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? Y* ○ *Yes, the app is to buy and sell shoes* ● *Does it do a lot of back-end processing?* ○ *Yes, there are many different backend processes such as logins, sign up, manage account, and messaging systems which all relate to a database.* ● *Are there industry regulations that need to be considered?* ○ *We will need to protect sensitive information according to any guidelines and frameworks.*
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. I would look at SQL as that is vulnerable to a SQL injection. SHA-256 & PKI is just encryption and is pretty secure.
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?* *2 threats could be SQL injection and session hijacking. Internal threats are threats from the inside such as a gruntled employee and external threats are from foreign actors such as someone*

	attacking through a network.
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 code can be written wrong which allows an attacker to exploit it with Javascript, HTML or a weakness in a SQL database.*
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. Being proactive about risks, using encryption, working with the programming team to make sure threats, risks, vulnerabilities are patched and secured in the right way.
