

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Test Case Description** | | **Test Steps** | **Expected Outcome** | **Actual Result** | **Verdict** |
| **Functional Test Cases:** |  | |  |  |  |
| 1. Valid User Login | | Entered a *valid username and password.* | The user is successfully logged in and redirected to the home page or dashboard. | The user successfully logged in and redirected to the home page. | Pass |
| 2. Invalid User ID | | Enter an *invalid user id* and a valid password. | The system displays an error message indicating invalid credentials. The user remains on the login page. | Error message displayed: "Username or password is incorrect". The user remains on the login page. | Pass |
| 3. Invalid Password | | Enter a valid user id and an *invalid password.* | System displays an error message indicating invalid credentials. The user remains on the login page. | Error message displayed: “Username or password is incorrect ". The user remains on the login page. | Pass |
| 4. Blank User ID | | Leave the user id field blank and input a valid password. | The system displays an error message indicating the user id is required. The user remains on the login page. | Error message displayed: "Please fill out the field". The user remains on the login page. | Pass |
| 5. Blank Password | | Enter a valid user id and leave the password field blank. | System displays an error message indicating the password is required. The user remains on the login page. | Error message displayed: "Please fill out the field". The user remains on the login page. | Pass |
| 6. Username Length Validation | | Input a user id with the maximum length. | The system accepts it and allows the user to log in successfully. | Error message displayed: "username is invalid. Should have 3-15 alphanumeric characters underscore and dash only". The user remains on the login page. | Fail |
| **Interface Test Cases:** | |  |  |  |  |
| 1. Layout Verification | | The layout of the login page with the specified design/layout. | The layout matches the design specifications. | The layout matches the design specifications. | Pass |
| 2. Placeholder Display | | Verify that placeholders in the user ID and password fields are correctly displayed. | Placeholders are visible within the input fields. | Placeholders are not visible within the input fields. | Fail |
| 3. Mandatory Field Indication | | Verify that asterisks (\*) are displayed next to mandatory fields (user id and password). | Asterisks are displayed next to the user id and password fields. | Asterisks (\*) are not displayed next to the user id and password fields. | Fail |
| 4. Field Alignment | | Verify the alignment of checkboxes, radio buttons, and text fields on the login page. | Fields aligned according to design specifications. | Fields aligned according to design specifications. | Pass |
| 5. Responsiveness Check | | Test the login page on various devices and screen sizes to ensure responsiveness. | The login page displays and functions correctly on different devices and screen sizes. | The login page displays and functions correctly on different devices and screen sizes. | Pass |
| **Security Test Cases:** | |  |  |  |  |
| 1. Session Timeout | | Log in as a user and wait for the session timeout duration. | The session expires, and the user is logged out. | The session expires after the timeout duration, and the user is automatically logged out. | Pass |
| 2. Back Button Logout | | Log in as a user, then navigate back using the browser's back button. | The user is logged out and must re-enter credentials to access the secure area. | The user is not logged out upon navigating back. | Fail |
| 3. Direct URL Access | | Attempt to access the secure area directly by entering its URL without logging in. | The user is redirected to the login page. | The user is redirected to the login page. | Pass |
| 4. Password Encryption | | Inspect network traffic during login to ensure password transmission is secure. | Password transmitted securely and not stored or transmitted in plaintext. | Password is transmitted securely over HTTPS and not stored or transmitted in plaintext. | Pass |