Agentic System Design:

1. Design me a solution for data transformation from one format into another format.
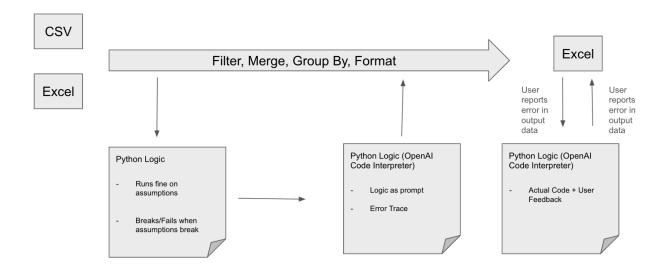
Your task is to create a secure FastAPI service that allows safe execution of Python code generated by LLMs for data processing.

Requirements:

- Build a system that accepts CSV/Excel files, processes them with Python code in a sandbox, and returns transformed data
- Implement proper security measures to isolate execution and prevent system vulnerabilities
- Create endpoints for file upload, code execution, results retrieval, and error reporting
- Ensure no sensitive data is exposed to LLMs
- Include appropriate error handling and timeout mechanisms

Evaluation Focus:

- Security implementation
- Error handling approach
- API design and data flow
- Code quality and organization

CSV

Excel

Filter, Merge, Group By, Format

Excel

Python Logic

- Runs fine on assumptions

- Breaks/Fails when assumptions break

Python Logic (OpenAI Code Interpreter)

- Logic as prompt

- Error Trace

Python Logic (OpenAI Code Interpreter)

- Actual Code + User Feedback

User reports error in output data

User reports error in output data

- No data to be shared to LLMs to avoid hallucinations and data manipulation
- Python logic should run on internal cloud system.
- Safe checks on input prompts to avoid system failures