Clara Valentina 5027221016

SafeGuard Solutions

Jay's Bank

Security Assessment Findings Report

Business Confidential

Date: June 1th, 2024

.

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.

The penetration was conducted by SafeGuard Solutions on May 28-June 1, 2024 focusing on five predefined scopes, with the primary objective of identifying and exposing possible vulnerabilities in the system. The actions were geared towards strengthening security defenses by finding weak points that attackers might exploit.

Contact Information

Name	Title	Contact Information
Jay's Bank		
Fort	Global Information Security Manager	Email: fort@Jay's Bank.com
SafeGuard Solutions		
Anda	Lead Penetration Tester	Email: anda@SafeGuard Solutions.com

Assessment Overview

From May 28, 2024 to June 1, 2024, Jay's Bank has contracted SafeGuard Solutions to conduct a security evaluation of the defined scope through a penetration test. This was intended to gain a deep understanding of the security vulnerabilities that may exist and to identify potential attacks that could occur.

Phases of penetration testing activities include the following:

1. Reconnaissance:
- Identify public information about the target, such as IP address, domain name, and company information.
- Network scanning to identify active hosts and running services.
- Further information gathering through open search and other techniques to understand the system architecture.
2. Vulnerability Assessment:
- Identification of weaknesses in the website running on the specified host.
- Automated scanning using specialized software to detect common vulnerabilities, including Broken Access Control (BAC) vulnerabilities and Cross-Site Scripting (XSS) vulnerabilities.
3. Reporting:
- Documentation of all findings related to the reconnaissance phase, including information gathered, targets identified, and potential areas of attack.
- A summary of the results of the vulnerability assessment, including a list of vulnerabilities found (including BAC and XSS), their severity, as well as appropriate remediation recommendations.

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
Jay's Bank Application Penetration Testing	167.172.75.216

Scope Exclusions

Application IP Address: 167.172.75.216

SafeGuard Solutions adheres to the highest ethical standards, including the avoidance of Denial of Service (DoS) and Phishing/Social Engineering. All other non-lossful attack techniques are permitted by Jay's Bank.

The scope of this penetration testing engagement includes:

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

Additionally, any vulnerabilities discovered during testing will be reported solely for the purpose of improving the security posture of Jay's Bank, and all sensitive information obtained during testing will be handled with the utmost confidentiality and care.

Client Allowances

Jay's Bank provided SafeGuard Solutions with the following allowances:

- Allowed to search for and identify vulnerabilities within Jay's Bank application.
- Focus on application vulnerabilities such as SQL injection, XSS, and authentication/authorization issues.
- Where possible, discovered vulnerabilities may be exploited to access other user accounts, but only within the application itself (not to server-level access).

Additionally, any sensitive data accessed during the penetration testing process must be handled in accordance with Jay's Bank confidentiality policies, and any potential risks introduced during testing must be communicated promptly to Jay's Bank security team for mitigation.

Executive Summary

JAY'S BANK evaluated CyberShield's internal security posture through penetration testing from June 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 5 (five) days.

Testing Summary

Both XSS (Cross-Site Scripting) and Broken Access Control represent significant security vulnerabilities that can have severe consequences for a system. XSS attacks occur when malicious scripts are injected into web applications, allowing attackers to execute unauthorized actions or steal sensitive information, potentially compromising user data and system integrity. On the other hand, Broken Access Control vulnerabilities enable attackers to bypass intended access control mechanisms, granting them unauthorized access to sensitive data or functionality. This can lead to data theft, system compromise, or other malicious activities. These vulnerabilities often arise due to flaws in input validation, inadequate sanitization of user input, and weaknesses in the implementation of access control mechanisms. If left unaddressed, both XSS and Broken Access Control vulnerabilities can pose significant risks to the confidentiality, integrity, and availability of the system, making it crucial to implement robust security measures and follow secure coding practices to mitigate these threats.

Tester Notes and Recommendations

It is necessary to implement input validation and output encoding mechanisms to sanitize user inputs and escape untrusted data before rendering it in the application and implement the principle of least privilege, enforce robust access control mechanisms like role-based access control (RBAC), and regularly review and adjust access rights to ensure users and processes have only the minimum required permissions

Key Strengths and Weaknesses

- The following identifies the key strengths identified during the assessment:

The system uses encryption techniques to mitigate the risk of script injection attacks like XSS, making it more difficult for attackers to execute malicious scripts successfully

- The following identifies the key weaknesses identified during the

  assessment:

  - The system is vulnerable to XSS attacks, which can allow attackers to inject malicious scripts and potentially execute unauthorized actions or steal sensitive information.
  - The system is vulnerable to Broken Access Control, enabling attackers to bypass intended access control mechanisms and gain unauthorized access to sensitive data or functionality, leading to potential data theft or system compromise.

