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 aim of the business is to allow people to buy and sell sneakers from all over the world. Features such as sign-up, log in,managing their accounts and transitions should function smoothly.*
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. SQL which is used to store all confidential information about the buyers and sellers is at higher risk of being attacked by the attacker. If proper controls are not in place, the attacker can steal the sensitive data. *Public key infrastructure (PKI) helps in encrypting the sensitive*

	information on the internet. *SHA-256, adds extra layer of security to the sensitive information by adding hash values.*
III. Decompose application	Sample data flow diagram The user searches for a valid product and does not enter any query that will bypass the database to reveal sensitive information.This is ensured by SQL's Prepared sentences.
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?* Types of threats: Injection Session Hijacking
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?* SQL which is used to store all confidential information about the buyers and sellers is at higher risk of being attacked by the attacker. If proper controls are not in place, the attacker can steal the sensitive data. *Application programming interface (API) is not checked properly then there can be a loophole in the API that can grant the attacker access into the system.*
VI. Attack modeling	Sample attack tree diagram SQL Injection: Here the attacker can gain access to the database if prepared statements are not in place Session Hijacking: If proper encryption methods are not implemented, the attacker can identify the session ID and enter into the system pretending to be a legitimate user.
VII. Risk analysis and	List **4 security controls** that you've learned about that can reduce

impact	risk. The following security controls can reduce the risk: SQL prepared statements Proper Encryption Algorithms Strong password policies Ensure API’s don't have any loopholes.
