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? This app will offer its users several payment options via the app.* ● *Does it do a lot of back-end processing? The app can be vulnerable to injection attacks and session hijackings, since the app uses forms that can be infiltrated if not properly protected.* ● *Are there industry regulations that need to be considered? Yes, there are industry regulations that need to be considered since the app is handling customer payments and storing user information.*
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. API, PKI, SHA-256 provide increased security. SQL Is needed to access the database of basketball shoes, and its user profiles. Therefore, I would prioritize SHA-256 since it aligns with the company's objective of keeping customer info safe.
III. Decompose application	Sample data flow diagram The technology I evaluated secures the users information such as personal information and credit card information from being stolen when searching for an item, and ultimately purchasing it.
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? The internal threats might be weak login credentials, and lack of prepared statements.* ● *What are the external threats? The external threats might*

	be SQL injection and session hijacking.
V. Vulnerability analysis	List **2 vulnerabilities** in the PASTA worksheet that could be exploited. ● *Could there be things wrong with the codebase? A third-party API could be vulnerable to attack. Since security can only assume they have a strong codebase. Such as the use of obsolete code.* ● *Could there be weaknesses in the database? An injection attack could take place within a user entry field that accesses the SQL database.* ● *Could there be flaws in the network? The network must be secure, ensuring that a threat actor does not access it.*
VI. Attack modeling	Sample attack tree diagram Threat actors can: input code into user entry fields for injection attacks. Hackers can portray themselves as the user in session hijacking and with weak passwords to steal private information.
VII. Risk analysis and impact	List **4 security controls** that you've learned about that can reduce risk. 1. Create strong password requirements for its users, and implement MFA. 2. Protect against injection attacks with good code and other measures. 3. SHA-256 to ensure data integrity and authentication. 4. Implement encryption for PII such as credit card information.