APflix Challenge Review

Tasks Completed:

Step 1: Create a local OpenAI Oracle

- Researched OpenAI's API.
- Developed a local Python script that accepts a user prompt and responds as ChatGPT.
- Addressed esoteric prompts by refining user input, a process that required some experimentation.
- Integrated the model's response with the book list.

Step 2: Security System Design

- Studied LLM vulnerabilities and categorized them into infrastructure and prompt engineering vulnerabilities.
- Due to time constraints, I initially focused on one feature, opting to implement a PII filter.

Step 3: Implement & Deploy on AWS

- As this was only my second project on AWS, I invested time in learning the best practices for project implementation. While I acknowledge there's room for improvement, I'm pleased with the outcome.
- Created a lambda function for receiving prompts and providing movie recommendations, followed by rigorous testing.
- Established an API Gateway to initiate the lambda function.
- Designed an HTML page (using a pre-existing template as a starting point).
- Linked the HTML page to the lambda function.
- At this juncture, the movie recommender page was functional.
- Explored PII filtering options and ultimately integrated AWS Comprehend.
- Developed a lambda function for PII filtering and set up an API Gateway for it.
- Integrated it with the HTML page.
- Implemented some front-end refinements.
- Created a draw.io diagram to illustrate the architecture.

Step 4: Add Engines

- Explored alternative engines apart from OpenAI. Since I didn't find a suitable free option, I added another OpenAI engine, providing users with a choice between two options.

Potential Enhancements with More Time:

1. Shifting PII processing to the backend, utilizing the initial lambda function.
2. Creating big scale for any scan
3. Exploring alternative methods (such as vector databases) for comparing the movie list with OpenAI's output.
4. Enhancing the frontend for improved aesthetics and flexibility in configuring PII.

Reflection: This project marked my initial exposure to OpenAI's API and cloud infrastructure. I encountered a steep learning curve but found the experience incredibly rewarding. Thank you for your time!