Jay's Bank Application

Security Assessment Findings Report

Business Confidential

Date: June 1st, 2024

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		
Jay's Bank	Global Information Security Manager	Email: jb@jaybank.com
SafeGuard Solutions		
Angella Christie	Lead Penetration Tester	Email: heath@cybersh.com

Assessment Overview

From May 28^{th}, 2024 to June 1^{st}, 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.

Phases of penetration testing activities include the following:

- Planning – Customer goals are gathered and rules of engagement obtained.
- Reconnaissance – To gather enough information to understand the network topology and services running on the target, so as to help in planning an effective penetration attack.
- Vulnerability Assessment – 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. 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

Scope Exclusions

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

- All application functions.
- User account mechanisms and authentication.
- Web interfaces and APIs.
- Database interactions and data handling processes.

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

Client Allowances

Jay's Bank provided SafeGuard Solutions the following allowances:

- Authorization is granted to search for and identify vulnerabilities within Jay’s Bank application.
- Emphasis should be placed on vulnerabilities such as SQL injection, XSS, and authentication/authorization issues within the application.
- If feasible, discovered vulnerabilities may be exploited to access other user accounts, albeit restricted solely to the application (not the server).

Executive Summary

SafeGuard Solutions evaluated Jay's Bank's 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 denial of service or social engineering across all testing components.

Time limitations were in place for testing. Internal network penetration testing was permitted for five (5) days.

Testing Summary

For the first vulnerability, Broken Authentication and Access Control, it's categorized as high severity, indicating it poses a significant risk to the system's security. This vulnerability typically involves weaknesses in the authentication mechanisms or access controls, potentially allowing unauthorized users to gain access to sensitive information or perform actions they shouldn't be able to.
The second vulnerability, Cross-Site Scripting (XSS), is another critical issue. XSS vulnerabilities allow attackers to inject malicious scripts into web pages viewed by other users. This can lead to various malicious activities, such as stealing session cookies or performing actions on behalf of the user.
Both vulnerabilities should be addressed promptly to mitigate the risk they pose to the security and integrity of the system. Measures such as patching, code review, and implementing proper security controls can help address these issues effectively.

Tester Notes and Recommendations

The application at IP 167.172.75.216 has significant security vulnerabilities, including broken authentication and access control, allowing unauthorized access to user accounts using just usernames, and weak session management practices with easily exploitable static tokens. Additionally, potential Cross-Site Scripting (XSS) vulnerabilities due to insufficient input validation and sanitization were identified. The application lacks robust mechanisms for handling user authentication and session management securely, and there is an absence of modern security practices such as Multi-Factor Authentication (MFA) and Content Security Policy (CSP). To enhance security, it is recommended to implement MFA, enforce strong password policies, use secure session tokens with attributes like `HttpOnly`, `Secure`, and `SameSite`, validate and sanitize all user inputs, implement CSP, use Role-Based Access Control (RBAC) to ensure authorized access only, and conduct regular security audits and penetration

testing to identify and rectify vulnerabilities. By addressing these recommendations, the application can significantly enhance its security posture, protecting user data and ensuring system integrity.

Key Strengths and Weaknesses

The following identifies the key strengths identified during the assessment:

1. Functional User Authentication System: The application has a user authentication mechanism in place, allowing user registrations and logins, which is fundamental for controlling access to resources.
2. Standard Web Protocols and Headers: The use of standard web protocols and headers, including Content-Type, Accept-Encoding, and User-Agent, indicates a compliance with basic web standards and practices.

The following identifies the key weaknesses identified during the assessment:

1. Broken Authentication and Access Control: The application allows access to user accounts using only usernames, bypassing authentication. This critical vulnerability exposes sensitive information and compromises data privacy, leading to potential data breaches and identity theft.
2. Session Management Issues: Weak session management is evident from the use of static session tokens, which can be easily exploited. This allows unauthorized access to user profiles without proper validation.
3. Cross-Site Scripting (XSS) Vulnerability: The application may be susceptible to XSS attacks, which can lead to the injection of malicious scripts. These scripts can steal sensitive information, hijack user sessions, and perform unauthorized actions.
4. Lack of Secure Token Handling: Tokens are not securely generated, stored, or validated, increasing the risk of token reuse and unauthorized access.
5. Insufficient Input Validation: There is inadequate validation and sanitization of user inputs, making the application vulnerable to various injection attacks.

