PASTA worksheet

Stages	Sneaker company
I. Define business and security objectives	• - The app will process **user transactions**, including payments and listing updates.- It performs real-time **search and inventory queries** on a backend database. It must comply with **data protection laws** like GDPR to protect customer information.
II. Define the technical scope	- Application programming interface (**API**)- Public key infrastructure (**PKI**)- **SHA-256**- **SQL**APIs are prioritized due to their role in handling user requests, authentication, and database operations. Poorly secured APIs are prime targets for attackers. SQL is also critical due to injection risks, and PKI ensures secure data transmission.
III. Decompose application	- Users search sneakers via the mobile app interface.- API forwards search query to backend.- Database fetches and returns results to user.- Sensitive data flows during login, listings, and payments.
IV. Threat analysis	• - **External Threats**: - SQL Injection - Session Hijacking- **Internal Threats**: - Lack of input validation - Hardcoded credentials or exposed test endpoints
V. Vulnerability analysis	• - Missing **prepared statements** in backend code.- Plaintext data or **improper database permissions**.- No MFA or insecure session handling logic.- Incomplete HTTPS/TLS coverage across app.
VI. Attack modeling	- Attackers could exploit login or search APIs to inject SQL commands.- Use stolen cookies to hijack a user session.- Abuse insecure endpoints for unauthorized access.- Perform brute-force or enumeration attacks on login pages.
VII. Risk analysis and impact	- Enforce **prepared SQL statements** and sanitize inputs.- Implement **multi-factor authentication (MFA)**.- Use **HttpOnly, Secure cookies** with session expiration.- Encrypt all communication with **TLS 1.3** and hash sensitive data using **SHA-256**.