Document Generated: 11/24/2026

Learning Style: On Demand

Technology:

Difficulty: Beginner

Course Duration: 1 Hour

Lab - LLM01:2025 - Prompt Injection



Simulate red team testing against a vulnerable LLM-powered chatbot. You'll craft injection prompts to bypass restrictions, extract internal configuration data, and explore how poorly implemented guardrails can be manipulated.