

# SafeGuard Solutions Security Assessment Findings Report

Business Confidential

*Date: June 1<sup>st</sup>, 2024*  
*Version 1.0*

---

## Table of Contents

Table of Contents .....	2
Confidentiality Statement.....	3
Disclaimer .....	3
Contact Information.....	3
Assessment Overview .....	4
Assessment Components.....	4
External Penetration Test .....	4
Finding Severity Ratings.....	5
Scope .....	6
Scope Exclusions.....	6
Client Allowances.....	6
Executive Summary .....	7
Attack Summary .....	7
Vulnerabilities by Impact.....	8
External Penetration Test Findings.....	9
Blind Time-Based SQL injection in User Authentication System – Register (Critical).....	9
Broken Access Control (IDOR) on change password functionality – Profile (Critical).....	12

## 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 SafeGuard Solutions and Jay's Bank.

SafeGuard Solutions 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

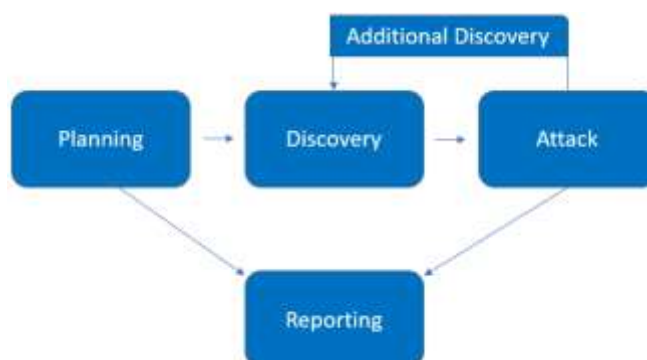
Name	Title	Contact Information
<b>Jay's Bank</b>		
Kiseki	Information Security Consultant	Office: (555) 555-5555 Email: <a href="mailto:kisekichan@jaysbank.com">kisekichan@jaysbank.com</a>
Ruhzun	IT Guy	Office: (666) 666-6666 Email: <a href="mailto:ruhzun@jaysbank.com">ruhzun@jaysbank.com</a>
<b>SafeGuard Solutions</b>		
Jac	Lead Penetration Tester	Office: (555) 555-5555 Email: <a href="mailto:jac@cybershield.com">jac@cybershield.com</a>

## Assessment Overview

From May 28<sup>th</sup>, 2024 to June 1<sup>st</sup>, 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 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 SafeGuard Solutions engineer 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

## Scope Exclusions

Jay's Bank specified restrictions namely:

- Jay's Bank grants permission to search for and identify vulnerabilities in Jay's Bank applications.
- Focus on application vulnerabilities such as SQL injection, XSS, and authentication/authorization issues.
- If possible, the vulnerabilities found can be exploited to access other user accounts, but only to the application (not to the server).
- It is not allowed to carry out attacks that can damage data or application infrastructure.
- It is not permitted to exploit vulnerabilities that could grant access to the server (example: RCE, privilege escalation).
- Avoid DoS/DDoS attacks that can disrupt application service availability.

## Client Allowances

Jay's Bank did not provide any allowances to assist the testing.

## Executive Summary

SafeGuard Solutions evaluated Jay's Bank's external security posture through an external network penetration test from May 28<sup>th</sup>, 2024 to June 1<sup>st</sup>, 2024. By leveraging a series of attacks, SafeGuard Solutions found medium level vulnerabilities that allowed SafeGuard Solutions to discover multiple vulnerabilities such as SQL Injection. It is highly recommended that Jay's Bank address these vulnerabilities as soon as possible as the vulnerabilities are easily found through basic reconnaissance and exploitable without much effort.

