## **OrangeHRM Project - Summary Report**

**Project Name:** OrangeHRM  
**Reported By:** Sahil Khan  
**Date:** 19 January 2025

### **1. Test Scenarios & Test Cases Overview**

The testing of the **OrangeHRM** platform focused on verifying the functionality and performance of several key features. The test scenarios provided critical insights into how the system is performing across different functionalities. Below is a summary of the test cases for each key area.

#### **1.1. User Login**

* **Objective:** Test login functionality with both valid and invalid credentials.
* **Test Cases:**
  + Login with valid username and password
  + Login with invalid username
  + Login with invalid password
  + Login with empty fields
  + Login with case-sensitive credentials
* **Expected Results:** Successful login with valid credentials; error messages for invalid input.

#### **1.2. Forgot Password**

* **Objective:** Test the password recovery and email trigger functionality.
* **Test Cases:**
  + Reset password with a valid registered email
  + Reset password with an unregistered email
  + Reset password with an empty email field
  + Verify email trigger and reset link
* **Expected Results:** Password reset email triggered correctly; error for unregistered email.

#### **1.3. Session Management**

* **Objective:** Verify session expiry and logout behavior.
* **Test Cases:**
  + Session expiry after inactivity
  + Successful logout
  + Session destruction after logout
* **Expected Results:** User should be logged out after session timeout; successful logout and session clearance.

#### **1.4. Admin Dashboard Access**

* **Objective:** Test access control for admin functionalities.
* **Test Cases:**
  + Admin login to dashboard
  + Non-admin access restriction
* **Expected Results:** Admin users can access HR functionalities; non-admin users are restricted.

#### **1.5. Role-Based Access Control**

* **Objective:** Verify permissions for admin and employee roles.
* **Test Cases:**
  + Admin permissions for employee management
  + Employee restricted access to admin features
* **Expected Results:** Admins have full access to employee management; employees are restricted.

#### **1.6. Multi-Language Support**

* **Objective:** Test language selection and content translation.
* **Test Cases:**
  + Language selection option
  + Content translation across languages
* **Expected Results:** Language should change according to selection; all content should be translated accurately.

#### **1.7. Responsive Design**

* **Objective:** Validate UI responsiveness across devices.
* **Test Cases:**
  + Desktop layout
  + Tablet layout
  + Mobile layout
* **Expected Results:** UI should adjust to the screen size of each device without issues.

### **2. Bug Report Overview**

The **bug report** provided insights into various issues encountered during testing. Below is a summary of the key bugs found:

#### **2.1. Critical & High Priority Bugs**

* **Invalid Credentials Not Triggering Error**: The system failed to show error messages when invalid credentials were entered, causing confusion for users. This was identified as a **critical issue**.
* **Role-Based Access Control Issues**: Employees were able to access the admin dashboard, which led to **critical security vulnerabilities**.
* **Admin Dashboard Not Visible for Admin User**: Admin users were unable to access the HR functionalities, which is a **critical access control failure**.
* **Failed Login Attempt Lockout Not Triggered**: There was no lockout mechanism in place after multiple failed login attempts, leading to **potential brute-force attack risks**.

#### **2.2. Major Bugs**

* **Password Recovery Email Not Triggered**: Password reset emails were not being sent to users after submitting a valid email for password recovery.
* **Session Timeout Not Triggering Logout**: Users remained logged in even after the session timed out, causing potential security risks.
* **Error Message Clarity**: When fields were left empty, the error message displayed was generic, making it unclear that both username and password were required.
* **Missing Validation for Password Strength**: The password change page allowed weak passwords without enforcing strength requirements, creating **security concerns**.
* **Notification for Pending Tasks Not Triggered**: The system failed to notify users about pending tasks, potentially causing delays in work processes.

#### **2.3. Minor Bugs**

* **Multi-Language Dropdown Not Functional**: The language dropdown did not function properly, preventing users from changing the language.
* **Inconsistent Button Colors**: Buttons displayed inconsistent colors across the platform, violating the UI design standards.
* **Missing Logout Confirmation Prompt**: The system lacked a confirmation prompt before logging users out, leading to unintentional logouts.
* **Incorrect Display of Time Zone in Profile**: Users' time zones were displayed incorrectly in their profiles.

#### **2.4. Low Priority Bugs**

* **Database Connection Error Not Handled Gracefully**: When the database connection was unavailable, the system displayed technical error messages to users instead of user-friendly alerts.

### **3. Overall Observations**

* **Critical Issues**: The bugs related to **invalid credentials** and **role-based access control** are of utmost importance as they can directly affect security and user experience. Immediate fixes are required.
* **Functionality**: Key features such as **login**, **password recovery**, and **session management** are mostly functioning well, with minor issues needing attention.
* **UI/UX**: Issues related to **responsive design** and **UI consistency** across different devices and platforms need to be addressed for improved usability.
* **Security**: There are several security concerns, including the lack of password strength validation and session timeout handling. These should be prioritized.
* **Localization**: Multi-language support requires attention as it is not functioning as expected.

**4. Recommendations**

* **Security Enhancements**: Implement proper error handling for invalid credentials, session timeout, and failed login attempts. Ensure that password strength is validated and roles are enforced properly.
* **Bug Fixes**: Resolve the bugs identified in critical areas (e.g., role-based access control, password recovery email, etc.).
* **UI Improvements**: Focus on mobile responsiveness and consistent button styling. Ensure that language settings are functioning correctly.
* **User Experience**: Improve error message clarity and add confirmation prompts where necessary (e.g., logout).

**Conclusion:**The **OrangeHRM** platform is generally functional but requires attention to several critical and high-priority issues. Addressing the identified bugs will improve both security and user experience, ensuring a more reliable and user-friendly system.