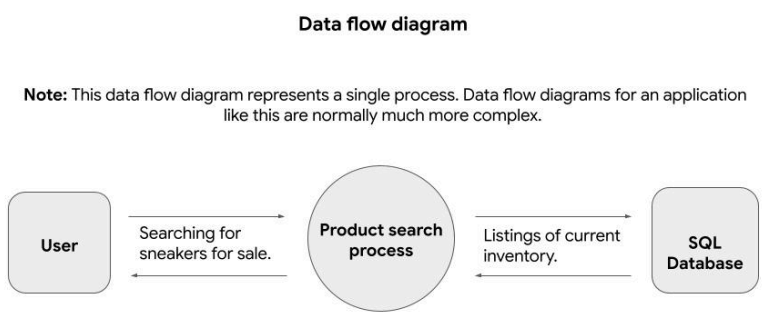
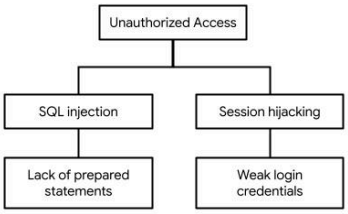
PASTA worksheet

Stages	Sneaker company
I. Define business and security objectives	• *The app will process secure transactions for buying and selling sneakers.* • *It must handle real-time back-end processing for inventory, orders, and payments.* • *Compliance with industry standards such as PCI-DSS for payment security and data privacy regulations (e.g., GDPR) is required.*
II. Define the technical scope	List of technologies used by the application: • *Application programming interface (API)* • *Public key infrastructure (PKI)* • *SHA-256* • *SQL* We prioritize securing the API and using PKI because the app relies heavily on real-time, secure client-server interactions. Ensuring encrypted authentication protects user data and transactions. SHA-256 ensures data integrity, and the SQL database is central for storing sensitive user and order data, so it must be well protected.
III. Decompose application	

IV. Threat analysis	• ***Internal Threat:*** *Insider threat with unauthorized access to user data or manipulation of sneaker listings.* • ***External Threat:*** *Man-in-the-middle attacks intercepting API communication or credential theft via phishing.*
V. Vulnerability analysis	• *Potential SQL Injection vulnerabilities if input validation is insufficient in the API.* • *Weak encryption key management or expired certificates in PKI, leading to compromised authentication.*
VI. Attack modeling	**Sample attack tree** **Note:** Applications like this normally have large, complex attack trees with many branches. 
VII. Risk analysis and impact	• Enforce multi-factor authentication (MFA) to prevent unauthorized account access. • Implement input validation and prepared statements to prevent SQL injection. • Use TLS with strong cipher suites for all API communications. • Regularly rotate and manage PKI certificates and encryption keys to maintain secure authentication.