PASTA worksheet

Stages	Sneaker company
I. Define business and security objectives	*-Enable seamless connection between sellers and shoppers with secure direct messaging.* *-Support easy sign-up, login, and account management while ensuring user data privacy and compliance with regulations.* *-Provide multiple payment options and ensure proper transaction handling to avoid legal and financial risks.*
II. Define the technical scope	*I prioritized the API because it directly manages user interactions, messaging, and transactions over the internet, making it the primary attack surface. Securing API endpoints is fundamental to preventing injection, authentication bypass, or data leakage before addressing internal components.*
III. Decompose application	*The data flow shows user requests sent via the API to query the SQL database, responses encrypted with AES in transit, and key exchanges handled by PKI. Sensitive data such as credentials and payment information traverse these components, highlighting endpoints, data stores, and cryptographic processes as critical trust boundaries.*
IV. Threat analysis	*-Internal threat: A malicious insider or compromised developer abusing API keys or elevated privileges to exfiltrate data.* *-External threat: Attackers exploiting SQL injection or broken auth controls to read or modify user records.*
V. Vulnerability analysis	*-Lack of input validation and parameterized queries in API endpoints, allowing SQL injection exploits.* *-Missing TLS configuration on non-API communication channels, risking interception of sensitive data.*
VI. Attack modeling	*An attacker could chain SQL injection via the API to gain database access, then leverage stolen credentials to escalate privileges and pivot to internal services. The attack tree branches from initial API exploitation to data theft, privilege escalation, and network compromise.*
VII. Risk analysis and impact	*-Enforce parameterized queries and rigorous input validation to prevent injection.* *-Implement TLS for all API and backend communication*

	and AES encryption for data at rest. *-Require multi-factor authentication and OAuth/JWT for API access.* *-Segment networks with firewall rules to isolate public-facing APIs from internal databases and services.*
