**Login Page Test Scenarios**

1. **Valid login with correct username and password**
2. **Login attempt with invalid username**
3. **Login attempt with invalid password**
4. **Login attempt with both invalid username and password**
5. **Login attempt with empty username**
6. **Login attempt with empty password**
7. **Login attempt with both username and password fields empty**
8. **Login attempt with SQL injection in the username field**
9. **Login attempt with SQL injection in the password field**
10. **Login with username containing special characters**
11. **Login with password containing special characters**
12. **Login attempt with long username (max length)**
13. **Login attempt with long password (max length)**
14. **Login attempt with leading and trailing whitespaces in the username**
15. **Login attempt with leading and trailing whitespaces in the password**
16. **Login attempt with the username in different cases (upper, lower, mixed)**
17. **Login attempt with the password in different cases (upper, lower, mixed)**
18. **Login with previously valid credentials after password change**
19. **Login attempt after multiple failed attempts (account lockout)**
20. **Login attempt with a disabled account**
21. **Login attempt with an expired account**
22. **Login attempt with a temporary account**
23. **Remember me functionality verification**
24. **Automatic logout after a period of inactivity (session timeout)**
25. **Multiple sessions for the same user (logging in from different browsers/devices)**
26. **Cross-browser compatibility (testing in different browsers)**
27. **Mobile responsiveness and functionality on different devices**
28. **Login attempt with browser autofill**
29. **Login attempt with cookies disabled**
30. **Login attempt with JavaScript disabled**
31. **Password masking functionality verification**
32. **Error message visibility and clarity for invalid login attempts**
33. **Password recovery link functionality**
34. **Password recovery process and email verification**
35. **Two-factor authentication (2FA) functionality**
36. **Login attempt with 2FA enabled account**
37. **Security testing for XSS (cross-site scripting) vulnerabilities**
38. **Security testing for CSRF (cross-site request forgery) vulnerabilities**
39. **Performance testing under load (simultaneous logins)**
40. **Usability testing (tab navigation, accessibility features)**
41. **Captcha verification during login attempts**
42. **Error logging and alerting for failed login attempts**
43. **Audit log entries for successful and failed login attempts**
44. **Localization and language support for error messages**
45. **Login page UI and layout verification**
46. **Data encryption for login credentials**
47. **Testing with network interruptions during login**
48. **Login attempt using saved passwords from password managers**
49. **Brute force attack prevention mechanism verification**