OWASP Top 10 Report

Name: Tony Jiang

Semester: 6

Class: RB04

Introduction

This document aims to determine if the application addresses the OWASP Top 10 security risks. It will provide insights on how these risks will be covered in the application and assess whether this coverage is necessary in application.

Top 10 security risks

This outlines the current security risks for Sprint 3. Planned actions to address these risks are scheduled for the next sprint, Sprint 4. Documentation will include steps to mitigate each risk. Some risks are not yet scheduled and will be decided upon later.

	Likelihood	Impact	Risk	Action possible	Planned
A01:2021-Broken Access Control	High	High	High	Add authentication and authorization to the authentication service to create roles that control access, allowing users to sign in and view specific information, such as their personal details.	Yes, for sprint 4
A02:2021-Cryptographic Failures	High	High	High	Add salt and password hashing to securely store	Yes, for sprint 4

				passwords in the user service and authentication service.	
A03:2021-Injection	High	High	High		N/A for sprint 4
A04:2021-Insecure Design	High	High	High		N/A for sprint 4
A05:2021-Security Misconfiguration	High	High	High		N/A for sprint 4
A06:2021-Vulnerable and Outdated Components	High	High	High	Implement Snyk for automated security testing in the CI/CD pipeline to identify any outdated dependencies.	Yes, for sprint 4
A07:2021-Identification and Authentication Failures	High	High	High		N/A for sprint 4
A08:2021-Software and Data Integrity Failures	High	High	High		N/A for sprint 4
A09:2021-Security Logging and Monitoring Failures	High	High	High		N/A for sprint 4
A10:2021-Server-Side Request Forgery	High	High	High		N/A for sprint 4