## TITLE:

# Security Features of Semester Project

**Student Name:**

**Urwah Rasheed**

**Registration No:**

**03-3-1-055-2022**

**Subject:**

**Internet Application Development**

**Submitted to:**

**Mr. Irfan Hameed**

**Submitted Date:**

**May 13, 2025**

# Problem 1

**What are the necessary security features of your semester project? After identifying the security features of your project, prepare a list of at least 07 security features and write a brief description about each of them?**

## Solution:

Security is one of the most critical aspects of any data-driven web application, especially when handling sensitive information such as customer details, product inventory, and order transactions. In my Supply Chain Management System project, I have carefully integrated several security features to ensure that the data is protected, users are properly authenticated, and unauthorized access is prevented.

Here are key security features I have implemented in the project:

### 1. Role-Based Access Control (RBAC)

This feature ensures that users can only access the pages meant for their role. In my system, the Admin has access to customer management, product management, and order overview pages, whereas a Customer can only place orders and view available products. If a user tries to access a page outside their role, they are redirected or shown an error. This separation helps prevent misuse of the system.

### 2. Input Validation

All input fields in the system—whether it's a registration form, login form, or order form—are validated both on the client side (using JavaScript) and server side (using VB.NET). This prevents users from submitting incomplete, invalid, or harmful data, reducing the chances of errors or security breaches.

### 3. SQL Injection Protection

To prevent SQL injection attacks, I have avoided raw queries and used parameterized queries with AddWithValue() when interacting with the SQL Server database. This means that user inputs are treated strictly as data and not executable commands, which keeps the database safe from manipulation.

### 4. Session Management

Each time a user logs in, a session is created. Pages like dashboards and management panels can only be accessed if the session is valid. If a session expires or the user logs out, they cannot access these pages by simply typing the URL. This helps ensure that only active, authenticated users can view protected content.

### 5. Secure Data Transmission (HTTPS Ready)

Although my database is hosted locally during development, the system is ready to be deployed under HTTPS. This will ensure that all data exchanged between users, and the server is encrypted and safe from eavesdropping when deployed on a secure web hosting platform.

### 6. Form-Based Authentication

Admin credentials are hardcoded into the system for secure and controlled access, while customer credentials are stored securely in the database. Only users with valid credentials are allowed to log in. If incorrect credentials are entered, the system displays a meaningful error without exposing any backend information.

### 7. Error Handling and Custom Messages

To avoid leaking system information, all exceptions are caught using Try...Catch blocks. Instead of showing technical error messages, the system displays user-friendly messages and logs the actual error (if needed) for the admin to review. This protects internal details from being exposed to potential attackers.

These security features collectively make my Supply Chain Management System safer and more reliable. They help protect both the business and the customers by ensuring that only verified users can interact with the system and that sensitive data remains secure.