QUALITY ASSURANCE PROJECT – LOGIN FORM TESTING

1. PROJECT OVERVIEW

This project evaluates the functionality, error handling, and UI behavior of a standard web-based login form. Testing focused on validating expected behavior under valid, invalid, and boundary input conditions, including error messaging, button state control, password masking, and navigation reliability.

2. TEST SCOPE

In Scope:
- Username/Email input field
- Password field
- Login button behavior
- Error messages and validation
- Forgot Password navigation
- Input formatting rules

Out of Scope:
- Backend authentication
- Two-factor authentication
- Password recovery flow
- Account lockout handling

3. TEST CASES

TC-LOGIN-001 – Successful Login

Steps:
1. Enter a valid username.
2. Enter a valid password.
3. Click Login.

Expected Result:
User is authenticated and redirected to the dashboard.

TC-LOGIN-002 – Invalid Password

Steps:
1. Enter a valid username.
2. Enter an incorrect password.
3. Click Login.

Expected Result:

Error message displayed: “Incorrect username or password.” Login attempt blocked.

TC-LOGIN-003 – Invalid Email Format

Steps:
1. Enter an invalid email format (e.g., test@@mail).
2. Enter any password.
3. Click Login.

Expected Result:
System displays email format validation error.

TC-LOGIN-004 – Empty Fields

Steps:
1. Leave both fields empty.
2. Click Login.

Expected Result:
Error displayed stating fields cannot be empty. Login prevented.

TC-LOGIN-005 – Password Masking

Steps:
1. Type characters in the password field.

Expected Result:
All characters display as masked dots or symbols.

TC-LOGIN-006 – Login Button Disabled on Empty Inputs

Steps:
1. Ensure both fields are empty.

Expected Result:
Login button remains disabled until valid input is provided.

TC-LOGIN-007 – SQL Injection Attempt Handling

Steps:
1. Enter `' OR 1=1--` in the username field.
2. Enter any password.
3. Click Login.

Expected Result:
Login attempt blocked. Generic error message displayed.

TC-LOGIN-008 – Forgot Password Navigation

Steps:
1. Click the Forgot Password link.

Expected Result:
User is redirected to the password recovery page.

TC-LOGIN-009 – Username Case Sensitivity

Steps:
1. Enter correct username with incorrect letter casing.
2. Enter correct password.

Expected Result:
Login fails if system enforces case-sensitive usernames.

TC-LOGIN-010 – Error Message Display Formatting

Steps:
1. Trigger an error by entering invalid credentials.

Expected Result:
Error message is clearly visible, styled correctly, and does not overlap UI elements.

4. BUG REPORTS

BUG-LOGIN-001 – Login Button Enabled When Fields Are Empty

Severity: High
Priority: High

Steps to Reproduce:
1. Navigate to login page.
2. Leave both fields empty.
3. Observe Login button state.

Expected Result:
Button remains disabled.
Actual Result:
Button becomes active.

BUG-LOGIN-002 – Invalid Email Format Not Blocked

Severity: Medium
Priority: Medium

Steps to Reproduce:
1. Enter an invalid email format such as “test@@gmail”.
2. Click Login.

Expected Result:
Validation error displayed.
Actual Result:

System proceeds without validation.

BUG-LOGIN-003 – Password Masking Delay

Severity: Low
Priority: Low

Steps to Reproduce:
1. Slowly type into the password field.

Expected Result:
All characters remain masked immediately.
Actual Result:
Last character remains visible briefly.

5. SUMMARY OF RESULTS

Testing identified deficiencies in input validation, button state control, and password masking timing. Most core functionality behaved as expected, but corrective actions are needed to ensure consistent user experience and security alignment.

6. RETEST RECOMMENDATIONS

- Revalidate all input validation rules, especially email formatting
- Confirm proper Login button disabling logic
- Verify consistent password masking behavior
- Retest Forgot Password link behavior after fixes
- Conduct cross-browser validation across Chrome, Safari, and Firefox