PASTA worksheet

Stages	Sneaker company
I. Define business and security objectives	• The app should allow user registration, login and account management. • It must ensure safe and quick processing of financial transactions with multiple payment options. • User data privacy and legal compliance (e.g., with data protection regulations) are top priorities.
II. Define the technical scope	List of technologies used by the application: • *Application programming interface (API)* • *Public key infrastructure (PKI)* • *SHA-256* • *SQL* I would prioritize evaluating the **API** because it acts as the main communication channel between the frontend and backend services. APIs are frequent targets of attacks such as injection and improper authorization. Ensuring strong authentication, rate limiting, and secure coding practices in APIs is critical to protecting data and application integrity.
III. Decompose application	Sample data flow diagram APIs facilitate these operations and must ensure secure data handling between user interfaces and backend systems. SQL is crucial here, and poor handling can expose the app to SQL injection risks.
IV. Threat analysis	• Internal Threat : Malicious insider gaining unauthorized access to customer data through backend systems. • External Threat : An attacker exploiting API endpoints or injecting malicious SQL queries to access or manipulate data.

V. Vulnerability analysis	• ***SQL Injection***: *Improperly sanitized inputs or lack of prepared statements in the SQL database could be exploited.* • ***Weak Login Authentication***: *Session hijacking due to poorly implemented login mechanisms and weak password enforcement.*
VI. Attack modeling	Sample attack tree diagram
VII. Risk analysis and impact	**4 Security Controls** to reduce risk: 1. **Use of prepared SQL statements** to prevent injection attacks. 2. **Strong password policies and multi-factor authentication (MFA)** for secure logins. 3. **Input validation and sanitization** across APIs and user inputs. 4. **TLS encryption and proper use of PKI** to protect data in transit and ensure authenticity.
