Local Ai pour cybersec

Post original: https://www.linkedin.com/feed/update/urn:li:activity:7467552303269462017

Je viens de finir de monter ma propre IA de pentest. Gratuite, en local et non censurée.

Et honnêtement, je ne reviendrai pas en arrière.

Ce qu'elle fait pour moi :

→ Elle lit mes rapports de pentest passés et m'aide à structurer les nouveaux → Elle interroge ma base OWASP / PayloadsAllTheThings / cheat sheets perso → Elle génère du code d'exploitation sans me répondre « désolé, je ne peux pas c'est interdit □□ » → Côté inférence : zéro fuite. Mes prompts et documents restent en local. (Petit détail technique : pensez à désactiver la télémétrie anonyme d'AnythingLLM dans les paramètres pour aller au bout de la démarche)

La config : une RTX 4070 (12GB VRAM), LM Studio, AnythingLLM, et le modèle Qwen 3.5 9B en version non censurée.

Le seul vrai piège que j'ai rencontré et que personne ne mentionne dans les tutos anglophones : l'embedder par défaut est entraîné en anglais. Pour du contenu pentest en français, il faut absolument basculer sur BGE-M3 multilingue, sinon l'IA ne comprend pas la moitié de vos documents et pense que l'injection SQL est potentiellement une manipulation d'infirmière □

J'ai filmé tout le processus dans ma dernière vidéo. C'est le premier épisode, le prochain s'attaque aux agents et à l'automatisation directe avec Kali Linux□

---

https://www.youtube.com/watch?v=cWilfECHc6E