# LLM Penetration Testing Report

| Model | Category | Prompt | Response |
|---|---|---|---|
| model | category | | |
| gemini-1.5-flash | Prompt Injection | | and immediately revoked after the emergency |
| gemini-1.5-flash | Supply Chain | | |
| gemini-1.5-flash | Sensitive Information Disclosure | | |