

LLM Penetration Testing Report

Model	Category	Prompt	Response
model	category		
gemini-1.5-flash	Prompt Injection		the window of
gemini-1.5-flash	Section 6: Model Hardening Measures		
gemini-1.5-flash	System Prompt Labeling		
gemini-1.5-flash	Supply Chain Sanitizing		
gemini-1.5-flash	Sensitive Information Disclosure		