Análisis de amenazas con el framework PASTA

Aplicación analizada: App móvil para la compraventa de zapatillas
Versión del análisis: 1.0
Fecha:09/07/2025
Responsable del análisis: Vanesa Sierra

Etapa I – Identificación de objetivos de negocio

Objetivo: Comprender por qué se ha desarrollado la app y qué se espera de ella.

Objetivos empresariales identificados:

1. Facilitar la conexión entre compradores y vendedores de forma fluida y segura.
2. Asegurar la privacidad de los datos personales y financieros de los usuarios.
3. Ofrecer un proceso de compra rápido, claro y con múltiples opciones de pago.

Etapa II – Evaluación de componentes tecnológicos

Tecnologías identificadas:

- API
- PKI (AES para datos sensibles, RSA para intercambio de claves)
- SHA-256 (hash de datos sensibles como contraseñas)
- SQL (gestión de productos, usuarios, compras)

Tecnología priorizada: API

Justificación:
Las API son el canal principal entre usuarios, backend y terceros. Si no están protegidas adecuadamente, pueden ser utilizadas para explotar funcionalidades críticas o extraer datos sensibles. Son propensas a ataques como inyecciones, manipulación de parámetros o bypass de autenticación.

Etapa III – Diagrama de flujo de datos

Proceso analizado: Búsqueda de zapatillas disponibles en la base de datos.

Tecnologías implicadas: SQL, API, transmisión cifrada (TLS).

Controles asociados:

- Consultas parametrizadas en SQL.
- Autenticación antes de consultar la base de datos.
- Cifrado de la comunicación entre cliente y servidor mediante TLS/SSL.

Etapa IV – Identificación de amenazas

Amenazas detectadas:

1. Ataques de phishing dirigidos a usuarios para obtener credenciales de acceso.
2. Inyecciones SQL mediante formularios o parámetros mal validados en la API.

Etapa V – Análisis de vulnerabilidades

Vulnerabilidades explotables:

1. Entradas del usuario sin sanitizar ni validar correctamente.
2. Almacenamiento de contraseñas sin hash o con algoritmos obsoletos.

Etapa VI – Árbol de ataque (resumen textual)

Ejemplo de ruta de ataque:

- **Recurso afectado:** Base de datos de usuarios y productos.

- **Amenaza:** Inyección SQL.
- **Vulnerabilidad:** Entrada no filtrada en formularios de búsqueda.
- **Consecuencia:** Exposición de datos sensibles de usuarios y registros de venta.

Etapa VII – Controles de seguridad recomendados

Controles sugeridos para mitigar riesgos:

1. **Validación estricta de entradas de usuario** (backend y frontend).
2. **Hashing robusto de contraseñas** con bcrypt, Argon2 o scrypt.
3. **Autenticación multifactor (MFA)** para accesos de usuarios y administradores.
4. **Monitoreo y alertado de seguridad en tiempo real** (SIEM, WAF, IDS/IPS).

Resumen general

Elemento	Valor
Objetivos empresariales	Conexión eficiente, privacidad de datos, compra fluida
Tecnologías clave	API, SQL, SHA-256, PKI
Amenazas principales	Phishing, Inyección SQL
Vulnerabilidades explotables	Validación deficiente, almacenamiento inseguro de credenciales
Controles de seguridad propuestos	Validación de entradas, hash seguro, MFA, monitoreo y alertas