ChatGPT 플러그인

외부 서비스와 API와의 상호작용을 가능하게 하여, AI가 실시간 데이터를 가져오거나, 예약을 진행하거나, 웹에서 정보를 검색할 수 있도록 합니다. 개발자들은 ChatGPT의 기능을 확장하여 특정한 필요나 기능에 맞춤화된 플러그인을 생성할 수 있었습니다.

GPTs

프롬프트 엔지니어링, 데이터, api 연결을 통해 만드는 나만의 챗gpt 커스터마이징

독립적인 AI 모델로, LLM에 기반하여 훈련됩니다. 이들은 텍스트 생성, 질문 응답, 컨텐츠 생성 등 다양한 작업을 수행할 수 있습니다. GPTs는 내장된 능력(예: 브라우징, DALL·E, 코드 해석기)을 포함하며, 새롭고 기존 사용자를 위한 사전 설정된 시작 프롬프트를 제공합니다.

API를 통해 외부 서비스와 상호작용도 가능

Chat gpt 플러그인

1. 어떤 것들 ex) chat gpt 플러그인을 통한 항공권 예약

2. 연동방식

3. 정보 유출 여부

4. 프로토콜

5. 플러그인 취약성 ex) askthecode에서 공격자가 피해자의 github 계정 제어

OAuth : 인터넷 사용자들이 비밀번호를 제공하지 않고 다른 웹사이트상의 자신들의 정보에 대해 웹사이트나 애플리케이션의 접근 권한을 부여할 수 있는 공통적인 수단으로서 사용되는 접근 위임을 위한 개방형 표준이다.

malicious plugin install with link -> victim이 type하는 민감한 정보가 plugin과 attacker에게 전달됨

AskThecode plugin이 user의 GitHub repositories와 interact하게 함 -> security flaw가 있다면 attacker는 victim's github account와 repository access를 zero-click exploit(user의 어떠한 action도 없이 뚫림)

attacker가 user가 link를 누르게 속여 victim account를 가져오고 plugin과 상호작용할 수 있음

1) web pilot - selenium web crawling

web page, pdf, data 접근을 도와주는 플러그인

3) canva - 이미지를 통한 링크 연결, 링크에서 디자인 다운

7) askyourpdf - 구글 계정 필요, 링크를 통한 pdf 공유

8) KAYAK ,flights, hotels, cars - 항공편 추천을 위한링크

9) code copilot

10) askthecode - github 계정 필요,

KAYAK

: 예산 안에서 항공편, 숙소, 렌탈이나 그 밖에 추천사항들을 search