Jay's Bank

Jay's Bank
Security Assessment Findings Report

Business Confidential

Date: June 1th, 2024
Project: 897-19
Version 1.0

Table of Contents

Confidentiality Statement

This document is the exclusive property of FortifyTech (FT) and CyberShield (CS). This document contains proprietary and confidential information. Duplication, redistribution, or use, in whole or in part, in any form, requires consent of both FT and CS.

CS 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. CS prioritized the assessment to identify the weakest security controls an attacker would exploit. CS recommends conducting similar assessments on an annual basis by internal or third-party assessors to ensure the continued success of the controls.

Contact Information

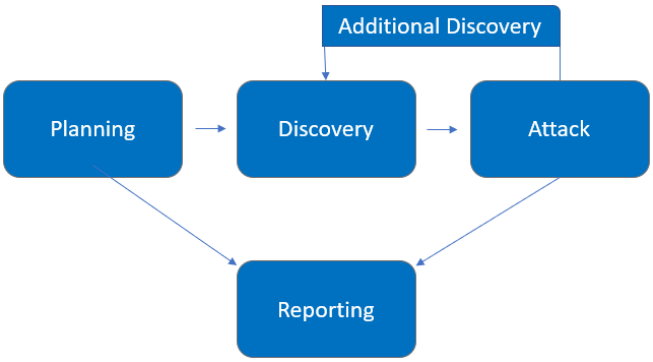
Name	Title	Contact Information
Jay's Bank		
Muhammad Azril	CEO	azril@gmail.com
CyberShield		
Gabriella Erlinda	Penetration Tester	gabriella8803@gmail.com

Assessment Overview

From May 28th, 2024 to June 1st, 2024, JB engaged CS to evaluate the security posture of its infrastructure compared to current industry best practices that included an external 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

External Penetration Test

An external penetration test emulates the role of an attacker attempting to gain access to an internal network without internal resources or inside knowledge. A CS engineer attempts to gather sensitive information through open-source intelligence (OSINT), including employee information, historical breached passwords, and more that can be leveraged against external systems to gain internal network access. The engineer also performs scanning and enumeration to identify potential vulnerabilities in hopes of exploitation.

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.
Medium	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.

Scope

Assessment	Details
External Penetration Test	167.172.75.216

- The only scope information provided by JB was that IP Address mentioned above

Scope Exclusions

Per client request, it is not permitted to conduct attacks that can damage the data or infrastructure of the application. Client does not permitted to exploit vulnerabilities that can provide access to the server (e.g., RCE, privilege escalation). Avoid DoS/DDoS attacks that can disrupt the availability of the application's services.

Client Allowances

Client did not provide any allowances to assist the penetration testing

Executive Summary

CS evaluated JB's external security posture through an external network penetration test from May 28th, 2024 to June 1st, 2024. By leveraging a series of attacks, CS did not really found critical level vulnerabilities that allowed full internal network access to the JB headquarter office. It is highly recommended that JB address these vulnerabilities as soon as possible as the vulnerabilities are easily found through basic reconnaissance and exploitable without much effort.

Attack Summary

The following table describes how CS gained internal network access, step by step:

Step	Action	Recommendation
1	Managed to run script through login page	Use Content Security Policy to restrict script execution. Validate user input to ensure that user only input the expected data
2	Managed to get user cookies	Set HttpOnly attribute to prevent the cookies from being accessed by intruders via JavaScript. Set Secure attribute to prevent cookies from being transmitted over non-HTTPS connections.

