Core Functional Test Cases

TC01 - Successful Login with Valid Credentials

- **Objective**: Ensure users can log in with a valid email and password.
- **Precondition**: User has a registered account.
- **Steps**:
  1. Go to the login page.
  2. Enter valid email and password.
  3. Click the **Login** button.
- **Expected Result**: User is redirected to the dashboard/home page.

TC02 - Login with Invalid Password

- **Objective**: Verify login fails when password is incorrect.
- **Steps**:
  1. Enter a valid email and an incorrect password.
  2. Click **Login**.
- **Expected Result**: Error message is shown: "Invalid email or password."

TC03 - Login with Invalid Email

- **Objective**: Verify login fails when email does not exist in the system.
- **Steps**:
  1. Enter an unregistered email and any password.
  2. Click **Login**.
- **Expected Result**: Error message is shown: "Invalid email or password."

TC04 - Attempt Login with Blank Fields

- **Objective**: Ensure the system does not allow login with empty inputs.
- **Steps**:
  1. Leave both email and password fields blank.
  2. Click **Login**.
- **Expected Result**: Inline validation errors like “Email is required” and “Password is required.”

TC05 - Attempt Login with Only Email Filled

- **Objective**: Ensure login fails if the password is missing.
- **Steps**:

    1. Enter a valid email.
    2. Leave the password blank.
    3. Click **Login**.
- **Expected Result**: Show “Password is required” message.

TC06 - Password Masking

- **Objective**: Verify the password input is masked by default (not in plain text).
- **Steps**:
    1. Start typing into the password field.
- **Expected Result**: Password is displayed as dots or asterisks.

TC07 - Brute Force Attempt Blocking (Security)

- **Objective**: Check if the system blocks login after multiple failed attempts.
- **Steps**:
    1. Enter incorrect credentials 5 times in a row.
- **Expected Result**: Account is locked temporarily or CAPTCHA appears.

TC08 - Secure Protocol (HTTPS)

- **Objective**: Ensure the login page is served over HTTPS.
- **Steps**:
    1. Open the login page.
- **Expected Result**: The URL uses **https://** and shows a secure padlock icon.

Optional Cross-Platform Test Cases

TC09 - Login on Different Browsers

- **Objective**: Verify login functionality works across major browsers.
- **Browsers to test**: Chrome, Firefox, Safari, Edge.
- **Expected Result**: Login behavior and UI are consistent across all tested browsers.

TC10 - Mobile Responsiveness

- **Objective**: Validate login page on mobile devices.
- **Steps**:
    1. Open the login page on a mobile browser.
    2. Attempt login with valid credentials.

- **Expected Result**: Page is responsive and login works without issues on mobile.

Test Coverage Observations

Coverage Summary

Area	Coverage Level	Observations
Successful Login	Covered	
Invalid Credentials Handling	Covered	Includes blank fields, incorrect email/password, and partial input cases.
Security Features	Partial	Password masking and brute-force protection covered, but 2FA not tested.
Input Validation	Covered	Validation on required fields confirmed.
Cross-Browser Support	Covered	Recommended browsers tested.
Mobile Responsiveness	Covered	Mobile login flow verified.
HTTPS / Secure Protocol	Covered	Ensures secure communication during login.
Accessibility	Not Covered	
Performance/Load Testing	Not Covered	