PROBLEM 1

Problem Statement:

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?

Security Features of Semester Project – Movie Rental System

Below is a list of **seven key security features** that are essential for the Movie Rental System along with their brief descriptions.

---

1. Input Validation

All user inputs, including text fields for Customer ID, Name, Contact, and Address, must be properly validated both on the client side and server side. This prevents common attacks such as **SQL injection** and **Cross-Site Scripting (XSS)**. Proper input validation ensures that only the expected data is processed by the application.

---

2. Authentication

The system supports role-based authentication, allowing **customers** and **staff** to log in separately. Secure authentication requires verifying user credentials against a database. Implementing secure login methods such as **password protection** and limiting login attempts helps prevent unauthorized access.

---

3. Session Management

Once a user logs in, a secure session should be established to track their activity. Session timeouts should be set to automatically log out inactive users after a specified period. This helps protect against **session hijacking** and **unauthorized usage** of the system.

---

4. Authorization

The system uses panels to control access based on user roles. Customers can only access their rental and payment options, while staff can manage movies and rental records. This ensures that users are only allowed to access features they are authorized for, preventing **privilege escalation**.

---

5. Password Encryption

While not shown in the front-end code, storing user passwords in **plain text** is highly insecure. Passwords should be stored using strong hashing algorithms such as **SHA-256** or **bcrypt**, with added **salting**. This ensures password protection even if the database is compromised.

6. Secure Navigation & Redirection

The use of PostBackUrl must be handled carefully. Redirects should be validated to prevent **open redirect** vulnerabilities, which can redirect users to malicious websites. All internal navigation should be secured and verified before executing any redirection.

7. Safe Error Handling and Status Messaging

Error messages displayed to the user through labels like lblCustomerStatus and lblRegisterStatus should be generic and should not expose internal system details such as SQL queries or stack traces. This prevents attackers from gaining insights into the system's structure.