3	Managed to redirect login page to another website page	Sanitize user's input and encode it before sending back the response to user

Security Strengths

Encoded Login Information

During the assessment, the CS engineers managed to find that the login information was all encoded and cannot be decode easily

Secured Update Form

During the assessment, the CS engineers find that the update form page is secure and not prone to xss attack or sql injection

Security Weaknesses

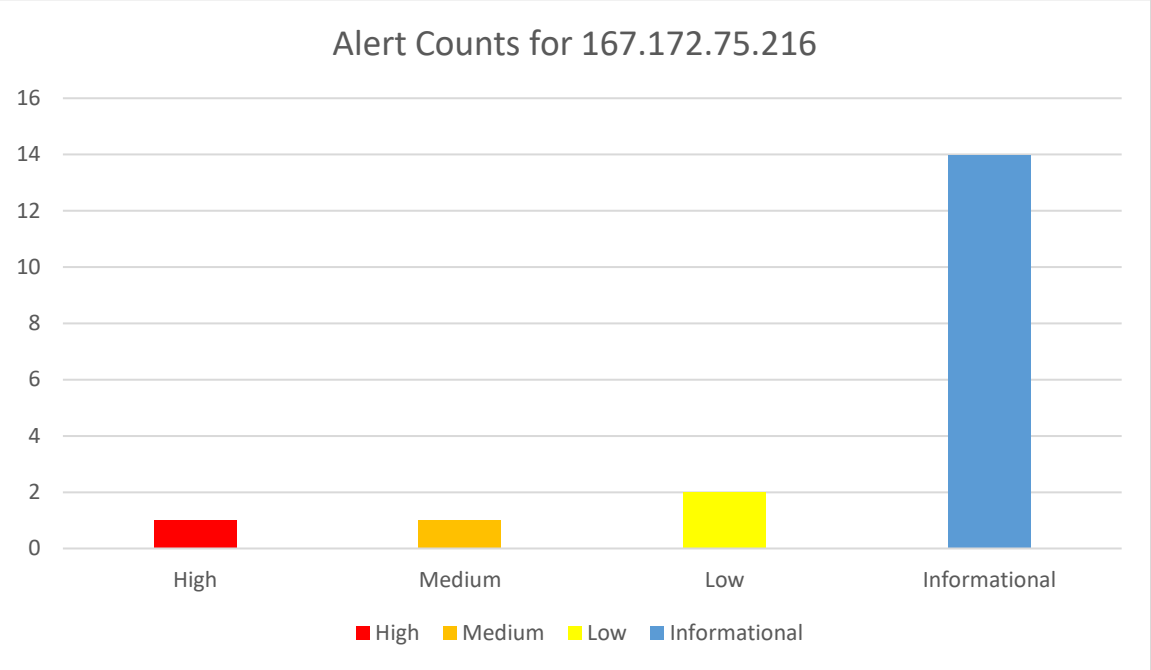
XSS Vulnerability

Pentester managed to do XSS attack, especially reflected xss. Register and Login page are able to be accessed by putting script as username. After updating the profile, pentester was able to re-login and perform xss attack.

Vulnerabilities by Impact

The following chart illustrates the vulnerabilities found by impact:

167.172.75.216



External Penetration Test Findings

Reflected XSS Vulnerability (High)

Description:	The product does not neutralize or incorrectly neutralizes user-controllable input before it is placed in output that is used as a web page that is served to other users. The server reads data directly from the HTTP request and reflects it back in the HTTP response. Reflected XSS exploits occur when an attacker causes a victim to supply dangerous content to a vulnerable web application, which is then reflected back to the victim and executed by the web browser.
Impact:	High
System:	167.172.75.216
References:	CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

Web Application Potentially Vulnerable to Clickjacking (Medium)

Description:	The web application does not restrict or incorrectly restricts frame objects or UI layers that belong to another application or domain, which can lead to user confusion about which interface the user is interacting with.
Impact:	Medium
System:	167.172.75.216
References:	CWE-693: Protection Mechanism Failure

Web Server Transmits Cleartext Credentials (Low)

Description:	The product transmits or stores authentication credentials, but it uses an insecure method that is susceptible to unauthorized interception and/or retrieval. Login pages do not use adequate measures to protect the user name and password while they are in transit from the client to the server.
Impact:	Low
System:	167.172.75.216
References:	CWE-522: Insufficiently Protected Credentials CWE-312: Cleartext Storage of Sensitive Information

