CCS6344 T2410 Database & Cloud Security

Assignment 1

Title: Bookstore System with Security Measures Implementation

Tutor: Dr. Navaneethan

Group 9

	Name	Student ID
1.	NOR LIYANA NATASHA BINTI MUHAMMAD SYAFIQ CHELVAM	1211304656
2.	PARTHASARTHY A/L MOGANESVARAN	1211304155
3.	YEE JING CHI	1211305113

Links:

Youtube - https://youtu.be/XYc1v_Pqs4I

Task 1 Preparation of the proposal

Introduction:

In this assignment, we have proposed a bookstore system which enables users to purchase books online. A web application will be developed to be user friendly and secure from threats. We will implement security functions into the web application in order to protect the server and users from malicious attacks. A web application with weak security architecture or even no security protection is vulnerable to various attacks, especially injection attacks and man-in-the-middle attacks, causing the leakage of data information from the attacked web application. Therefore, we are trying to mitigate this problem while developing the web application.

Objectives:

1. To develop a user-friendly website which allows users to easily access books, read the details of each book and place order.
2. To create a safe environment for users to purchase books via online website implemented.
3. To apply various security practices in website development.
4. To secure the database using traditional database system.

Hardware and Software Implementation:

1. Processor: Quad-core or higher, with a clock speed of 2.5 GHz or above.
2. Storage: A solid-state drive (SSD) with a minimum of 256 GB for faster data access or change to traditional HDD (Hard Disk Drive) if SSD is not available.
3. RAM: 8GB DDR4 or higher will be efficient for multitasking and handling multiple requests at once.
4. Software Application: Visual Studio Code
5. Programming Language: Python & HTML
6. Database Implementation: All of the data will be stored in a MySQL database managed through a MySQL server and maintained using MySQL Workbench.

These specifications are meant to offer a flexible and adaptable server architecture that can

meet the needs of the website application. To ensure the server's ongoing performance and availability, regular monitoring and maintenance procedures will also be put in place.

System and Database Design Overview:

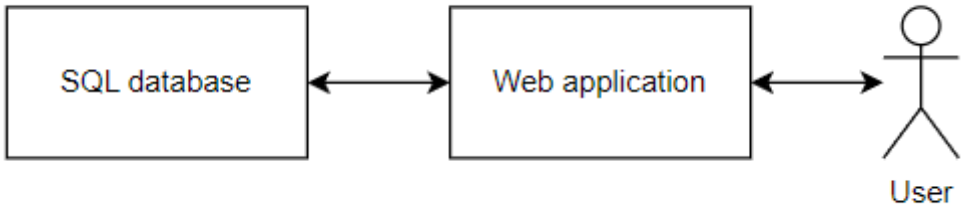


Figure 1 System Architecture Overview

Attribute Name	Data Type	Format	PK / FK	Description
bookID	varchar(255)	XXXXX	**PK**	Book ID number.
bookTitle	varchar(255)	XXXXX		Title of book.
bookAuthor	varchar(255)	XXXXX		Author of book.
bookPrice	decimal(5,2)	XXX.XX		Price of book sold.
bookCategories	varchar(255)	XXXXX		Category of book.
bookOriginalPrice	decimal(5,2)	XXX.XX		Original price of book.
bookDescription	text	XXXXX		Brief introduction of book.

Table 1 Example of Database Design

Implementation of Security Measures:

1. Authentication and Authorization
2. Password hashing
3. Data masking
4. Backup
5. Firewall and Network Security

Task 2 Implementation of the application using SQL Database

The "Online Bookstore System" is a web-based application designed exclusively for users to browse, purchase, and manage books online. Figure 2.1 below shows the user interface diagram of the online book store system.

