**Student Name**: Syed Hassan Raza
**Registration Number**: 03-3-1-052-2022
**Project Title**: Online Tutoring Platform
**Submission**: Lab 13
**Submission Date**: 13th May 2025

### Problem 1: Security Features for Semester Project

#### Security Feature 1: User Authentication

#### The system verifies the identity of users through a secure login mechanism. Only users with valid credentials (username/password) can access the application. Passwords are stored securely in the database.

#### Security Feature 2: Role-Based Access Control (RBAC)

The system assigns roles to users (e.g., Admin, Tutor, Student). Each role has specific permissions and restricted access to different functionalities. For example, only admins can delete users or manage course listings.

#### Security Feature 3: SQL Injection Prevention

All SQL queries are parameterized to prevent attackers from injecting malicious SQL commands through input fields. This secures the application against data leakage or manipulation.

#### Security Feature 4: Input Validation

All user inputs are validated on both client and server sides. This prevents malformed or malicious data from being submitted to the database.

#### Security Feature 5: Session Management

User sessions are managed securely using ASP.NET session handling. Session timeout and invalidation on logout are implemented to prevent session hijacking.

#### Security Feature 6: HTTPS Protocol Enforcement

The application enforces HTTPS protocol to encrypt data transmitted between the client and server, preventing man-in-the-middle attacks.

#### Security Feature 7: Error Handling and Logging

The system uses custom error pages and logs all exceptions. This prevents detailed error messages from being exposed to users and helps developers track suspicious activities.

### Problem 2: Implementation of Security Features

* **Login system** with username and password authentication
* **User roles** Admin, Student, Tutor
* **Parameterized SQL queries**
* **Server-side validation** in all registration and login forms
* **Session variables** like Session("UserID") and Session("Role")
* **All pages validate session before access**
* **Custom error messages**

**Live Demo**: http://labs1052.somee.com/tutoringCopy

**Problem 3)** Develop test cases for all security features and prepare a report about testing of security features?

### ****Test Case 1:** User Authentication – Valid Login**Ensure that only users with correct credentials can log in.

### ****Test Case 2:** User Authentication – Invalid Login**Ensure that users with incorrect credentials cannot log in.

### ****Test Case 3:** Input Validation – Empty Fields**Verify form fields are not submitted empty.

### ****Test Case 4:** Role-Based Access Control**Check that restricted pages are accessible only to allowed roles.

### ****Test Case 5:** Session Management – Access Without Login**Ensure users cannot access secure pages without logging in.

### ****Test Case 6:** SQL Injection Protection**Verify that SQL injection attempts are blocked.

### ****Test Case 7:** Password Visibility & Protection**Ensure passwords are masked during input and not visible in logs or source code.