Below is a comprehensive **Test Plan** and **Test Cases** for a Login Page with Username, Password, and "Remember Me" functionality, presented in tabular form. The solution follows best practices, including test case prioritization, coverage of positive and negative scenarios, and clear, concise documentation.

### Test Plan

|  |  |
| --- | --- |
| **Section** | **Details** |
| **Test Plan ID** | TP\_LOGIN\_001 |
| **Test Objective** | Verify the functionality, usability, and security of the Login Page with Username, Password, and "Remember Me" features. |
| **Scope** | - Login with valid/invalid credentials<br>- "Remember Me" functionality<br>- Error handling<br>- UI validation |
| **Out of Scope** | - Backend database integrity<br>- Password encryption algorithms |
| **Test Environment** | - Browser: Chrome (latest), Firefox (latest)<br>- OS: Windows 10<br>- Test URL: [TBD] |
| **Test Data** | - Valid Username: testuser@example.com<br>- Valid Password: Password123!<br>- Invalid Username: invalid@xyz.com<br>- Invalid Password: wrongpass |
| **Entry Criteria** | - Login page UI is deployed<br>- Test data is prepared<br>- Test environment is stable |
| **Exit Criteria** | - All high-priority test cases pass<br>- 90% of all test cases pass<br>- Critical defects resolved |
| **Test Deliverables** | - Test Plan<br>- Test Cases<br>- Test Execution Report<br>- Defect Log |
| **Roles and Responsibilities** | - Tester: Execute test cases<br>- Developer: Fix defects<br>- QA Lead: Review results |
| **Risks** | - Unstable test environment<br>- Missing test data<br>- Tight deadlines |
| **Mitigation** | - Pre-test environment validation<br>- Backup test data<br>- Prioritize critical tests |
| **Test Strategy** | - Manual testing<br>- Functional testing (positive/negative)<br>- Usability testing |
| **Prioritization** | - P1 (High): Core login functionality<br>- P2 (Medium): "Remember Me" feature<br>- P3 (Low): UI edge cases |