Vulnerability Summary & Report Card

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

Internal Penetration Test Findings

0	2	0	0	0
Critical	High	Moderate	Low	Informational

Finding	Severity	Recommendation
IPT-001: : Cross-Site Scripting (XSS) Vulnerability (High)	High	implement input validation and output encoding mechanisms to sanitize user inputs and escape untrusted data before rendering it in the application
IPT-002: Broken Authentication and Access Control Vulnerability(High)	High	implement the principle of least privilege, enforce robust access control mechanisms like role-based access control (RBAC), and regularly review and adjust access rights to ensure users and processes have only the minimum required permissions

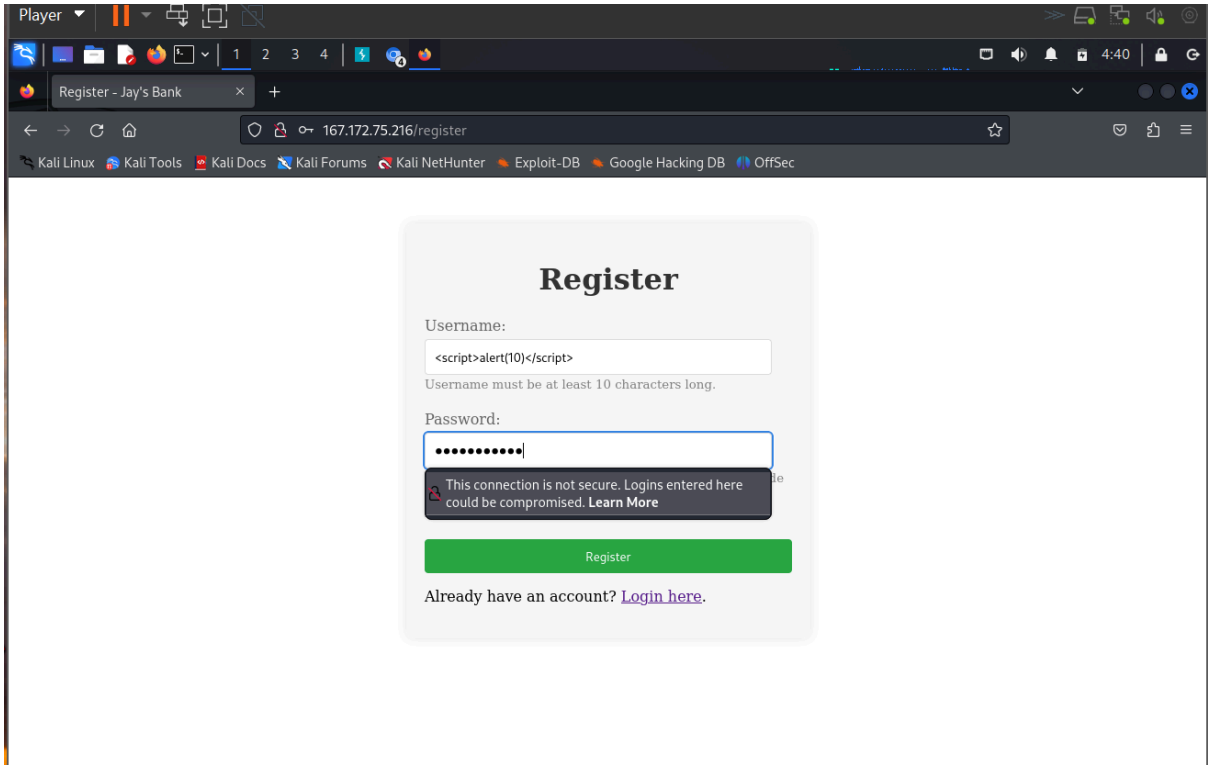
Technical Findings

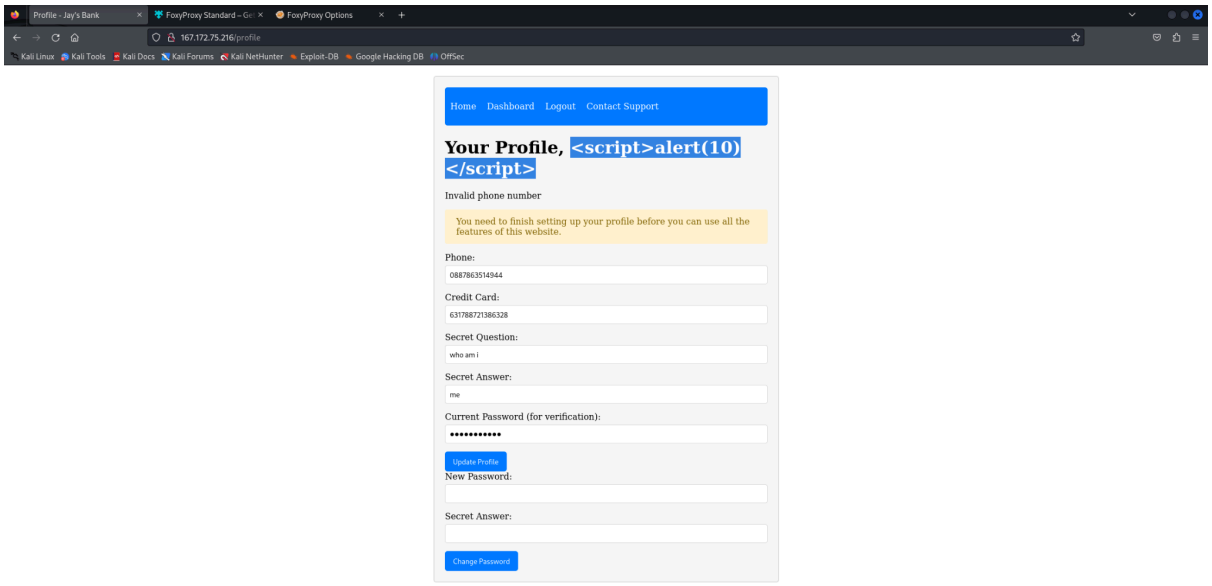
Internal Penetration Test Findings

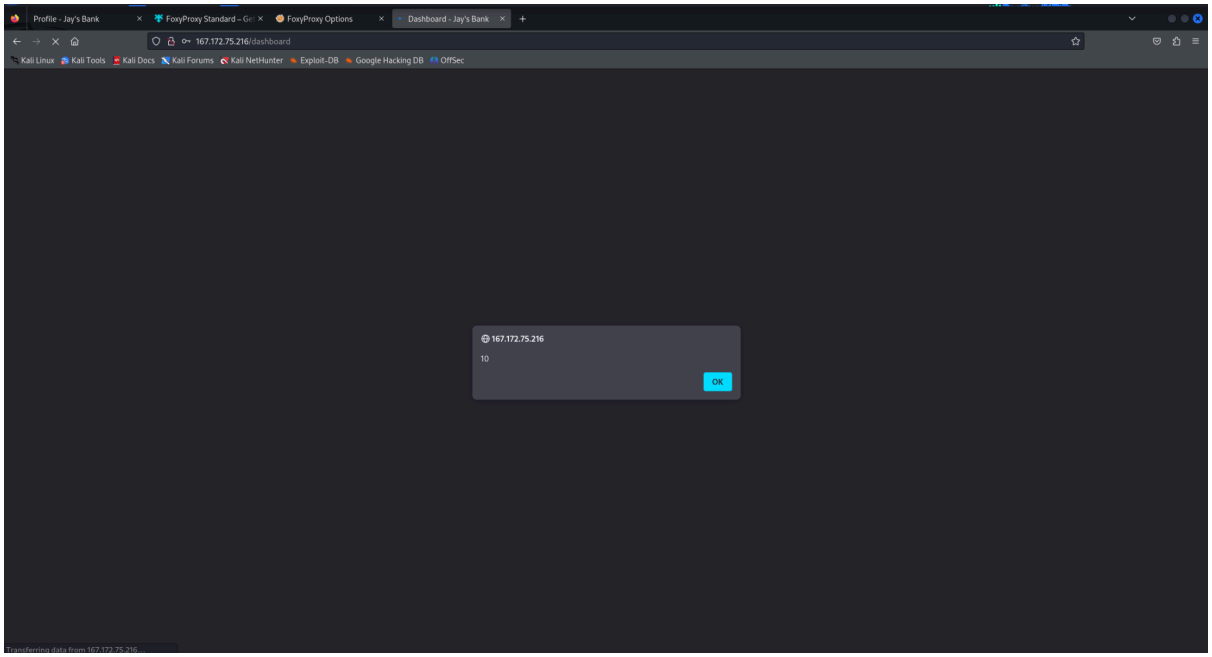
Finding IPT-001: : Cross-Site Scripting (XSS) Vulnerability (High)

