PASTA worksheet

Stages	Sneaker company
I. Define business and security objectives	- The app must allow seamless signup, login, and account management for users. - It must ensure the secure handling of user data and transactions to avoid legal issues. - Customers must be able to message sellers, make payments securely, and leave reviews.
II. Define the technical scope	I would prioritize evaluating the API first, as it handles communication between the mobile app and backend services. APIs often expose sensitive data and functions, making them a common target for attackers. If not secured properly, APIs can be exploited for unauthorized access or data leaks.
III. Decompose application	The app allows users to search for sneakers from a product database. This involves user input being processed and query results being displayed. Technologies like SQL and API must securely handle this interaction to prevent data leaks or injection attacks.
IV. Threat analysis	- **SQL Injection** – A threat actor could manipulate database queries to access or delete sensitive data. - **Session Hijacking** – An attacker could steal session tokens to impersonate users and access their accounts.
V. Vulnerability analysis	- **Lack of Prepared SQL Statements** – This leaves the system vulnerable to SQL injection. - **Weak Login Security** – Insecure password storage or lack of MFA could lead to account breaches.
VI. Attack modeling	The app is vulnerable to SQL injection due to poor input handling. Weak login credentials also open it to session hijacking or brute force attacks. These attacks target both the database and authentication processes, potentially exposing user data and financial information.
VII. Risk analysis and impact	- Implement **input validation and parameterized SQL queries** to prevent SQL injection. - Use **multi-factor authentication (MFA)** for all user

	accounts. ● Encrypt sensitive data using **AES for storage and RSA for key exchange**. ● Enforce **strong password policies and secure session handling** to avoid hijacking.