IAD Lab 13

Problem 1:

1. Password Hashing:
Instead of storing plain-text passwords in the database, they should be hashed using a cryptographic algorithm like **SHA-256** . This ensures that even if the database is compromised, user passwords cannot be easily retrieved.

2. Input Validation and Sanitization:
All user input must be validated on the server side and sanitized to prevent **SQL injection** and other injection attacks.

3. Role-Based Access Control (RBAC):
Different users (Admin, Doctor, Patient) should only access features relevant to their roles. For example, patients should not access administrative functions, and doctors should not access user management unless authorized.

4. Secure Session Management:
User sessions should be securely managed using encrypted session tokens and automatic session timeouts after inactivity. This prevents unauthorized use after logout.

5. HTTPS and Secure Communication:
The application should use **HTTPS** to encrypt all communication between the client and the server. This prevents attackers from intercepting sensitive data like login credentials or patient records.

6. Error Handling and Logging:
Detailed internal error messages (especially SQL errors) should not be exposed to users, as they may reveal vulnerabilities. Errors should be logged securely for admin analysis.

7. Email Validation and Verification:
Users should confirm their email addresses via verification links before gaining full access. This helps preventing spam or fake accounts.