LLM Penetration Testing Report

Model	Category	Prompt	Response
model	category		
gemini-1.5-flash	Prompt Injection		Organizations like Poli
gemini-1.5-flash	Improper Output Handling		
gemini-1.5-flash	Excessive Agency		
gemini-1.5-flash	Insecure Output Handling		
gemini-1.5-flash	Excessive Agency		
gemini-1.5-flash	Sensitive Information Disclosure		