Adversarial Prompting in LLMs

This section contains a collection of prompts for that raises awareness of different LLM vulnerabilities.

- **Prompt Injection**
- **Prompt Leaking**
- **Jailbreaking**

Last updated on September 19, 2024