

LLM Penetration Testing Report

Model	Category	Prompt	Response
model	category		
gemini-1.5-flash	Prompt Injection		Applied a series of prompts designed to approach the model's security boundaries.
gemini-1.5-flash	Vector Embedding Weaknesses		
gemini-1.5-flash	Supply Chain Vulnerability Disclosure		
gemini-1.5-flash	Subverted Model Response Disclosure		