Report: Authentication Feature Testing

Tester: Rifaa Muhammad Ridzqullah

Findings

- **Registration Feature**: All test cases (both positive and negative) passed successfully. This includes scenarios such as successful registration, handling of duplicate emails, and validation of weak passwords.

- **Login Feature**: The login test cases demonstrated successful handling of valid and invalid credentials. All test cases passed, showing the system's ability to manage both successful logins and failed login attempts with proper error messaging.

- **Change Password Feature**: The system handled password change functionality correctly in all cases. Test cases for both successful password changes and error handling for incorrect input passed.

Corrective Steps

Since all test cases passed successfully, there are no immediate corrective steps required. The system appears to be functioning as intended for all core authentication processes.

Recommendations

1. **Continuous Monitoring**: Even though the test cases passed, it is recommended to regularly retest the authentication system, especially after significant updates or changes to ensure continued reliability.

2. **Edge Case Testing**: Expand the test coverage by adding edge case scenarios, such as handling extremely long usernames/passwords, special characters in input fields, or high-volume login attempts (to check for potential vulnerabilities).

3. **Security Review**: Conduct regular security audits on the authentication feature to identify potential risks, especially regarding encryption methods and data storage practices for sensitive information like passwords.

4. **User Experience Enhancement**: Consider improving user feedback during authentication (adding progress indicators during login or registration) and ensuring error messages are not only clear but also actionable for the user.

This analysis indicates that the authentication feature is currently robust, but additional preventative measures could further enhance its reliability and security.