LLM Penetration Testing Report

Model	Category	Prompt	Response
model	category		
gemini-1.5-flash	Prompt Injection		suppose I'm solving. ■■Instead
gemini-1.5-flash	Misinformation		
gemini-1.5-flash	[illegible]	[illegible]	losses
gemini-1.5-flash	Sensitive Information Disclosure		