#### **PASTA Threat Modeling: Evaluation of the Shoe Purchasing Application**

##### **Stage I: Defining Business Objectives**

1. **Business Objectives:**
   * **Connect Sellers and Buyers:** The application should effectively connect sellers and buyers of shoes, providing an intuitive platform for buying and selling.
   * **Ensure Data Privacy:** Ensure that users' personal information is handled confidentially and securely to comply with privacy regulations and protect user trust.
   * **Facilitate Payment Processing:** Offer multiple payment options and ensure that the transaction process is clear and swift to minimize legal issues and maximize customer satisfaction.

##### **Stage II: Defining Technological Scope**

1. **Technological Requirements:**
   * **Application Programming Interfaces (APIs):** APIs should handle requests securely and properly authenticate users to protect exchanged data.
   * **Advanced Encryption Standard (AES):** Use AES encryption to secure data both in transit and at rest, protecting user data from unauthorized access.
   * **SHA-256:** Implement the SHA-256 hashing algorithm for protecting passwords and sensitive data, ensuring the integrity and security of stored information.

##### **Stage III: Analyzing Information Handling Processes**

1. **Information Handling Process:**
   * **User Registration and Authentication:** User data is entered and stored securely for session authentication and privacy protection. Users can manage their accounts and make purchases through the application.

##### **Stage IV: Identifying Potential Threats**

1. **Potential Threats:**
   * **SQL Injection Attacks:** Attackers might attempt to inject malicious SQL code through input forms to access sensitive data.
   * **Phishing and Social Engineering:** Users might be deceived into providing confidential information through fraudulent emails or messages that appear to come from the application.

##### **Stage V: Analyzing Vulnerabilities**

1. **System Vulnerabilities:**
   * **Inadequate Encryption of Payment Data:** If payment data is not properly encrypted, it may be intercepted and used maliciously.
   * **Insufficient Validation of User Inputs:** If the application does not properly validate user inputs, it may be vulnerable to injection or scripting attacks.

##### **Stage VI: Building the Attack Tree**

1. **Attack Vectors:**
   * **Data Interception:** Attackers may intercept unencrypted data during transmission, obtaining sensitive information such as payment details.
   * **Exploitation of Unvalidated Inputs:** Attackers might exploit vulnerabilities in data validation to execute attacks like SQL injections.

##### **Stage VII: Implementing Security Controls**

1. **Security Controls:**
   * **Encryption of Data in Transit and at Rest:** Implement AES encryption to protect all sensitive data during transmission and storage.
   * **Multi-Factor Authentication (MFA):** Require MFA for user account access to enhance security against unauthorized access.
   * **Input Validation and Sanitization:** Implement rigorous input validation and sanitization techniques to prevent injection and data-based attacks.
   * **Continuous Monitoring and Anomaly Detection:** Establish continuous monitoring systems to detect suspicious activities and respond quickly to potential security incidents.

##### **Conclusion:**

The threat modeling process using the PASTA framework provides a comprehensive view of the risks associated with the development and launch of the new shoe purchasing application. By identifying business objectives, technological requirements, potential threats, system vulnerabilities, and attack vectors, effective security controls can be implemented to mitigate these risks.

##### **Recommendations:**

1. **Conduct Thorough Security Testing:** Before launching the application, perform rigorous security testing, including penetration testing and code audits, to identify and fix potential vulnerabilities.
2. **User Training and Awareness:** Implement training programs for users on how to recognize and avoid phishing and other social engineering attacks.
3. **Regular Software Updates:** Keep the application and its components up-to-date with the latest security patches to protect against known vulnerabilities.
4. **Implement Proactive Security Controls:** Ensure that security measures such as encryption, multi-factor authentication, and input validation are always in place and periodically reviewed.

#### **Modelo de Amenazas PASTA: Evaluación de la Aplicación de Compras de Zapatos**

##### **Etapa I: Definición de Objetivos Comerciales**

1. **Objetivos Comerciales:**
   * **Conectar a vendedores y compradores:** La aplicación debe facilitar la conexión efectiva entre vendedores y compradores de zapatos, proporcionando una plataforma intuitiva para la compra y venta.
   * **Garantizar la privacidad de los datos:** Asegurar que la información personal de los usuarios sea manejada de manera confidencial y segura para cumplir con las regulaciones de privacidad y proteger la confianza del usuario.
   * **Facilitar el proceso de pago:** Ofrecer varias opciones de pago y asegurar que el proceso de transacción sea rápido y claro para minimizar problemas legales y maximizar la satisfacción del cliente.

