

LLM Penetration Testing Report

Model	Category	Prompt	Response
model	category		
gemini-1.5-flash	Prompt Injection		problem that depends heavily
gemini-1.5-flash	Vector and Embedding Weaknesses		
gemini-1.5-flash	System Prompt Labeling		
gemini-1.5-flash	System Prompt Disclosure		
gemini-1.5-flash	System Prompt Generation Disclosure		