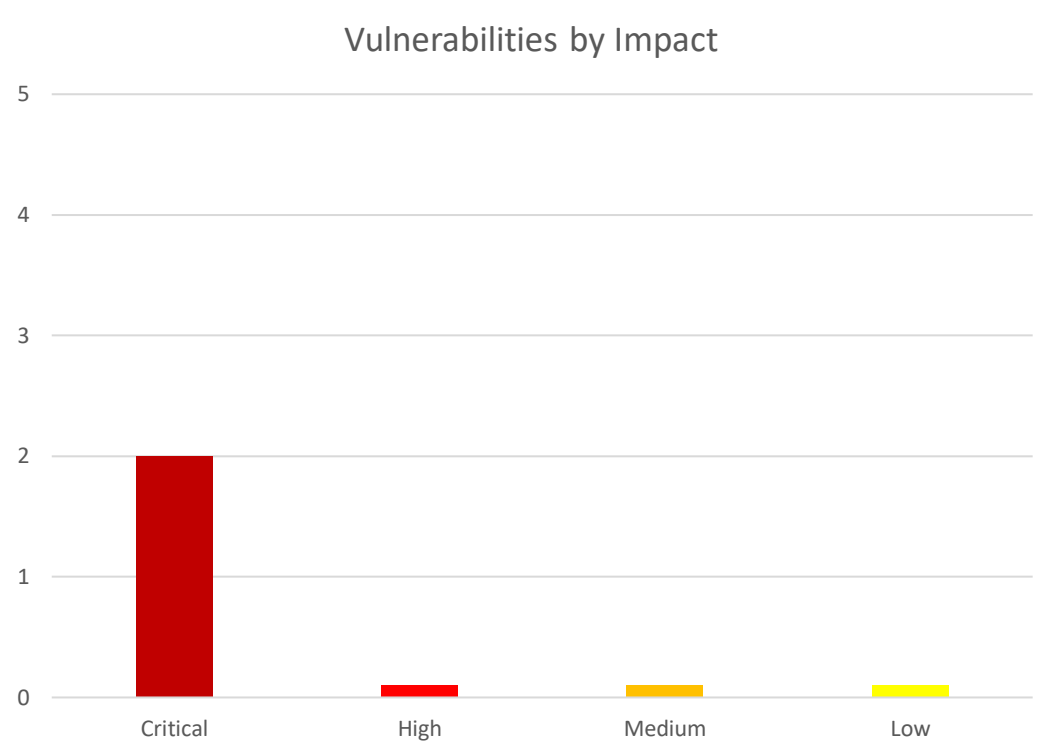
## Attack Summary

The following table describes vulnerabilities discovered by SafeGuard Solutions:

Step	Action	Recommendation
1	Performed successful SQL Injection in register page.	Include input validation and sanitization, use parameterized queries and prepared statements, and limit user registration in the register page.
2	Performed IDOR due to broken access control in change password functionality of profile page.	Add authorization checks and use indirect references such as using tokens instead of username. Validate session and limit user controls.

# Vulnerabilities by Impact

The following chart illustrates the vulnerabilities found by impact:





## External Penetration Test Findings

### Blind Time-Based SQL injection in User Authentication System – Register (Critical)

<b>Description:</b>	A critical blind SQL injection vulnerability exists in the user authentication system of the web application. This vulnerability allows remote attackers to execute arbitrary SQL commands on the database server, leading to data leak, unauthorized access, data exfiltration, data manipulation, and denial of service.
<b>Impact:</b>	<b>Critical (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H   Score: 10.0)</b>
<b>System:</b>	167.172.75.216
<b>References:</b>	<a href="https://book.hacktricks.xyz/pentesting-web/sql-injection">https://book.hacktricks.xyz/pentesting-web/sql-injection</a> - SQL Injection <a href="https://book.hacktricks.xyz/pentesting-web/sql-injection/sqlmap">https://book.hacktricks.xyz/pentesting-web/sql-injection/sqlmap</a> - SQLMap Cheatsheet

### Exploitation Proof of Concept

SafeGuard Solutions tested injection a single quote (') in the username parameter of the register page which returned a 500 Internal Server Error response.

