Pakistan Institute of Engineering and Applied Sciences

INTERNET APPLICATION DEVELOPMENT (IAD)

LAB_13

SEMESTER PROJECT REPORT
(SECURITY FEATURES)

NAME: HAFSA

DEPARTMENT: CIS (22-26)

Security Features Implementation Report

Project Name: Grocery Store Management System

1. Authentication

Authentication is used to verify a user's identity through login credentials.

Implementation:

A login page is created for different roles (Supplier, Customer). Valid username and password are required to access dashboards. Credentials are checked from the database using SQL queries. If a match is found, the user is redirected to their respective dashboard. An error message is displayed if authentication failed.

2. Authorization

Authorization is used to control access to pages based on user roles.

Implementation:

After login, the user's role is stored in a session variable. Redirection is performed based on the user's role to ensure only authorized users could access them. Unauthorized users are redirected to the login page.

3. Input Validation

Input validation is used to ensure that the data entered by users is valid and safe.

Implementation:

Validation was performed on the server side for form fields. In registration page Validation is also implemented on:

1. Name
2. Email

In Name field only alphabets and spaces are allowed. In Email field standard mail format is implemented.

4. Password Hashing

Password hashing is used to convert the original password into an unreadable format for secure storage.

Implementation:

The SHA256 algorithm is used to hash the password before storing it. The hashed password is saved in the database instead of the plain text password. During login, the entered password is hashed and compared to the stored hash. Authentication is performed only if the hashes matched.

5. Session State Management

Session state is used to store user information during a user's visit to the website.

Implementation:

Session variables are created after successful login to store username and role. After authentication, the user's email and role are saved in session variables (Session("email") and Session("role")).These session variables are then accessed on each page to verify the user's identity and role. Redirection to the appropriate dashboard is performed based on the role stored in the session.

6. Secure Redirection

Secure redirection is used to make sure users are sent only to pages they are allowed to access.

Implementation:

Session values were checked on every restricted page. If a session was missing or invalid, the user was redirected to the login page. This prevented users from directly accessing dashboard URLs without logging in.

7. Session State Timeout:

Session Timeout is a security feature where a user's session is automatically ended after a certain period of inactivity. This helps in protecting user accounts and sensitive data.

Implementation:

A timeout value is defined in the Web.config file of the ASP.NET project.
<sessionState timeout="20" />
As a result, the session is configured to expire after 20 minutes of user inactivity.