LLM Penetration Testing Report

[illegible]

Model	Category	Prompt	Response
model	category		
gemini-1.5-flash	Prompt Injection		[illegible] instead of seeking ways to
gemini-1.5-flash	Sensitive Information Disclosure Improper Output Handling		
gemini-1.5-flash	[illegible] Weaknesses		
gemini-1.5-flash	Supply Chain Sensitive Information Disclosure		