PASTA worksheet

Stages	**Sneaker company**
I. Define business and security objectives	The company is planning to build an E-commerce mobile app, where customers can create an account, login to their account and manage their account. The app will be handling PII, data privacy should be handled properly. Customers will be able to search for their choice of product, rate the product and be able to pay for the product with several payment options. This will require a lot of backend processing and during this processing the app will be handling customer SPII.
II. Define the technical scope	List of technologies used by the application: ● *Application programming interface (API)* ● *Public key infrastructure (PKI)* ● *SHA-256* ● *SQL* The API is a general technology used to deliver information to the device user. For example when a customer searches for a product or attempts to login, requests are sent to the backend server then the server sends the information back to the frontend user using the API. An API can be vulnerable to an attacker if the developer fully depends on a third party API. PKI is important when securing online information. The mobile app will be handling customer SPII, PKI uses AES to encrypted customer information such as credit. SHA-256 used the strongest hash function to secure an input data and it is considered the strongest of all because it takes in any length of input and digest it to 256 length which will make it difficult for an attacker to guess. SQL is a database programming language and it is supported by many databases. SQL is also vulnerable to SQL injection, developers must know how to code **prepared statements** that validate input before sending them to the database.

III. Decompose application	Data flow diagram
IV. Threat analysis	● *SQL Injection* ● *Session hijacking*
V. Vulnerability analysis	● *Lack of input validation on user input* ● *Fail-open error handling* ● *Not closing the database connection properly* ● *Broken AP token*
VI. Attack modeling	Attack tree diagram
VII. Risk analysis and impact	*SHA-256, incident response procedures, password policy, principle of least privilege*