### Test Cases

The test cases are prioritized (P1, P2, P3) and cover both positive and negative scenarios. Each test case follows best practices: unique ID, clear preconditions, steps, expected results, and status fields.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Test Case ID** | **Priority** | **Test Scenario** | **Preconditions** | **Test Steps** | **Expected Result** | **Status** |
| TC\_LOGIN\_001 | P1 | Successful login with valid credentials | - Login page is accessible<br>- User has valid credentials | 1. Navigate to login page<br>2. Enter valid username (testuser@example.com)<br>3. Enter valid password (Password123!)<br>4. Click "Login" | User is redirected to the dashboard/home page | TBD |
| TC\_LOGIN\_002 | P1 | Login with invalid username | - Login page is accessible | 1. Navigate to login page<br>2. Enter invalid username (invalid@xyz.com)<br>3. Enter valid password (Password123!)<br>4. Click "Login" | Error message: "Invalid username or password" displayed | TBD |
| TC\_LOGIN\_003 | P1 | Login with invalid password | - Login page is accessible | 1. Navigate to login page<br>2. Enter valid username (testuser@example.com)<br>3. Enter invalid password (wrongpass)<br>4. Click "Login" | Error message: "Invalid username or password" displayed | TBD |
| TC\_LOGIN\_004 | P1 | Login with empty username | - Login page is accessible | 1. Navigate to login page<br>2. Leave username blank<br>3. Enter valid password (Password123!)<br>4. Click "Login" | Error message: "Username is required" displayed | TBD |
| TC\_LOGIN\_005 | P1 | Login with empty password | - Login page is accessible | 1. Navigate to login page<br>2. Enter valid username (testuser@example.com)<br>3. Leave password blank<br>4. Click "Login" | Error message: "Password is required" displayed | TBD |
| TC\_LOGIN\_006 | P1 | Login with empty username and password | - Login page is accessible | 1. Navigate to login page<br>2. Leave username blank<br>3. Leave password blank<br>4. Click "Login" | Error messages: "Username is required" and "Password is required" displayed | TBD |
| TC\_LOGIN\_007 | P2 | "Remember Me" retains credentials | - Login page is accessible<br>- User has valid credentials | 1. Navigate to login page<br>2. Enter valid username/password<br>3. Check "Remember Me"<br>4. Click "Login"<br>5. Log out<br>6. Return to login page | Username and password fields are pre-filled | TBD |
| TC\_LOGIN\_008 | P2 | "Remember Me" not checked, no retention | - Login page is accessible<br>- User has valid credentials | 1. Navigate to login page<br>2. Enter valid username/password<br>3. Do not check "Remember Me"<br>4. Click "Login"<br>5. Log out<br>6. Return to login page | Username and password fields are empty | TBD |
| TC\_LOGIN\_009 | P1 | Login with incorrect case-sensitive credentials | - Login page is accessible<br>- Credentials are case-sensitive | 1. Navigate to login page<br>2. Enter username (TESTUSER@example.com)<br>3. Enter password (password123!)<br>4. Click "Login" | Error message: "Invalid username or password" displayed | TBD |
| TC\_LOGIN\_010 | P2 | Login with excessively long username | - Login page is accessible | 1. Navigate to login page<br>2. Enter username (256 chars, e.g., a...a@example.com)<br>3. Enter valid password<br>4. Click "Login" | Error message: "Username exceeds maximum length" or truncated login attempt fails | TBD |
| TC\_LOGIN\_011 | P2 | Login with excessively long password | - Login page is accessible | 1. Navigate to login page<br>2. Enter valid username<br>3. Enter password (256 chars, e.g., a...a!)<br>4. Click "Login" | Error message: "Password exceeds maximum length" or truncated login attempt fails | TBD |
| TC\_LOGIN\_012 | P3 | Login with special characters in username | - Login page is accessible | 1. Navigate to login page<br>2. Enter username (test#@user.com)<br>3. Enter valid password<br>4. Click "Login" | Either successful login (if allowed) or error message: "Invalid username format" | TBD |
| TC\_LOGIN\_013 | P3 | Login with special characters in password | - Login page is accessible | 1. Navigate to login page<br>2. Enter valid username<br>3. Enter password (Pass!@#$%)<br>4. Click "Login" | Successful login (assuming special chars are allowed) | TBD |
| TC\_LOGIN\_014 | P1 | Multiple failed login attempts (lockout) | - Login page is accessible<br>- Lockout policy exists | 1. Navigate to login page<br>2. Enter invalid credentials 5 times<br>3. Enter valid credentials on 6th attempt | Error message: "Account locked due to multiple failed attempts" on 6th try | TBD |
| TC\_LOGIN\_015 | P3 | UI - Login button disabled with empty fields | - Login page is accessible | 1. Navigate to login page<br>2. Leave username and password blank<br>3. Observe "Login" button | "Login" button is disabled or greyed out | TBD |

### Best Practices Followed

1. **Test Case Prioritization**:
   1. **P1 (High)**: Core login functionality and critical error handling (e.g., TC\_LOGIN\_001 to TC\_LOGIN\_006, TC\_LOGIN\_009, TC\_LOGIN\_014).
   2. **P2 (Medium)**: "Remember Me" and boundary cases (e.g., TC\_LOGIN\_007, TC\_LOGIN\_008, TC\_LOGIN\_010, TC\_LOGIN\_011).
   3. **P3 (Low)**: UI and less critical edge cases (e.g., TC\_LOGIN\_012, TC\_LOGIN\_013, TC\_LOGIN\_015).
2. **Positive Scenarios**: Successful login (TC\_LOGIN\_001), "Remember Me" retention (TC\_LOGIN\_007), special characters (TC\_LOGIN\_013).
3. **Negative Scenarios**: Invalid credentials (TC\_LOGIN\_002, TC\_LOGIN\_003), empty fields (TC\_LOGIN\_004 to TC\_LOGIN\_006), lockout (TC\_LOGIN\_014).
4. **Clarity**: Each test case has a unique ID, clear steps, and expected results.
5. **Coverage**: Functional (login success/failure), usability ("Remember Me", UI), and security (lockout, case sensitivity).
6. **Reusability**: Preconditions and test data are standardized for consistency.

### Notes

* **Assumptions**:
  + Username is an email format.
  + Case sensitivity and special character policies depend on system requirements (adjust TC\_LOGIN\_009, TC\_LOGIN\_012, TC\_LOGIN\_013 accordingly).
  + Lockout policy assumes 5 failed attempts (adjust TC\_LOGIN\_014 as per spec).
* **Execution**: Status is "TBD" until executed; update with "Pass" or "Fail" post-execution.
* **Enhancements**: Add performance tests (e.g., login response time) or automated scripts if required.