PASTA worksheet

Stages	Sneaker company
I. Define business and security objectives	• The app must securely handle user transactions, including payments and sneaker purchases. • It should provide real-time product search with accurate inventory listings. • The app must comply with industry standards such as PCI DSS for payment processing and protect customer data under privacy regulations.
II. Define the technical scope	Technologies Used: • Application Programming Interface (API) • Public Key Infrastructure (PKI) • SHA-256 • SQL Why SQL is prioritized: SQL is prioritized because the sneaker application relies heavily on database queries for inventory, transactions, and user data. Improper handling of SQL queries can expose the application to severe threats like SQL injection. While PKI and SHA-256 provide cryptographic security, securing the SQL database is essential to prevent data breaches and maintain trust.
III. Decompose application	Sample data flow diagram
IV. Threat analysis	• Internal Threats: ○ Malicious insider modifying the database. ○ Developer error introducing insecure code. • External Threats: ○ Attackers attempting SQL injection. ○ Hackers trying session hijacking to steal user

	accounts.
V. Vulnerability analysis	● Insecure coding practices leading to lack of prepared statements, making SQL injection possible. ● Weak database access controls that allow unauthorized queries or data exfiltration.
VI. Attack modeling	Sample attack tree diagram
VII. Risk analysis and impact	4 Security Controls to Reduce Risk: 1. Input Validation & Prepared Statements → Prevent SQL injection. 2. Multi-Factor Authentication (MFA) → Protect against weak credentials. 3. Database Access Controls & Encryption → Limit insider misuse and external theft. 4. Regular Security Patching & Code Reviews → Prevent exploitation of known vulnerabilities.