IAD Lab 13

Problem 1:

1. Password Hashing:

- Register a new patient.

- Check the `USERS` table for stored password. Password is stored as a hashed value (e.g., long string of characters).

2. Input Validation and Sanitization:

- Try to register with a malicious name: `OR 1=1`.

- Observe server behaviour and DB entries. Input is rejected and not executed.

3. Role-Based Access Control (RBAC):

- Log in as patient.

- Try to navigate to `AdminDashboard.aspx`. User is redirected to login or error page.

4. Secure Session Management:

- Log in as any user

- Stay idle for 20 minutes

- Try to access any page. User is redirected to login page.

5. HTTPS and Secure Communication:

- Access the site with `http://`

- Observe redirection. Automatically redirected to https://.

6. Error Handling and Logging:

- Cause a database error (e.g., disconnect DB)
- Submit the signup form
- Check the log file. Error is logged in secure location; no stack trace shown to user.

7. Email Validation and Verification:

- Register a new user
- Check `IS_VERIFIED = 0`
- Try to log in. Cannot log in until verification link is clicked