Description:	A system is vulnerable to XSS attacks when malicious scripts are injected, allowing attackers to execute unauthorized actions or steal sensitive information. This type of attack exploits vulnerabilities in web applications, potentially compromising user data or system integrity.
Risk:	Likelihood: Moderate - Can be carried out by attackers with basic knowledge of XSS and access to attack tools available on the internet. Impact: High - Can lead to leakage of sensitive user data, session hijacking, credential theft, and even result in financial losses and reputational damage to the company.
System:	Web Application
Tools Used:	Script Injection

Evidence







Remediation

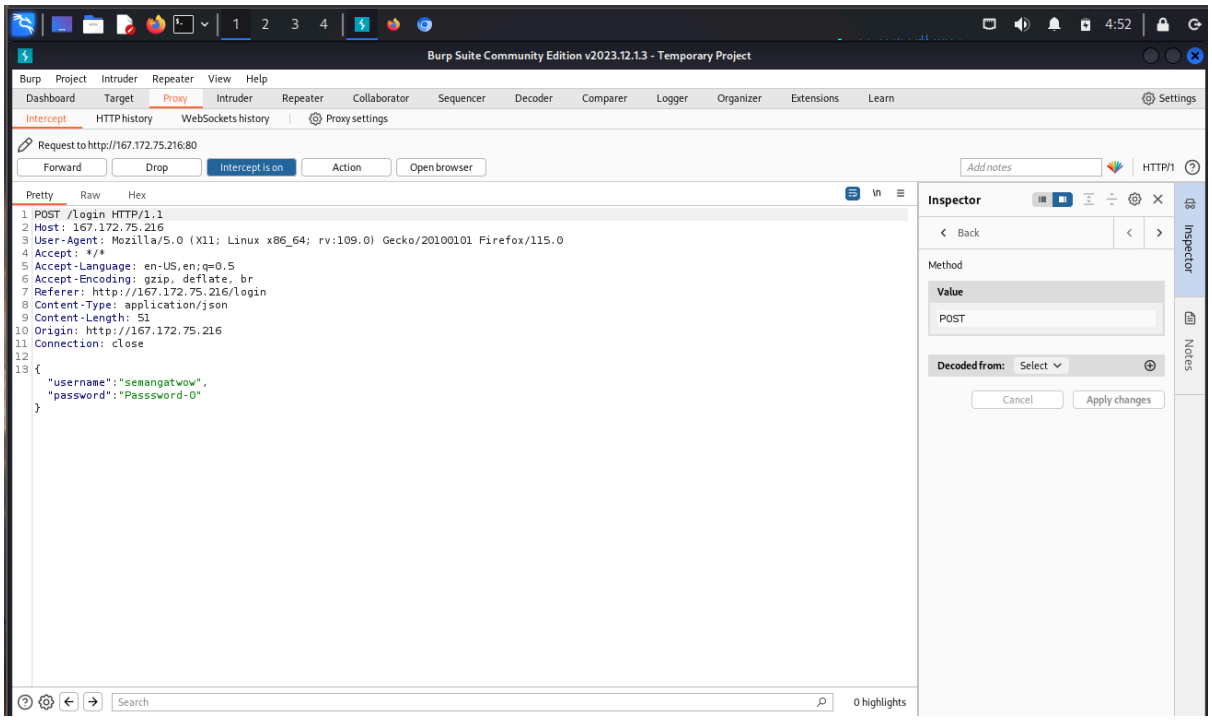
Remediating XSS vulnerabilities requires a multifaceted approach aimed at both preventing the injection of malicious scripts and mitigating their potential impact. This includes implementing input validation and output encoding mechanisms within web applications to sanitize user inputs and prevent the execution of harmful scripts. Additionally, employing Content Security Policy (CSP) headers can restrict the sources from which scripts can be loaded, reducing the attack surface for XSS exploits. Regular

