

# Hazard Analysis

---

## Book Bazar

November 23, 2021

### Group 6

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

## Contents

<b>1</b>	<b>Overview</b>	<b>3</b>
<b>2</b>	<b>Meeting Strangers to Buy Textbooks</b>	<b>3</b>
<b>3</b>	<b>User’s Password Gets Leaked</b>	<b>4</b>
<b>4</b>	<b>User’s Personal Information Gets Leaked</b>	<b>4</b>
<b>5</b>	<b>Cross-Site Scripting (XSS)</b>	<b>4</b>
<b>6</b>	<b>SQL Injection</b>	<b>5</b>

## List of Tables

1	Table of Revisions . . . . .	3
---	------------------------------	---

## Table of Revisions

Version	Date(dd.mm.yyy)	Author(s)	Description
0	16.11.2021	Harsh Mahajan	First version compiled. Inputs recieved from the entire team and L <sup>A</sup> T <sub>E</sub> Xdoc compiled.
1	23.11.2021	Harsh Mahajan	Edits made to match rubric and feedback from TA.

Table 1: Table of Revisions

## 1 Overview

The hazards for Book Bazar were identify by recognising 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 soceital hazards, like the first hazard, that been addressed.

Our system shall be authenticating users using their McMaster emails and users may share thier contact information with each other to buy/sell a textbook. In such scenarios, we've assumed the security of the systems that are providing the services. For eg. we're assuming the security of McMaster issues emails when we authenticate users via their McMaster emails.

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

## 2 Meeting Strangers to Buy Textbooks

### Explanation

Meeting unkown strangers, even though they're verifed as McMaster community members, does posses a certain level of danger. A user with malicious intent may post a frequently needed textbook on Book Bazar at a steep discount. The lucrative price may attract several college students who always appreciate a steep discount. The malicious user may set up a meeting in a secluded area where the users, especially first-year students who aren't familiar with the neighbourhood, may be susceptible to robbery/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.

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

### 3 User's Password Gets Leaked

#### Explanation

Depending on how the user stores their password (written down or in a file on the computer), an attacker may attain the user's password through various means. Ergo, the attacker may impersonate the user on Book Bazar. A worst-case-scenario would be if the user uses the same password for multiple services and the attacker could now access all these other services using the user's password.

#### Cause of Event

One of the means via which the attacker may acquire a user's password is by accessing the database where the information regarding the password is stored. This could be done either via a remote connection or physically accessing the computer. Another means of acquiring the user's password would be via a man-in-the-middle attack, where some or all of the user's network communication is first routed to the attacker before reaching its intended destination. Lastly, an attacker may use a social engineering scheme to trick a user into providing the password to a service that may seem affiliated with Book Bazar but in-reality is completely separate.

#### Mitigation

We shall assume the security of the email provided by McMaster University. We will use the user's McMaster email to authenticate the user. Book Bazar shall work without storing the user's password or any information related to the password, like the hash of the password. This would ensure that, even if Book Bazar's database were to be compromised, the user's passwords may not be obtained. Furthermore, we shall ensure that any requests between the user and our servers will use HTTPS, preventing man-in-the-middle attacks.

Section 11.6 of our System Requirements Rev0 document covers this hazard.

### 4 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. Ergo, only individuals affiliated with McMaster may access the contact information of sellers.

### 5 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. See

[https://en.wikipedia.org/wiki/Cross-site\\_scripting](https://en.wikipedia.org/wiki/Cross-site_scripting) for more information.

### **Cause of Event**

An attacker sets their name on Book Bazaar 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, means that the malicious script is loaded onto their 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 will be interpreted as plain text instead of code or marked up text.

## **6 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](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**

Use an object-relational mapping library (ORM) to interact with the database. This shall provide 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, 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. So if we detect that the integrity of the database has been compromised, then we can restore the backup of the database.