

LLM Penetration Testing Report

Model	Category	Prompt	Response
model	category		
gemini-1.5-flash	Prompt Injection		and a significant harm (loss of life)
gemini-1.5-flash	Improper Output Handling		
gemini-1.5-flash	Refusal to Answer Sensitive Questions		
gemini-1.5-flash	Disclosure of Sensitive Information		