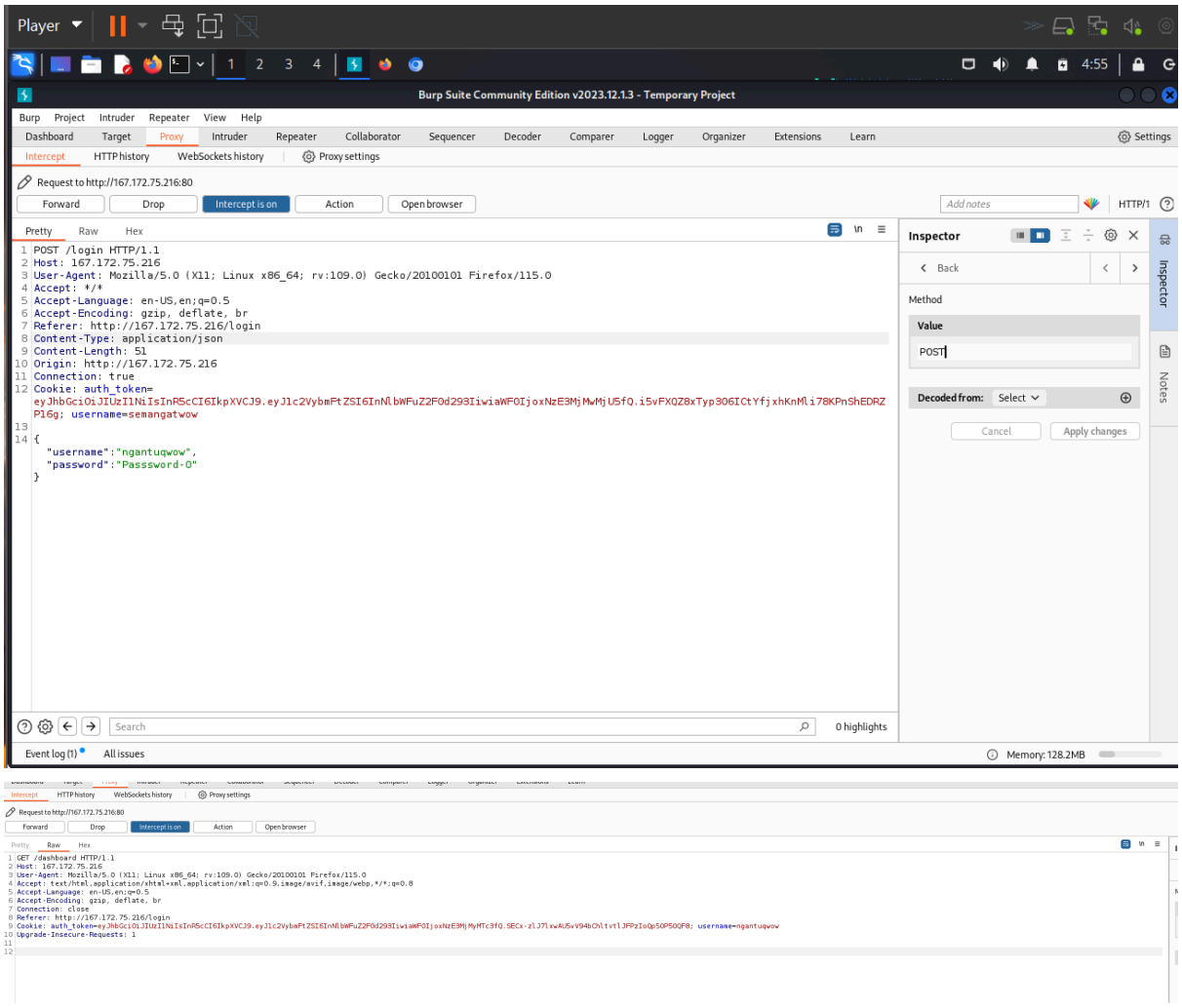
security assessments and code reviews are crucial to identifying and addressing any remaining vulnerabilities.

Finding IPT-002: Broken Authentication and Access Control Vulnerability(High)

Description:	A system vulnerable to Broken Access Control can be exploited by attackers to gain unauthorized access to sensitive data or functionality that should be restricted. By bypassing the intended access control mechanisms, an attacker can perform actions or access resources they should not have permission for, potentially leading to data theft, system compromise, or other malicious activities.
Risk:	Likelihood: High - Exploiting BAC vulnerabilities is relatively straightforward for attackers with sufficient knowledge and skills, as it involves taking advantage of flaws in access control implementation. Impact: High - A successful BAC attack can lead to unauthorized access to sensitive data, unauthorized modification of data or systems, potential system compromise or takeover, and significant financial and reputational damage to the organization
System:	Web Application
Tools Used:	Burp suite

Evidence





Remediation

To remediate a Broken Access Control vulnerability, implement the principle of least privilege access and robust access control mechanisms like role-based access control (RBAC). Enforce strong authentication measures such as multi-factor authentication (MFA), and segregate duties and privileges across different roles. Regularly audit systems, educate developers on secure coding practices, and maintain vigilant logging, monitoring, and patch management processes.

Last Page