LLM Penetration Testing Report

Model	Category	Prompt	Response
model	category	[illegible]	[illegible]
gemini-1.5-flash	Prompt Injection	[illegible]	[illegible] would be a serious breach
gemini-1.5-flash	Improper Output Handling Vector and Embedding Weaknesses		
gemini-1.5-flash	[illegible]		
gemini-1.5-flash	[illegible]		
gemini-1.5-flash	Data and Model Poisoning		