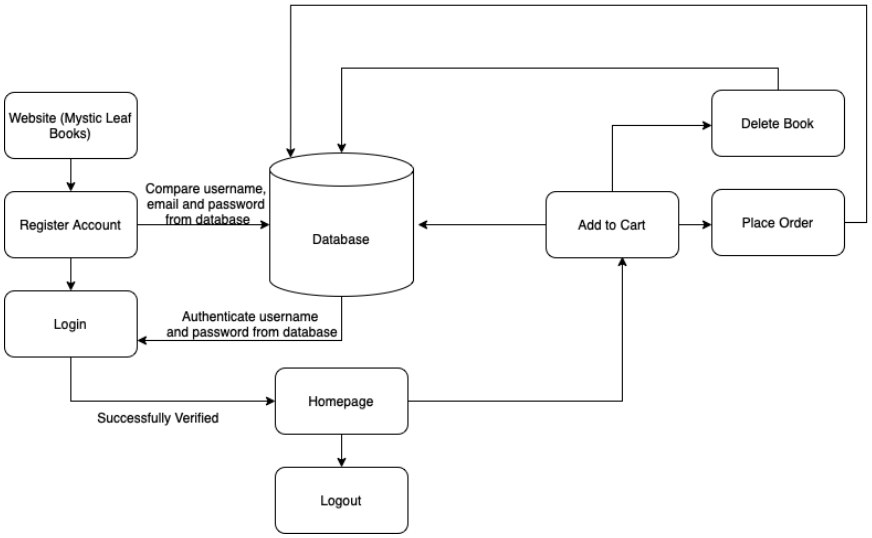


Figure 2.1 User interface diagram of the Online Book Store system.

Entity Relationship Diagrams (ERDs) are essential tools in database design and architecture. An ERD offers a visual illustration of the data model of a system and visually represents the relationships between entities, such as tables in a relational database, within a system. These diagrams are crucial for comprehending and conveying the organisation and architecture of a database, particularly prior to its actual implementation. Figure 2.2 below represents the ERD diagram of the Online Book Store system.

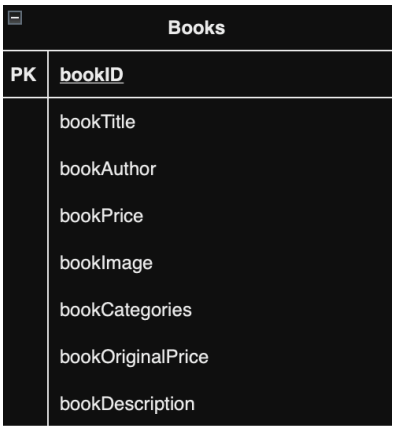


Figure 2.2 ERD diagram of the Online Book Store system.

The ERD above includes the following elements:

Entities:

- bookID: A unique identifier for each book and primary key(PK) of the table.
- bookAuthor: The author of the book.

- bookPrice: The cost of the product after discount.
- bookImage: The image of the book cover.
- bookCategories: The category or type of the book.
- bookOriginalPrice: The book's original price, before discount.
- bookDescription: The description of the book.

Implementation:

- Language used:
    1. Python: Backend logic.
    2. Flask: As the web framework.
    3. HTML: Frontend design
- Database:
    1. MySQL: For storing and managing data.

Functional Requirements:

- Register account: New users can create a new account by providing details such as username, email and password. Figure 2.3 below shows the registration page.

