Hazard Analysis
SFWRENG 4G06

Team #12, Team 12.0
Kanugalawattage, Anton
Subedi, Dipendra
Rizkalla, Youssef
Leung, Tamas
Zhao, Zhiming

Table 1: Revision History

Date	**Developer(s)**	**Change**
3/30/2023	Anton Kanugalawattage Dipendra Subedi Youssef Rizkalla Tamas Leung Zhiming Zhao	Added additional hazards, failure modes and modified old failure modes. Rewrote in Latex. Fixed grammatical and spelling errors.
10/18/2022	Anton Kanugalawattage Dipendra Subedi Youssef Rizkalla Tamas Leung Zhiming Zhao	Initial Document

Contents

List of Tables

List of Figures

1 Introduction

To ensure the system that is being built is safe, unsafe behaviours must be identified. This document aims to identify potential hazards and describes the effects that they could have on the CodeChamp system. Additionally, requirements are specified to mitigate or prevent the identified hazards from occurring or negatively affecting the system.

2 Scope and Purpose of Hazard Analysis

A hazard is a property or condition in the system together with a condition in the environment that has the potential to cause harm or damage. The scope of a hazard analysis is to identify possible hazards from each component of the system, and the purpose of a hazard analysis is to document hazards, the cause and effect of each hazard and how to mitigate each hazard.

3 System Boundary

Hazard analysis will be conducted on the following components of CodeChamp:

1. Judge Server
2. Connected Communication
3. Database
4. Authentication
5. Deployment
6. Users

The system boundary includes five components of the application: the judge server, connected communication services, the database, authentication services and deployment services. The reliability of the database and deployment services in terms of up time is out of the control of CodeChamp but still play a role in ensuring appropriate storage and retrieval of data, so it is necessary to be included in the hazard analysis.

4 Definition of Hazard

The definition of a hazard used throughout this document is anything that poses a threat to the security, performance, or functionality of the CodeChamp web application.

5 Critical Assumptions

There are no critical assumptions being made.

6 Failure Modes & Effects Analysis Table

The Failure Modes and Effects Analysis model was chosen to identify and analyze the system's hazards as well as to define recommended actions and requirements to mitigate them.

6.1 Hazards Out Of Scope

These are hazards which are not managed directly the developers, so our system cannot be directly control them. In the case of such hazards, we can attempt to minimize their effects or work around them but cannot completely mitigate them. The out of scope hazards are as follows:

1. Deployment issues and outages by the cloud provider
2. Database provider outages
3. Failures of the external identity management system

6.2 Failure Modes and Effect Analysis Table

Component	Failure Modes	Effect of Failure	Causes of Failure	Recommended Action	SR	REF
Judge Server	Malicious Use of Server	Denial of Service	1. Execution of malicious user code 2. Failure to timeout code beyond specified time limit	Ensure that code is checked before compilation, similar to accounting for a SQL injection attack. Enforce a time and memory limit for each problem.	IR.3 & AR.2	HR1
Connected Communications	Loss of connections	Communication between server and clients are lost.	1. Unintentional server restart 2. Loss/out of memory	Backup states of the current connections to be used when restarting.	IR.4	HR2
Database	Data Deleted	All data is lost. No problems will be able to be sent to users. No profile information can be viewed	1. SQL injection attacks 2. Unintentional deletes	Maintain automatic backups and restore database to latest backup version.	IR.1 & IR.2	HR3
Database	Overload of database	Server requests will be slowed drastically	1. Too many requests	Automatic scaling of database	IR.5	HR4

Server	Server Outage	Denial of Service	1. DDoS Attack 2. Hardware Issues	Introducing load balancing and server redundancy to ensure one server having outages does not affect the entire platform.	IR.6	HR5
Server	Overload of server	Server requests will be slowed drastically	1. Too many client requests	1. Rate Limiting, which will only affect unusually high traffic. 2. Vertical scaling of servers.	IR.6 & IR.5	HR6
Authentication	Unauthenticated use of services	1. Services are used without an identity, preventing the system from logging events 2. Jeopardizes the integrity of the games the user participates in	1. Failure of the external Identify Management system 2. Failure of authentication middleware in the server	Safeguard the authentication middleware so that on failure all requests are rejected.	AR.1 & AR.2	HR7
Authentication	Failure to login to service	Users are unable to use service	1. Failure of the external Identify Management system 2. Failure of authentication middle ware in the server	Safeguard the authentication middleware so that on failure all requests are rejected.	AR.3	HR8
Users	Frustrated Users	Low engage-ability on the platform	1. Repetitive losses from users	System will adapt the difficulty of the game to the skill of the player, preventing enjoyable experiences	IR.7	HR8

Table 2: Failure Modes and Effects Analysis

7 Safety & Security Requirements

7.1 Access Requirements

AR.1 Users must be logged in to view data they are authorized to view.

AR.2 Only admins will be allowed to modify and add new problem data.

AR.3 Requests from unauthenticated users should be rejected.

7.2 Integrity Requirements

IR.1 Problem data will be automatically backed up on a weekly basis.

IR.2 User profile data will be automatically backed up on a daily basis.

IR.3 All problems must have a time and memory limit set.

IR.4 Backup connection state every minute to ensure connectivity on restart.

IR.5 Clients will be rate-limited on requests with unusually high traffic to the server.

IR.6 Connection and requests must be distributed evenly among servers.

IR.7 The application should not be detrimental to the user's mental health.

7.3 Privacy Requirements

PR.1 Users will not be able to access unauthorized data of other users.

7.4 Audit Requirements

N/A

7.5 Immunity Requirements

N/A

8 Roadmap

The hazard analysis has brought forward more requirements that will be implemented within the final application. The development team will try to implement all requirements based on priority, but may not be able to due to time constraints of the project. As the team approaches the end of the project, the hazard analysis will be revisited, to verify that the intended hazards were mitigated and to identify hazards which still persist or require additional work.