AI-Powered Q&A Platform - Project Document

1. Project Overview

The AI-Powered Q&A Platform is a full-stack Rust-based web application that allows users to ask technical questions, receive AI-generated responses, and execute code to detect and fix compilation or runtime errors. The platform integrates AI models for intelligent suggestions and runs code in a secure environment to analyze errors.

2. Tech Stack

- Frontend: Leptos or Yew (Rust-based UI)
- Backend: Axum or Actix-web
- Database: PostgreSQL with SQLx or Diesel
- AI Integration: OpenAI API or on-prem LLM (llama.cpp)
- Code Execution: Secure sandbox using WebAssembly (wasmtime) or Dockerized runtime
- Authentication: OAuth (GitHub, Google)

3. Features & Functionality

1. User Authentication & Reputation System
2. AI-Powered Answer Suggestions
3. Secure Code Execution & Error Detection
4. Search & Tagging System
5. Community Voting & Moderation
6. Real-time Notifications & WebSockets

4. Architecture

The system follows a microservices-inspired architecture:
- The frontend interacts with the backend via a REST API or GraphQL.
- The backend processes questions, calls AI services, and manages code execution.
- The AI module analyzes questions and suggests answers.
- A sandboxed execution environment safely runs submitted code.

5. Implementation Plan

Phase 1: Set up project structure and basic UI
Phase 2: Implement backend APIs and database models
Phase 3: Integrate AI-powered Q&A system
Phase 4: Implement secure code execution
Phase 5: Add voting, search, and real-time notifications
Phase 6: Final testing and deployment

6. Security Considerations

- Prevent malicious code execution by using sandboxing (wasmtime, Docker)

- Implement rate limiting and authentication to prevent spam
- Sanitize user input to prevent XSS and SQL injection
- Monitor and log system activity for security analysis

7. Deployment Strategy

- Use Docker for containerized deployment
- Deploy backend using AWS, DigitalOcean, or Fly.io
- Use PostgreSQL hosted on a managed service
- Set up CI/CD with GitHub Actions