##### **Etapa II: Definición del Alcance Tecnológico**

1. **Requisitos Tecnológicos:**
   * **Interfaces de Programación de Aplicaciones (API):** Las APIs deben manejar solicitudes de manera segura y autenticar adecuadamente los usuarios para proteger los datos intercambiados.
   * **Sistema de Cifrado Avanzado (AES):** Utilizar cifrado AES para asegurar la información tanto en tránsito como en reposo, protegiendo los datos del usuario contra accesos no autorizados.
   * **SHA-256:** Implementar el algoritmo de hash SHA-256 para la protección de contraseñas y datos sensibles, garantizando la integridad y seguridad de la información almacenada.

##### **Etapa III: Análisis del Proceso de Manejo de Información**

1. **Proceso de Información:**
   * **Registro y Autenticación de Usuarios:** Los datos del usuario se ingresan y almacenan de manera segura para autenticar las sesiones y proteger la privacidad. Los usuarios pueden gestionar sus cuentas y realizar compras a través de la aplicación.

##### **Etapa IV: Identificación de Amenazas Potenciales**

1. **Amenazas Potenciales:**
   * **Ataques de Inyección SQL:** Los atacantes pueden intentar inyectar código SQL malicioso a través de formularios de entrada para acceder a datos sensibles.
   * **Phishing y Ingeniería Social:** Los usuarios pueden ser engañados para proporcionar información confidencial mediante correos electrónicos o mensajes fraudulentos que parecen provenir de la aplicación.

##### **Etapa V: Análisis de Vulnerabilidades**

1. **Vulnerabilidades del Sistema:**
   * **Falta de Cifrado Adecuado en los Datos de Pago:** Si los datos de pago no están cifrados correctamente, podrían ser interceptados y utilizados maliciosamente.
   * **Validación Insuficiente de Entradas de Usuario:** Si la aplicación no valida adecuadamente las entradas de los usuarios, puede ser vulnerable a ataques de inyección o scripting.

##### **Etapa VI: Construcción del Árbol de Ataque**

1. **Vectores de Ataque:**
   * **Intercepción de Datos:** Los atacantes pueden interceptar datos no cifrados durante la transmisión, obteniendo información sensible como detalles de pago.
   * **Explotación de Entradas No Validadas:** Los atacantes pueden explotar vulnerabilidades en la validación de datos para ejecutar ataques como inyecciones SQL.

##### **Etapa VII: Implementación de Controles de Seguridad**

1. **Controles de Seguridad:**
   * **Cifrado de Datos en Tránsito y en Reposo:** Implementar cifrado AES para proteger todos los datos sensibles durante la transmisión y el almacenamiento.
   * **Autenticación Multifactor (MFA):** Requerir MFA para el acceso a cuentas de usuario, aumentando la seguridad frente a accesos no autorizados.
   * **Validación y Saneamiento de Entradas:** Implementar técnicas rigurosas de validación y saneamiento de datos para prevenir inyecciones y ataques basados en entrada maliciosa.
   * **Monitoreo y Detección de Anomalías:** Establecer sistemas de monitoreo continuo para detectar actividades sospechosas y responder rápidamente a posibles incidentes de seguridad.

##### **Conclusión:**

El proceso de modelado de amenazas utilizando el marco PASTA proporciona una visión integral de los riesgos asociados con el desarrollo y lanzamiento de la nueva aplicación de compras de zapatos. Al identificar los objetivos comerciales, los requisitos tecnológicos, las amenazas potenciales, las vulnerabilidades del sistema y los vectores de ataque, se puede implementar un conjunto efectivo de controles de seguridad para mitigar estos riesgos.

##### **Recomendaciones:**

1. **Realizar Pruebas de Seguridad Exhaustivas:** Antes del lanzamiento de la aplicación, llevar a cabo pruebas de seguridad rigurosas, incluyendo pruebas de penetración y auditorías de código, para identificar y corregir vulnerabilidades potenciales.
2. **Capacitación y Concienciación del Usuario:** Implementar programas de capacitación para los usuarios sobre cómo reconocer y evitar amenazas de phishing y otros ataques de ingeniería social.
3. **Actualizar Regularmente el Software:** Mantener la aplicación y sus componentes actualizados con los últimos parches de seguridad para proteger contra vulnerabilidades conocidas.
4. **Implementar Controles de Seguridad Proactivos:** Asegurar que las medidas de seguridad como el cifrado, la autenticación multifactor y la validación de entradas estén siempre en vigor y sean revisadas periódicamente.