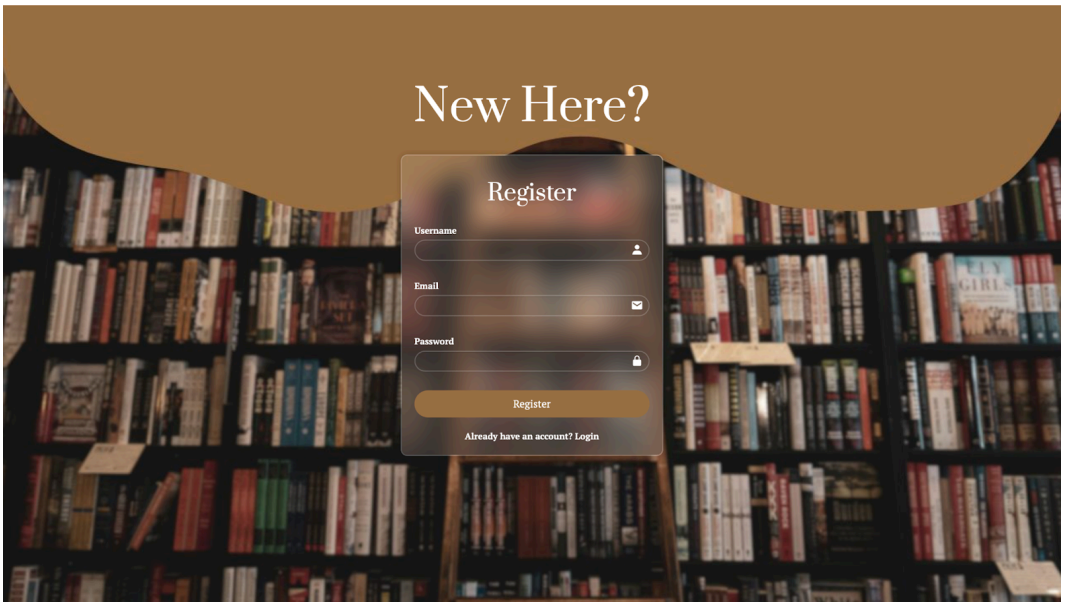


Figure 2.3 Registration page of the Online Book Store system.

- Login: Existing users can log in to their account by entering their username and password. Figure 2.4 below shows the login page.

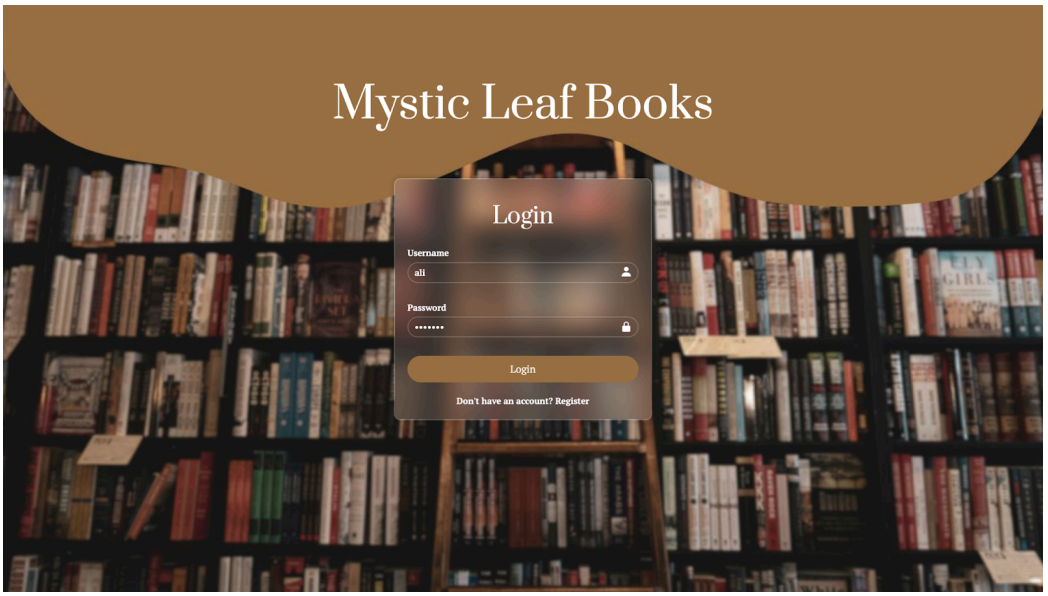


Figure 2.4 Login page of the Online Book Store system.

- Logout: Logged in users can log out of their account. Figure 2.5 below shows the logout button being highlighted at the homepage.

