Jay's Bank
Security Assessment Findings Report

Business Confidential

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

Confidentiality Statement

This document is the exclusive property of JAY'S BANK and TCM Security (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

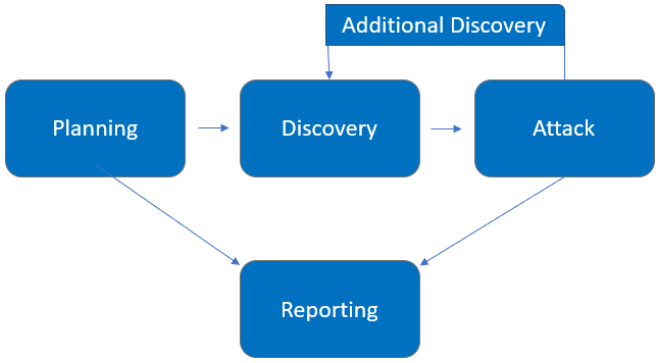
Name	Title	Contact Information
Jay's Bank		
Smith J	Global Information Security Manager	Email: jsmith@democorp.com
SafeGuard Solutions		
Monika Damelia Hutapea	Lead Penetration Tester	Email: monicc@gmail.com

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 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

Scope Exclusions

Per client request, CYBERSHIELD 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.

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 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) business days.

Testing Summary

The testing process, involving both Black-box Testing (BAC) and Cross-Site Scripting (XSS) evaluations, provided critical insights into the security vulnerabilities of Jay's Bank application. Using Black-box Testing tools like Burp Suite, the assessment revealed flaws in user authentication systems and insufficiently validated data inputs. The XSS evaluation aimed to uncover vulnerabilities prone to script injection attacks. This assessment identified multiple entry points in the application susceptible to XSS, posing risks of session hijacking or user data breaches. These findings highlight the urgent need for remediation to enhance the application's security. Suggested measures include strengthening authentication mechanisms, improving data input validation processes, and implementing strong security controls to reduce XSS attack risks and protect user information.

Tester Notes and Recommendations

A discovered vulnerability in the application permits access to other users' accounts simply by using their usernames. Additionally, a Cross-Site Scripting (XSS) flaw has been identified, allowing malicious scripts to be injected, which would trigger a pop-up alert when the compromised page is accessed. These vulnerabilities present serious threats to the application's security and the integrity of user data.

The username-based account access vulnerability reveals a critical weakness in the authentication system, enabling unauthorized individuals to access sensitive user information and potentially compromise data privacy. It is crucial to implement strong authentication measures, such as requiring both a username and a robust password, to effectively address this risk.

Furthermore, the XSS vulnerability provides a gateway for attackers to inject and execute malicious code on the client side, which could result in data theft, session hijacking, or further exploitation of the application's weaknesses. This issue highlights the necessity of thoroughly sanitizing and validating all user inputs and adhering to secure coding practices to prevent XSS attacks.

Key Strengths and Weaknesses

For IP Address 167.172.75.216

The following identifies the key strengths identified during the assessment: The program's endpoints are highly secure, making it difficult for SQL injection and XSS attacks to penetrate.

The following identifies the key weaknesses identified during the assessment:

1. Vulnerability allowing account access using only the username.
2. Cross-Site Scripting (XSS) vulnerability enabling the injection of malicious scripts.

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
IPT-001: Broken Authentication and Access Control Vulnerability	High	Implement strong authentication measures by requiring both a username and a strong password for user accounts. Additionally, ensure that proper access control mechanisms are in place to prevent unauthorized access to user accounts and sensitive information.
IPT-002: Cross-Site Scripting (XSS) Vulnerability	High	Thoroughly clean and validate every user input to block the insertion of harmful scripts. Integrate secure programming methods, such as encoding output and validating input, to reduce the chances of XSS attacks. Moreover, contemplate the deployment of a Web Application Firewall (WAF) to add an extra level of protection against XSS and other web-based assaults.

