Manual Testing Task

Test scenarios:

1. Login Functionality

Functional Scenarios

1. Verify login with valid credentials.
2. Verify login with invalid username and/or password.
3. Verify login with blank username and/or password fields.
4. Verify login functionality with leading/trailing spaces in username or password.
5. Verify login functionality using keyboard shortcuts (Tab/Enter).
6. Verify users are redirected to the dashboard upon successful login.
7. Verify users are redirected to the login page after clicking logout.
8. Verify "Forgot Password" link redirects to the appropriate password recovery page.

Validation & Error Handling

9. Verify appropriate error messages are displayed when credentials are incorrect.
10. Verify error message disappears when corrected input is entered.
11. Verify login fails when the username field contains only whitespace.
12. Verify login fails when the password field contains only whitespace.
13. Verify login fails when special characters are used in the username (e.g., !@#$%^&*()).
14. Verify login does not work with deactivated or deleted user accounts.
15. Verify the user account gets locked after a defined number of failed login attempts.
16. Verify captcha (if enabled) appears after multiple failed attempts and functions properly.

UI/UX & Accessibility

17. Verify the password input field masks the characters while typing.
18. Verify login page responsiveness and usability across different screen resolutions.
19. Verify browser "Remember Password" functionality behaves as expected.
20. Verify login is not case-sensitive if usernames are stored in lowercase.

Security & Session Handling

21. Verify that the session is invalidated properly after logout (cannot use back button to access dashboard).
22. Verify URL manipulation does not allow unauthorized access to authenticated pages.
23. Verify session timeout behavior after the user is idle for a configured time.
24. Verify login from multiple devices/sessions and check if the session is handled properly.
25. Verify auto-logout functionality works correctly if the tab/browser is closed without logging out.
26. Verify if the password is not exposed in browser developer tools or URL parameters.
27. Verify system logs unsuccessful login attempts (for security auditing).

Performance & Reliability

28. Verify performance of login process (e.g., login completes within 2 seconds under normal conditions).
29. Verify system behavior when attempting login during server downtime.
30. Verify login functionality across different browsers (Chrome, Firefox, Edge, Safari).

2. Employee Management (View, Update, Delete)

Core Functionality

1. Verify navigation to the **PIM → Employee List** tab.
2. Verify the full list of employees is displayed upon navigating.
3. Verify searching for an employee by **valid name or ID** shows correct results.
4. Verify **appropriate message is shown** when no match is found in search.
5. Verify the user can view **full details** of a selected employee.
6. Verify **adding a new employee** with all valid inputs succeeds.
7. Verify that the added employee appears in the list **immediately or after refresh**.
8. Verify **mandatory fields** during add/update throw validation errors if left blank.
9. Verify **editing existing employee information** updates the data correctly.
10. Verify **canceling an update** does not change employee information.
11. Verify **confirmation dialog** appears before deleting an employee.
12. Verify **deleted employee** no longer appears in the list.
13. Verify behavior when trying to **delete without selecting** any employee.
14. Verify **multiple employees can be selected and deleted together**.
15. Verify that a **logged-in user cannot delete their own employee account**.

Usability & Data Handling

15. Verify **filters** (Status, Job Title, Sub Unit, Include) work as expected.

16. Verify **filtering by Supervisor name** returns correct results.

17. Verify **search by partial match or case-insensitive** terms works correctly.

18. Verify **clearing filters** resets the employee list.

19. Verify **searching with blank input** doesn't apply any filters.

20. Verify **invalid combinations** in filters show no results.

21. Verify **sorting functionality** (by name, ID, job title, etc.) works correctly.

22. Verify **character limits** for input fields (e.g., name, address), and truncation if exceeded.

23. Verify **special characters** in names/addresses (e.g., José, O'Connor) are handled correctly.

24. Verify **phone number/email formats** are validated correctly while adding or updating employees.

25. Verify **error messages for invalid inputs** (e.g., email, phone) are clear and actionable.

26. Verify **responsiveness** and layout of employee list and detail page on different devices/screens.

27. Verify **filter fields** (dropdowns) are keyboard accessible and clearly labeled.

28. Verify keyboard navigation (Tab, Shift+Tab) works properly in employee forms.

29. Verify real-time field validation (e.g., email format error appears as you type).

Validation, Roles & Permissions

30. Verify user role permissions:
    - Admin can view/edit/delete
    - Regular users can view only

31. Verify system **prevents duplicate employee ID or email** during creation and update.

32. Verify adding employees with **duplicate details** shows appropriate validation.

33. Verify **data consistency** across modules (e.g., changes reflect in reports or dashboards).

34. Verify **audit logs** are created for add/update/delete employee actions.

35. Verify **concurrent updates** to the same profile are handled gracefully.

Profile Photo Upload

36. Verify **uploading a valid profile photo** during employee creation.

37. Verify **uploading invalid file types** (e.g., .exe, .txt) is prevented with a clear error.

38. Verify **uploading large images** (exceeding size limit) is blocked or resized with a message.

39. Verify **common image formats** (jpg, png, gif, bmp) are supported.

40. Verify **profile photo preview** appears before saving.

41. Verify **updating profile photo** reflects immediately in employee list and details.

Performance (Basic Manual Checks)

