CHRISTIAN VARI

LLMS FOR AUDIT REPORTING

Why security researchers must avoid cloud LLMs and how to build a safe, private AI assistant

WHY USE LLMS FOR WRITING AUDIT REPORTS

- Quickly translate raw GitHub comments into structured findings
- Enforce a consistent format and style across the entire report
- Improve clarity and tone of writing to match client expectations
- Reduce time spent drafting while preserving technical depth

LLMS ACCELERATE THE REPORTING PHASE WITHOUT COMPROMISING ON QUALITY

THE PROBLEM

Cloud-based LLMs = NDA violation risk

01

BREACH OF CONFIDENTIALITY

Using cloud LLMs like ChatGPT or Claude can inadvertently expose client code, including unfixed vulnerabilities, to external servers — violating strict NDAs.

02

LEGAL & ETHICAL RISKS

Many audit contracts include legal obligations. Using third-party cloud models without consent may breach data protection laws and intellectual property agreements.

03

LOSS OF CLIENT TRUST

Clients rely on auditors for discretion. Sharing even snippets of proprietary code externally undermines this trust and can damage reputation.

THE SOLUTION

Use Locally Hosted LLMs

Full data privacy: nothing leaves your machine

No risk of external leaks

Complete control over models and prompts

Note: We'll use Ollama + Open WebUI

SETUP OVERVIEW

Steps to create the local environment:

01

INSTALL OLLAMA
(LLM RUNTIME)

02

LOAD MODEL
(E.G. LLAMA 3, GEMMA 3)

03

INSTALL OPEN WEBUI
(GUI FOR CHAT INTERFACE)

STEP-BY-STEP INSTALLING OLLAMA

CODE

```
curl -fsSL https://ollama.com/install.sh | sh
ollama run gemma3:latest
```

MODELS AVAILABLE

- llama3
- deepseek-r1
- gemma3

STEP-BY-STEP: SETTING UP WEBUI

CODE

```
docker run -d -p 3000:8080 \
--add-host=host.docker.internal:host-gateway \
-v open-webui:/app/backend/data --name open-webui \
--restart always ghcr.io/open-webui/open-webui:v0.6.5
```

ACCESS VIA: `http://localhost:3000`

CHAT CUSTOMIZATION FOR REPORTING

ADD A SYSTEM PROMPT:

https://raw.githubusercontent.com/christianvari/secure-audit-reporting-with-llms/refs/heads/main/system_prompt.md

DRAFTING ISSUES FROM GITHUB

01 Copy a vulnerability summary from GitHub

02 Paste into Open WebUI chat with custom prompt

03 LLM outputs a formatted issue ready to go into your audit report

BENEFITS COMPARISON

Feature	Cloud LLMs	Local LLMs
Data Privacy	✗	✓
NDA Compliance	✗	✓
Prompt Customization	Limited	Full Control
Offline Capability	✗	✓

DEMO TIME

Use Case

From GitHub note → Oak-style draft in seconds

WORKS WITHOUT BREAKING ANY LEGAL AGREEMENTS

FINAL TAKEAWAY

LLMs can transform your audit workflow, just make sure they're working for your security, not against it.

Q&A

QUESTIONS?

Let’s discuss how you can make your audit process more efficient and secure.