Gathering Results

Evaluation will focus on verifying that the core functional and non-functional requirements are met. This will include:

1. **Functional Validation**
    - Verify that local login/signup works correctly and securely.
    - Test login with Google and GitHub for both new and existing users.
    - Confirm that `Admin` users can perform all user CRUD operations via the UI.
    - Confirm that `User` role has read-only access and is correctly restricted from create/update/delete operations.
    - Ensure refresh token flow works as intended and access tokens are refreshed without forcing logout.
2. **Security Checks**
    - Validate password hashes are stored using bcrypt.
    - Ensure JWTs include expiration and role claims.
    - Manually and automatically test role-based endpoint access.
    - Review OAuth implementation against provider docs for token validation and user identity.
3. **Scalability Testing**
    - Load test login and token generation endpoints under simulated user traffic.
    - Test database performance with a few thousand user records.
4. **Code & Infrastructure Review**
    - Ensure code adheres to SOLID and clean architecture principles.
    - Confirm all secrets are managed via environment configs.
    - Validate that the system can be extended with more SSO providers with minimal effort.
5. **Success Criteria**
    - All Must/Should requirements fulfilled with passed QA.
    - No major security vulnerabilities detected in authentication/authorization flows.
    - Deployed system stable under moderate concurrent load (e.g., 100–500 concurrent users).