Jay's Bank
Security Assessment Findings Report

Business Confidential

Date: June 1st, 2024
Project: Modul8-10
Version 1.0

Confidentiality Statement

This document is the exclusive property of SafeGuard Solutions and Jay's Bank. 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 Modul 8-10 Ethical Hacking.

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

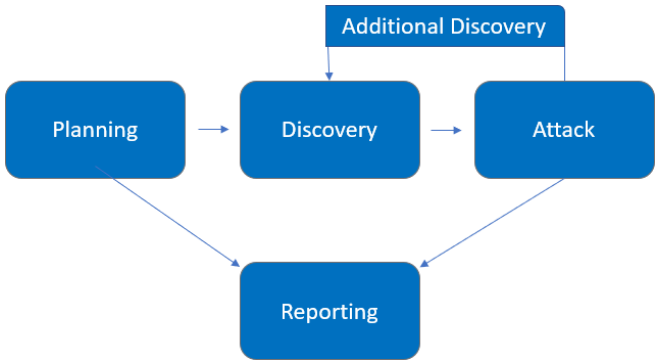
Name	Title	Contact Information
Jay's Bank		
Admin	Jay's Bank Website Admin	Email: admin@bankjay.com
SafeGuard Solutions		
Muhammad Afif	Penetration Practicum Tester	Email: afifsdi@gmail.com

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 external network penetration test. All testing performed is based on the 8th to 10th module of Ethical Hacking Practicum by KCKS Lab.

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

External Penetration Test

An external penetration test emulates the role of an attacker from outside the network. An outsider will scan the network to identify potential host vulnerabilities and perform common and advanced blackbox network attacks, such as: man-in-the-middle attacks, password brute force, and more. The outsider 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
External Penetration Test	• http://167.172.75.216

Scope Exclusions

Per client request, SafeGuard Solutions only performing perform the following attacks during testing:

- SQL injection
- XSS
- Authetication / Authorization Issues

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

Client Allowances

Jay's Bank provided SafeGuard Solutions the following allowances:

- Default access to the scope IP

Executive Summary

SafeGuard Solutions evaluated Jay's Bank's 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. External network penetration testing was permitted for four (4) business days.

Testing Summary

The network assessment evaluated Jay's Bank's external network security posture. From an outsider perspective, the SafeGuard Solutions team performed vulnerability scanning throughout the website and performing basic XSS attack.

The SAFEGUARD SOLUTIONS team discovered that the register page are allowing user to input a JS Script within the username and thus, allowing them to execute the script in the dashboard page. This kind of vulnerability can hold risk at user since their password and cookies can be gathered by unauthorized people.

Unfortunately, the SAFEGUARD SOLUTIONS team was not able to receiving admin access in both provided Ips. More information and time are needed to get more valuable information. The remainder of the findings were high, moderate, low, or informational. For further information on findings, please review the Technical Findings section.

Tester Notes and Recommendations

During testing, the register page are allowing user to input a JS Script within the username and thus, allowing them to execute the script in the dashboard page. This kind of vulnerability can hold risk at user since their password and cookies can be gathered by unauthorized people.

We recommended that Jay's Bank patch the current website by doing some sanitation for any of user input within the registration form and might be in all other form.

Key Strengths and Weaknesses

The following identifies the key strengths identified during the assessment:

1. Observed some scanning of common enumeration tools (Nuclei)
2. Performing a basic XSS attack throughout the website

The following identifies the key weaknesses identified during the assessment:

1. Register page allow user to put some JS script

Vulnerability Summary & Report Card

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

Internal Penetration Test Findings

13	5	6	0	1
Critical	High	Moderate	Low	Informational

Finding	Severity	Recommendation
External Penetration Test		
PT-001: XSS Vulnerability	Moderate	Do some sanitation and filtering for each user input

Technical Findings

External Penetration Test Findings

Finding PT-001: XSS Vulnerability (Moderate)

Description:	User are allowed to put some JS script in register page form
Risk:	Moderate – It allow user to hijack and listen other people input so other user data like password and cookies can be read by other user
System:	http://167.172.75.216/register
Tools Used:	-
References:	https://portswigger.net/web-security/cross-site-scripting/reflected#how-to-find-and-test-for-reflected-xss-vulnerabilities