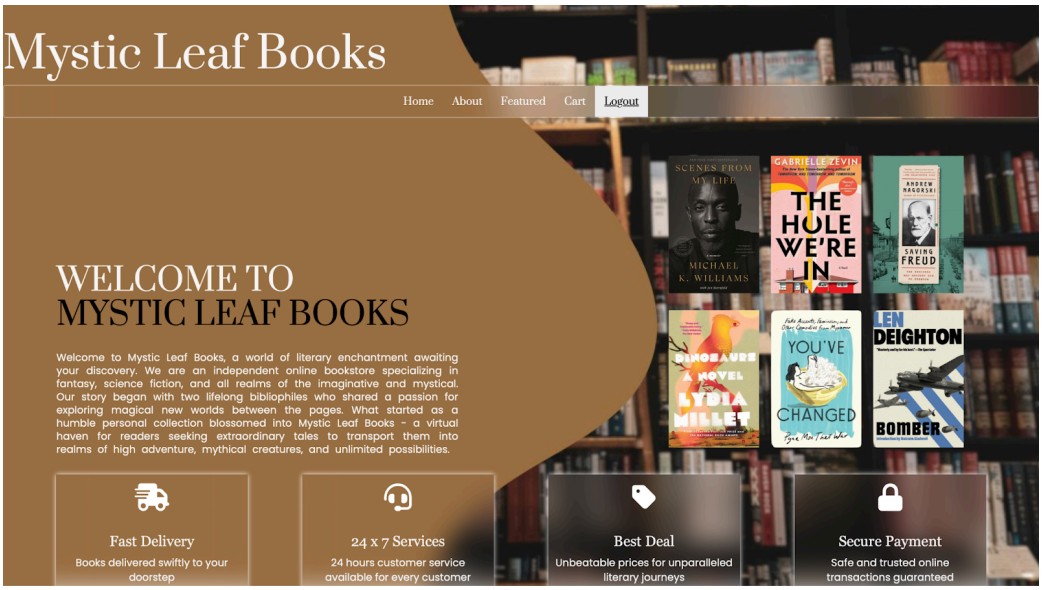


Figure 2.5 Highlighted logout button at the homepage of the Online Book Store system.

- View books with details: Users can browse and view detailed information about each book. Figure 2.6 below shows the book details of the book selected.

Figure 2.6 Book details of the book selected.

- Add books to cart: Users can add books to cart. Figure 2.7 below shows the books being added to the shopping cart.

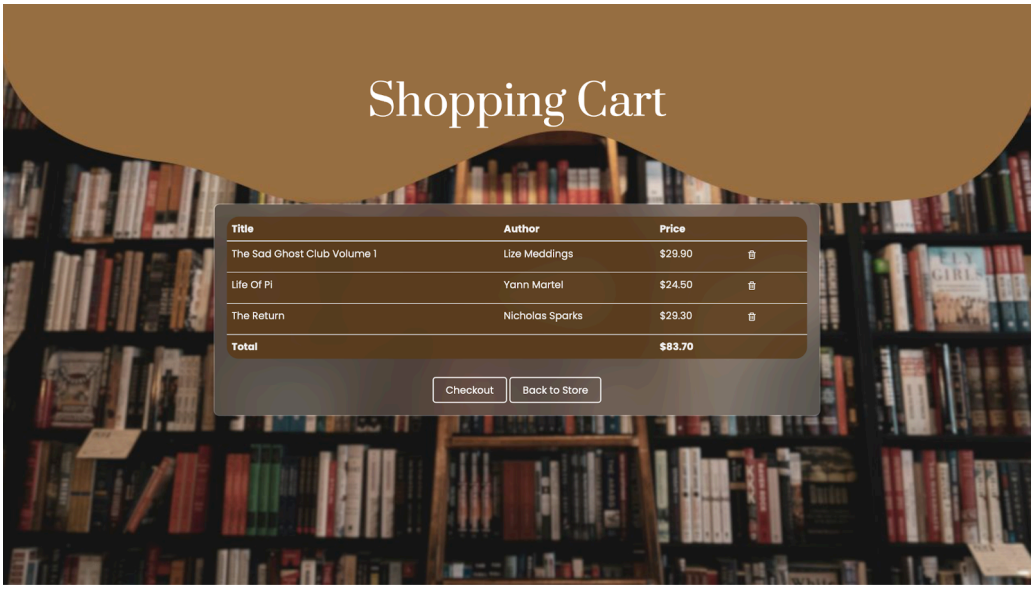


Figure 2.7 Books added to the shopping cart of the Online Book Store system.

- Remove books: Users can remove books from their cart. Figure 2.8 below shows the books being removed from the shopping cart.

