⚙️ Desafío Técnico: Diseño de Sistema de Evaluación de Vulnerabilidades Asistido por IA

En Mercado Libre, la gestión de riesgos asociados al uso extensivo de dependencias open source en un ecosistema de desarrollo de gran escala plantea desafíos importantes en términos de seguridad, escalabilidad y automatización.

Te proponemos diseñar una solución que permita evaluar de forma más precisa y contextualizada la severidad de vulnerabilidades encontradas en dependencias OSS, integrando inteligencia artificial como soporte para el análisis.

🎯 Objetivo del Desafío

Diseñar una solución (API Backend) que, mediante el uso de IA (idealmente LLMs), asista en el análisis y evaluación de vulnerabilidades de seguridad sobre dependencias open-source, considerando la descripción / definición de la vulnerabilidad y el contexto tecnológico de la aplicación potencialmente afectada:

Se espera que el diseño:

- Proponga una arquitectura que escale y sea mantenible.
- Refleje buenas prácticas de desarrollo seguro.
- Aborde críticamente los límites y riesgos asociados al uso de IA en este contexto.

📌 Alcance Mínimo Esperado

- Entrada: Información textual de vulnerabilidades (por ejemplo, CVEs) y nombre de la aplicación potencialmente afectada.
- Salida: Evaluación de severidad (inspirada en CVSS, puedes elegir la versión, justificada), incluyendo una justificación del puntaje sugerido.
- Documentación de la solución: Qué decisiones se tomaron y por qué, incluyendo cómo y cuándo se usa IA, modelado de arquitectura, etc.

🧠 Qué Evaluamos

- **Diseño de arquitectura:** modularidad, escalabilidad, mantenibilidad. Buenas prácticas de desarrollo, código limpio, etc.
- **Modelado del dominio:** claridad en la representación del problema, entidades, flujo de datos.
- **Enfoque en seguridad:** manejo del riesgo, integración con prácticas de desarrollo seguro.
- **Uso de IA/LLMs:** pertinencia del uso, manejo de limitaciones (ej: alucinaciones, ambigüedad), validación y control.
- **Pensamiento crítico:** tradeoffs tecnológicos, decisiones de diseño, integración con procesos existentes.
- **Proceso de Investigación**: Detallar e ilustrar el enfoque investigativo (si fue necesario) adoptado para alcanzar la solución óptima al problema.
- **Creatividad / Iniciativa**.

🛠️ Tecnologías y recursos

No hay restricciones sobre el lenguaje o herramientas. Puedes usar cualquier tecnología con la que te sientas cómodo, incluyendo servicios de IA (como Hugging Face, OpenAI, u otros), herramientas de visualización o prototipado, etc.