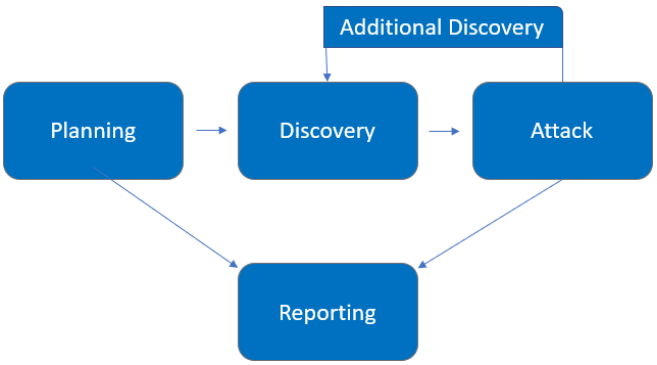
Name	Title	Contact Information
Jay's Bank		
John Smith	Global Information Security Manager	Email: jsmith@jaysbank.com
Safeguard Solutions		
Ilhan Ahmad Syafa	Penetration Tester	Email: ilhan@sgsolutions.com

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: LLMNR/NBT-NS poisoning and other man- in-the-middle attacks, token impersonation, kerberoasting, pass-the-hash, golden ticket, and more. 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
Internal Penetration Test	167.172.75.216 including all application functions, user account and authentication mechanisms, web interface and API and database interaction and data handling processes

Scope Exclusions

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

- Denial of Service (DoS) and DDoS
- Exploit vulnerabilities that can grant access to the server (e.g. RCE, privilege escalation)
- Damage data or application infrastructure

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

Client Allowances

Jay's Bank provided SafeGuard Solutions the following allowances:

- Search for and identify vulnerabilities in the Jay's Bank application
- Focus on application vulnerabilities such as SQL injection, XSS, and authentication/authorization issues
- Exploit access to other user accounts, but only within the application (not to the server)

Executive Summary

SafeGuard Solutions evaluated Jay's Bank internal security posture through penetration testing 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 DoS/DDoS, privilege excalations and damage infrastructure across all testing components.

Time limitations were in place for testing. Internal network penetration testing was permitted for four (4) business days.

Testing Summary

SafeGuard Solutions conducted a penetration test on Jay's Bank, a mockup banking application under development. The objective was to identify and address vulnerabilities before the application's public release. The test encompassed all functionalities of the application, user account mechanisms, authentication processes, web interfaces, API endpoints, database interactions, and data handling processes. The primary focus was on identifying application-level vulnerabilities, such as SQL injection, Cross-Site Scripting (XSS), and authentication/authorization issues, without extending to server-level exploitation.

During the assessment, a significant horizontal privilege escalation vulnerability was discovered in the user authentication mechanism. This vulnerability allowed user credentials, including usernames, passwords, and authentication tokens, to be exposed and intercepted using BurpSuite upon login. This flaw posed a high risk as it enabled unauthorized users to access other user accounts, leading to potential misuse and exposure of sensitive information. For instance, by intercepting a login request, the captured details included usernames, passwords, and authentication tokens, which unauthorized users could use to log in as other users.

To address this critical issue, several recommendations were made. Firstly, it is crucial to implement secure transmission protocols, ensuring that sensitive information is transmitted over HTTPS to prevent interception. Additionally, adopting token-based authentication mechanisms like OAuth2, with securely generated and stored tokens, limited lifetimes, and scopes, would enhance security. Improving session management by incorporating mechanisms such as session expiration, session token regeneration upon login, and monitoring unusual session activity was also advised. Regular security audits and penetration tests were recommended to promptly identify and remediate vulnerabilities.

In conclusion, the penetration test uncovered a critical vulnerability within Jay's Bank application, necessitating immediate attention to safeguard user data and privacy. Implementing the recommended security measures will significantly enhance the application's security posture, ensuring it is prepared for a secure public deployment. A detailed technical report with step-by-step

exploitation paths and additional findings is provided for further review and action to mitigate identified security risks.

Tester Notes and Recommendations

The penetration testing results for Jay's Bank indicate an application in its early development stages, undergoing one of its initial security assessments. Several vulnerabilities were identified, with a significant issue related to horizontal privilege escalation in the user authentication mechanism.

The primary finding was the exposure of user credentials during the login process. This vulnerability allowed usernames, passwords, and authentication tokens to be intercepted using BurpSuite. The intercepted credentials could potentially be used by unauthorized users to access other user accounts, leading to a breach of sensitive information and misuse of user accounts.

A major contributing factor to this vulnerability is the lack of secure transmission protocols. Without HTTPS, sensitive information is transmitted in plaintext, making it easily interceptable. Additionally, the current session management practices are insufficient, failing to secure sessions adequately against unauthorized access.

