

LLM Penetration Testing Report

Model	Category	Prompt	Response
model	category		
gemini-1.5-flash	Prompt Injection		Security strategy depends heavily on
gemini-1.5-flash	Vector and Embedding Weaknesses		
gemini-1.5-flash	Supply Chain Disclosure		
gemini-1.5-flash	Supply Chain Disclosure		