Vulnerability Summary & Report Card

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

Internal Penetration Test Findings

0	2	6	0	1
Critical	High	Moderate	Low	Informational

Finding	Severity	Recommendation
Internal Penetration Test		
IPT-001:Broken Authentication and Access Control Vulnerability (High)	High	Implement Multi-Factor Authentication (MFA) and enforce strong password policies to enhance authentication security. Additionally, use secure, randomly generated session tokens with proper expiration and renewal mechanisms, along with Role-Based Access Control (RBAC) to ensure only authorized access to resources.
IPT-002: Cross-Site Scripting (XSS) Vulnerability	High	Implement input validation and output encoding to ensure all user inputs are properly sanitized and encoded before being rendered on the web pages.

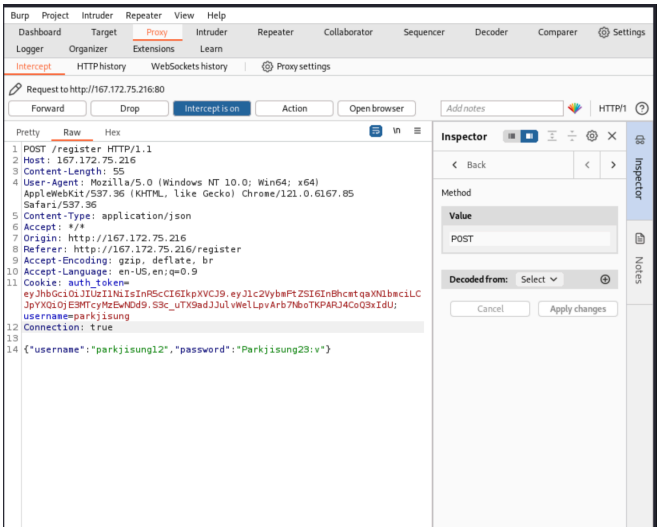
Technical Findings

Internal Penetration Test Findings

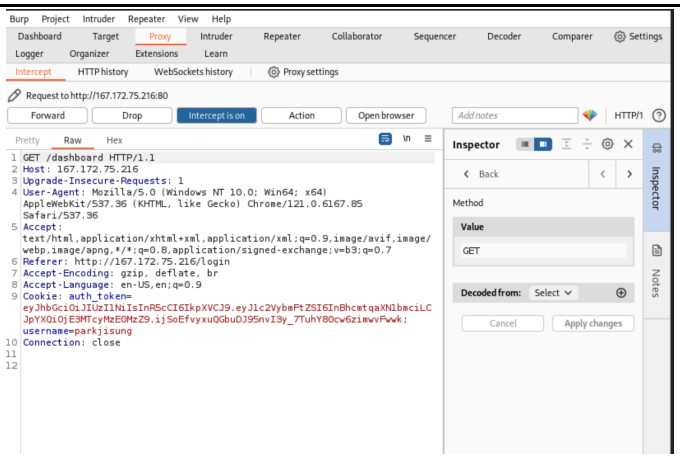
Finding IPT-001: Broken Authentication and Access Control Vulnerability (High)

Description:	The application suffers from a critical vulnerability in its authentication and access control mechanisms, allowing unauthorized access to user accounts simply by knowing the usernames. This security flaw bypasses the authentication process and exposes sensitive user information, compromising data privacy and security.
Risk:	Likelihood: High - Given the simplicity of the exploit, it is highly likely that attackers will exploit this vulnerability to gain unauthorized access. Impact: Very High - Successful exploitation can lead to severe consequences including unauthorized access to user accounts, data breaches, identity theft, and other malicious activities. The resultant damage could be extensive, affecting both financial standing and reputational integrity.
System:	All
Tools Used:	Burp Suite

