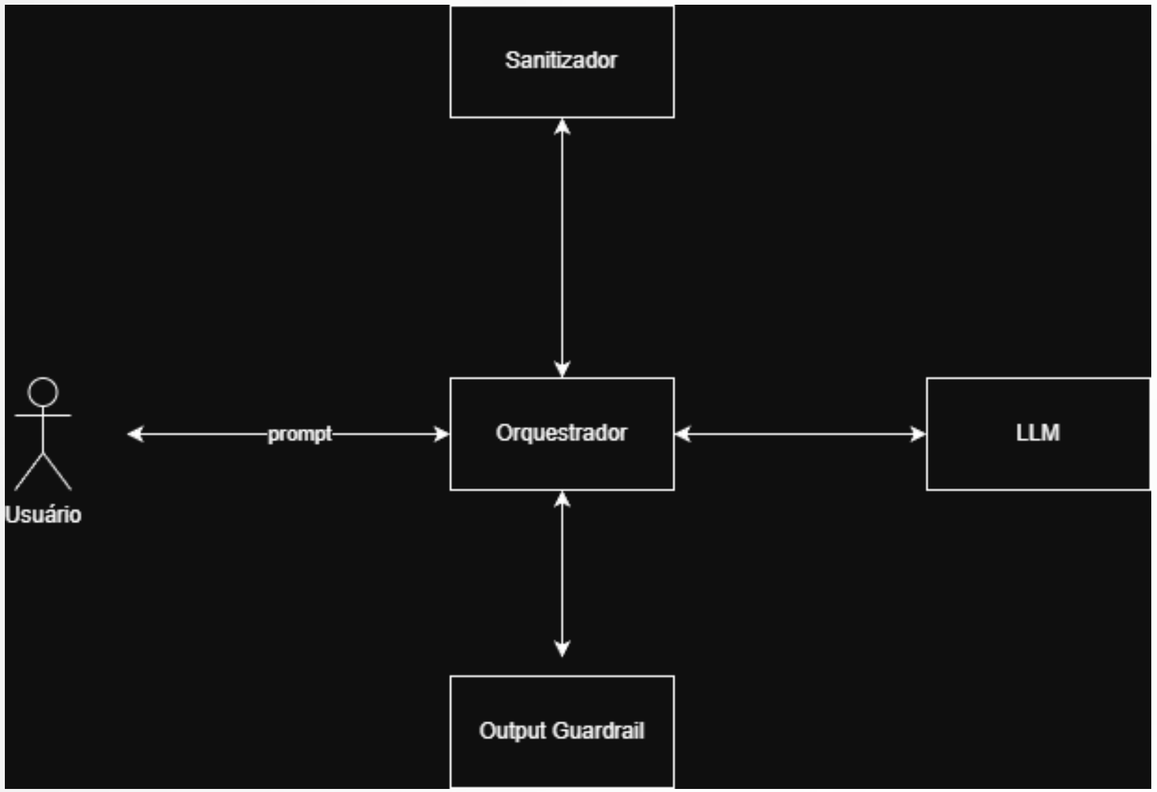
PLANEJAMENTO E IMPLEMENTAÇÃO

Grupo: Segurança de prompts em modelos de LLMS

Juan Gustavo, Lucas Emanoel, Lucas Messias, Joás Vitor e João Victor



ARQUITETURA

Composta por 4 entidades:

- Usuário (prompt)
- orquestrador
- sanitizador
- Serviço de LLM
- Output guardrail

