

# PASTA Threat Modeling Report

Project: Sneaker Enthusiasts Mobile App

Prepared by: Abubakari-Sadique Hamidu

## 1. Define the Objectives

The goal is to ensure secure transactions and protect users' personal and financial data on the sneaker enthusiasts mobile app. The app facilitates buying and selling shoes, so security must support confidentiality, integrity, and availability of user data.

## 2. Define the Technical Scope

The technical environment includes mobile clients (iOS and Android), a backend API, a payment gateway integration, cloud-based hosting, and a user authentication system. Sensitive data such as personal info, credit card details, and transaction history is handled.

## 3. Application Decomposition

The app includes user registration/login, product listings, chat/messaging features, payment processing, and user profile management. Components interact via secure API endpoints. Third-party integrations include payment services and notification APIs.

## 4. Threat Analysis

Potential threats include account takeovers, data breaches, payment fraud, and man-in-the-middle attacks. Threat actors may exploit weaknesses in session handling, data transmission, or poorly validated input forms.

## 5. Vulnerability and Weakness Analysis

Common vulnerabilities to address: Insecure APIs, weak encryption, missing input validation, and insufficient authentication protocols. Also includes potential insecure storage of sensitive information on mobile devices.

## 6. Attack Modeling

Attackers might use phishing to steal credentials, inject malicious scripts (XSS), or perform SQL injections on vulnerable endpoints. Threat actors could target admin panels or exploit third-party payment integrations if not properly secured.

## 7. Risk and Impact Analysis

Risks include loss of user trust, legal/regulatory penalties (e.g., for GDPR non-compliance), and financial loss due to fraud. Prioritize fixes for critical threats (like payment and login systems), and ensure continuous monitoring and patching.

---

© 2025 Abubakari-Sadique Hamidu — All rights reserved.