PASTA worksheet

Scenario:

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.

Stages	Sneaker company
I. Define business and security objectives	• *It should be easy for users to sign-up, log in, and manage their accounts.* • *All customer data should be secure and confidential.* • *Availability is a major concern, customers should be able to access customer support when needed as well as have access to different payment channels.* • *Input handling for customer payment is integral in order to achieve compliance as per PCI-DSS.*
II. Define the technical scope	• *SQL: The application will use a database to store product and customer information. Proper input sanitization and validation is required in order to prevent SQL injection.* • *SHA 256: The app will use SHA-256 to protect sensitive user data, like passwords and credit card numbers.* • *PKI: The mobile app uses a combination of symmetric and asymmetric encryption algorithms: AES and RSA. AES to encrypt customer data such as credit card information. And RSA for exchange of keys between the application and the user's device.* • API: Third-party APIs are commonly used to add

	functionality without having to program it from scratch. These APIs should be fully secure and trusted.
III. Decompose application	Sample data flow diagram

IV. Threat analysis	• *What are the internal threats?*
	  ○ *Authentication could be attacked if a threat actor social engineers an employee.*
	  ○ *Internal system logs can be compromised leading to exposure of sensitive company processes.*
	• *What are the external threats?*
	  ○ *The app can be subjected to a denial of service attack by a hacker, Affecting the services the app renders.*
	  ○ *A hacker can exploit an app vulnerability via an API or server side validation process.*

V. Vulnerability analysis	• *The form used to collect credit card information might be vulnerable to injection attacks if it fails to encrypt data. This applies to other fields as well that require input such as the search bar and customer service contact forms.* • *Insecure third-party domain access caused by the use of third party APIs which can hosted content from an untrusted server into a trusted application: affecting the server, server environment, and client device*
VI. Attack modeling	Sample attack tree diagram
VII. Risk analysis and impact	SHA-256, incident response procedures, password policy, principle of least privilege