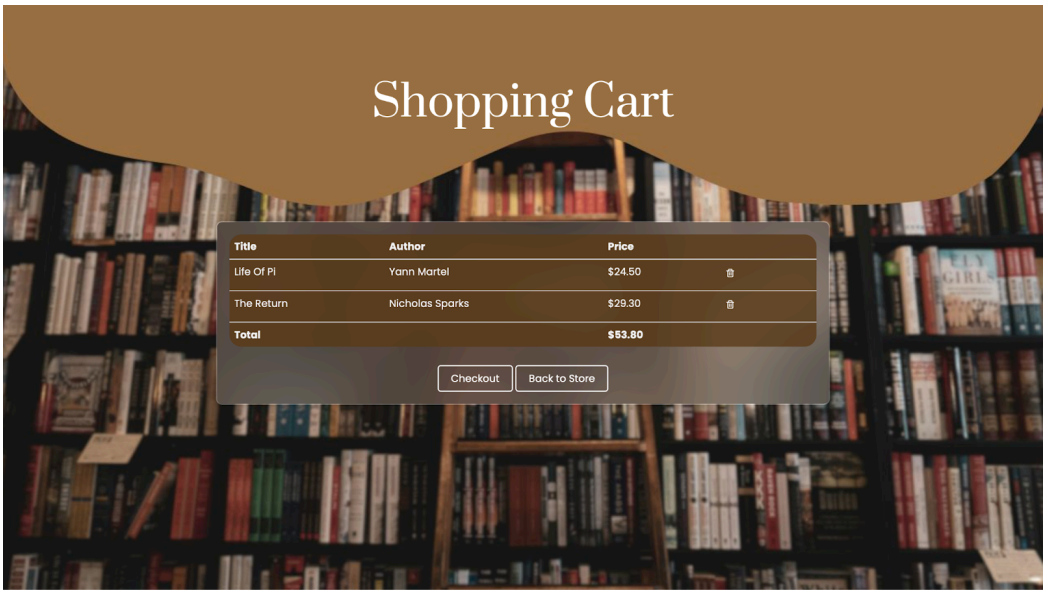


Figure 2.8 Books removed to the shopping cart of the Online Book Store system.

- Place order: Users can place orders for books by pressing the checkout button. Figure 2.9 below shows the checkout button being highlighted.

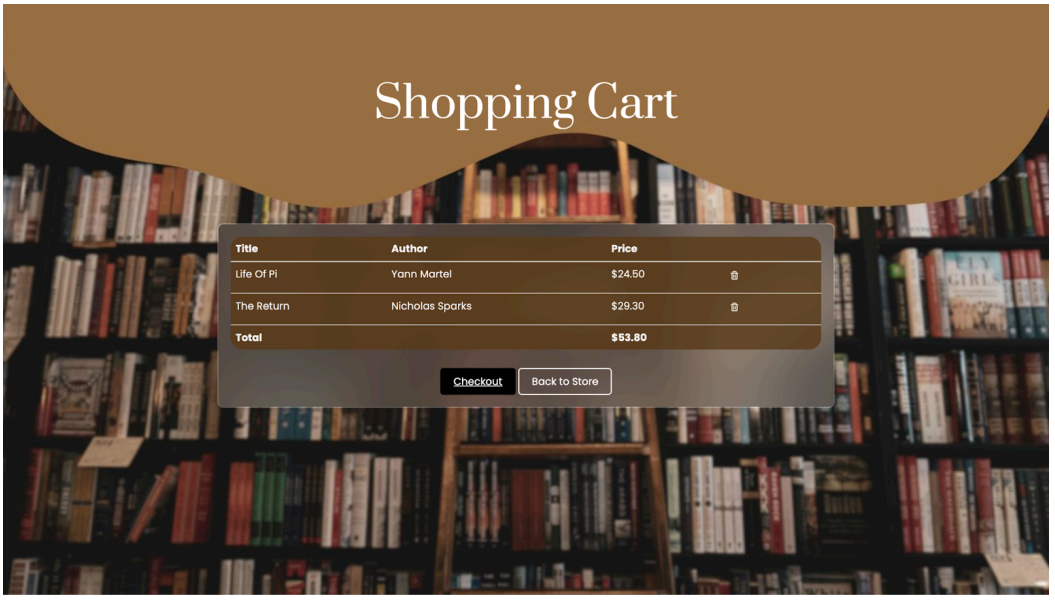


Figure 2.9 Highlighted checkout button at the shopping cart of the Online Book Store system.

Task 3 Threat Modeling

The implementation of threat modelling methodologies on our Book Store system will be elaborated upon in this section. The STRIDE and DREAD frameworks will be applied in order to evaluate potential security threats and ascertain suitable countermeasures.

a. STRIDE Threat Analysis

The STRIDE model helps us to categorise and understand the types of security threats our application may face. Each letter in STRIDE stands for a different threat category:

Spoofing (S): This involves an attacker impersonating another user or device to gain unauthorised access to the system.

