Test Case 1:

Password Hashing

Objective: Ensure passwords are stored as hashes, not plain text.

Steps:

1. Register a new user with email "test@example.com" and password "Test@1234".
2. Query the USERS table to check the USER_PASSWORD column.

Expected Outcome: Password is stored as a bcrypt hash (e.g., starts with "$2a$").

Result: Pass (assuming bcrypt is implemented).

Test Case 2:

SQL Injection Prevention

Objective: Verify that malicious SQL inputs do not execute.

Steps:

1. Attempt to log in with email "test@example.com' OR '1'='1" and any password.
2. Check if login succeeds.

Expected Outcome: Login fails with "No user found" message.

Result: Pass (parameterized queries prevent injection).

Test Case 3:

XSS Prevention

Objective: Ensure malicious scripts in posts are not executed.

Steps:

1. Create a post with content "".
2. View the post on the Posts page.

Expected Outcome: Script is displayed as text, not executed.

Result: Pass (HtmlEncode prevents script execution).

Test Case 4:

CSRF Protection

Objective: Verify that posts cannot be created without a valid CSRF token.

Steps:

1. Submit a post request via a forged form without the CSRF token.
2. Check if the post is created.

Expected Outcome: Request fails with "Invalid CSRF token" message.

Result: Pass (CSRF token validation enforced).

Test Case 5:

Session Management

Objective: Ensure sessions are secure and timeout correctly.

Steps:

1. Log in and note the session ID.
2. Log out and log in again, check if session ID changes.
3. Leave the session idle for 21 minutes, then try to create a post.

Expected Outcome: Session ID regenerates on login; session expires after 20 minutes.

Result: Pass (session settings enforced).

Test Case 6:

Role-Based Access Control

Objective: Ensure only admins can delete users.

Steps:

1. Log in as a non-admin user (Member role).
2. Attempt to delete a user via the Posts page.
3. Log in as an admin and repeat.

Expected Outcome: Non-admin sees "Only admins can delete users"; admin can delete.

Result: Pass (RBAC enforced).

Test Case 7:

Input Validation

Objective: Verify that invalid inputs are rejected.

Steps:

1. Register with an invalid email ("test"), short password ("123"), and future birth date ("2026-01-01").
2. Check error messages.

Expected Outcome: Error messages indicate invalid inputs.

Result: Pass (input validation enforced).