42. Verify the employee list loads within acceptable time for large datasets (e.g., 500+ entries).

43. Verify app responsiveness when switching between filters or pages quickly.

Bugs or usability issues in the login page:

Bug 1: Password Field Can Be Revealed via Browser Inspect Tools

Title: Password is visible in plain text in Chrome DevTools Network payload during login

Test Case ID: TC_Login_26

Description:

When a user submits the login form, the password is sent in plain text within the network request payload, which is visible in Chrome DevTools under the Network tab. This exposes sensitive user credentials and poses a significant security risk. Passwords should be encrypted or hashed during transmission using HTTPS and not visible in plain text in developer tools.

Expected Result:

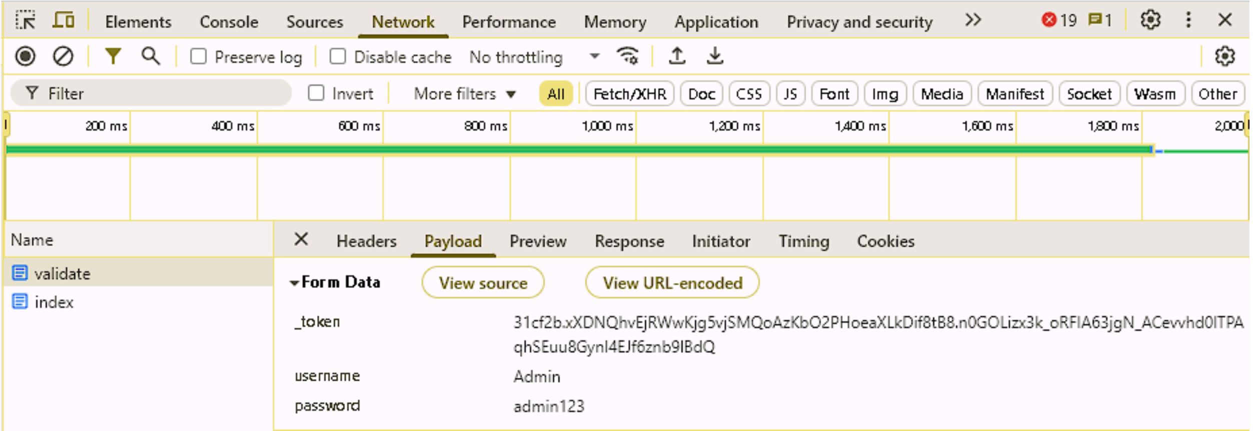
Passwords should be securely handled and not visible in plain text in network requests or any client-side tools. The connection should be encrypted (HTTPS), and sensitive data should be protected.

Actual Result:

Password is visible in plain text in the network request payload under Chrome DevTools.

Severity: Critical

Justification: Exposing passwords in plain text can lead to serious data breaches and compromises user security.



Form Data

_token 31cf2b.xXDNQhvEjRWwKjg5vjSMQoAzKbO2PHoeaXLkDif8tB8.n0GOLizx3k_oRFIA63jgN_ACevhd0ITPAqhSEuu8Gynl4EJf6znb9IBdQ

username Admin

password admin123

Bug 2: Session persists even after closing tab

Title: Session persists even after closing browser tab without logout
Test Case ID : TC_Login_25

Description:
When a user logs into the application and then closes the browser tab without logging out, the session is expected to end. However, reopening the application in the same browser sometimes grants access to the dashboard without requiring the user to re-authenticate. This behavior indicates improper session termination.

Expected Result:
On closing the browser/tab without logout, and reopening the application, the user should be required to log in again — the session should be invalidated.

Actual Result:
Session is still active; user can access dashboard without logging in again.

Severity: High
Justification: This is a security flaw as unauthorized access could occur if a user closes the tab on a shared or public system without logging out. Session management must be strict to prevent hijacking.

