PASTA worksheet

Stages	Sneaker company
I. Define business and security objectives	The app is expected to process payments securely and protect buyer and seller financial information. The application will comply with PCI DSS to ensure credit and banking information is secure. User credentials also need to be secured and protected when they create new accounts.
II. Define the technical scope	A PKI will be implemented to ensure data encryption for sensitive information. AES will be used to encrypt customer credit card information. RSA will be used to create public and private keys to communicate between the users device and the application. This is one of the most secure methods of ensuring user data is protected alongside using SHA256 hashing on the users passwords and payment information.
III. Decompose application	Sample data flow diagram
IV. Threat analysis	Potential internal threats to the PKI that could be exposed could include the encryption key from a disgruntled employee. External threats could be any kind of SQL injection being attempted while using the search bar or any input field on the application.
V. Vulnerability analysis	SQL injection could compromise sensitive user information if proper input sanitization is not implemented alongside a prepared statement. Any potential failure in encrypting a users data is also a risk so making sure transit of data is always secure is a priority.
VI. Attack modeling	Sample attack tree diagram
VII. Risk analysis and impact	MFA and strong password requirements are a good security control to prevent brute force attacks on customers. Proper input sanitization and prepared statements when dealing with user input is a essential security measure to prevent abuse of search bars and other input fields. Encrypting customer data with SHA256 hashing method and using public and private keys when the application communicates between the user and the server is

	another great security control.