PASTA worksheet

Stages	Sneaker company
I. Define business and security objectives	• Enable a secure and user-friendly platform that connects sneaker sellers and buyers, allowing account management, messaging, and ratings to support trust and engagement. • Ensure safe and efficient processing of transactions with multiple payment options, minimizing legal and financial risks. • Protect user data and privacy to comply with data protection regulations (e.g., GDPR) and maintain customer confidence.
II. Define the technical scope	SQL would be evaluated first because the database stores critical user, payment, and transaction data, making it a primary target for attacks such as SQL injection or unauthorized access. A compromise at this layer could impact the entire application. PKI and APIs would be reviewed next to ensure secure data transmission and controlled system interactions.
III. Decompose application	During the product search process, the user sends a request to the application, which forwards it to the inventory listing service. This service queries the database to retrieve available products and returns the results to the user. Encryption mechanisms protect data in transit, while improper query handling could expose the database to injection or data leakage risks.
IV. Threat analysis	Two potential threats to the sneaker application include SQL injection attacks targeting the database through improperly validated search queries, and phishing attacks aimed at stealing user credentials to gain unauthorized access to accounts and payment information.
V. Vulnerability analysis	Two vulnerabilities in the application include insufficient input validation on SQL queries, which could allow injection attacks, and improper encryption or configuration of the payment form, potentially exposing sensitive credit card data during transmission.
VI. Attack modeling	An attacker could exploit a lack of prepared SQL statements to

	perform SQL injection attacks and directly access or extract user data from the database. Alternatively, weak login credentials could allow session hijacking, enabling unauthorized access to active user sessions and exposure of sensitive personal and payment information.
VII. Risk analysis and impact	• Input validation and prepared SQL statements • Multi-Factor Authentication (MFA) for user access • Role-Based Access Control (RBAC) for database and services • Encryption of sensitive data in transit and at rest