Technical Findings

Internal Penetration Test Findings

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

Description:	The application permits entry into other users' accounts solely by utilizing their usernames, circumventing the authentication procedure. This flaw exposes confidential user data and may jeopardize data privacy.
Risk:	Likelihood: High – There's a significant likelihood of exploitation given that attackers can effortlessly circumvent authentication using just usernames. Impact: Critical – If successfully exploited, unauthorized entry to user accounts, data breaches, identity theft, and other malicious activities could occur, causing substantial financial and reputational harm.
System:	Web Application
Tools Used:	Burp suite, Manual testing, web browser on Kali Linux
References:	OWASP Top 10 2021 - A07:2021 – Identification and Authentication Failures

Evidence

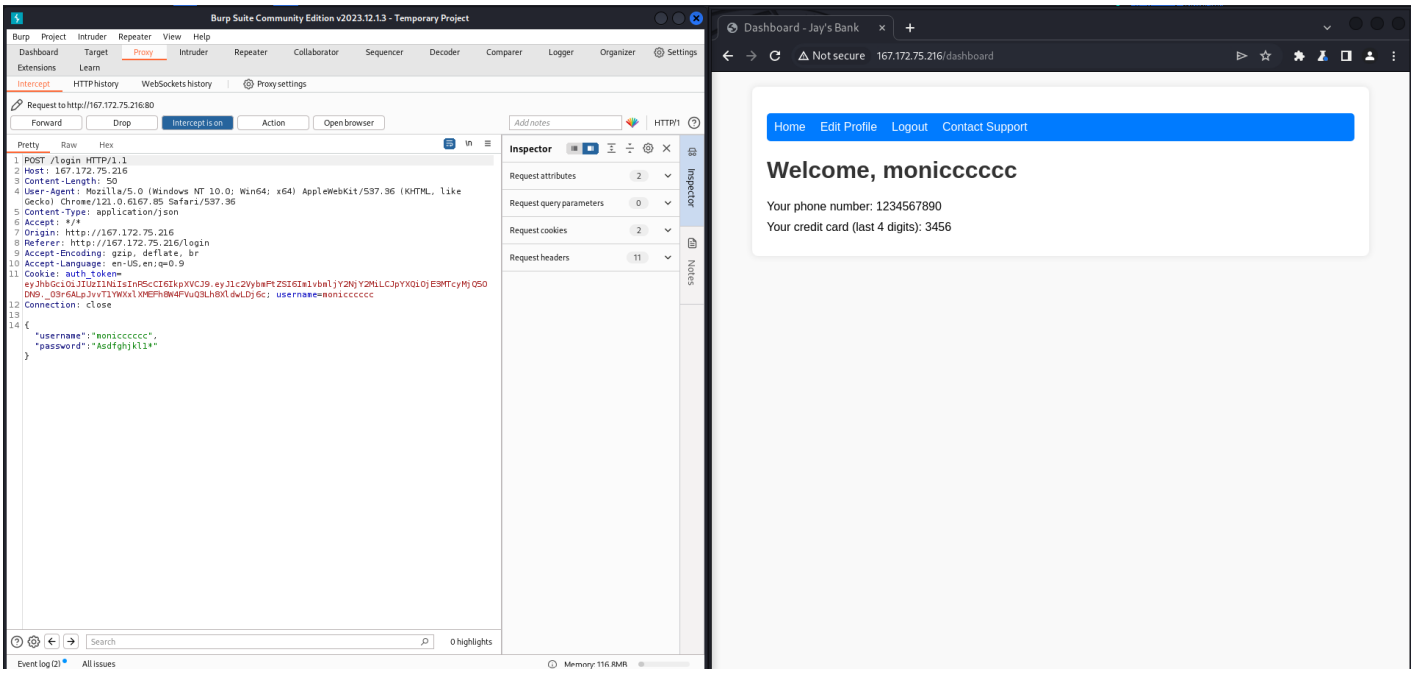


