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 business wants to sell sneakers and they would like to do it in a way that is user friendly has good security and able to sell without any issues. The business plan is to improve on data privacy to ensure shoppers' confidentiality and avoid any issues that can lead to a legal dispute. They will need to ensure to gather the proper equipment to be able to keep files secured*
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 technology that I will prioritize is the public key infrastructure(PKI), this is because the company wants to make sure that the customer's data is private but still have good communication between the user and the database. The other reason is because it will help ensure card information stays safe and encrypted to ensure nobody can get access to it.
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?* ● *What are the external threats?* *An internal risk can be if one of the employees starts to break the privacy policy of the customer and getting private information or credit card information. An external threat will be if the shoe company is using an internet provider and that provider gets hacked leaking the information from their system*
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?* *2 vulnerabilities can be flaws in the network where their provider gets hacked and the customer information gets leaked and the code that protects the database can have flaws where a previous worker can still have access to those files using their old login information*
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.
