Hazard Analysis
Software Eng 4G06

Team 2, Parnas' Pals
William Lee
Jared Bentvelsen
Bassel Rezkalla
Yuvraj Randhawa
Dimitri Tsampiras
Matthew McCracken

Contents

1 Revision History

Table 1: Revision History

Date	**Developer(s)**	**Change**
19/10/22	All	Initial Draft
05/04/23	All	Revision 1

2 Introduction

The purpose of this document is to identify the components of Olympian and its dependencies that could represent potential risks for Olympian's stakeholders. This document will analyze the risk levels of potentially hazardous components and their associated failures, as well as recommend actions which can be taken to eliminate the resulting risks or mitigate them to an acceptable level.

2.1 Definition of a Hazard

For Olympian's purposes (and throughout this document), a hazard will be defined as any condition or event which can lead to a state that is likely to negatively affect Olympian's stakeholders.

3 Scope and Purpose of Hazard Analysis

This document aims to provide an in-depth analysis to potential system hazards of the Olympian app. These hazards encompass categories including security, authorization, input correctness and error handling.

4 System Boundaries and Components

The system upon which the Hazard Analysis will be performed on consists of the following components:

1. The Olympian mobile application, which is composed of a front-end interface served by a back-end server, supports the following major functionalities:
   (a) Profile Creation
   (b) Workout Routine Creation
   (c) Workout Routine Discovery and Browsing
   (d) Workout Routine Reviewing
   (e) Workout Progress Tracking
   (f) Long Term Goal Progress Tracking
2. The physical Android or iOS mobile device.
3. The AWS Redshift Database where relational user information is stored.

Although integral to the system, the physical mobile device and Redshift Database availability are not under the control of Parnas' Pals. The physical mobile device is manufactured by a third party company, and operated by the user. The Redshift Database is operated by Amazon Web Services, making them responsible for database availability.

5 Critical Assumptions

- The user is assumed to have the Olympian application downloaded.
- The user's mobile device is assumed to have internet access.
- The user is assumed to have basic mobile device skills such as tapping the screen and swiping.

6 Failure Mode and Effect Analysis

6.1 Hazards Out of Scope

1. Native Mobile Device Software Failures: Because this is a mobile application, many native features will be used to provide application functionality. These features can include haptic feedback, notifications, accessibility controls, etc. It is possible that some of these features may fail on the mobile device, which would create a hazard for the application, but is outside the control of the application developers. Additionally, the application will only function on iOS 10 / Android 5.0 and above (React Native is unsupported). The version of software used by the user mobile device is not within the control of the application developers, and therefore the application will not be available to devices with operating system software older than iOS 10 or Android 5.0.
2. Database and Cloud Hosting Service Failures: The application relies on external services such as AWS Redshift to store and retrieve data, and process user requests. The availability of these services is not under the control of the developers of the application, and interruptions in their availability present a hazard for the application.

These hazards cannot be prevented by the application developers but will be mitigated to the fullest possible extent.

6.2 Failure Modes & Effects Analysis Table

Component	Failure Modes	Effects Of Failure	Causes Of Failure	Recommended Action	SR	Ref.
User Login & Authentication	User cannot log in to application	User cannot utilize site functionality	a. User uses incorrect login credentials.	User is prompted to re-enter login credentials.	PRR1	H1-1
User Private Data Access	Data that is meant to be kept private is displayed publicly	User privacy is breached and sensitive data is released	a. User privacy settings are incorrectly stored. b. Malicious third party gains access to user data.	User data will be stored in a secure database. User data will be backed up frequently and hashed to keep secure.	ACR1, ACR2, IR1, IR2, ADR1	H2-1
Workout Suggestion Algorithm	Workouts are incorrectly or illegally accessed by users	Users are able to access unavailable, restricted or uncatered routines	Suggestion algorithm failure	Display detailed message to user on attempt to access restricted routine	PRR1	H3-1
Application Server	Application Server terminates unexpectedly	Current data transactions and communication will cease	a. Host failure b. server exceeds data limit	Communicate server issues to users and store unsaved data locally on the user device	IR3, IR4, IR5	H4-1

Database	Data is deleted unintentionally	Collected data will not be available for user display or system analysis	a. Database failure	Regularly and automatically backup database and allow admin permissions to rollback	IR5, ADR1	H5-1
	Database is unavailable	Data transactions will be unavailable	a. Database failure b. Host failure	Refer to H5-1	IR3, IR4	H5-2
	Required data is not accessible	Data transactions will be unavailable to certain users.	a. Database failure b. Host failure	Refer to H5-1	IR3, IR4	H5-3
User Interface	Components and component data does not successfully render onto to UI component	User will miss vital cues, prompts, and information required to operate the app	Native libraries, components, and properties used on incompatible operating systems	The system should accommodate various operating systems and their versions. Animated components using native drivers need to be disabled on devices and OS versions that do not support them. The system should frequently check which OS platform the app is running on to ensure the use of OS specific UI elements.	PRR2, PRR3	H6-1

7 Safety and Security Requirements

7.1 Access Requirements

ACR1: The application must not display other users private details to the user.
Rationale: User data should be private and only visible to the user themself.

Associated Hazard: H2-1

ACR2: Only the developers and system administrators will be able to access all user details except their passwords.
Rationale: Developers require user details in order to accurately track and manage the application database.
Associated Hazard: H2-1

7.2 Integrity Requirements

IR1: Passwords must be encrypted with SHA-256 when stored.
Rationale: Password encryption increases user information security.
Associated Hazard: H2-1

IR2: User data will not be modified void of user permission.
Rationale: Users control the modifying of any and all user information.
Associated Hazard: H2-1

IR3: User data will be automatically backed up to the database upon connection to the internet.
Rationale: User data will be backed up to ensure databases correspond to local user information.
Associated Hazard: H4-1, H5-2, H5-3

IR4: User data transactions will be stored locally when user device is offline.
Rationale: User data will be stored locally to ensure that no data is lost when users are offline.
Associated Hazard: H4-1, H5-2, H5-3

IR5: Database will be backed up daily.
Rationale: Database will be backed up daily to ensure all information is safe and updated at all times.
Associated Hazard: H4-1, H5-1,

7.3 Privacy Requirements

PRR1: The application must use OAuth protocols to verify communication between the client and server.
Rationale: Application utilizes OAuth to ensure communication between client and server is accurate and corret.
Associated Hazard: H1-1, H3-1

PRR2: The application will ensure users are aware of data collection practices before collecting any data from them.
Rationale: Users will be made aware of data collection to ensure consent to all data collection practices.
Associated Hazard: H6-1

PRR3: The application will communicate any changes to the privacy policy with the users.
Rationale: Users will be notified of changes to privacy policies to ensure they are kept informed about all changes relating to their information.
Associated Hazard: H6-1

7.4 Audit Requirements

ADR1: Data will be stored in a secure database. When data is deleted or edited a record of this data will be kept for up to 30 days.
Rationale: Data records will be kept for 30 days to ensure deleted data can be referenced if needed after deletion.
Associated Hazard: H2-1, H5-1

7.5 Immunity Requirements

- N/A

8 Roadmap

Based on the safety requirements listed above, the table below displays which of the requirements are planned for the current timeline of the project and those that planned implementations for the future.

Planned	Future
ACR1	ADR1
ACR2	
IR1	
IR2	
IR3	
IR4	
IR5	
PRR1	
PR2	
PR3	