castlebbs /
augmented-software-engineer

Code | Issues | Pull requests | Actions | Projects | Security | Insights

Code presented during the meetup Augmented Software Engineer

0 stars **0** forks **1** watching Branches Activity
Tags

Public repository

1 Branch **0** Tags Go to file t Go to file + Add file Code ···

castlebbs First commit 91513dc · 2 days ago

cryptoagent	First commit	2 days ago
designdoc	First commit	2 days ago
vulnerablecode	First commit	2 days ago
.gitignore	First commit	2 days ago
README.md	First commit	2 days ago

README

Augmented Software Engineer Security Demo Repository

This repository was created for a live demo at the **Augmented Software Engineer** meetup group in May 2025. It showcases how large language models (LLMs) and agentic workflows can be used to analyze, reason about, and review code and technical documents for security purposes.

Repository Structure

- `cryptoagent/`
  Contains a proof-of-concept smolagent agent that automates security reviews of source code using cryptographic features. Demonstrates orchestrating multiple LLMs for specialized tasks, such as code search and security analysis.
- `vulnerablecode/`
  Includes intentionally vulnerable code samples. These are designed for testing LLMs' ability to identify insecure patterns and vulnerabilities. **Do not use these samples in production.**

- `designdoc/`
  Contains a fictional design document (`ecommerce.md`) for a baseball e-commerce website. Used to test LLMs' reasoning and threat modeling capabilities on technical documentation.

Purpose

This repo demonstrates how LLMs and agentic tools can augment software engineers by automating code review, vulnerability detection, and design analysis. Each directory contains examples or workflows used during the demo.

> **Note:** All code and documents are for demonstration and educational purposes only. Do not use any code here in production environments.

Releases

No releases published

Packages

No packages published

Languages

● **C#** 52.6% ● **Python** 28.3% ● **Java** 17.7% ● **C** 1.4%