Web Server Allows Password Auto-Completion (Low)

Description:	The remote web server contains at least one HTML form field that has an input of type 'password' where 'autocomplete' is not set to 'off'. While this does not represent a risk to this web server per se, it does mean that users who use the affected forms may have their credentials saved in their browsers, which could in turn lead to a loss of confidentiality if any of them use a shared host or if their machine is compromised at some point.
Impact:	Low
System:	167.172.75.216
References:	CWE-200

Proof of finding

Using reflected xss, I was able to:

1. Redirect the login page to another website
2. Display alert message containing cookie

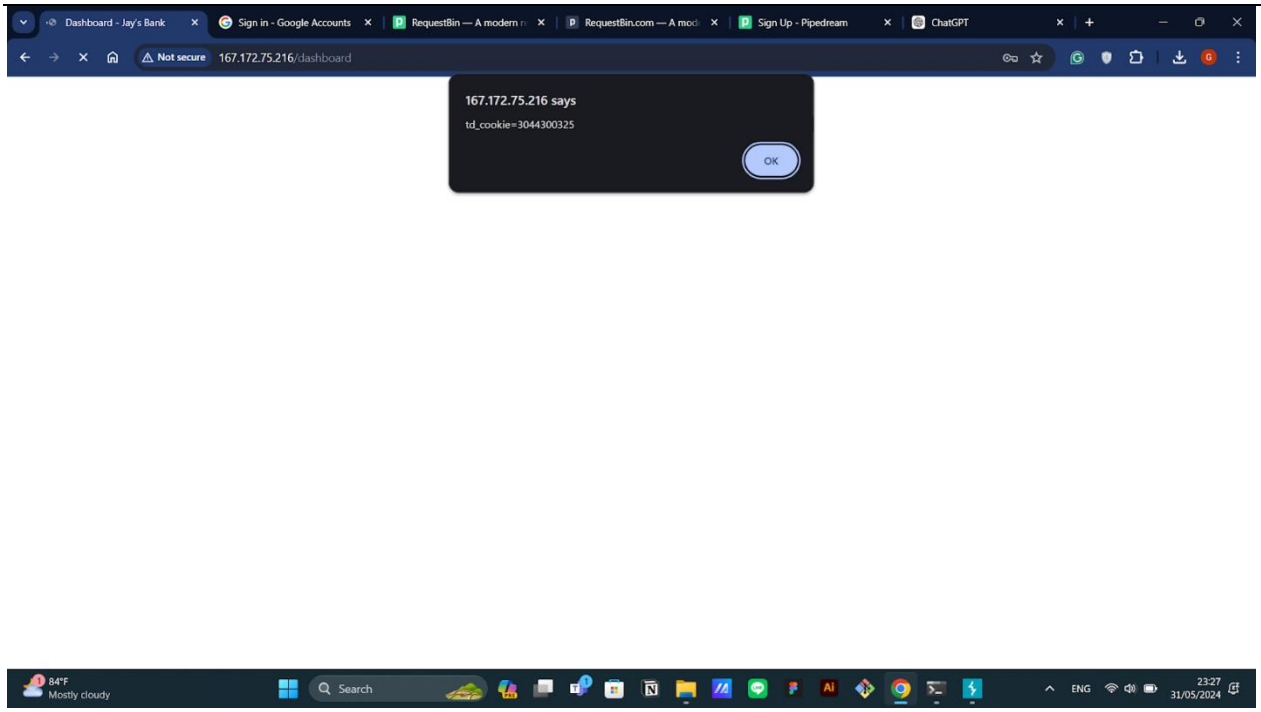


Figure 1. Cross-Site Scripting alert window

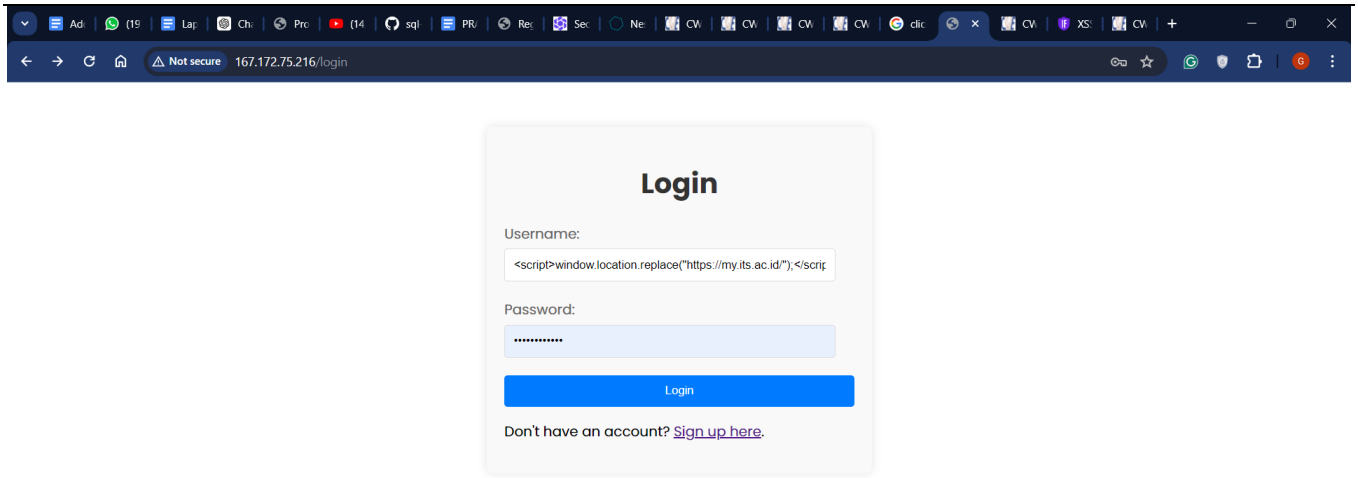