We recommend the following actions to mitigate the identified vulnerabilities:

- Implement Secure Transmission: Ensure all sensitive information, including usernames, passwords, and authentication tokens, is transmitted over HTTPS. This will encrypt the data, preventing interception during transmission.

- Adopt Token-Based Authentication: Implement a robust token-based authentication mechanism, such as OAuth2. Tokens should be securely generated and stored, with limited lifetimes and scopes to minimize potential misuse.

- Enhance Session Management: Improve session management practices by incorporating session expiration, session token regeneration upon login, and monitoring for unusual session activities. These measures will help secure sessions against unauthorized access.

- Regular Security Audits: Conduct regular security audits and penetration tests to continuously identify and address vulnerabilities. This proactive approach will help maintain a secure application environment.

The findings from this assessment highlight the critical need for robust security measures, especially in the early stages of application development. By implementing the recommended actions, Jay's Bank can significantly enhance its security posture, ensuring a safer environment for its users and preparing for a secure public release

Key Strengths and Weaknesses

The following identifies the key strengths identified during the assessment:

1. Comprehensive Functionality Testing
2. User Role Segregation
3. Good sanitization of SQL injection filtering as the command will be encoded so that it is not executed

The following identifies the key weakness identified during the assessment:

1. Insufficient Secure Transmission
2. Horizontal Privilege Escalation Vulnerability
3. Weak Session Management
4. Lack of Token-Based Authentication
5. Regular Security Audits Missing

Vulnerability Summary & Report Card

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

Internal Penetration Test Findings

0	1	0	0	0
Critical	High	Moderate	Low	Informational

Finding	Severity	Recommendation
Horizontal Privilege Escalation Vulnerability	High	Implementing Multi-Factor Authentication (MFA), enforcing the Principle of Least Privilege, regularly monitoring account activities, and conducting security training for users.

Technical Findings

Internal Penetration Test Findings

Finding Horizontal Privilege Escalation Vulnerability

Description:	On the login page, when a user submits the login button and we intercept it with Burpsuite, then we get the login details of a user such as username, password, cookie and auth token. this vulnerability has the potential to cause Horizontal Privilege Escalation where other users can log in based on these login details.
Risk:	Likelihood: High This vulnerability is highly likely to be exploited, especially since it involves intercepting plaintext user credentials during the login process. Given that sensitive information such as usernames, passwords, and authentication tokens are easily accessible without the need for sophisticated tools, the attack can be executed by anyone with basic knowledge of interception tools like BurpSuite. Impact: Very High The impact of this vulnerability is very high, as it allows unauthorized users to gain access to other user accounts. This can lead to severe consequences, including exposure of sensitive user data, unauthorized financial transactions, and complete compromise of user privacy and security. The potential for misuse of user accounts could damage the trust of users and the reputation of the bank, and may result in significant financial and legal repercussions.
System:	Login Page
Tools Used:	Burpsuite
References:	OWASP - Testing for Horizontal Privilege Escalation NIST SP800-53 r4 AC-6 - Least Privilege SANS Institute - Web Application Security: Authentication and Session Management CWE-284: Improper Access Control ISO/IEC 27002:2013 - Information Technology Security Techniques