Tampering (T): This threat involves the unauthorised modification of data.

Repudiation (R): This refers to the ability of users (or attackers) to deny their actions within the system.

Information Disclosure (I): This occurs when sensitive information is exposed to unauthorised parties.

Denial of Service (D): This threat aims to disrupt the service, making it unavailable to legitimate users.

Elevation of Privilege (E): This involves an attacker gaining higher access levels than initially granted, potentially leading to full system control.

b. DREAD Risk Assessment

The DREAD model is used to evaluate the severity of the threats identified by STRIDE. It assesses five different criteria:

Damage Potential (D): How much harm could the threat cause?

Reproducibility (R): How easily can the threat be replicated?

Exploitability (E): How easy is it to exploit the vulnerability?

Affected Users (A): How many users could be impacted?

Discoverability (D): How easy is it for the threat to be discovered?

By evaluating every risk according to these criteria, we can rank them depending on their potential influence on the system. Table 2 below shows the structured evaluation of potential security threats to the Bookstore system using the DREAD threat modelling framework.

Threat Category	D	R	E	A	D	Threat Rating
Spoofing	7	6	5	4	5	5
Tampering	8	7	6	5	6	6
Repudiation	5	4	3	2	4	3
Information Disclosure	9	8	7	9	8	8
Denial of Service	7	6	5	8	6	6
Elevation of Privilege	8	7	6	4	5	6

Table 2 Evaluation of potential security threats of the Book Store system using DREAD.

Table 3 below outlines the threat categories, their respective threat ratings, and suggested countermeasures for the Bookstore system:

Threat Category	Threat Rating	Countermeasures
Spoofing	5	Implement multi-factor authentication and secure session management to prevent identity spoofing.
Tampering	6	Use encryption for data at rest and in transit, and employ checksums or hashing for data integrity.
Repudiation	3	Enable detailed logging and auditing features to track user actions and changes to data.
Information Disclosure	8	Apply strict access controls and encryption to protect sensitive data from unauthorised access.
Denial of Service	6	Deploy rate limiting, DDoS protection, and redundant system design to ensure service availability.
Elevation of Privilege	6	Enforce the principle of least privilege and conduct regular access reviews and system audits.

Table 3 Countermeasures for identified risks.

Task 4 PDPA 2010

a) Categorisation of the personnel according to the categorization of the PDPA2010.

Category	Responsibility	Responsible Personnel
Data User	Ensure personal data is processed according to PDPA principles by obtaining consent, implementing adequate security measures, maintaining accuracy and relevance, and allowing data subjects to access and correct their data.	● Database Administrators ● Customer Service Representatives ● Marketing Team ● Bookstore Management and IT Team
Data Processor	Process data only as instructed by the Data User, implement appropriate technical and organisational measures to protect personal data, and assist the Data User in complying with data protection obligations.	● Cloud Service Provider ● Payment Gateway Provider ● Data Analysis Service ● Website Hosting Provider
Data Subject	Have the right to be informed about data collection and use, access their data, correct inaccuracies, withdraw consent, and request data deletion.	● Customers ● Employees ● Suppliers
Data Controller	Oversees the processing of personal data by determining its purposes and means, ensuring compliance with data protection laws, implementing policies for data handling, assigning roles, and monitoring activities to uphold data protection principles.	● Compliance Officer ● Dedicated Data Protection Officer (DPO): ● Legal Advisor ● IT Manager ● Database Administrator

Table 4

b) For each stage of your company's data lifecycle, map it to the requirements of the PDPA2010, how you will achieve compliance and the personnel who will oversee compliance. Also state the penalties for non-compliance accordingly.

1. **Data collection**

   PDPA2010 Requirements:

   Users are notified with the reason for data collection; Users' consent must be received and only necessary data information is collected.

Penalties for Non-Compliance:

Fines and/or imprisonment are the penalties for unauthorised data collection or personal data processing under PDPA 2010 (vary depending on the nature and severity of the breach).

