PASTA worksheet

Stages	Sneaker company
I. Define business and security objectives	● *Users can create member profiles internally or by connecting external accounts, such as:* ○ *Google* ○ *Facebook* ● *Back-end processing:* ○ *Account: The system must manage user data. including registration login and user account management to enable users to edit their personal information. and manage account settings with ease.* ○ *Database: The database stores important information for the application, such as user information, seller information, and trading history. and conversation information Database design should make it efficient and secure to prevent data loss and unauthorized access.* ○ *Financial transaction: Accurate and secure processing of financial transactions is important, for example by using the services of a reliable payment system. Transaction validation and recording financial history.* ● *The app should be in compliance followings:* ○ *PCI-DSS* ○ *GDPR*
II. Define the technical scope	List of technologies used by the application: ● *Application programming interface (API)* ● *Public key infrastructure (PKI)* ● *SHA-256* ● *SQL* 1. **API**: *Evaluate how the APIs are implemented and secured, ensuring that third-party APIs are properly integrated and that data exchanges between software components are protected from unauthorized access and data leakage.* 2. **SQL**: *Review the usage of SQL in storing and accessing*

	data within the application's database. Evaluate the implementation of input validation, prepared statements, and other security measures to prevent SQL injection attacks and unauthorized data retrieval. 3. **SHA-256**: *Examine the use of SHA-256 for hashing sensitive user data like passwords and credit card numbers. Ensure that the hashing process is properly implemented to safeguard data integrity and protect against unauthorized access or tampering.* 4. **PKI**: Assess the implementation of symmetric and asymmetric encryption algorithms (AES and RSA) to ensure that sensitive data, such as credit card information, is securely encrypted during transmission and storage. Evaluate the key exchange process and its resistance to cryptographic attacks.
III. Decompose application	Sample data flow diagram
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	Sample attack tree diagram
VII. Risk analysis and impact	List **4 security controls** that you've learned about that can reduce risk. ● *Principle of least privilege* ● *Security awareness training* ● *MFA* ● *Patch management and vulnerability scanning*