Bug 3: No loading indicators

Title: Login page lacks loading indicator after clicking the Login button
Test Case ID : TC_Login_30

Description:
After clicking the Login button, there is no loading spinner or indication that the system is processing the request, which might confuse users or lead to multiple clicks.

Expected Result:
A loading spinner or disabled state should appear while the request is being processed.

Actual Result:
No feedback is shown during authentication, and users might think the click didn't register.

Severity: Medium
Justification: Can lead to duplicate requests and confusion during slow network responses.

Bug 4 : Username Field Fails with Leading Spaces but Allows Trailing Spaces

Title: Username field allows only trailing spaces to be trimmed, not leading spaces
Test Case ID: TC_Login_05

Description:
If a user enters a username with leading spaces (e.g., " Admin"), login fails. However, if the username contains trailing spaces (e.g., "Admin "), login succeeds. This inconsistency can confuse users.

Expected Result:
Both leading and trailing spaces in the username field should be trimmed automatically before login submission.

Actual Result:
Login fails with leading spaces, but works with trailing spaces.

Severity: Medium
Justification: Affects user experience and could lead to unnecessary login errors.

Bug 5 : Generic and Unhelpful Invalid Credentials Error Message

Title: Error message for invalid credentials is not specific or user-friendly
Test Case ID : TC_Login_14

Description:
When invalid credentials are entered, the error message displayed is generic (e.g., “Invalid credentials”). It does not indicate if the username or password is incorrect, or if the account is locked. This can frustrate users and reduce usability.

Expected Result:
Error messages should be clear and provide actionable feedback, e.g., “Username not found” or “Incorrect password,” without compromising security.

Actual Result:
A generic error message is displayed regardless of the actual error cause.

Severity: Low
Justification: Doesn’t break functionality but affects user clarity and experience.

Bug 6: Missing Show/Hide Toggle for Password Field

Title: No toggle option to show/hide password in password field

Description:
Many modern login forms include an eye icon to allow users to toggle visibility of the password for ease of input. This feature is missing here, reducing usability especially on mobile devices.

Expected Result:
Password input should offer a "show/hide" toggle icon for user convenience.

Actual Result:
Password is always masked, with no toggle option provided.

Severity: Low
Justification: Usability issue, not critical to functionality but improves accessibility.

Bug 7: No Caps Lock Warning During Password Entry

Title: Login does not warn user if Caps Lock is ON during password entry

Description:
If the user accidentally has Caps Lock enabled, the system doesn't alert them. This often leads to failed login attempts, especially for complex passwords.

Expected Result:
When Caps Lock is detected, a small warning tooltip or icon should appear near the password field.

Actual Result:
No feedback or warning is shown.

Severity: Low
Justification: A common UX improvement found in modern secure login forms.

Bug 8: Username Field Accepts Excessively Long Input

Title: Username field accepts very long input (no character limit)

Description:
You can paste or type an excessively long string into the Username field (e.g., 500+ characters), and the system attempts to process it.

Expected Result:
There should be a reasonable character limit (e.g., 50-100 characters) on the username field to prevent performance issues or injection risks.

Actual Result:
No character limit is enforced on the username field.

Severity: Medium
Justification: Could lead to security, performance, or buffer overflow issues.

Test cases for the login functionality:

Test Case ID	Test Steps	Expected Result	Actual Result	Status
TC_Login_01	1. Navigate to the login page. 2. Enter valid username and password. 3. Click the Login button.	User is successfully logged in and redirected to the dashboard.	User logged in successfully and redirected to dashboard.	Pass
TC_Login_02	1. Navigate to the login page. 2. Enter invalid username and/or password. 3. Click Login.	Appropriate error message "Invalid credentials" is displayed.	Error message "Invalid credentials" displayed.	Pass
TC_Login_03	1. Navigate to the login page. 2. Leave username and/or password fields blank. 3. Click Login.	Error message prompting to fill mandatory fields is displayed.	Error message "Username and Password required" displayed.	Pass
TC_Login_04	1. Enter username with leading spaces (e.g., " Admin"). 2. Enter valid password. 3. Click Login.	Login should not trim spaces and succeed.	Login will not trim spaces and succeed.	Pass
TC_Login_05	1. Enter username with trailing spaces (e.g., "Admin "). 2. Enter valid password. 3. Click Login.	Login should not trim spaces and succeed.	Login trims trailing spaces and succeeds.	Fail
TC_Login_06	1. Enter valid credentials. 2. Use Tab key to move between username and password fields. 3. Press Enter to submit.	Login is submitted and processed correctly, redirecting users to the dashboard.	Login successful and redirected.	Pass

