| Fontys University of Applied Sciences

Security Report

Himalayan Bus Management System

Himal Aryal

2023

Table of Contents

[Introduction 2](#_Toc154149427)

[Assessment of OWASP Top 10 Risks 2](#_Toc154149428)

[1. Broken Access Control 2](#_Toc154149429)

[2. Cryptographic Failures 2](#_Toc154149430)

[3. Injection 2](#_Toc154149431)

[4. Insecure Design 2](#_Toc154149432)

[5. Security Misconfigurations 3](#_Toc154149433)

[6. Vulnerable and Outdated Components 3](#_Toc154149434)

[7. Identification and Authentication Failures 3](#_Toc154149435)

[8. Software and Data Integrity Failures 3](#_Toc154149436)

[9. Security Logging and Monitoring Failures 3](#_Toc154149437)

[10. Server-Side Request Forgery 3](#_Toc154149438)

# Introduction

The Himalayan Bus Application has been subjected to a meticulous security assessment aimed at evaluating its resilience against the top 10 security risks highlighted by OWASP. This report presents a thorough analysis of the application's security posture, assessing its capability to handle critical security challenges commonly faced by modern web applications.

## Assessment of OWASP Top 10 Risks

### 1. Broken Access Control

* **Prevention Measures:**
  + Implementation of Spring Security and JWT token-based authorization to prevent unauthorized requests.
* **Concern Identified:**
  + The absence of a logging system creates a blind spot in comprehending user interactions within the application, making it challenging to monitor user activities effectively and understand the application's behavior, which can hinder security monitoring, troubleshooting, and detecting potential threats or issues.

### 2. Cryptographic Failures

* **Implemented Measures:**
  + Use of Bcrypt for password encryption and JWT tokens for login responses.
* **Concern Identified:**
  + Lack of TLS encryption in an application poses significant security risks by potentially exposing transmitted data to interception and unauthorized access, compromising user privacy and data integrity.

### 3. Injection

* **Implemented Measures:**
  + Use of JPA (Object Relational Mapping) to prevent direct database access.
  + Restricted database user permissions to avoid dangerous operations.

### 4. Insecure Design

* **Implemented Measures:**
  + Careful handling of user input across frontend, backend, and database layers.
  + Encryption applied to sensitive data like user passwords.
  + Conducted unit testing for business layer. Other are considered will be implement later.
* **Concern Identified:**
  + Lack of usability testing might leave potential problems undetected.

### 5. Security Misconfigurations

* **Implemented Measures:**
  + Service limitations based on roles and utilization of JWT tokens.
* **Concern Identified:**
  + Non-utilization of OAuth2 and OpenID poses potential security risks.

### 6. Vulnerable and Outdated Components

* **Implemented Measures:**
  + Use of regularly updated and commonly used libraries.

### 7. Identification and Authentication Failures

* **Implemented Measures:**
  + Application of password policies and encryption of user passwords.
* **Concern Identified:**
  + Absence of multi-factor authentication potentially weakens application security.

### 8. Software and Data Integrity Failures

* **Implemented Measures:**
  + Validation of data modifications and deletions to ensure authorization.
  + Use of JPA for protection against injections.
* **Concern Identified:**
  + Vulnerability to SSRF attacks poses risks to data integrity.

### 9. Security Logging and Monitoring Failures

* **Concern Identified:**
  + The lack of a logging system poses significant security risks due to unmonitored user activities.

### 10. Server-Side Request Forgery

* **Implemented Measures:**
  + CORS configuration to limit unauthorized requests.
* **Concern Identified:**
  + Absence of HTTPS exposes the system to potential SSRF attacks, compromising network security.

**Conclusion**

This security assessment provides an overview of the Himalayan Bus Management System's security posture, outlining both implemented measures and areas of concern. Recommendations for improvements have been highlighted to ensure a more robust security framework, safeguarding user data and system resources against potential threats and vulnerabilities.