Image 1. Username and password first user

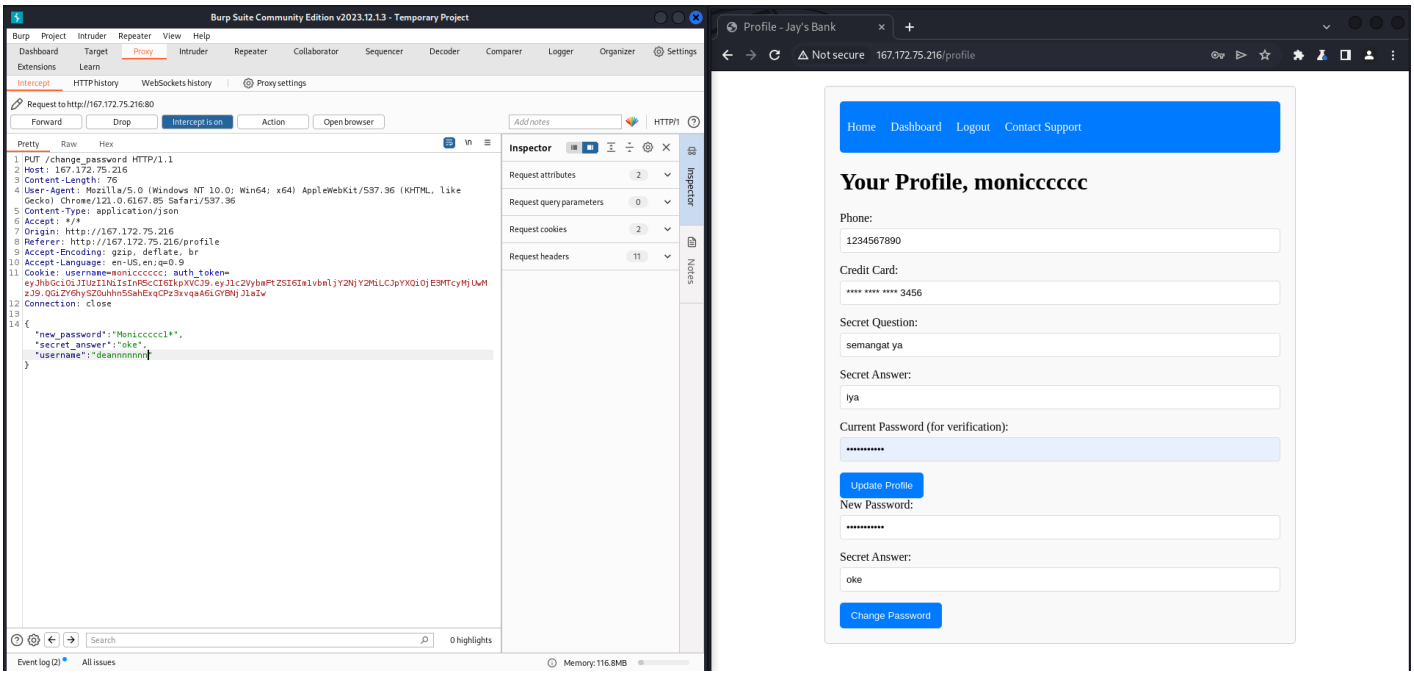


Image 2. Make new password and change username with second user on Burpsuite

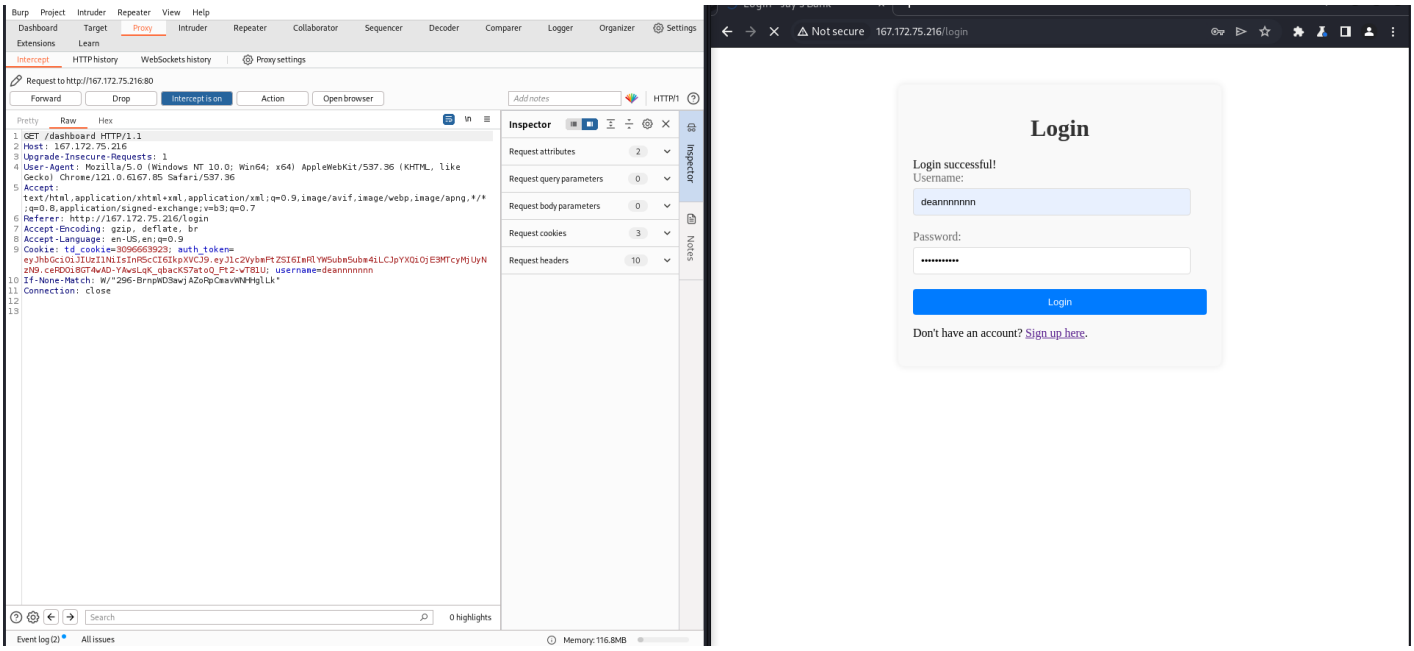


Image 3. Successful login

Remediation:

- Implement a robust authentication system mandating both a username and a secure password for user accounts.
- Enforce stringent password requirements and periodic password changes to bolster security.
- Integrate multi-factor authentication (MFA) for an extra layer of protection.
- Conduct routine security assessments and penetration tests to pinpoint and resolve any potential authentication and access control vulnerabilities.
- Deploy access control mechanisms like role-based access control (RBAC) to restrict user access to authorized resources and data only.
- Regularly reassess and update access controls to adhere to the principle of least privilege.
- Implement secure session management and logout features to prevent unauthorized access to active sessions.

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

Description:	The application is vulnerable to Cross-Site Scripting (XSS) attacks, permitting the injection of harmful scripts that execute in the user's browser upon loading the affected page. This flaw can be exploited by inserting scripts into input fields or other user-controllable areas.
Risk:	Likelihood: High – XSS vulnerabilities are prevalent in web applications and can be readily exploited if user input is not properly sanitized. Impact: Critical – Successful exploitation can result in multiple attacks, such as stealing user session tokens, hijacking user sessions, and potentially compromising the entire application or system, leading to data breaches and financial losses.
System:	Web Application
Tools Used:	Manual testing, web browser, script injection
References:	OWASP Top 10 2021 - A03:2021 – Injection