TC_Login_07	1. Enter valid credentials. 2. Click Login.	User redirected to dashboard.	User redirected to dashboard.	Pass
TC_Login_08	1. Login successfully. 2. Click the Logout button.	User is logged out and redirected to the login page.	User logged out and redirected correctly.	Pass
TC_Login_09	1. On login page, 2. click the "Forgot Password" link.	User is redirected to the password recovery page.	Redirected to password recovery page.	Pass
TC_Login_10	1. Enter invalid credentials. 2. Observe the error message. 3. Correct username and password. 4. Observe if the error message disappears.	Error message disappears after input correction.	Error message disappears after correction.	Pass
TC_Login_11	1. Enter username containing only whitespace (e.g., " "). 2. Enter valid password. 3. Click Login.	Login fails with an error message.	Login fails with an error message.	Pass
TC_Login_12	1. Enter password containing only whitespace. 2. Enter valid username. 3. Click Login.	Login fails with an error message.	Login fails with an error message.	Pass
TC_Login_13	1. 1. Enter special characters in username (e.g., !@#$%^&*()). 2. Enter valid password. 3. Click Login.	Login fails with an error message about invalid characters.	Login fails with an error message.	Pass
TC_Login_14	1. Attempt login with deactivated or deleted user account credentials. 2. Click Login.	Login fails with an error message indicating the account is inactive.	Login fails with generic error message.	Fail

TC_Login_15	1. Enter wrong credentials multiple times (exceeding threshold). 2. Observe account lock behavior.	Account locks after defined failed attempts, preventing further login.	Account locks after 5 failed attempts.	Pass
TC_Login_16	1. Enter wrong credentials multiple times. 2. Verify CAPTCHA appears. 3. Complete CAPTCHA and attempt login.	CAPTCHA appears after multiple failed attempts and works correctly.	CAPTCHA appears and functions properly.	Pass
TC_Login_17	1. Enter password. 2. Observe input field.	Password characters are masked (hidden).	Passwords are masked during typing.	Pass
TC_Login_18	1. Resize the browser window or test on different devices. 2. Open login page.	Login page is responsive and usable across screen sizes.	Page responsive and usable on all tested devices.	Pass
TC_Login_19	1. Enter valid credentials. 2. Use the browser "Remember Password" feature. 3. Reload login page.	Passwords are remembered or auto-filled by browsers securely.	Password auto-filled by browser.	Pass
TC_Login_20	1. Enter username in different cases (e.g., "ADMIN" vs "admin"). 2. Enter valid password. 3. Click Login.	Login is case-insensitive for username and succeeds.	Login is case-insensitive and successful.	Pass
TC_Login_21	1. Login successfully. 2. Click Logout. 3. Use the browser back button.	User is redirected to the login page; cannot access the dashboard without login.	Users cannot access the dashboard via back button.	Pass
TC_Login_22	1. Try to access the dashboard URL without login. 2. Observe redirection.	Users should be redirected to the login page (no	Unauthorized access blocked and redirected to login.	Pass

		unauthorized access).		
TC_Login_23	1. Login and stay idle for configured timeout duration. 2. Observe session expiration behavior.	User is logged out automatically after timeout.	User logged out after inactivity timeout.	Pass
TC_Login_24	1. Login from one device. 2. Login from another device. 3. Verify session behavior on both devices.	Sessions handled properly; no session conflicts or security issues.	Sessions work properly without conflict.	Pass
TC_Login_25	1. Login and close browser/tab without logout 2. Reopen and try accessing dashboard.	Session ends properly; user is logged out or prompted to login again.	Session is not invalidated; login required.	Fail
TC_Login_26	1. Submit login credentials. 2. Open browser devtools → Network tab. 3. Inspect request payload for password.	Password should NOT be visible in plain text in network requests.	Password visible in plain text in payload.	Fail
TC_Login_27	1. Attempt login during server downtime. 2. Observe system response.	System shows maintenance or error messages without crashing.	System shows a "Server not reachable" message.	Pass
TC_Login_28	1. Login from different browsers (Chrome, Firefox, Edge, Safari). 2. Verify login works consistently.	Login works properly and consistently across browsers.	Login successful on all tested browsers.	Pass
TC_Login_29	1. Enter valid credentials. 2. Click Login. 3. Observe login processing time.	Login completes within 2 seconds under normal conditions.	Login took 1.8 seconds; performance acceptable.	Pass

TC_Login_30	1. Enter valid credentials. 2. Click Login. 3. No loading indicator appears.	Loading spinner or indicator is shown during login processing.	No loading indicator shown; user confused (usability issue).	Fail