Title: Registered User Login From a New Device

Test plan

Objective: The login functionality should be secure, easy to use, and implemented according to the given requirements, including account access from a single device.

Scope**:**

1. Functional Testing:
    a. Validate login functionality.
    b. Validate OTP authentication.
    c. Validate session management (logout from other devices).
2. Non-functional Testing:
    a. Performance testing (response times for login operations)
    b. Usability testing (ease of navigation and input validation).
    c. Security testing (unauthorized access prevention, OTP expiry, Session expiry).
    d. Network testing: Stable and unstable internet connections.

Entry Criteria:

1. Development for the login feature is completed.
2. Completion of dev documentation.
3. Test environments are set up.

Exit Criteria:

1. All acceptance criteria are met.
2. Test coverage is 100% for functional scenarios and 80% for edge cases.
3. All high-severity defects are fixed.

Risk based testing (RBT)

1. Incorrect Credential Handling:
    a. Risk: Unauthorized users accessing accounts due to weak validation.

    b. Mitigation: Thorough testing of input validation and authentication logic.
2. Session Management:
    a. Risk: Failure to log out from all other devices.
    b. Mitigation: Test session termination functionality rigorously.
3. OTP Handling:
    a. Risk: OTP bypass or brute force attempts.
    b. Mitigation: Validate OTP expiry and rate limiting.

Possible Test Cases

Acceptance Criteria Test Cases:

1. Successful Login:
    a. Verify the login page loads correctly.
    b. Verify users can input phone numbers and passwords.
    c. Validate that an OTP is sent to the registered number.
    d. Verify entering the correct OTP logs the user in.
    e. Verify a success message is displayed after login.
    f. Verify the account is logged out from all other devices.
2. Session Management:
    a. Ensure all active sessions on other devices are terminated after login.
    b. Validate attempts to use old sessions result in a forced logout.

Edge Cases:

1. Verify behavior when invalid phone numbers or passwords are entered.
2. Verify behavior when empty field and space are entered
3. Test with incorrect OTPs (expired, reused, or wrong codes).
4. Attempt login with SQL injection inputs.
5. Test brute force protection for login credentials and OTPs.
6. Simulate SMS delivery failures and ensure the system handles them gracefully.
7. Validate OTP behavior under poor network conditions.
8. Simultaneously attempt login from multiple devices and validate only one session remains active.

Test Runs

Run 1: Functional Test Run
Run 2: Security Test Run
Run 3: Usability Test Run
Run 4: Performance Test Run
Run 5: Regression Test Run