Executive Summary

4. Executive Summary: Echogpt.live Sign-Up & Authentication Test

4.1 High-Level Overview of Findings

This report summarizes the testing activities and outcomes for the sign-up and authentication feature of the Echogpt.live platform. A comprehensive test suite of 31 test cases was executed to validate functional, security, usability, and compatibility requirements.

The testing revealed that the core functionality of the sign-up and login process is working as intended. All primary user flows, including email registration and third-party authentication (Google, Twitter, GitHub), passed successfully. However, this positive result is severely undermined by the discovery of a critical security vulnerability and a significant accessibility issue.

Key Statistics:

- Test Coverage: 96.8% (30 of 31 test cases executed)
- Pass Rate: 90.3% of all planned tests, 93.3% of executed tests
- Critical Defects: 2 High-Severity defects identified

4.2 Quality Assessment

The overall quality of the sign-up feature is moderate. While the core functionality is working (account creation, OTP verification, duplicate prevention), several critical usability and error-handling gaps remain. These could lead to confusion, poor user experience, and potential support escalations if released in production.

Strengths :

- **User Registration:** The process for new users to sign up with an email and verify via OTP is smooth and reliable.
- **Third-Party Integration:** Signing up and logging in via Google, Twitter, and GitHub works flawlessly, providing a good user experience.
- **Input Validation:** The system correctly validates and rejects invalid inputs, such as empty fields, overly long names, and incorrect email formats.
- **Cross-Platform Compatibility:** The feature performs consistently across different web browsers and device types.

Critical Weaknesses:

- **Security Flaw (Critical):** The most severe finding is a session management vulnerability. The system fails to terminate a user's active session when another login is attempted on the same browser. This allows users to inadvertently access each other's accounts and data by using the browser's back button, representing a major data privacy breach.
- **Accessibility Issue:** The sign-in buttons for Twitter and GitHub have insufficient color contrast in dark mode, failing WCAG guidelines and making them unusable for individuals with visual impairments.
- **Lack of Error Feedback:** In specific failure scenarios (e.g, entering an incorrect OTP), the system fails silently or redirects without providing a clear error message, leading to user confusion.

4.3 Risk Assessment and Recommendations

Risk Level: High if released without fixes, as users may face account creation or login failures, damaging trust.

4.3.1 Primary Risks:

1. **Incorrect handling of unregistered emails**
   - **Impact:** Users may be redirected to the OTP screen without notification that the email is unregistered.
   - **Risk:** High
2. **Weak input validation (symbols, special cases)**
   - **Impact:** Invalid or malformed data may enter the system, leading to data integrity and security issues.
   - **Risk:** Low
3. **Accessibility compliance gaps**
   - **Impact:** Users with disabilities may face difficulty using the system, resulting in legal and inclusivity concerns.
   - **Risk:** Medium
4. **Session Mixing Vulnerability**

    - **Impact:** Active sessions may overlap between users, causing potential data leakage or unauthorized access.
    - **Risk:** Critical (High – Blocking, must be fixed immediately before release)

5. **Poor Accessibility (UI)**
    - **Impact:** Users with visual impairments may not be able to navigate due to poor contrast and labeling.
    - **Risk:** Medium
6. **Silent Failure Modes**
    - **Impact:** Some actions fail without error messages, leaving users unaware of system issues.
    - **Risk:** Medium (Address in the next development sprint)

4.3.2 Recommendations:

- Fix error messaging for unregistered emails during sign-in.
- Improve user feedback for failed scenarios (OTP not received, invalid input).
- Conduct additional security testing (brute force OTP attempts).
- Perform cross-device/browser testing for consistency.
- Fix the session mixing vulnerability before release.
- Improve accessibility features and compliance.
- Monitor and document silent failures to prevent user confusion.

4.4 Next Steps for the QA Process

1. Share the defect report with the development team and prioritize fixes.
2. Re-run regression testing after fixes are deployed.
3. Conduct additional **exploratory testing** to validate edge cases.
4. Plan for a **UAT (User Acceptance Testing)** round with real users.
5. Prepare automation test scripts for regression to ensure long-term stability.