Jay's Bank
Ethical Hacking 3rd Lab Work

Business Confidential

Date: June 1st, 2024
Project: DC-001

Version 1.0

Table of Contents

Confidentiality Statement

CyberShield and Fortitech proprietary documents containing proprietary and confidential information. Their reproduction, redistribution or use, in whole or in part, in any form, requires the consent of CyberShield and FortifyTech.

CyberShield may share this document with auditors under confidentiality agreements to demonstrate compliance with penetration test requirements.

Disclaimer

The penetration test is considered a snapshot in time. The findings and recommendations reflect information gathered during the assessment and not changes or modifications made outside of that period.

Time-limited engagements do not allow for a full evaluation of all security controls. CyberShield prioritized the assessment to identify the weakest security controls that would be exploited by attackers. CyberShield recommends conducting a similar assessment annually by an internal or third-party assessor to ensure continued control success.

Contact Information

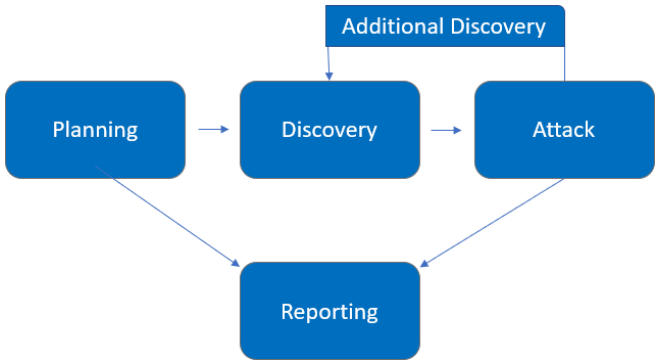
Name	Title	Contact Information
ITS Information Technology Student		
Nur Azka	Student	Email: nurazkarahadian@gmail.com

Assessment Overview

From May 28, 2024 to June 1, 2024, SafeGuard Solutions engaging Jay's Bank to evaluate the security posture of its application infrastructure compared to current industry best practices which included internal network penetration tests. All conducted tests were built upon the NIST SP 800-115 Technical Guide for Information Security Testing and Assessment, OWASP Testing Guide (v4), and customized testing frameworks.

Phases of penetration testing activities include the following:

- Planning – Gather customer objectives and derive rules of engagement.
- Discovery – Perform scans and enumerations to identify potential vulnerabilities, weak areas, and exploits.
- Attack –Confirm potential vulnerabilities through exploitation and perform additional discovery on new access.
- Reporting – Document all discovered vulnerabilities and exploits, failed attempts, and company strengths and weaknesses.



Assessment Components

Internal Penetration Test

Internal penetration tests are intended to emulate the actions of an attacker from within the network by scanning and identifying potential vulnerabilities on the host. The engineer then performs internal network attacks, both common and sophisticated, to gain access to the host through lateral movement and compromise user accounts and domain admins. Finally, engineers will attempt to exfiltrate any sensitive data found.

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

Quantifying the impact of potential vulnerabilities involves assessing operations, including aspects of confidentiality, integrity and availability of systems and client data. It also includes an evaluation of potential reputational damage and financial loss.

Scope

Assessment	Details
Internal Penetration Test (Bank Mockup Application)	• 167.172.75.216

Scope Exclusions

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

- RCE and Privilege Escalation.
- Phishing/Social Engineering.
- Attacks that may damage data or application infrastructure.

All other attacks not specified above were permitted by SafeGuard Solutions.

Client Allowances

FortifyTech provided CyberShield the following allowances:

- Internal access to the network via dropbox and port allowances.
- Application vulnerabilities are mainly SQL Injections, XSS, and authentication issues

Executive Summary

SafeGuard Solutions has evaluated the internal security posture of the Jay's Bank application through penetration testing conducted from May 28, 2024 to June 1, 2024. The following sections provide a comprehensive overview of the vulnerabilities discovered, successful and failed attack attempts, and an analysis of system strengths and weaknesses.

Scoping and Time Limitations

Scope restrictions during the engagement precluded denial of service or social engineering across all testing components.

Time constraints were enforced for testing purposes. Internal network penetration testing was allocated a duration of five (5) business days.

Testing Summary

The application assessment conducted by SafeGuard Solutions focused on evaluating Jay's Bank internal application security posture. Internally, the SafeGuard Solutions team executed vulnerability scanning against the IP address provided by Jay's Bank to assess the network's overall patching health. In addition to vulnerability scanning, the team probed for other potential risks.

During the evaluation, SafeGuard Solutions identified vulnerabilities within the IP address 167.172.75.216. These vulnerabilities were subject to attempted exploitation through methods such as SQL injection, manual scripting, and man-in-the-middle intercepts.

However, the team was unable to successfully exploit and thoroughly examine these vulnerabilities due to challenges in verifying the authenticity of associated risks identified during scans.

.

Tester Notes and Recommendations

The testing results of the Jay's Bank website application suggest that the organization is undergoing its inaugural penetration test, as is evident from the findings. A significant number of identified issues stem from the absence of essential security headers. These headers play a pivotal role in mitigating vulnerabilities such as cross-site scripting (XSS), which can be exploited by malicious actors.

Additionally, during the assessment of the IP address 167.172.75.216, a potential exploitation avenue was discovered within the web application, specifically related to CVE-2023-37528. This susceptibility exposes the website to the risk of XSS and cross-site scripting attacks.

Vulnerability Summary & Report Card

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

Internal Penetration Test Findings

0	0	0	0	2
Critical	High	Moderate	Low	Informational

Finding	Severity	Recommendation
Internal Penetration Test		
XSS (Cross site scripting)	High	Review action and remediation steps.
CVE-2023-37528	Moderate	Review action and remediation steps.

Technical Findings

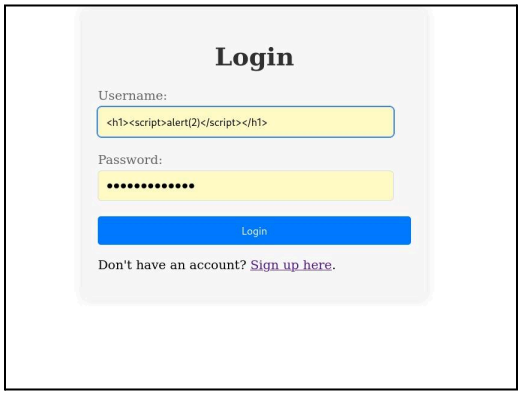
Internal Penetration Test Findings

Finding IPT-001: Cross-site Scripting (Critical)

Description:	There are missing security headers Found CVE-2023-37528
Risk:	Likelihood: High – This attack is effective in web application environments. Impact: Unknown
System:	Website Aplication
Tools Used:	XSS
References:	CVE-2023-37528

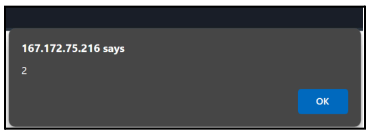
Evidence and Documentation

"After registering an account to scope"



"login using script"

.



“Script result”