2. **Data Storage**

PDPA2010 Requirements:

Companies are required to take reasonable precautions to guard against unauthorised access to, damage, or disposal of personal data.

Penalties for Non-Compliance:

Violations of the PDPA2010's data storage requirements could end up in fines and/or prison sentences.

3. **Data Processing**

PDPA2010 Requirements:

All the personal data collected must be processed legally, and the processing steps should be restricted to align with the reason for collection.

Penalties for Non-Compliance:

Fines and/or imprisonment for unauthorised access, processing or disclosure of user's personal data, under the PDPA2010 rules.

4. **Database Security Implementation**

PDPA2010 Requirements:

Relevant database security practices are implemented to safeguard the stored data, which involve encryption, access control, and regular security audits.

Penalties for Non-Compliance:

Fines and/or imprisonment for failure to secure personal data stored in the database.

5. ***Data Sharing***

PDPA2010 Requirements:

It is a must to get individuals' agreement before revealing their personal information to third parties.

Penalties for Non-Compliance:

Penalties and/or prison sentences for failing to fulfil the requirements of data sharing, according to PDPA2010.

6. **Data Disposal**

   PDPA2010 Requirements:

   Personal data should be securely disposed of when it's no longer needed; Users must be informed about the data retention policies.

   Penalties for Non-Compliance:

   Penalties and/or prison sentences for failure to follow its requirements in data sharing.

7. **Monitoring and Auditing:**

   PDPA2010 Requirements:

   Regular monitoring and auditing of data processing activities to ensure compliance and to identify and resolve security breaches.

   Penalties for Non-Compliance:

   Fines and/or imprisonment for failure to monitor or audit data processing activities.

Task 5 Security Measures Implementation

Securing the database is very crucial to protect it from internal and external threats. Therefore several security measures have been implemented in order to safeguard the data and at the same time help ensure that the database remains secure and reliable.

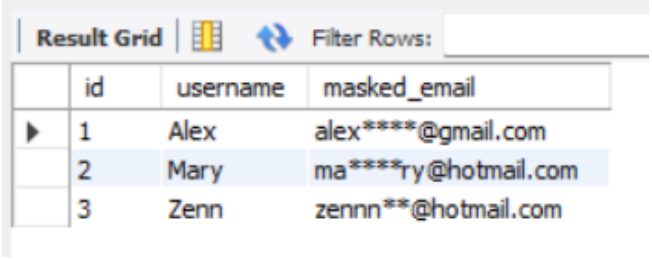
Security measure implemented on the database:

1. **User Login Authentication and Authorization**

   Implemented a user login authentication and authorization system for the application using email and password credentials. This system ensures that only authenticated users can access the application, and it also provides different levels of access based on user roles. The authentication process involves validating user credentials against stored data, while the authorization process determines the user's access rights within the application. The role-based access control ensures that users only have access to resources appropriate to their role, enhancing the overall security and integrity of the application.

2. **Data masking**

Data masking as a technique employed to safeguard information in a database by obscuring or altering original data. Data masking is particularly valuable in non-production environments for secure development and testing, allowing realistic datasets without exposing actual sensitive information.

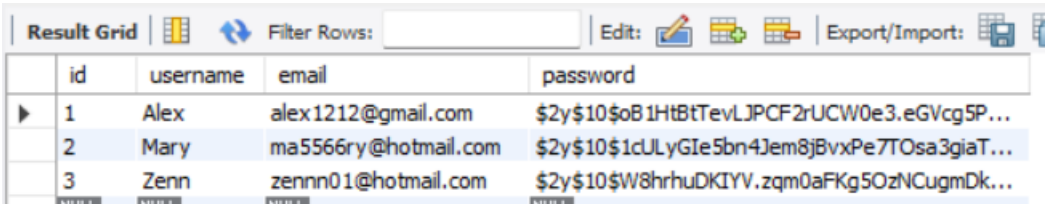


Result Grid | Filter Rows:

id	username	masked_email
1	Alex	alex****@gmail.com
2	Mary	ma****ry@hotmail.com
3	Zenn	zennn**@hotmail.com

3. **Password hashing**

The implemented security measure involves password hashing which by creating the password_hash function, to protect user's credentials stored in the database. Password hashing ensures that even in the event of a data breach, plain-text passwords remain undisclosed, adding a crucial layer of security.

