Portfolio – Jathin Varma Mandapati

AI Engineer | Agentic AI | RAG & Security Systems

1. RAG Chatbot – Hybrid Retrieval with RBAC

Technical Standpoint

- Built a retrieval-augmented generation system combining MySQL (structured queries), Qdrant (semantic retrieval using all-MiniLM-L6-v2 embeddings), and ElasticSearch (BM25 keyword search).
- Designed hybrid retrieval logic in Python with LangChain to merge and label semantic vs. keyword hits.
- Enforced RBAC filters via SQLAlchemy, restricting visibility by organization, domain, and customer.
- Secured ElasticSearch inside Docker with localhost binding and validated isolation through curl-based health checks.
- Provided a Streamlit interface for role selection, query input, and combined summary visualization.

Business Standpoint

- Enabled secure, multi-tenant data access without requiring SQL knowledge.
- Increased efficiency by reducing dependency on DB engineers for everyday queries.

2. Schema-Aware SQL Chatbot

Technical Standpoint

- Implemented schema-aware query generation using Mistral-7B hosted on Hugging Face endpoints.
- Extracted schema dynamically via SQLAlchemy introspection instead of static JSON mappings.
- Managed token limits by chunking query outputs into smaller responses for processing.
- Delivered query visualizations through Plotly, ensuring outputs were both textual and graphical.
- Captured user feedback logs to continuously refine model accuracy over time.

Business Standpoint

- Allowed natural language to SQL conversion, eliminating the SQL barrier for business teams.

- Reduced reporting cycles by approximately 70%, boosting decision-making speed within Cybermindr.

3. Exploit Explanation Tool

Technical Standpoint

- Designed a FastAPI-based backend to ingest vulnerability metadata and screenshots.
- Processed and compressed images using Pillow for efficient GPT-4o Vision analysis.
- Generated Markdown reports covering issue, impact, severity, lifecycle, and flow diagrams with Mermaid.js.
- Managed token budgeting with tiktoken to balance metadata, image tokens, and output size.
- Built an interactive Streamlit interface to render explanations, flowcharts, and downloadable reports.

Business Standpoint

- Added explainability and visualization to vulnerability reports, making them human-readable.
- Accelerated remediation by transforming technical findings into structured outputs analysts could act on quickly.

4. LLM Security Testing Framework

Technical Standpoint

- Created playbook-driven test suites in JSON covering prompt injections, data leaks, hallucinations, and obfuscation exploits.
- Integrated a GPT-based judge model to evaluate outputs with PASS/FAIL labels and reasoning.
- Deployed FastAPI endpoints to expose automated execution of security tests.
- Provided monitoring via Streamlit to visualize verdict distributions and failure patterns.
- Incorporated pytest-inspired runners to maintain modular and repeatable testing flows.

Business Standpoint

- Introduced a repeatable AI security testing layer, strengthening Cybermindr's security-first positioning.

- Improved transparency in security validation with structured reports and explainable verdicts.

5. Gitleaks Augmentation – Secret Detection

Technical Standpoint

- Extended Gitleaks by parsing its outputs and enhancing results using GPT-4 via LangChain.
- Classified secrets by context (API keys, tokens, database credentials) instead of generic labeling.
- Generated AI-driven remediation steps to reduce manual triage overhead.
- Designed support for URL-based report ingestion to integrate seamlessly with CI/CD pipelines.

Business Standpoint

- Enhanced DevSecOps workflows by embedding contextualized secret detection into Cybermindr.
- Reduced remediation time through prioritized alerts and actionable recommendations.

Summary

Across these five projects, I have consistently combined **advanced AI engineering** with a **security-first mindset**. My work at Cybermindr demonstrates the ability to:

- Architect **retrieval and chatbot systems** that balance usability with strict role-based access control.
- Develop **explainable AI tools** that turn technical outputs into actionable insights.
- Build **security validation frameworks** that proactively test and harden LLM deployments.
- Enhance **Security pipelines** by embedding AI-driven intelligence into open-source security tools.

These projects highlight my strength in delivering solutions that are both **technically robust** and **aligned with real-world enterprise needs**, showing how I approach AI engineering with a balance of innovation and security.