PASTA worksheet

Stages	Sneaker company
I. Define business and security objectives	Make **2-3 notes** of specific business requirements that will be analyzed. ● *Will the app process transactions?* ● *Does it do a lot of back-end processing?* ● *Are there industry regulations that need to be considered?* *The application is intended to connect shoppers and sellers. It will allow for clear and quick sales through multiple payment options, while giving the user the ability to access and manage their accounts after signing-up and logging-in. The app will require back-end processing to store data in the database, and allow for SQL functioning when searching and selecting items to buy. Legal regulations pertaining to the secure storage of customer credentials are going to be heavily considered when implementing this new app.*
II. Define the technical scope	List of technologies used by the application: ● *Application programming interface (API)* ● *Public key infrastructure (PKI)* ● *SHA-256* ● *SQL* Write **2-3 sentences** (40-60 words) that describe why you choose to prioritize that technology over the others. *The first technology I would evaluate is the API, since it is will most likely use third-party functions, and there needs to be security measures in place for every component. Before any of the other technologies are even implemented, the application itself needs to have the least vulnerability, before even considering evaluating the network-oriented technologies. Threat actors usually need to find vulnerabilities in the front end of the application before accessing the tools in the backend applications through injection.*
III. Decompose	Sample data flow diagram

application	- The API protects user data at the search process step - The PKI encrypts data between the user and the app as they are searching for sneakers for sale. This will help prevent threat actors from being able to intercept information in transit - The SHA-256 hash will protect user PII in the database to make it near impossible for threat actors to decypher - SQL presents a potential vulnerability, so appropriate filters should be used with this
IV. Threat analysis	List **2 types of threats** in the PASTA worksheet that are risks to the information being handled by the application. ● *What are the internal threats?* ● *What are the external threats?* - *Disgruntled employee looking to disrupt business* - *Hacker looking to steal credit card information*
V. Vulnerability analysis	List **2 vulnerabilities** in the PASTA worksheet that could be exploited. ● *Could there be things wrong with the codebase?* ● *Could there be weaknesses in the database?* ● *Could there be flaws in the network?* - *The codebase could have issues, since third-party APIs would probably be used* - *The database seems very secure, with SHA-256 hashing as the base defense mechanism* - *There may be flaws present in the SQL that allow threat actors to access the back-end.*
VI. Attack modeling	Sample attack tree diagram - A lack of prepared statements on the SQL can lead to injection, which can compromise user data, if threat actors can manipulate the code through the application's input fields - If a user has weak login credentials, their account information may be compromised via a session hijacking made possible through brute force attacks.
VII. Risk analysis and impact	List **4 security controls** that you've learned about that can reduce risk.

	SHA-256, incident response procedures, password policy, and principle of least privilege are a few examples of technical, operational, and managerial controls that can be implemented before launch to reduce risk.