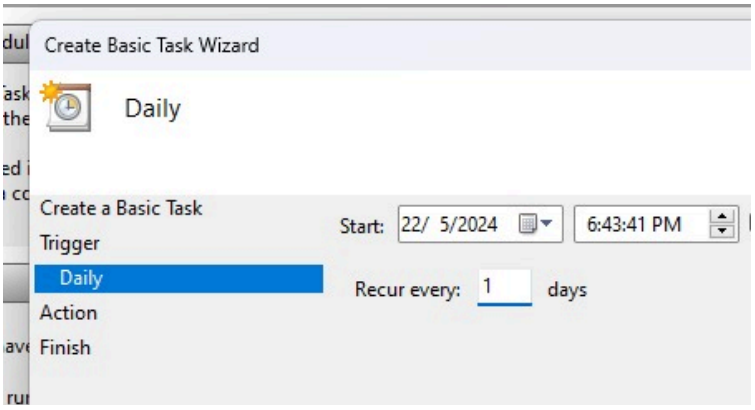


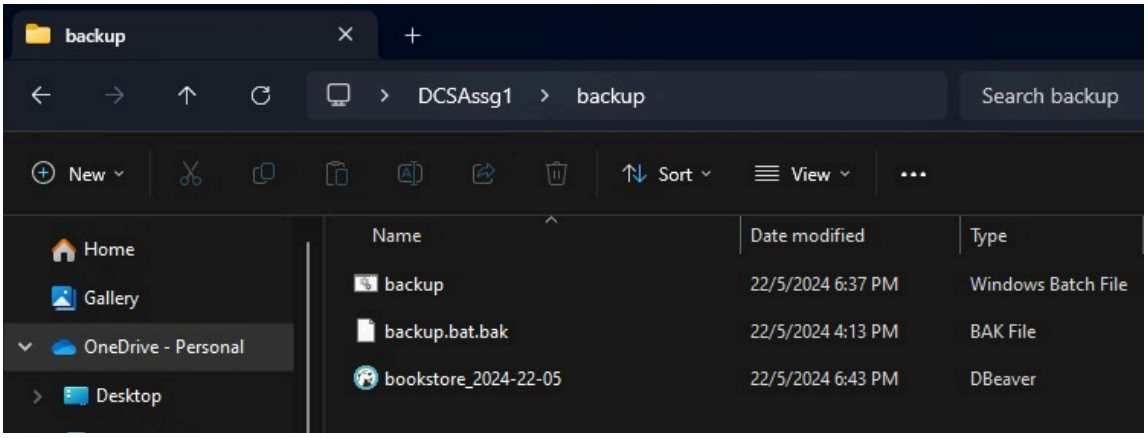
Result Grid | Filter Rows: | Edit: | Export/Import:

id	username	email	password
1	Alex	alex1212@gmail.com	$2y$10$oB1HtBtTevLJPCF2rUCW0e3.eGVcg5P...
2	Mary	ma5566ry@hotmail.com	$2y$10$1cULyGIe5bn4Jem8jBvxPe7TOsa3giaT...
3	Zenn	zennn01@hotmail.com	$2y$10$W8hrhuDKIYV.zqm0aFKg5OzNCugmDk...

4. **Backup and Recovery**

An automated backup system was implemented for the bookstore database using a batch file and Windows Task Scheduler. The batch file uses the mysqldump utility to create a backup of the specified database and saves it to a designated directory. The batch file also includes a mechanism to delete backups older than seven days, ensuring that storage space is managed effectively. The backup process is scheduled to run daily at a specified time "6.43pm" using Windows Task Scheduler. This setup ensures that the bookstore database is backed up daily without manual intervention, providing data redundancy and protection against data loss.





5. **Firewall and Network Security**

Configured Windows Firewall to enhance the network security of our MySQL database server by allowing connections only from specific IP addresses and blocking all other traffic. This was done by creating custom inbound firewall rules that specify the allowed IP addresses and block unwanted ones from accessing the MySQL server on port 3306. These firewall rules protect the MySQL server by ensuring that only authorised IP addresses can connect, reducing the risk of unauthorised access and potential attacks. Moreover, this layer of security helps safeguard sensitive data and maintain the integrity and availability of the database.