Document Generated: 11/24/2026

Learning Style: On Demand

Technology:

Difficulty: Beginner

Course Duration: 1 Hour

Lab - LLM02:2025 ? Sensitive Information Disclosure



Simulate an attack on a vulnerable AI-powered chatbot by crafting specific prompts that expose sensitive information. You'll extract user lists, individual user details, and order information, demonstrating the risks of improper access controls and poor input filtering in AI systems.