# Hazard Analysis

## Book Bazar

November 26, 2021

**Group 6**

| | |
|---|---|
| Caleb Mech | mechc2 |
| David Thompson | thompd10 |
| Matthew Williams | willim36 |
| Ahmed Al Koasmh | alkoasma |
| Harsh Mahajan | mahajanh |

# Contents

# List of Tables

# Table of Revisions

| Version | Date(dd.mm.yyy) | Author(s) | Description |
|---|---|---|---|
| 0 | 16.11.2021 | Harsh Mahajan | First version compiled. Inputs received from the entire team and LaTeX doc compiled. |
| 1 | 23.11.2021 | Harsh Mahajan | Edits made to match rubric and feedback from TA. |
| 2 | 26.11.2021 | David Thompson | Fixed some spelling, grammar, and formatting errors in the document. |

Table 1: Table of Revisions

# 1 Overview

The hazards for Book Bazar were identified by recognizing the vulnerabilities of Book Bazar that could be exploited by a malicious user. The causes of the events have been addressed by our mitigation strategies to either eliminate the hazard or to avoid it to the best of our capabilities. Our system is not a safety-critical system, yet it does possess some societal hazards, like the first hazard, that have been addressed.

Our system shall be authenticating users using their McMaster emails. As well, users may share their contact information with each other to buy or sell textbooks. In such scenarios, we've assumed the security of the systems that are providing the services. For example, when we authenticate users via their McMaster emails, we assume that the emails we send cannot be read by a third party.

Below are the hazards that we have identified and our means to mitigate them.

# 2 Book Bazar Hazards

## 2.1 Meeting Strangers to Buy Textbooks

### Explanation

Meeting unknown strangers, even though they're verified as McMaster community members, does possess a certain level of danger. A user with malicious intent may post a frequently needed textbook on Book Bazar at a steep discount. The low price may attract several university students. The malicious user may set up a meeting in a secluded area where the users, especially first-year students who aren't familiar with campus and the surrounding neighbourhoods, may be susceptible to robbery or assault.

### Cause of Event

This event occurs when there are malicious users using Book Bazar.

### Mitigation

Safety tips for meeting strangers via Book Bazar will be provided when a user makes a post to sell a textbook or contacts a seller. Tips may include links to awareness tools, like the McMaster Safety App, that could be used to improve safety. Furthermore, a means of reporting malicious users may be created if deemed necessary.

#### Safety Requirements

Section 11.9 of our System Requirements Rev0 document covers this hazard.

## 2.2 User's Password Gets Leaked

*Since we are no longer using a password-based system, we should rewrite this section*

## 2.3 User's Personal Information Gets Leaked

#### Explanation

Personal information may be valuable to attackers since contact information could be used to run scams. Furthermore, a collection of personal information could allow an attacker to imitate a user for personal gain. Lastly, an attacker could use the personal contact information of a user to harass the user.

#### Cause of Event

Misconfigured access levels to data or providing access to data without requiring authentication.

#### Mitigation

To mitigate leaking users' personal information, we will only store personal information required to operate Book Bazar, such as the user's McMaster email, their name, and photos of the textbooks that they intend to sell. Furthermore, we shall require users to sign in before viewing personal information related to textbook postings. This means that only individuals affiliated with McMaster may access the contact information of sellers.

#### Safety Requirements

*TODO*

## 2.4 Cross-Site Scripting (XSS)

#### Explanation

Cross-site scripting (often abbreviated as XSS) is a common form of arbitrary code execution that is prevalent in web applications. It allows an attacker to write JavaScript code in a textbox, then run this code on the computers of other users of the website. See `https://en.wikipedia.org/wiki/Cross-site_scripting` for more information.

#### Cause of Event

What follows is an example of an XSS attack. An attacker sets their name on Book Bazar to contain an HTML tag which contains JavaScript that mines cryptocurrency and deposits it in the attacker's cryptocurrency wallet. When a user views a textbook posting from the attacker, if the name set by the attacker is displayed, then the malicious script is loaded onto the user's computer, and their computer mines cryptocurrency for the attacker.

#### Mitigation

Input fields will be sanitized such that text with HTML or JavaScript content that is input into textboxes gets transformed into a form that, when displayed on another user's computer, will be interpreted as plain text instead of code or marked up text.

#### Safety Requirements

*TODO*

## 2.5 SQL Injection

### Explanation

An attacker performs an unauthorized SQL query through appending the query to one of the parameters of a service that interacts with the database. This query could compromise the integrity of the database, for instance, by erasing all the data. See `https://en.wikipedia.org/wiki/SQL_injection` for more information.

### Cause of Event

An attacker passes an SQL query to a service, and Book Bazar's server executes this SQL query.

### Mitigation

We will use an object-relational mapping library (ORM) to interact with the database. An ORM provides a layer of abstraction between the code that operates with data and the SQL calls. This way, developers don't need to write SQL queries directly, and instead interact with the database using object-oriented paradigms. This prevents making calls to the database that may contain SQL injections.

Another approach we shall take to mitigate the effects of an SQL injection is by creating backups of the database. If we detect that the integrity of the data has been compromised, then we can restore the backup of the database.

### Safety Requirements

*TODO*