PASTA worksheet

Stages	Sneaker company
I. Define business and security objectives	The app is being used to connect sellers and shoppers, they want easy access to user sign-up, sign-in, and manage their accounts. The app will handle transactions and include multiple payment methods. The users should be able to message and rate sellers. Data Privacy is the main concern. PCI DSS and possible GDPR is a concern.
II. Define the technical scope	List of technologies used by the application: ● *Application programming interface (API)* ● *Public key infrastructure (PKI)* ● *SHA-256* ● *SQL* The API and SQL technologies should be the main focus as they will be handling the sensitive data, so securing them from unauthorized access is a major priority. Which API's are being used? How is the database secured?
III. Decompose application	Sample data flow diagram
IV. Threat analysis	The main threats are SQL injection and session hijacking. These are external threats .
V. Vulnerability analysis	Vulnerabilities include a lack of prepared statements or not sanitizing user input, having weak API tokens or credentials.
VI. Attack modeling	Sample attack tree diagram
VII. Risk analysis and impact	A strict up to NIST CSF password policy should be implemented such as increased character length, frequent changes, special characters and numbers, etc. Having a Principle of Least Privilege in place to ensure that all access is on a need-to-know basis and that any SQL queries cannot access sensitive information that might be held on the database.

	Incident response procedures and policies should be reviewed in case of an incident to ensure a fast and effective response.