Evidence

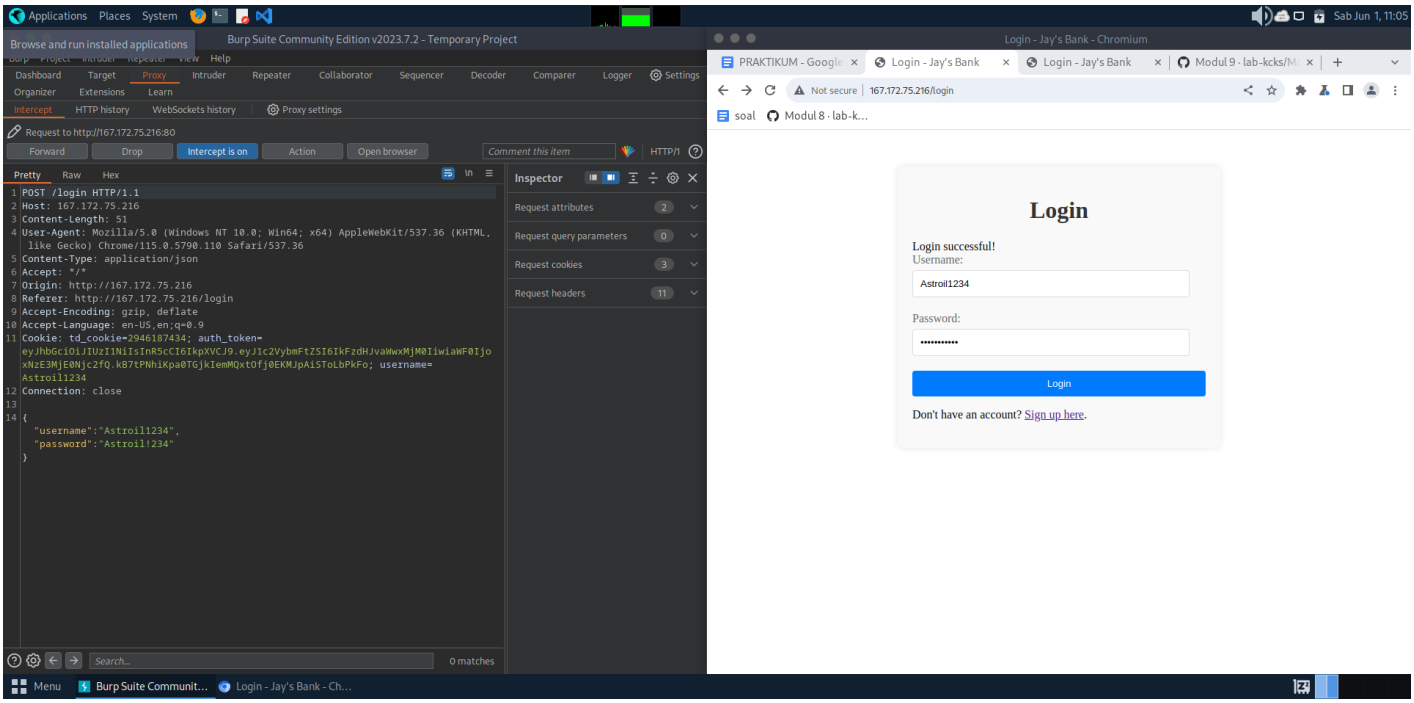
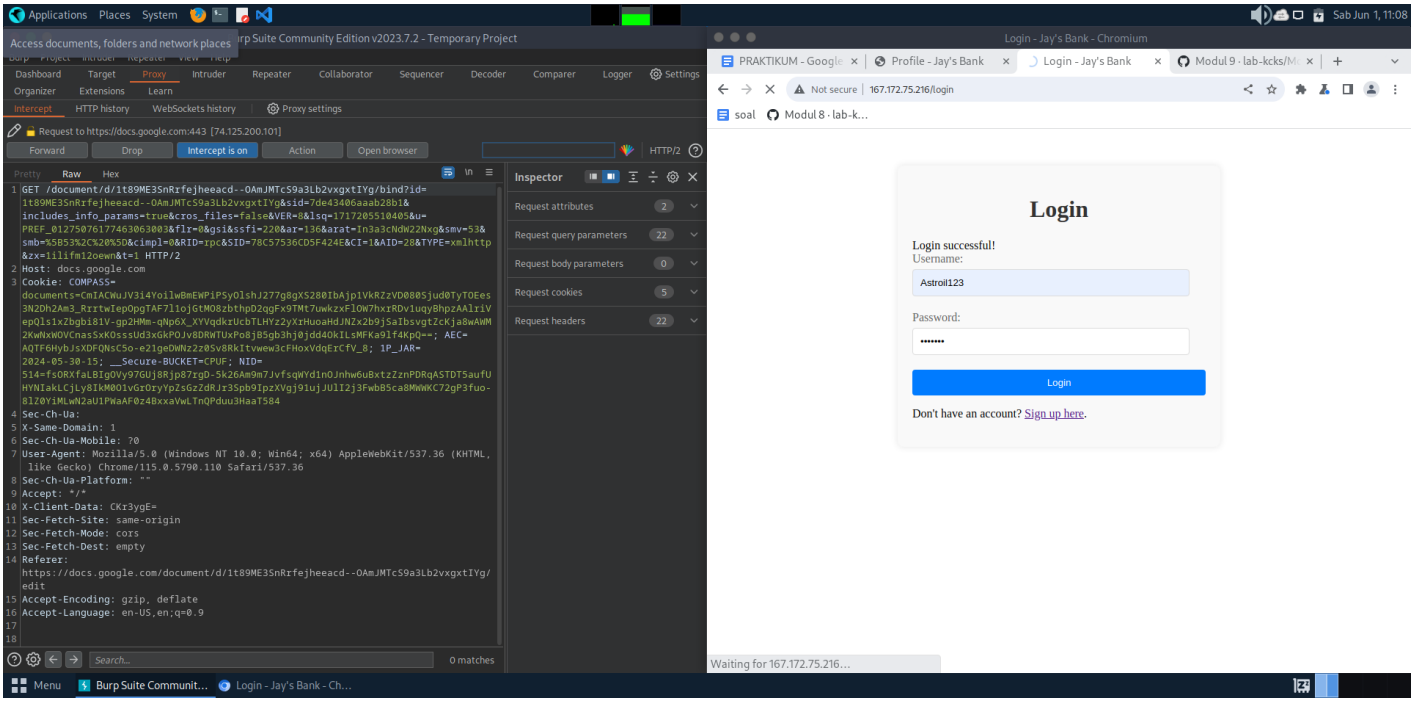


