PASTA worksheet

Stages	Sneaker company
I. Define business and security objectives	• *Users can create user/seller accounts* • *PCI DSS compliance due to processing financial transactions*
II. Define the technical scope	List of technologies used by the application: • *Application programming interface (API)* • *Public key infrastructure (PKI)* • *SHA-256* • *SQL* *API and SQL because the sneaker company uses a database to store buyers' and sellers' information I would focus on SQL to see the current infrastructure around it and what kind of security measures are in place now.* *Due to multiple payment methods being used securing API is another aspect I would consider due to tokens being misused if not*
III. Decompose application	Sample data flow diagram The process of searching for sneakers for sale can be used to do a SQL injection attack

IV. Threat analysis	• *What are the internal threats?*
	  ○ *Internal threats are employees*
	• *What are the external threats?*
	  ○ *Third-party vendors and malicious actors*

V. Vulnerability analysis	• *Could there be things wrong with the codebase?*
	  ○ *Code not sanitized*
	• *Could there be weaknesses in the database?*
	  ○ *Proper encryption / Hashing is not used*

	● Could there be flaws in the network? 　　*○ Firewalls are not properly setup* 　　*○ Weak passwords* 　　*○ XXS*
VI. Attack modeling	[Sample attack tree diagram](#)
VII. Risk analysis and impact	Password policy MFA Prepared statements Input validation Input sanitization