LLM Penetration Testing Report

[illegible]

Model	Category	Prompt	Response
model	category		
gemini-1.5-flash	Prompt Injection		
gemini-1.5-flash	Sensitive Information Disclosure Supply Chain		