Figure 1: Captured cookie, auth token, username and password from user



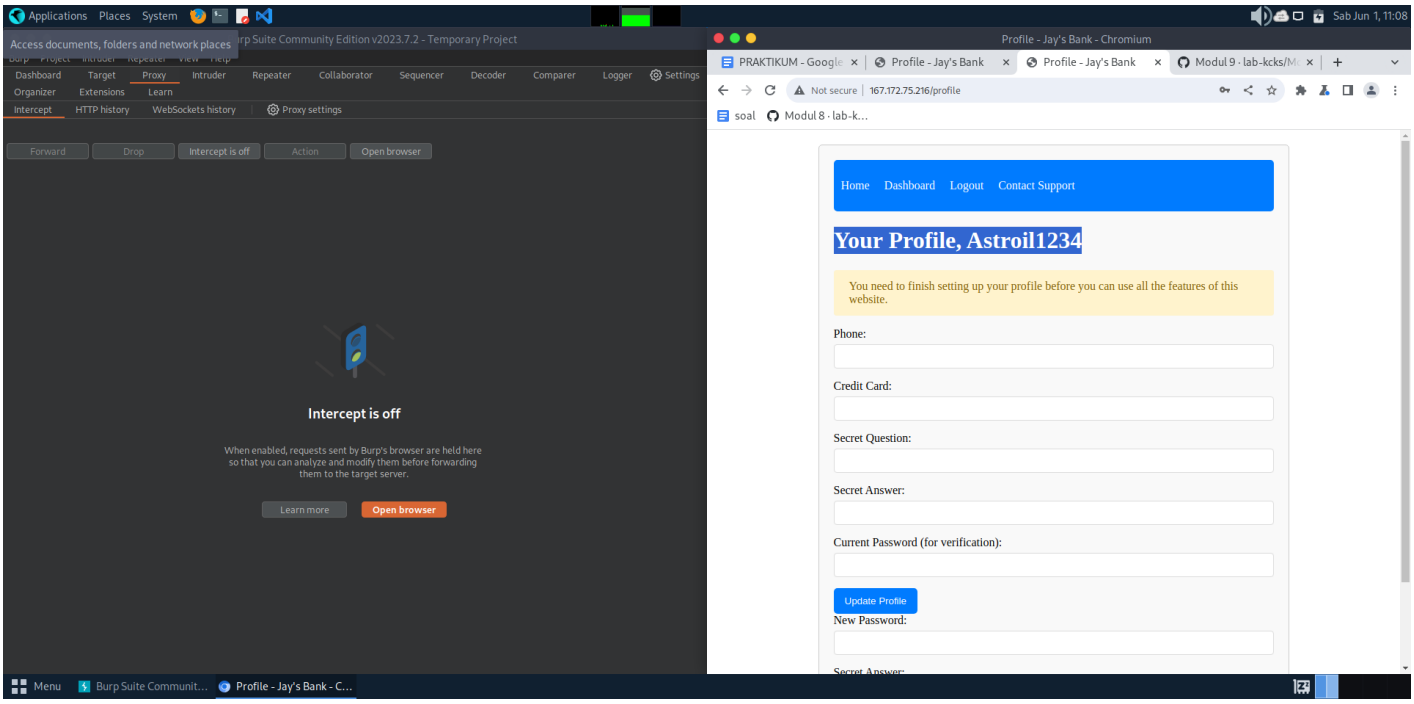


Figure 2: Successful login to another user

Remediation

To remediate the horizontal privilege escalation vulnerability identified in Jay's Bank application, several critical steps must be taken. Firstly, ensure all sensitive information, such as usernames, passwords, and authentication tokens, is transmitted over HTTPS to encrypt the data and prevent interception. Implement a robust token-based authentication mechanism like OAuth2, which involves securely generating and storing tokens with limited lifetimes and scopes to minimize the risk of misuse. Additionally, enhance session management practices by incorporating mechanisms such as session expiration and session token regeneration upon login, and continuously monitor for unusual session activities. Regular security audits and penetration tests should be conducted to identify and address vulnerabilities proactively. By implementing these measures, Jay's Bank can significantly improve its security posture, protecting user data and ensuring a secure application environment before its public release.

Last Page