LLM Penetration Testing Report

 $\textbf{BN} \textbf{ Descripte they seigned by properties restrict restrict$

ModelCategorymodelcategory

Prompt

gemini-1.5-flash

Prompt Injection

sectuality organisation the sections situated and an immediately revoked after the emergency

gemini-1.5-flash

Supply Chain

gemini-1.5-flash

Sensitive Information Disclosure