**Proyecto:**

Plataforma Centralizada de Herramientas de Seguridad Informática

**Objetivo:**

* Desarrollar una aplicación que centralice herramientas de análisis de vulnerabilidades para páginas web y entornos cloud, facilitando tanto la detección como la mitigación de riesgos de seguridad.

**Características principales:**

* Análisis centralizado: Integración de múltiples herramientas de seguridad para el análisis automático de vulnerabilidades en diferentes entornos (web y cloud).
* Informe de mitigación: Generación de recomendaciones y pasos detallados para mitigar las vulnerabilidades detectadas.

**Sistema modular de “toquens”:**

* Toquen de antesala: Un módulo que intercepta y analiza la información antes de que llegue al disco duro.
* Determina el tipo de archivo.
* Redirige el archivo a otros “toquens” responsables según la aplicación o el sistema.
* Realiza un análisis de inocuidad antes del almacenamiento.
* Toquens especializados: Cada “toquen” se instala con el sistema y puede apoyarse en otros para aumentar su eficacia frente a vulnerabilidades específicas.
* Colaboración de toquens: Los toquens pueden comunicarse y apoyarse entre sí para ofrecer una protección más robusta.

**Notas de innovación:**

- El concepto de “toquen de antesala” permite un filtro y análisis preventivo, reduciendo el riesgo de almacenamiento de archivos maliciosos.

- La arquitectura modular facilita la actualización y expansión del sistema, agregando nuevos toquens conforme evolucionan las amenazas.

**1 Desarrollo y Tecnología.**

**Lenguajes y Herramientas:**

* Backend: Python, Node.js o Java para la lógica del servidor.
* Frontend: React, Angular o Vue.js para la interfaz de usuario.
* Base de Datos: PostgreSQL o MongoDB para el almacenamiento de datos.
* Integración de Herramientas: APIs de herramientas de análisis de vulnerabilidades.

**2 Herramientas iniciales de análisis de vulnerabilidades.**

(ej: OWASP ZAP, Nikto, herramientas de escaneo cloud).

**3 Definir la arquitectura básica del sistema y el flujo de los toquens.**

**Componentes Principales:**

* Interfaz de Usuario (UI): Un panel de control intuitivo donde los usuarios pueden iniciar análisis, ver resultados y recibir recomendaciones.
* Módulo de Análisis: Integración de herramientas de análisis de vulnerabilidades (por ejemplo, OWASP ZAP, Nessus).
* Sistema de Tokens: Implementación del sistema de tokens de antesala, con lógica para el análisis y la inoculación de archivos.
* Base de Datos: Almacenamiento de resultados de análisis, configuraciones de usuario y registros de actividad.
* Documentar la API para la integración de nuevos toquens.

**4 Crear una primera interfaz para visualizar resultados y recomendaciones.**

**5 Plan de Implementación.**

**Fases del Proyecto:**

* Investigación y Análisis: Estudio de mercado y análisis de herramientas existentes.
* Diseño de la Arquitectura: Definición de la arquitectura de la aplicación y diseño de la interfaz.
* Desarrollo del Prototipo: Creación de un prototipo funcional con las características básicas.
* Pruebas y Validación: Realización de pruebas de seguridad y funcionalidad.
* Lanzamiento y Mantenimiento: Despliegue de la aplicación y establecimiento de un plan de mantenimiento y actualizaciones.

**6 Consideraciones Finales.**

* Cumplimiento Normativo: Asegurarse de que la aplicación cumpla con las normativas de protección de datos y ciberseguridad.
* Educación del Usuario: Incluir recursos educativos para ayudar a los usuarios a entender las vulnerabilidades y cómo mitigarlas.
* Actualización Continua: Mantener la aplicación actualizada con las últimas amenazas y vulnerabilidades.