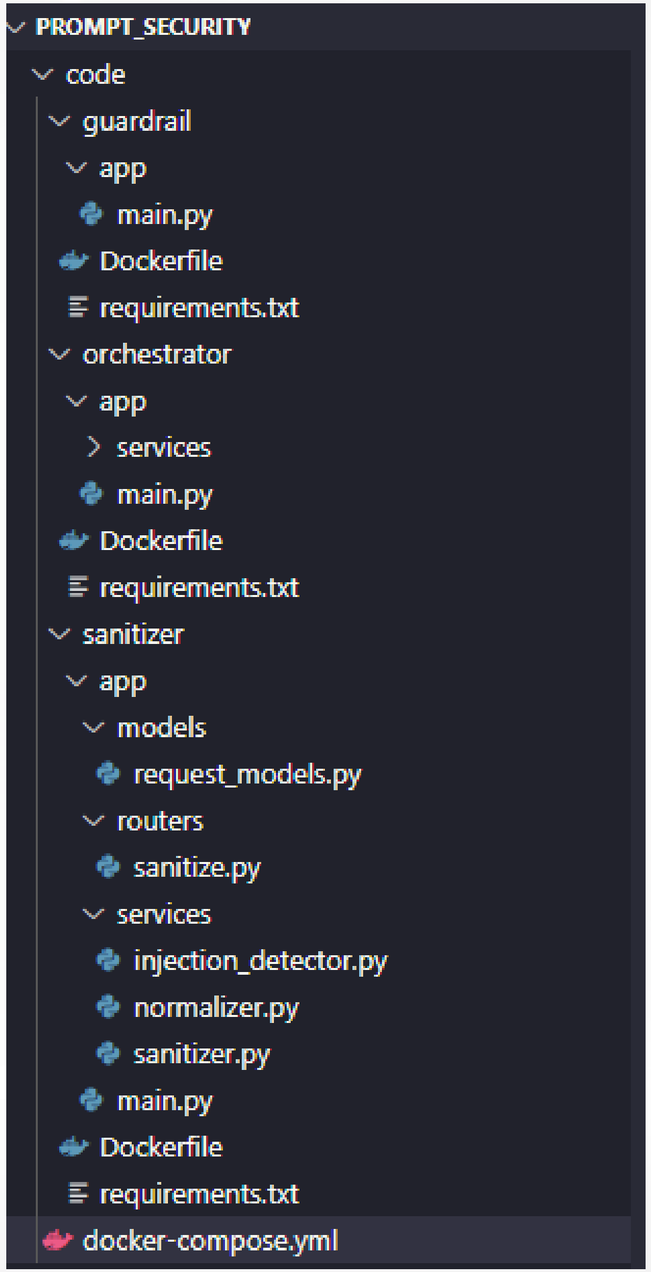
TECNOLOGIAS

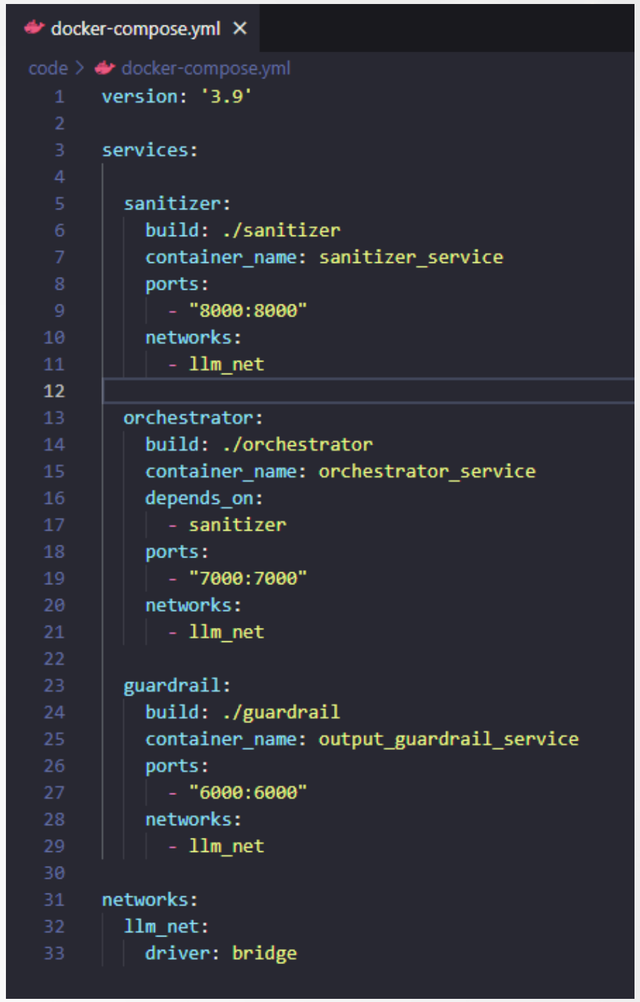
- Python
- FastApi/Uvicorn
- OpenAi Api
- Docker
- Draw.io

ESTRUTURA DO PROJETO

Foi montado o código inicial das entidades envolvidas no projeto

Foi montado o arquivo Dockerfile e docker-compose para automatizar a criação da estrutura do projeto





OBRIGADO