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?* • *Apps should handle payments in a secure way as we want to avoid legal issues.* • *Does it do a lot of back-end processing?* • *There is a lot of backend processing involved* • *Are there industry regulations that need to be considered?* • *We might need to adhere to 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* 1. We are using API keys instead of normal requests as it will give faster response time, Also third party API will help add functionality without having to code from scratch. 2. PKI will provide protection to data by encrypting it, as the app will be dealing with sensitive information like credit card details. 3. SHA is an advanced hashing algorithm so it will be very secure. 4. SQL is a widely known and used language for database queries, the mobile app uses SQL to store information about the sneakers that are for sale, as well as the sellers who are selling them. It also uses SQL to access that data during a purchase.
III. Decompose application	Sample data flow diagram The technologies we are using will allow our app to provide a seamless buying and selling experience to both buyer and sellers, As we will provide encryption for data, quick response time and

	securely handle payments as well.
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?*
V. Vulnerability analysis	List **2 vulnerabilities** in the PASTA worksheet that could be exploited. ● *The database can be vulnerable to SQL injections if the user input in the login forms or search bar are not properly sanitized and validated.* ● *The password policy also needs to be strong as weak credentials can lead to unauthorized access or session hijacking.* ● *Also the network can be vulnerable to Denial of service attack.*
VI. Attack modeling	Sample attack tree diagram ● Malicious hackers will be able to steal login and payment credentials if the system fails to encrypt the data. ● Without proper access control an attacker might gain unauthorized access to sensitive information. ● *The database can be vulnerable to SQL injections if the user input in the login forms or search bar are not properly sanitized and validated*
VII. Risk analysis and impact	List **4 security controls** that you've learned about that can reduce risk. ● Input validation and sanitization ● Encrypting user data. ● Using MFA (Multi Factor Authentication) ● Using advance hashing algorithms to secure user information