# Task

## Những gì đã làm được (theo code + mô tả)

1. **Đọc & xử lý tài liệu**
   - Đã hỗ trợ upload **PDF** → đọc text (`PyPDF2`), tách chunks (`CharacterTextSplitter`).
   - Đã có `get_vectorstore()` với **FAISS + HuggingFace embeddings** → đúng yêu cầu tuần 3 (KB + indexing).
2. **Vector Store + RAG cơ bản**
   - Đã build **FAISS index**.
   - Có retrieval chain (`ConversationalRetrievalChain`) → đúng tuần 7 (RAG).
3. **LLM Layer**
   - Dùng **Groq LLM (open-source GPT-OSS-20b)**.
   - Prompt đã nâng cấp: không chỉ trích xuất mà còn **"tự sáng tạo biến thể payload"**.
   - Có memory (`ConversationBufferMemory`) → lưu hội thoại (đúng scope tuần 7).
4. **UI**
   - Có giao diện **Streamlit**: nhập câu hỏi, chat, upload PDF → đúng scope tuần 4 (UI cơ bản).
5. **Guardrails ở mức nhẹ**
   - Prompt template đã có hướng dẫn **không bịa sai ngữ cảnh** → chạm vào scope tuần 3 (guardrails cơ bản).

---

## ❌ Những gì **chưa có** (so với scope)

- **Tuần 5–6 (ZAP/Burp integration + phân tích kết quả)**:

  Chưa tích hợp API ZAP, chưa parse JSON alerts, chưa gom nhóm kết quả.
- **Tuần 6 (Report)**:

Chưa có module export **báo cáo PDF/HTML**, chưa có JSON/YAML “finding template”.

- **Tuần 8 (Evaluation)**:

  Chưa có kịch bản đánh giá (offline/online).

- **Tuần 9 (Ops/Security)**:

  Chưa có rate-limit, retry, cache payload, ẩn PII.

- **Tuần 10–12 (Hoàn thiện & Demo)**:

  Chưa kiểm thử đầy đủ, chưa có i18n, chưa có demo slides.