1. Password Hashing (SHA-256)

- **Description**: The user's password is stored in the database in an encrypted form (SHA-256) rather than in plain text.
- **Benefit**: In case of a database breach, the risk of password leakage is minimized.

2. Account Locking After Multiple Failed Login Attempts

- **Description**: If a user enters incorrect passwords multiple times, their account is temporarily locked.
- **Benefit**: Prevents brute force attacks, where attackers try to guess the password repeatedly.

3. Session Management

- **Description**: After login, session variables like "UserID" and "Role" are set and verified on each page request.
- **Benefit**: Prevents session hijacking and ensures every request is made by a valid user.

4. Role-Based Access Control

- **Description**: Users are assigned different roles (e.g., Admin, Customer), and each role is granted access to specific pages and actions.
- **Benefit**: Ensures that unauthorized users do not gain access to sensitive pages (e.g., Admin Dashboard).

5. Input Validation

- **Description**: User inputs are validated (e.g., Required Field Validators, Email format, etc.) to prevent invalid or malicious data.
- **Benefit**: Protects against XSS (Cross-Site Scripting) and SQL Injection attacks.

6. Session Timeout

- **Description**: If a user remains inactive for a certain period, the session expires, and they are required to log in again.
- **Benefit**: Prevents unauthorized access in case the user leaves their session unattended.

7. SQL Injection Prevention

- **Description**: User inputs in SQL queries are handled using parameterized queries, preventing the injection of malicious SQL code.
- **Benefit**: Protects against SQL Injection attacks that can corrupt or steal data from the database.