Evidence

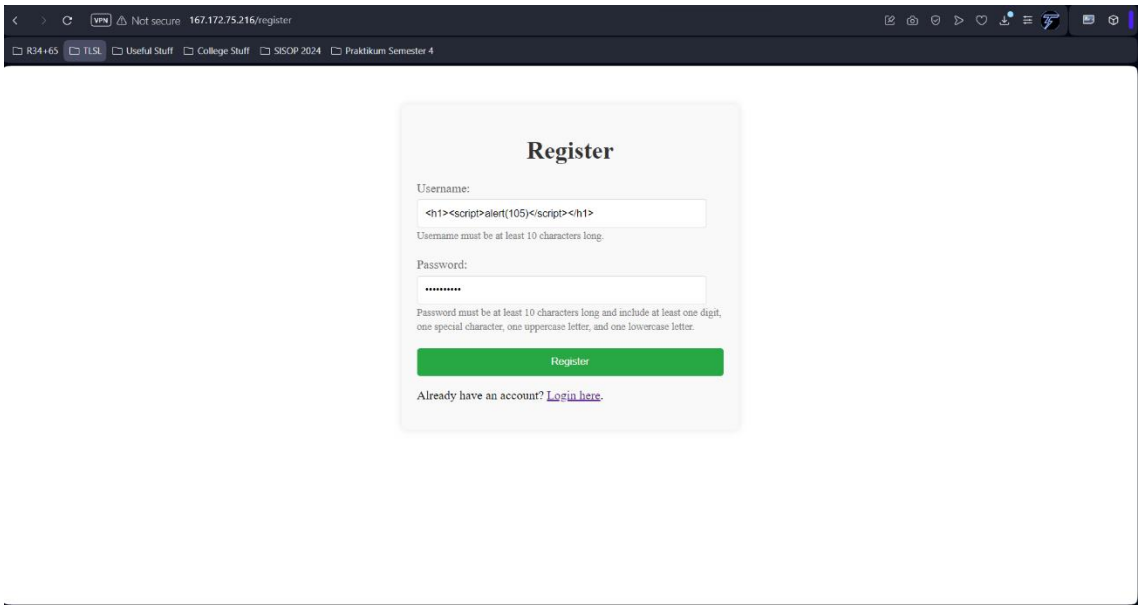


Figure 1: User putting the JS script

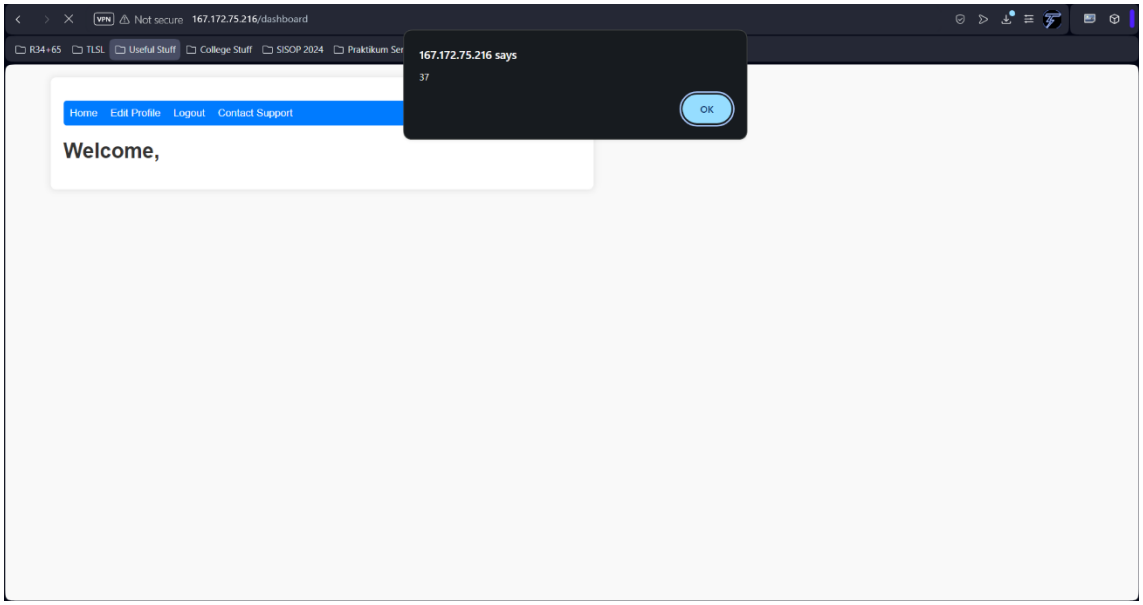


Figure 2: Script can be executed by accessing the dashboard page

Remediation

patch the current website by doing some sanitation and filtering for any of user input within the registration form and might be in all other form.