PASTA Worksheet - Sneaker Company App

I. Define Business and Security Objectives

Business objectives identified:

1. Secure payment transaction processing - The app must handle clear and quick sales with multiple payment options to avoid legal issues

2. User data privacy protection - Ensure users feel confident that their personal information is being handled responsibly

3. Facilitate secure communication - Enable buyers to directly message sellers while maintaining communication security

II. Define Technical Scope

Technologies used by the application:

- API (Application Programming Interface)
- PKI (Public Key Infrastructure)
- AES (symmetric encryption)
- RSA (asymmetric encryption)
- SHA-256 (hash function)
- SQL (database)

Technology prioritization:

> I would prioritize evaluating SQL and PKI first. SQL represents a critical risk because it directly handles sensitive user data and transaction information, and is vulnerable to SQL injection attacks. PKI is equally important as it protects the exchange of sensitive information such as credit card data using AES and RSA encryption. A compromise of these systems could expose financial and personal data, making them the highest priority for security assessment.

III. Decompose Application

Reference: See the provided data flow diagram (PASTA-data-flow-diagram.pptx) which shows the product search process and how data flows between user, application, and database.

IV. Threat Analysis

Identified threats:

1. SQL Injection - External threat where malicious actors could manipulate SQL queries to access, modify, or delete unauthorized data from the database, compromising information about sellers, buyers, and transactions

2. Session Hijacking / Credential Compromise - Threat that can be both internal (employee compromised through social engineering) and external (brute force attack or phishing). Attackers could steal weak authentication credentials to impersonate legitimate users and access sensitive data

V. Vulnerability Analysis

Identified vulnerabilities:

1. Lack of Prepared Statements in SQL code - Codebase vulnerability that allows SQL injection execution if user input is not properly sanitized. This weakness could be exploited to extract sensitive data from the database

2. Weak login credentials / Inadequate session management - Vulnerability in the authentication system that includes: lack of strong password requirements, absence of multi-factor authentication (MFA), inadequate session timeouts, and failure to implement secure tokens for session management

VI. Attack Modeling

Reference: See the provided attack tree (PASTA-attack-tree.pptx) which shows identified attack vectors including SQL injection and session hijacking with their root causes.

VII. Risk Analysis and Impact

Recommended security controls:

1. Prepared Statements and Input Validation - Implement parameterized prepared statements for all SQL queries and rigorously validate/sanitize all user inputs to prevent SQL injection attacks

2. Multi-Factor Authentication (MFA) - Require MFA for all user accounts, especially for sensitive transactions, to significantly reduce the risk of unauthorized access even if credentials are compromised

3. End-to-End Encryption and Secure Key Management - Maintain AES encryption for sensitive data at rest and RSA for secure key exchange, ensuring proper cryptographic key management and regular rotation

4. Logging, Monitoring and Incident Response - Implement comprehensive logging of all sensitive activities, real-time monitoring for anomalous behavior, and an incident response plan to detect and respond quickly to potential security breaches

Summary

This PASTA threat model has identified critical risks related to data handling and authentication in the sneaker app. Top priorities are: protecting against SQL injection through prepared statements, strengthening authentication with MFA, and maintaining robust encryption for sensitive data. Implementation of these controls will significantly reduce the risk of data breaches and protect both the company and its users.