Scenario

Review the following scenario. Then complete the step-by-step instructions.
You're part of the growing security team at a company for sneaker enthusiasts and collectors. The business is preparing to launch a mobile app that makes it easy for their customers to buy and sell shoes.
You are performing a threat model of the application using the PASTA framework. You will go through each of the seven stages of the framework to identify security requirements for the new sneaker company app.

Data flow / Attack tree

PASTA worksheet

Stages	Sneaker company
I. Define business and security objectives	Make **2-3 notes** of specific business requirements that will be analyzed. • P2P shoes platform, required to have a secure way for payment. • Users should be able to pass the authentication and authorization process, post auctions and bids, additionally chatting with others. • Should adhere to GDPR or PCI DSS.
II. Define the technical scope	List of technologies used by the application: • *Application programming interface (API)* • *Public key infrastructure (PKI)* • *SHA-256* • *SQL* *API in data flow, is proxy to SQL and partners, so we should defend it first. API provides a large attack surface.* *Second, we will protect data in use (SQL), which is critical for continuous business operation.* *SHA-256 for secure data in rest, and decrease sense of attacks.* *PKI should secure data in transit, and protect users against sniffing.*

III. Decompose application	Sample data flow diagram
IV. Threat analysis	List **2 types of threats** in the PASTA worksheet that are risks to the information being handled by the application. ○ SQL injection ○ Session Hijacking
V. Vulnerability analysis	List **2 vulnerabilities** in the PASTA worksheet that could be exploited. ○ Lack of prepared statements ○ Broken API token
VI. Attack modeling	Sample attack tree diagram
VII. Risk analysis and impact	List **4 security controls** that you've learned about that can reduce risk. - Strong password policy - Incident response procedures - Cryptography (hashing for credentials, encryption for in transit data) - Principle of least privilege (PoLP)
