PASTA worksheet

Stages	Sneaker company
I. Define business and security objectives	**Will the app process transactions?** The app must process financial transactions. **Does it do a lot of back-end processing?** Users can create member profiles internally or by connecting external accounts. **Are there industry regulations that need to be considered?** 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* **Application Programming Interface (API):** APIs play a crucial role in data exchange between customers, partners, and employees. Given their involvement in connecting various users and systems, their security should be a top priority. However, it's essential to assess specific APIs in use before prioritizing security measures, considering potential vulnerabilities due to a broader attack surface. **Public Key Infrastructure (PKI):** PKI is a fundamental technology for securing communications through the use of public and private key pairs. Its role in providing authentication and encryption services makes it vital for safeguarding sensitive data. Regularly reviewing and updating PKI configurations ensures the continued integrity and security of the application. **SHA-256:** The use of SHA-256, a cryptographic hash function, contributes to data integrity and secure storage. This technology is vital for ensuring the integrity of transmitted and stored data, adding an

	extra layer of protection against tampering or unauthorized modifications. **SQL:** SQL, or Structured Query Language, is commonly used for database management in applications. While SQL itself is not inherently a security technology, securing SQL queries and databases is critical to prevent SQL injection attacks. Implementing secure coding practices and regularly auditing SQL queries enhance the overall security of the application.
III. Decompose application	**Sample data flow diagram:** https://docs.google.com/presentation/d/12dfPGpj66EbnDQ21Q5oajtjo9oV6Om4gs8KncCj2ZLc/edit?resourcekey=0-wcvHEH4vdb7j2HUsxxtSZQ#slide=id.g1da1bf17772_0_0
IV. Threat analysis	**What are the internal threats?** Injection **What are the external threats?** Session Hijacking
V. Vulnerability analysis	• Lack of Prepared Statements. • Broken API token.
VI. Attack modeling	**Sample attack tree diagram** https://docs.google.com/presentation/d/1O6MdNVR4qOgVzH6xQysrry8A8qrxWxCgOyB09Ganzlk/edit?resourcekey=0-QKDYQ5WCF4RB6_Bcnc3D0w#slide=id.p
VII. Risk analysis and impact	SHA-256, incident response procedures, password policy, principle of least privilege