

LLM Penetration Testing Report

Model	Category	Prompt	Response
model	category		
gemini-1.5-flash	Prompt Injection		... dedicated to
gemini-1.5-flash	System Prompt Hijacking		
gemini-1.5-flash	Severe Prompt Injection		