A logo for a university

Description automatically generated

CCS6344 T2430 Assignment 1

Inventory Management System and User Authentication System

Grp: 10

|  |  |
| --- | --- |
| NAME | ID |
| Pang Ding Yuan | 1211102575 |
| Fam Yi Qi | 1211101198 |
| SAMUEL YOONG WEN JUN | 1191201810 |

(points can be change later after system have been develop)

# Objectives of the project

**Inventory Management System (IMS):**

* To design and implement a web-based application that enables efficient management of inventory by tracking products, stock levels, and inventory transactions in real time.
* To provide an intuitive user interface that allows users to easily add, update, and manage products, categories, and suppliers, as well as monitor inventory movement through transactions.
* To generate automated reports for inventory analysis, helping businesses make informed decisions regarding stock levels, ordering, and supplier management.
* Provide real-time stock level alerts when inventory falls below reorder thresholds.

**User Authentication System:**

* To develop a secure user authentication mechanism that ensures only authorized users can access the IMS application, with support for different roles (e.g., admin, manager, employee).
* To implement secure login procedures, including encrypted password storage, multi-factor authentication (MFA), and user role-based access control (RBAC) to protect sensitive data and restrict access to certain functionalities based on user roles.

**Database Security:**

* To ensure the integrity and security of the underlying SQL database by implementing measures such as prepared statements to prevent SQL injection attacks, data encryption for sensitive information, and regular backups to ensure data recovery in case of failures.
* To design the database schema with tables for users, products, categories, suppliers, and inventory transactions, ensuring proper relationships and normalization to maintain data consistency and reduce redundancy.

# Design and Implementation

* **User Authentication System Design:** A secure login system with multi-factor authentication (MFA), user roles (admin, manager, employee), password hashing, and account lockout mechanisms to protect against brute-force attacks.

# Hardware and Software

## Programming Language and Database Program

HTML, CSS, and JavaScript for the front end. MSSQL for database.

## Server OS and Webserver

Windows Server 2019 for the server OS.

# System Design and Database Design

The system will consist of a web-based user interface and an SQL database. The database schema will include tables for users, products, categories, suppliers and inventory transactions.

# Security Measures

# Instance Level Security: Server Roles

# Assign appropriate roles

* Manager: Access to inventory management, order processing
* Employee: Limited access to view inventory and orders

# Implement SQL Server Audit

* Log failed login attempts to detect brute-force attacks.

# Ownership Chaining

* Ensure that stored procedures and views have consistent ownership to prevent unauthorized access.

# Row-Level Security

* Restrict access to data based on user roles

# Dynamic Data Masking

* Mask sensitive data

# Encrypting Data

* Encrypt sensitive data

# Transparent Data Encryption (TDE) / Always Encrypted

* Enable TDE to encrypt the entire database at rest
* Encrypt both data at rest and in transit

# Protect the sa account

* Rename the sa account

# Protecting Against Hijacking

* Implement a trigger to prevent unauthorized users from gaining privileges.

# Backup

* Perform regular backups of the database

# Backup Encrypt

* Encrypt database backups to protect them from unauthorized access.

# Protecting Against Code Injection – Policy-based Management

* + 1. Condition
    2. Policy