Informe Explicativo: Web Security Advisor

Introducción

En un mundo digital donde las amenazas cibernéticas crecen a un ritmo alarmante, es crucial contar con herramientas que ayuden a los usuarios a navegar por internet de manera segura. El proyecto "Web Security Advisor" nace de la necesidad de ofrecer a sus usuarios una forma sencilla y efectiva de determinar si una página web es segura o no, utilizando tecnologías avanzadas de inteligencia artificial como ChatGPT. Este proyecto fue desarrollado en el contexto de la capacitación "IA for Developers" organizada por el equipo de CONSUL.Ti, con el propósito de demostrar cómo la inteligencia artificial puede aplicarse para resolver problemas sociales reales.

Descripción del Problema Social

La seguridad en línea es un problema crítico en la sociedad moderna. Los usuarios a menudo no cuentan con los conocimientos necesarios para evaluar los riesgos asociados con los sitios web que visitan. Esto los hace vulnerables a ataques como el phishing, el malware, y el robo de información personal. Este proyecto tiene como objetivo cerrar esta brecha de conocimiento al proporcionar una herramienta que automáticamente evalúa la seguridad de una página web, ofreciendo recomendaciones claras y fáciles de entender. De esta manera, se empodera a los usuarios, reduciendo su exposición a riesgos cibernéticos y promoviendo un uso más seguro de internet.

Implementación Técnica

El proyecto fue desarrollado como una extensión para Google Chrome, y su implementación se basa en los siguientes componentes clave:

- **manifest.json:** Este archivo define los permisos necesarios para la extensión, como el acceso a la red y la capacidad de ejecutar scripts en las páginas web visitadas.
- **background.js:** Es el script que se ejecuta en segundo plano y maneja la lógica principal, incluyendo la comunicación con la API de ChatGPT.
- **content.js:** Se encarga de interactuar con la página web actual, extrayendo información relevante para la evaluación de seguridad.

CONSULTi
code to build

Flujo de Trabajo

1. **Detección de la Página Web:** Cuando un usuario visita una página web, el script content.js extrae la URL y analiza aspectos básicos como el protocolo (HTTP/HTTPS) y el certificado SSL.
2. **Análisis con ChatGPT:** La información recolectada se envía al script background.js, que a su vez realiza una petición a la API de ChatGPT, proporcionando la información de la página web. Esta API utiliza modelos de lenguaje avanzados para analizar los datos proporcionados y determinar la seguridad de la página.
3. **Presentación de Resultados:** Basado en la respuesta de ChatGPT, se genera una notificación *push* indicando si la página es segura o no, junto con una explicación resumida para cada caso.

Uso de la API de ChatGPT

El uso de ChatGPT es crucial en la solución, ya que permite evaluar la seguridad de una página web no solo en términos de reglas estáticas, sino también utilizando un análisis contextual basado en patrones de riesgo identificados por el modelo de inteligencia artificial. Esto añade un nivel adicional de precisión y adaptabilidad, haciendo la herramienta más robusta frente a amenazas emergentes.

Impacto Social

El "Web Security Advisor" aborda un problema social significativo: la falta de educación en ciberseguridad entre los usuarios comunes. Al proporcionar una herramienta que hace el análisis automáticamente y presenta resultados en un lenguaje comprensible, se fomenta una cultura de seguridad en línea. Esto es especialmente relevante en un contexto donde la información personal y financiera está cada vez más expuesta en la red.

Conclusión

Este proyecto demuestra el poder transformador de la inteligencia artificial cuando se aplica con propósito y creatividad. Al integrar ChatGPT en una extensión de Chrome, se ha creado una solución que no solo mejora la seguridad en línea de los usuarios, sino que también les educa en el proceso. Este es un ejemplo de cómo la tecnología puede y debe ser utilizada para resolver problemas sociales reales, creando un impacto positivo en la sociedad.

Recomendaciones

- Implementar capacidades para analizar contenido dinámico como scripts de terceros, iFrames, y anuncios, que a menudo son vectores de ataque.
- Agregar una sección educativa dentro del popup o como una página adicional en la extensión donde los usuarios puedan aprender más sobre las amenazas cibernéticas y cómo protegerse.
- Introducir mecanismos de recompensación, como puntos o logros, para incentivar a los usuarios a revisar activamente la seguridad de las páginas que visitan y a aprender más sobre ciberseguridad.
- Permitir que los usuarios ajusten los niveles de sensibilidad para las alertas de seguridad, dando más control sobre lo que consideran como seguro o no.
- Implementar la extensión en otros navegadores, como Firefox, Edge y Safari, para alcanzar un público más amplio.