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?* *Yes, the app will process transactions. Proper payment handling is necessary as the company needs to avoid any security and/or legal issues.* • *Does it do a lot of back-end processing?* *There is quite a lot of back-end processing that needs to be done while a user navigates through the shopping app. The database in the back-end needs to interact seamlessly with the front end to display the product and the quantity and also update the shoppers cart. It also needs to process payments without encountering errors.* • *Are there industry regulations that need to be considered?* *There are industry regulations that need to be kept in mind while taking security measures. The app should be in compliance with 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* Write **2-3 sentences** (40-60 words) that describe why you choose to prioritize that technology over the others. APIs facilitate the exchange of data between customers, partners, and employees, so they should be prioritized. They handle a lot of sensitive data while they connect various users and systems together. However, details such as which APIs are being used should be considered before prioritizing one technology over another. So, they can be more prone to security vulnerabilities because there's a larger attack surface.
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. ● *What are the internal threats?* *Injection attack* ● *What are the external threats?* *Session hijacking*
V. Vulnerability analysis	List **2 vulnerabilities** in the PASTA worksheet that could be exploited. ● *Could there be things wrong with the codebase?* *Lack of prepared statements* ● *Could there be weaknesses in the database?* ● *Could there be flaws in the network?* *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. SHA-256, incident response procedures, password policy, principle of least privilege

---