Hazard Analysis
REVITALIZE

Team 13, REVITALIZE
Bill Nguyen
Syed Bokhari
Hasan Kibria
Youssef Dahab
Logan Brown
Mahmoud Anklis

Table 1: Revision History

Date	**Developer(s)**	**Change**
October 15th, 2022	Bill Nguyen	FMEA
October 19th, 2022	Youssef Dahab	Introduction, Purpose, and Scope
October 19th, 2022	Logan Brown	System Boundary, Components, and Critical Assumptions

Contents

1 Introduction

This document is a hazard analysis of REVITALIZE.

1.1 Hazard Definition

As per Nancy Leveson's work, a hazard is a property or condition in a system together with a condition in the environment that has the potential to cause harm or damage. In REVITALIZE, there are safety (keeping records) and security (restricting access to data) hazards.

1.2 Other Used Terms in this Document

1.2.1 Failure

A failure in the REVITALIZE mobile application could occur when there is a deviation between the actual and expected output. Furthermore, a failure could also occur when a certain state causes REVITALIZE, or a component of REVITALIZE (login, database, etc.), to fail and therefore not achieve its necessary function.

1.2.2 Safety

REVITALIZE's safety is its freedom from harm. However, it's not an absolute. Safety is a global property of REVITALIZE. Therefore, when two or more REVITALIZE components interact together, the resulting emergent behaviour may or may not be safe.

2 Purpose of Hazard Analysis and Scope

Hence, the purpose of this document is to identify hazards pertaining to the REVITALIZE mobile application, and their causes, and then specify ways to eliminate them or mitigate their effect. The team cannot "bolt on" safety after implementing the application. Therefore, by identifying hazards and developing safety requirements before implementing, REVITALIZE team members will be able to react when their application fails to be safe. This becomes beneficial when something "bad" happens. The team will have a recovery plan.

The scope of this project is to create an all in one health and wellness mobile application that allows users to manage their diet, exercise, and sleep by providing them with meal recipe's based on their nutritional preferences, a personalized workouts planner and a sleep tracker.

3 System Boundaries and Components

3.1 System Boundaries

The system boundary can be outlined using the following elements of the system:

1. Main application (with the following subsystems)
    - Login/Authentication
    - Database
    - Backend server
    - Main calendar
    - Diet menu
    - Workout menu
    - Sleep menu
2. APIs
    - Recipe API
    - Workout tracker API
    - Google sleep tracker API
3. Android device (device app is installed on)

The system boundary includes the application as a whole, the APIs used for its function, and the Android device the app is installed onto. Some of these elements are outside the direct control of REVITALIZE, namely the APIs, server uptime, database uptime, and the Android device itself. However, they are important elements of the system that must be taken into account for proper hazard analysis of the system.

3.2 Components

The components of the system are outlined as followed:

3.2.1 Login/Authentication System

System that allows users to create an account, login, and have their credentials verified. Users can then access their data and modify health goals and plans.

3.2.2 Database

System that stores and organizes user health data. Data will be stored to the user's account and is accessible to any device that logs in with said account.

3.2.3 Server Backend

System that controls the flow of data between the APIs and the application.

3.2.4 Main Calendar Interface

System that displays current diet, workout, and sleep goals/plans for selected day. Users can select a desired day on the calendar and navigate to the diet, workout, and sleep interfaces which are used to modify user goals and plans.

3.2.5 Diet Section Interface

System that allows users to search and add recipes aligned with their dietary goals. The recipes chosen by the user are then added to the plan of the selected day. Previously planned recipes are stored for easy access in the future.

3.2.6 Workout Section Interface

System that allows users to add existing or custom workouts to the selected calendar day. Previous workouts are stored for easy access in the future.

