



CYREX

IntelliAudit

Evaluate Smart Contracts on Security Vulnerabilities

Idea

- ✓ Evaluate code on security vulnerabilities using LLMs
- ✓ Upgrade static code analysis with LLM
- ✓ Problem: security audits are expensive
- ✓ Problem: people can overlook vulnerabilities
- ✓ Impact of a security issue can be very serious

MVP

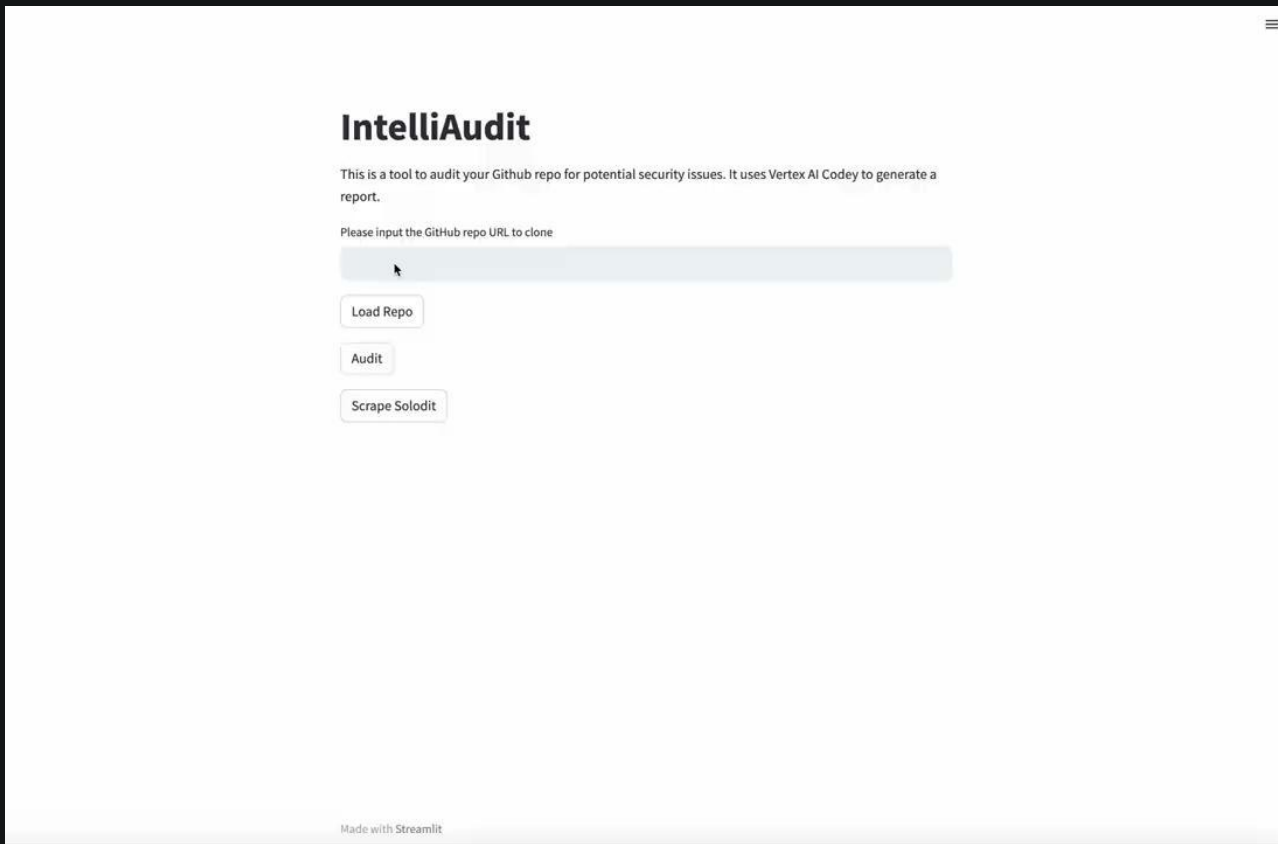
- ✓ Focus on smart contracts
- ✓ Use known static code analyzer (slither)
- ✓ Evaluate using vulnerable smart contracts

Product

- ▲ Pulls GitHub repo
- ▲ Installs dependencies (if any)
- ▲ Loads project or individual smart contract
- ▲ Analyzes data with Slither
- ▲ Uses langchain agent to determine vulnerabilities



Demo



The screenshot shows a web application interface for IntelliAudit. At the top right, there is a hamburger menu icon. The main heading is "IntelliAudit". Below it, a paragraph explains that the tool audits GitHub repositories for security issues using Vertex AI Codey. A text input field is provided for the user to enter a GitHub repository URL. Below the input field are three buttons: "Load Repo", "Audit", and "Scrape Solodit". At the bottom center, it says "Made with Streamlit".

IntelliAudit

This is a tool to audit your Github repo for potential security issues. It uses Vertex AI Codey to generate a report.

Please input the Github repo URL to clone

Load Repo

Audit

Scrape Solodit

Made with Streamlit

Lessons learned

- ? Vertex AI models don't work great as agents (GPT-4 is a lot better)
- ? Fine-tuning models was not possible
- ? Missing OpenAI functions



Next goals

- ✓ Support other programming languages
- ✓ Support more complex projects
- ✓ Improve the agent
- ✓ Use fine-tuned model

