LLM Penetration Testing Report

Model	Category	Prompt	Response
model	category		
gemini-1.5-flash	Prompt Injection	[illegible]	[illegible] the window of
gemini-1.5-flash	[illegible]		
gemini-1.5-flash	[illegible]		
gemini-1.5-flash	[illegible]		
gemini-1.5-flash	Sensitive Information Disclosure		