PASTA worksheet

Stages	Sneaker company
I. Define business and security objectives	Make 3-4 notes of specific business requirements that will be analyzed. ● *The search bar must be able search and show available sneakers according to a customer input.* ● *Users can create member profiles internally or by connecting external accounts with SSO.* ● *The app must process financial transactions.* ● *The app should be in compliance with PCI-DSS.*
II. Define the technical scope	List of technologies used by the application: ● *Application Programming Interface (API)* ● *Public Key Infrastructure (PKI)* ● *Advanced Encryption System (AES)* ● *Secure Hashing Algorithm (SHA-256)* ● *Structured Query Language (SQL)* ● *Non-relational Databases (NoSQL)* *To ensure there is minimal attack surface possible to be exploited by threat actors, only APIs that are of utmost importance to the business success and functionality shall be added the technologies stack. The leaner the attack vectors possible, the more secured the application shall be in the long-run.*
III. Decompose application	Sample data flow diagram
IV. Threat analysis	List 3 **types of threats** in the PASTA worksheet that are risks to the information being handled by the application. ● *XSS Attack* ● *SQL Injection* ● *Session Hijacking*
V. Vulnerability analysis	List 3 **vulnerabilities** in the PASTA worksheet that could be exploited. ● *Lack of Secure Hashing Algorithms (SHA)* ● *Lack of prepared statements*

	- *Broken API token*
VI. Attack modeling	Sample attack tree diagram
VII. Risk analysis and impact	List 5 **security controls** that can reduce risk. *Separation of duties, SHA-256, incident response procedures, password policy, principle of least privilege*