ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

FACULTAD: INFORMÁTICA Y ELECTRÓNICA

CARRERA: SOFTWARE

NOMBRES:

Alejandro Hidalgo – 6823
Jesús Tomalá - 7063

ASIGNATURA:
Aplicaciones informáticas II

TEMA:
Alcance del Proyecto

FECHA DE ENTREGA:
14/10/2024

Alcance del Proyecto

Título del Proyecto: Desarrollo de un sistema web para analizar y priorizar vulnerabilidades utilizando Machine Learning y APIs de herramientas de escaneo de seguridad.

1. Definir las Necesidades

Justificación del Proyecto: El aumento de amenazas de ciberataques y la importancia de la seguridad informática hacen que sea necesario un sistema que aparte de identificar vulnerabilidades en sistemas informáticos, también priorice las acciones a seguir. Esto permitirá a las organizaciones y empresas gestionar mejor sus riesgos de seguridad.

Se espera una aplicación web funcional que permita:

- Integrar múltiples APIs de herramientas para escaneo de vulnerabilidades.
- Recopilar y analizar datos sobre las vulnerabilidades encontradas.
- Implementar un sistema de Machine Learning para priorizar las vulnerabilidades según su contexto y gravedad.
- Ofrecer recomendaciones personalizadas para mitigar las vulnerabilidades identificadas.

Condiciones de Desarrollo: El proyecto se desarrollará colaborativamente usando metodologías ágiles, para que así sea adaptable a las necesidades continuas del usuario y también para que el producto vaya mejorando con el tiempo

2. Proyectar los Objetivos

Objetivos S.M.A.R.T.:

Específicos: Desarrollar una aplicación web que integre al menos tres APIs de escaneo de vulnerabilidades.

Medibles: Completar la implementación de la funcionalidad principal en un plazo de seis meses, con al menos tres ciclos de prueba y feedback.

Alcanzables: Utilizar tecnologías como Flask y React, que son adecuadas para el desarrollo de la aplicación.

Relevantes: Aumentar la eficiencia en la identificación y gestión de vulnerabilidades en sistemas informáticos.

Basados en el Tiempo: El proyecto debe completarse en un plazo aproximado de 2 semestres, incluyendo tiempo para desarrollo, pruebas y presentación final.

3. Describir las Actividades

Acciones a Completar:

Investigación de herramientas de escaneo: Analizar APIs de herramientas como Nessus, OpenVAS y OWASP ZAP.

Desarrollo de Backend: Implementar la lógica del servidor con Flask para manejar las interacciones con las APIs.

Desarrollo de Frontend: Crear una interfaz de usuario con React que permita visualizar los datos de vulnerabilidades y las recomendaciones.

Implementación de Machine Learning: Diseñar y entrenar un modelo para priorizar vulnerabilidades basadas en datos históricos y severidad.

Pruebas y Validación: Realizar pruebas funcionales y de usuario para asegurar el correcto funcionamiento de la aplicación.

Documentación y Presentación: Elaborar la documentación del proyecto y preparar la presentación para la defensa de tesis.

4. Analizar las Capacidades

Experticia Requerida:

- Conocimientos en desarrollo web (Flask, React).

- Familiaridad con APIs y su integración.
- Fundamentos de Machine Learning.
- Habilidades en análisis de datos y visualización.
- **Análisis de Viabilidad:** Se realizará un análisis de viabilidad técnica al inicio del proyecto para identificar posibles obstáculos y soluciones.

5. Entender las Limitaciones

Limitaciones del Proyecto:

Recursos: Se dispone de tiempo limitado y recursos tecnológicos (servidores, herramientas).

Dependencias: Dependencia de las APIs de terceros y su disponibilidad.

Restricciones Legales: Cumplir con las normativas de privacidad y manejo de datos durante los análisis que realice la aplicación

Riesgos Técnicos: Posibles dificultades en la integración de múltiples herramientas y la implementación del modelo de Machine Learning.