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.

My Remote Patient Monitoring System has the following security features:

1. Authentication

Ensures that only authorized patients, doctors and admins (created by admin) can access the system by verifying their credentials (e.g., username and password). The functionality of my system cannot be accessed without logging into the system as a legitimate user.

2. Role Based Access Control

Restricted access to specific pages/routes based on the user's role (e.g., Admin, Doctor, Patient). Pages can only be accessed by those roles for which there is permission.

3. Input Validation

Used input validation in all forms to prevent malicious input (SQL injection) by validating and sanitizing user inputs using parameters and validators.

4. Session Management

Ensures that user sessions are secure and cannot be hijacked or misused.

5. Password Hashing

Hashed passwords before storing them in the database using SHA256, which prevents password leakage.

6. Error Handling

Prevents the disclosure of sensitive information through error messages.

Problem 2 Implementation done on the Semester Project Link

Problem 3 Test Cases

1. **Authentication:**
   Input invalid username or password (e.g. username: sample1, password: sample123)
   Expected: Error message "Invalid username or password" displayed
   Verify: User remains on login page, no session variables set

2. **Role Base Access Control**
   Login as Admin and access Admin pages
   Expected: Access granted

   Login as Doctor/Patient and then attempt to access Admin pages (e.g. visit http://muhammadhuzaifa.somee.com/Semester_Project/Admin/View_Patients.aspx)
   Expected: Redirected to Default.aspx (login page)

3. **Input Validation**
   Enter SQL injection patterns in login form: ' OR '1'='1
   Expected: Login fails, no unauthorized access
   Verify: Query parameters properly sanitize input

4. **Session Management**
   Login from multiple browsers simultaneously
   Expected: Each session should work independently
   Verify: Actions in one session don't affect the other

5. **Password Hashing**
   Cannot create an end-to-end test for this, as this is an internal implementation
6. **Error Handling**
   Input invalid username or password (e.g. username: sample1, password: sample123)
   Expected: Generic error message
   Verify: Internal Error details not displayed