Actividad: Aplica la metodología PASTA de modelado de amenazas

Resumen de la actividad

En esta actividad, practicarás el uso del marco del modelo de amenazas del Proceso de Simulación de Ataques y Análisis de Amenazas (PASTA). Determinarás si es seguro lanzar una nueva aplicación de compras.
El modelado de amenazas es una parte importante del desarrollo de software seguro. Los equipos de seguridad suelen realizar modelos de amenazas para identificar vulnerabilidades antes de que lo hagan los actores maliciosos. PASTA es un marco de uso común para evaluar el perfil de riesgo de las nuevas aplicaciones.

Escenario

Revisa el siguiente escenario. Luego, completa las instrucciones paso a paso.
Formas parte del creciente equipo de seguridad de una empresa para entusiastas y coleccionistas de zapatos. La empresa se está preparando para lanzar una aplicación móvil que facilite a sus clientes la compra y venta de zapatos.
Estás realizando un modelo de amenazas de la aplicación utilizando el marco PASTA. Pasarás por cada una de las siete etapas del marco para identificar los requisitos de seguridad de la nueva aplicación de la empresa de zapatos.

Stages	Objetivos comerciales:

I. Define los objetivos comerciales y de seguridad	• Facilitar el registro y la gestión de cuentas para los usuarios, asegurando la privacidad de sus datos. • Permitir una experiencia de compra fluida y rápida, ofreciendo múltiples opciones de pago. • Garantizar un sistema seguro que proteja la información de los usuarios y evite problemas legales relacionados con las transacciones.
II. Flujo de datos:	**Tecnología priorizada: API** **Justificación:** Las APIs son fundamentales para la comunicación entre el cliente y el servidor, y su seguridad es crucial para proteger los datos personales y de pago de los usuarios. Si se ve comprometida, podría dar acceso no autorizado a información sensible, por lo que es esencial evaluar sus mecanismos de autenticación y autorización.
III. Descomponer la aplicación	**Flujo de datos:** La aplicación permite a los usuarios registrarse, iniciar sesión, buscar zapatos y procesar pagos. Cada uno de estos procesos debe ser revisado para garantizar que los datos de los usuarios estén seguros y se manejen correctamente.
IV. Análisis de amenazas	***Amenazas potenciales:*** 1. ***Amenaza interna:*** *Un empleado malintencionado que accede a información confidencial sin autorización.* 2. ***Amenaza externa:*** *Un ataque de phishing que intenta engañar a los usuarios para que revelen sus credenciales o datos de pago.*
V. Análisis de vulnerabilidades	***Vulnerabilidades potenciales:*** 1. ***Vulnerabilidad en el código:*** *Posibles fallos de codificación que podrían ser explotados para acceder a datos sensibles.* 2. ***Debilidades en la base de datos:*** *Falta de cifrado en los datos almacenados, lo que podría permitir a un atacante acceder a la información de los usuarios.* •
VI. Modelado de ataques	**Ejemplo de árbol de ataque:** • El árbol de ataque puede incluir ramas que describen cómo un atacante podría intentar obtener acceso a las

	credenciales de usuario a través de un ataque de inyección SQL o phishing.
VII. Análisis de riesgos e impacto	**Cifrado de datos:** Proteger la información sensible durante la transmisión y el almacenamiento. **Autenticación multifactor (MFA):** Asegurar que solo los usuarios autorizados puedan acceder a sus cuentas. **Auditorías de seguridad regulares:** Realizar evaluaciones periódicas para identificar y mitigar riesgos. **Firewalls y sistemas de detección de intrusos:** Monitorear y proteger la red contra accesos no autorizados.

Resumen de la Actividad

- **Objetivos comerciales:** Se identificaron 2-3 objetivos comerciales (privacidad de datos, experiencia de compra fluida, seguridad en transacciones).
- **Requisitos tecnológicos:** Descripción de la API como tecnología prioritaria (seguridad crítica para la comunicación).
- **Amenazas potenciales:** 2 amenazas (interna y externa) a la información manejada por la aplicación.
- **Vulnerabilidades del sistema:** 2 vulnerabilidades (en el código y en la base de datos) que podrían ser explotadas.
- **Defensas que limitan el riesgo:** 4 controles de seguridad implementados para mitigar los riesgos de seguridad.

Este enfoque ayudará a garantizar que la nueva aplicación de compras de zapatos esté bien protegida contra posibles amenazas y vulnerabilidades, proporcionando así una experiencia segura y confiable para los usuarios.
