PASTA worksheet

Stages	**Sneaker company**
I. Define business and security objectives	Some of the Business requirements to be analyzed ● *Users can create member profiles internally or by connecting external accounts.* ● *The app must process financial transactions.* ● *The application must be PCI-DSS compliant*
II. Define the technical scope	This app will be exchanging and storing a lot of user data. These are some of the technologies that it uses: ● *Application programming interface (API)* ● *Public key infrastructure (PKI)* ● *SHA-256* ● *SQL* *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.*
III. Decompose application	Sample data flow diagram To protect user data during the process of making searches from the database, we used: SHA-256: SHA-256 is a commonly used hash function that takes an input of any length and produces a digest of 256 bits. The sneaker app will use SHA-256 to protect sensitive user data, like passwords and credit card numbers. Structured query language (SQL): SQL is a programming language used to create, interact with, and request information from a database. For example, the mobile app

	uses SQL to store information about the sneakers that are for sale, as well as the sellers who are selling them. It also uses SQL to access that data during a purchase.
IV. Threat analysis	Example of **types of threats** in this PASTA worksheet are risks to the information being handled by the application ● Injection ● Session hijacking
V. Vulnerability analysis	**2 of these vulnerabilities** in the PASTA worksheet can be exploited. ● Lack of prepared statements ● Broken API token
VI. Attack modeling	Sample attack tree diagram Threat actors can use SQL injection to gain access into the database. Also weak login credentials can also give threat actors access into the application.
VII. Risk analysis and impact	**4 of these security controls will definitely reduce risk.** reduce risk. SHA-256, incident response procedures, password policy, principle of least privilege.