3.2.7 Sleep Section Interface

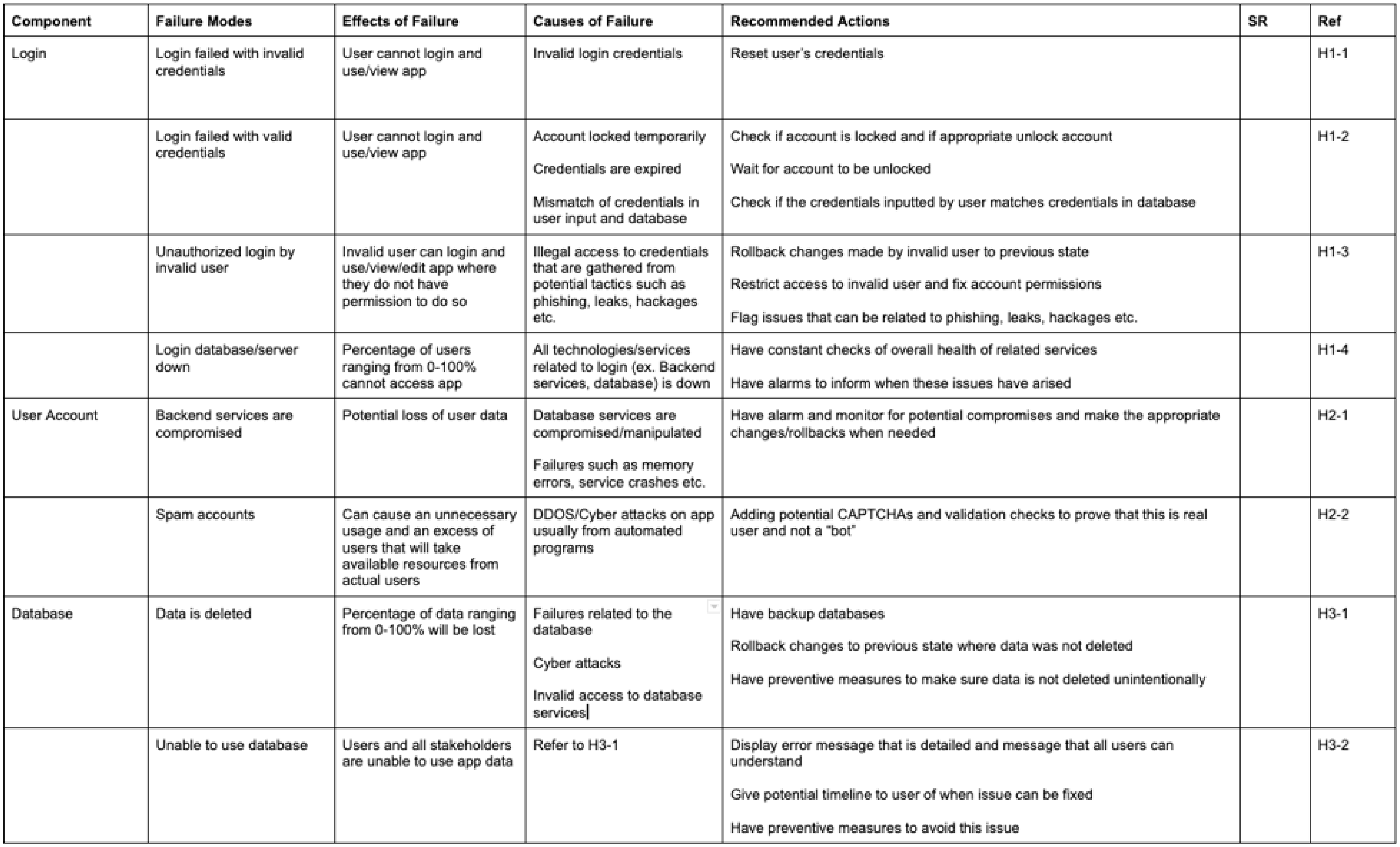
System that tracks and displays user sleep data. Also displays sleep/wake-up times based on user sleep goals and habits.

4 Critical Assumptions

1. Assume user is not intentionally acting in a malicious way
2. Assume user is not sharing username and password info with anyone else
3. Assume user's Android device is functioning properly
4. Assume user's Android device does not contain any vulnerabilities
5. Assume APIs are up and function properly
6. Assume APIs do not contain any vulnerabilities

5 Failure Mode and Effect Analysis

The next pages will show the full failure mode and effect analysis (FMEA) for REVITALIZE:



Component	Failure Modes	Effects of Failure	Causes of Failure	Recommended Actions	SR	Ref
Login	Login failed with invalid credentials	User cannot login and use/view app	Invalid login credentials	Reset user's credentials		H1-1
	Login failed with valid credentials	User cannot login and use/view app	Account locked temporarily Credentials are expired Mismatch of credentials in user input and database	Check if account is locked and if appropriate unlock account Wait for account to be unlocked Check if the credentials inputted by user matches credentials in database		H1-2
	Unauthorized login by invalid user	Invalid user can login and use/view/edit app where they do not have permission to do so	Illegal access to credentials that are gathered from potential tactics such as phishing, leaks, hackages etc.	Rollback changes made by invalid user to previous state Restrict access to invalid user and fix account permissions Flag issues that can be related to phishing, leaks, hackages etc.		H1-3
	Login database/server down	Percentage of users ranging from 0-100% cannot access app	All technologies/services related to login (ex. Backend services, database) is down	Have constant checks of overall health of related services Have alarms to inform when these issues have arised		H1-4
User Account	Backend services are compromised	Potential loss of user data	Database services are compromised/manipulated Failures such as memory errors, service crashes etc.	Have alarm and monitor for potential compromises and make the appropriate changes/rollbacks when needed		H2-1
	Spam accounts	Can cause an unnecessary usage and an excess of users that will take available resources from actual users	DDOS/Cyber attacks on app usually from automated programs	Adding potential CAPTCHAs and validation checks to prove that this is real user and not a "bot"		H2-2
Database	Data is deleted	Percentage of data ranging from 0-100% will be lost	Failures related to the database Cyber attacks Invalid access to database services	Have backup databases Rollback changes to previous state where data was not deleted Have preventive measures to make sure data is not deleted unintentionally		H3-1
	Unable to use database	Users and all stakeholders are unable to use app data	Refer to H3-1	Display error message that is detailed and message that all users can understand Give potential timeline to user of when issue can be fixed Have preventive measures to avoid this issue		H3-2

Figure 1: Part 1 of FMEA

6 Safety and Security Requirements

[Newly discovered requirements. These should also be added to the SRS. (A rationale design process how and why to fake it.) —SS]

7 Roadmap

[Which safety requirements will be implemented as part of the capstone timeline? Which requirements will be implemented in the future? —SS]