Figure 2. Cross-Site Scripting redirect login page

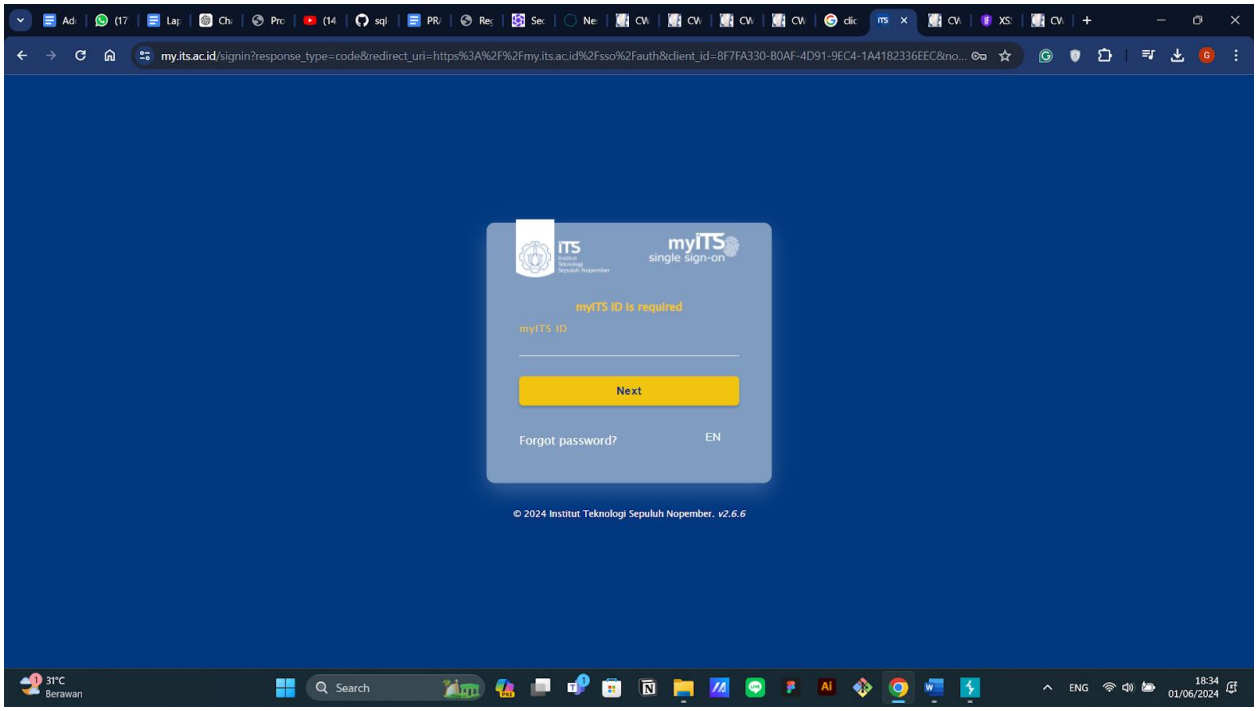
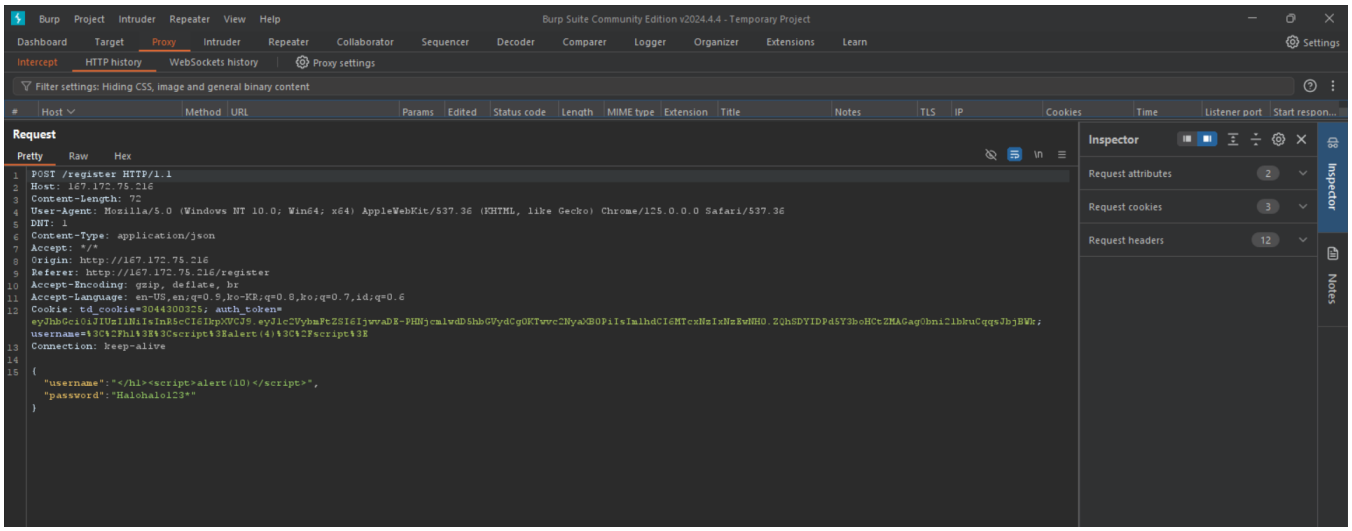


Figure 3. Redirected page

Gain Authentication Token through BurpSuite



Additional Reports and Scans (Informational)

For additionals report and finding, you can refer to my github repository on:

[Github Repository for Jay's Bank Pentesting Report]

Jay's Bank

Last Page