PASTA Threat Model Worksheet — SoleTrade App

Stages	SoleTrade sneaker marketplace app
I. Define business and security objectives	Key business objectives drawn from the product description: • *Give buyers and sellers a fast, low-friction way to create accounts, log in, and manage their profiles.* • *Safeguard customer data throughout the app and be able to demonstrate responsible data handling to users.* • *Support multiple checkout options while processing payments in a way that satisfies relevant payment-handling regulations.*
II. Define the technical scope	Technologies in use across the application: • *Application programming interface (API)* • *Public key infrastructure (PKI) — AES and RSA* • *SHA-256 hashing* • *Structured query language (SQL) database* *I'd start with the API layer. It's the connective tissue linking the mobile client, third-party services, and the backend, so any weakness there — like a poorly secured endpoint — could expose the systems it links together. Because it sits at so many boundaries, it's also the most exposed to outside attackers first.*
III. Decompose the application	Reviewed resource: PASTA data flow diagram (sneaker search process). *The diagram traces a shopper's search request from the User node into the Product search process and out to the Database, then back again with the matching listings. SQL is what retrieves the inventory records, while the API is what carries that request and response between the app and the backend — both are the pieces from Stage II that this single process depends on most directly.*
IV. Threat analysis	Threats that put the app's data at risk: • *Malware planted on a device or server to intercept login credentials* • *Social engineering (e.g., phishing) aimed at employees to gain unauthorized account access*
V. Vulnerability analysis	Weaknesses an attacker could take advantage of: • *Payment form fields that transmit or store card data without encryption* • *Outdated or unpatched third-party API libraries with known CVEs*
VI. Attack modeling	Reviewed resource: PASTA attack tree.

Stages	SoleTrade sneaker marketplace app
	The tree maps user data as the target, branching into SQL injection (rooted in missing prepared statements) and session hijacking (rooted in weak login credentials) as two distinct paths an attacker could take to reach that data.
VII. Risk analysis and impact	Security controls that would reduce the chance of an incident like a data breach: • *Multi-factor authentication on buyer, seller, and employee accounts* • *Parameterized queries / prepared statements to prevent SQL injection* • *End-to-end encryption (AES/RSA) for payment and personal data in transit and at rest* • *Ongoing security awareness training for employees to reduce social engineering risk*