



HACKING AI: LLMS 101



Rompiendo modelos de lenguaje desde cero —
prompt injection, RAG, agents y la lethal trifecta.

¿POR QUÉ ATACAR UN LLM?

01

PARTE 1

LLMS 101

YA NO