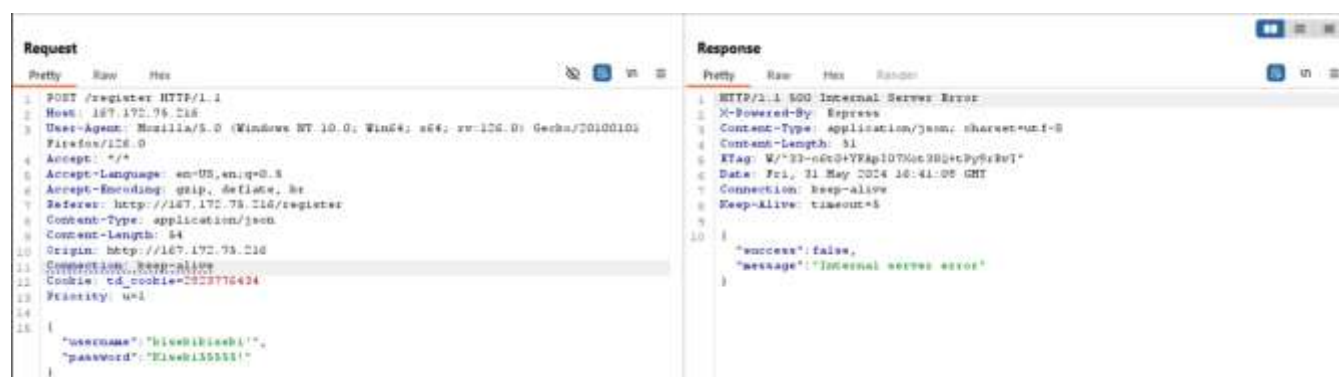


Figure 1: Response of injecting

This indicated that the single quote may have disrupted the query executed.

Since the system did not filter out special characters and there are no restrictions on the number of user registrations, it is possible to repeatedly attempt various injection payloads. Thus, SQLMap is performed by sending payloads using the request displayed above with a delay of 1 second to prevent denial of service. SQLMap discovered that there is blind time-based SQL injection vulnerability.



Figure 2: Snippet of successful payload

The payload works by injecting subquery.

SafeGuard Solutions then look for available databases using SQLMap, in which SQLMap returned two databases, ctf\_challenge and information\_schema.

```
web application technology: Express
back-end DBMS: MySQL > 5.0.12
available databases [2]:
[*] ctf_challenge
[*] information_schema
```

*Figure 3: Available databases*

To further investigate the database, SQLMap is used to retrieve tables that are available in ctf\_challenge.

```
Database: ctf_challenge
[2 tables]
+-----+
| queue |
| users |
+-----+
```

*Figure 4: Available tables at ctf\_challenge database*

To further investigate the database, SQLMap is used to retrieve tables and its columns that are available in ctf\_challenge database.

```
Database: ctf_challenge
Table: users
[2 columns]
+-----+-----+
| Column | Type   |
+-----+-----+
| id     | int(11)|
| username | varchar(25)|
+-----+-----+
```

*Figure 5: Available columns at users database*

**Remediation**

<b>Who:</b>	IT Team
<b>Vector:</b>	Remote
<b>Action:</b>	Include input validation and sanitization, use parameterized queries and prepared statements, and limit user registration.

**Broken Access Control (IDOR) on change password functionality – Profile (Critical)**

<b>Description:</b>	Change password functionality allowed on user-supplied input without proper authorization checks which allows an attacker to access or modify resources they should not be able to, such as changing another user's password.
<b>Impact:</b>	<b>Critical (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:N)</b>
<b>System:</b>	167.172.75.216
<b>References:</b>	<a href="https://portswigger.net/web-security/access-control/idor">https://portswigger.net/web-security/access-control/idor</a>

**Exploitation Proof of Concept**

On /profile, the change password functionality can be used after setting up the profile.

