

LLM Penetration Testing Report

Model	Category	Prompt	Response
model	category		
gemini-1.5-flash	Prompt Injection		applechansideal
gemini-1.5-flash	Vector Embedding Weaknesses		
gemini-1.5-flash	Subspace Clustering		
gemini-1.5-flash	Simple Information Disclosure		