Evidence



pict 1: change username with 2nd user and connection to true



pict 2: Successful login

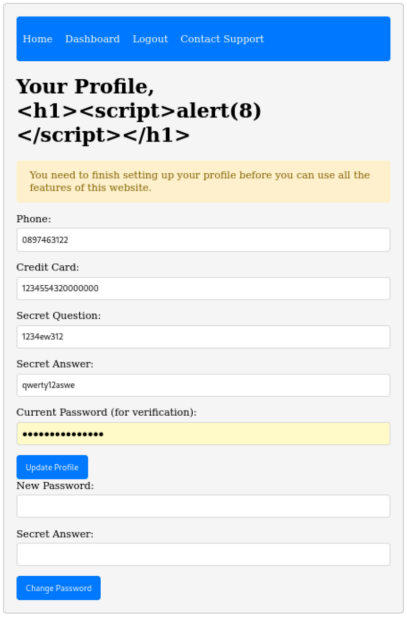
Remediation

- Enforce multi-factor authentication (MFA) to add an additional layer of security.
- Use more secure methods for session management, such as rotating session tokens.
- Ensure that tokens are securely generated, stored, and validated.
- Implement token expiration and revocation mechanisms to reduce the risk of token reuse.
- Conduct regular security audits and penetration testing to identify and rectify potential vulnerabilities.
- Implement automated security scanning tools to continuously monitor the application for vulnerabilities.
- Validate and sanitize all user inputs to prevent injection attacks and ensure that only valid data is processed.
- Implement comprehensive error handling to avoid exposing system internals through error messages.
- Use secure logging practices to monitor authentication attempts and detect anomalies in real-time.

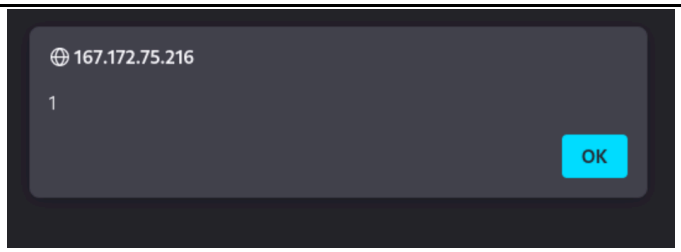
Finding IPT-002: Cross-Site Scripting (XSS) Vulnerability (High)

Description:	Cross-Site Scripting (XSS) is a security vulnerability that allows attackers to inject malicious scripts into web pages viewed by other users. These scripts can steal cookies, session tokens, or other sensitive information, and can even be used to impersonate users or manipulate the content of the site.
Risk:	Likelihood: High - XSS vulnerabilities are common and relatively easy to exploit, especially in web applications that handle user input without proper validation and sanitization. Impact: High - Successful exploitation can lead to data theft, session hijacking, and unauthorized actions performed on behalf of the users. This can result in significant data breaches, loss of user trust, and legal consequences.
System:	All
Tools Used:	Manual testing, web browser, script injection

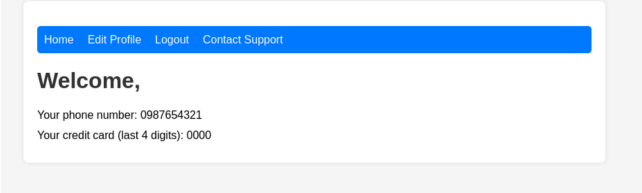
Evidence



pict 3: register and login with script



pict 4: Login again and a popup appears



pict 5: dashboard display after scripting

Remediation

- Input Validation and Sanitization: Ensure all user inputs are properly validated and sanitized. Use built-in functions or libraries that handle encoding and escaping of user inputs to prevent the injection of malicious scripts.
- Content Security Policy (CSP): Implement a robust CSP to restrict the sources from which scripts can be loaded and executed. This helps mitigate the impact of XSS by preventing the execution of unauthorized scripts.

Last Page