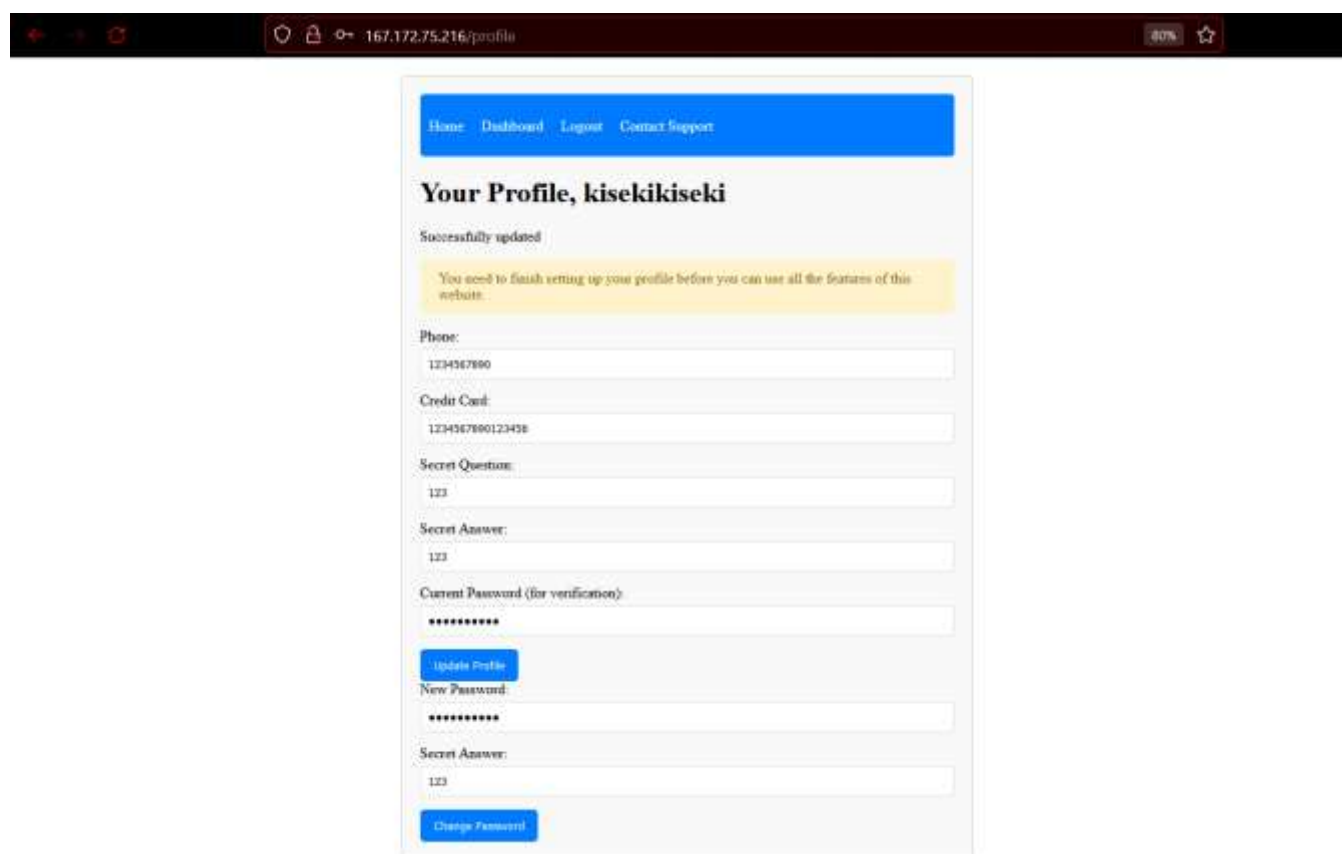


Figure 6: Profile page with change password functionality

To investigate further, SafeGuard Solutions intercept the PUT request and discovered the application passes the username parameter without authorization checks. This allows SafeGuard solutions to access other user's accounts by changing their username.



**Remediation**

<b>Who:</b>	IT Team
<b>Vector:</b>	Remote
<b>Action:</b>	Add authorization checks and use indirect references such as using tokens instead of username. Validate session and limit user controls.

Last Page