PASTA worksheet

You're part of the growing security team at a company for sneaker enthusiasts and collectors. The business is preparing to launch a mobile app that makes it easy for their customers to buy and sell shoes.

You are performing a threat model of the application using the PASTA framework. You will go through each of the seven stages of the framework to identify security requirements for the new sneaker company app.

First, review the following description of why the sneaker company decided to develop this new app:

Description: Our application should seamlessly connect sellers and shoppers. It should be easy for users to sign-up, log in, and manage their accounts. Data privacy is a big concern for us. We want users to feel confident that we're being responsible with their information.

Buyers should be able to directly message sellers with questions. They should also have the ability to rate sellers to encourage good service. Sales should be clear and quick to process. Users should have several payment options for a smooth checkout process. Proper payment handling is really important because we want to avoid legal issues.

Stages	Sneaker company
I. Define business and security objectives	Make 2-3 notes of specific business requirements that will be analyzed. ● *User Data CIA* ● *Users can create member profiles internally or by connecting external accounts.* ● *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)* ● *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	Data flow Diagram in folder
IV. Threat analysis	List **2 types of threats** in the PASTA worksheet that are risks to the information being handled by the application. ● *Injection* ● *Session hijacking*
V. Vulnerability analysis	List **2 vulnerabilities** in the PASTA worksheet that could be exploited. ● *Lack of prepared statements* ● *Broken API token*
VI. Attack modeling	Attack tree diagram in folder
VII. Risk analysis and impact	List **security controls** that can reduce risk. *SHA-256, incident response procedures, password policy, principle of least privilege, Proper OAuth for APIs, Proper Input sanitizations*