Evidence

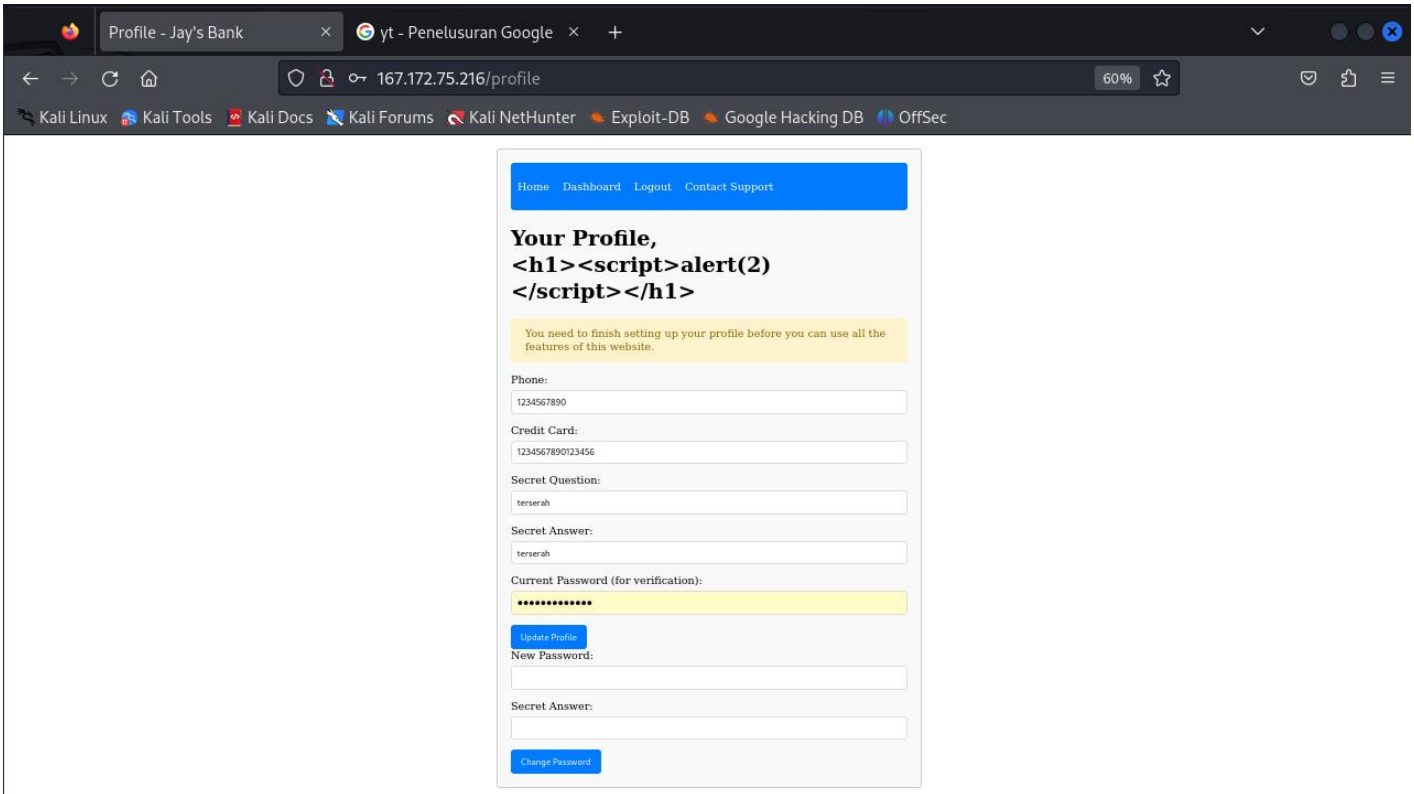


Image 4. Regist and login with script

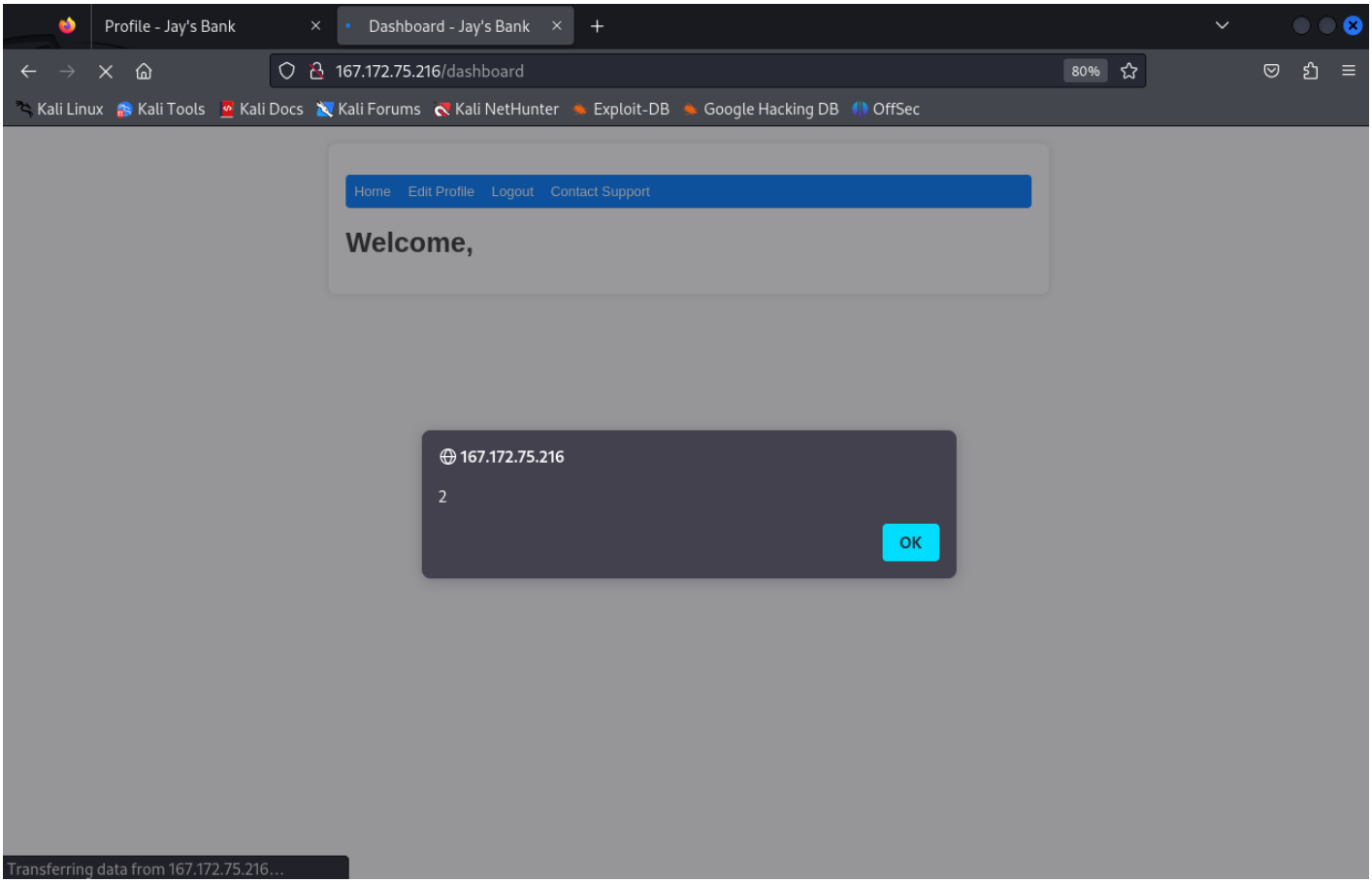


Image 5. Successful login and appear pop up

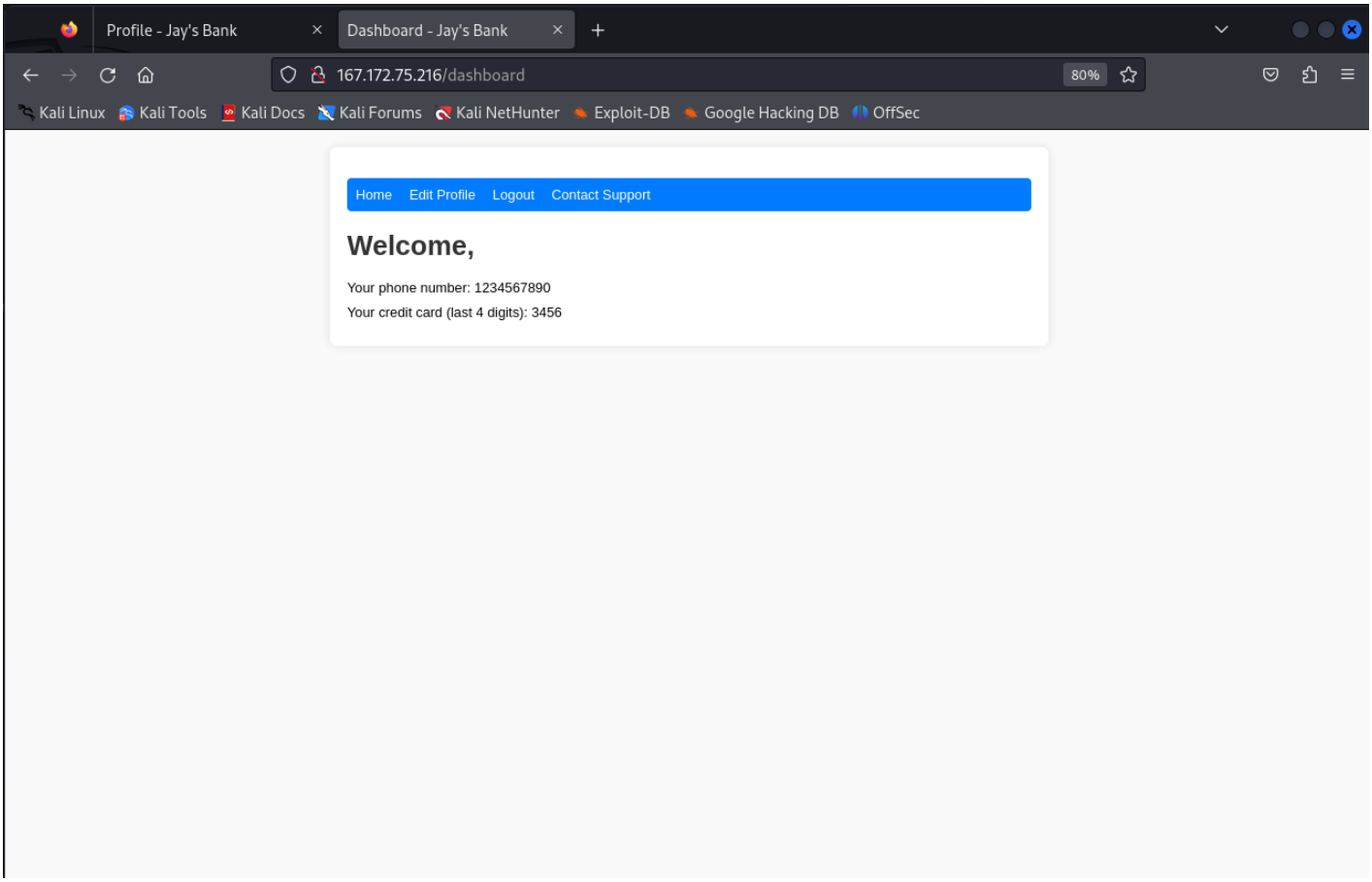


Image 6. Dahboard after scripting

Remediation:

- Apply input validation and sanitization for all user-provided data to block the injection of malicious scripts.
- Utilize context-sensitive output encoding for all user-supplied data before displaying it in the browser.
- Implement a Content Security Policy (CSP) to limit the execution of untrusted scripts and reduce the impact of XSS vulnerabilities.
- Regularly update and patch the web application and its dependencies to fix known XSS vulnerabilities.
- Deploy a Web Application Firewall (WAF) to add an extra layer of protection against XSS and other web-based threats.
- Conduct regular security testing, including static code analysis and dynamic application security testing (DAST), to identify and fix XSS vulnerabilities.
- Adopt secure coding practices and provide security awareness training to developers to prevent the introduction of XSS vulnerabilities in the codebase.

Additional Scans and Reports: No additional scans or reports were included in this assessment. This report only covers the primary vulnerability findings identified during the web application security assessment.

Last Page