PASTA worksheet

Stages	Sneaker company
I. Define business and security objectives	- Ensure user data privacy to build user confidence.- Provide a seamless and quick transaction process to enhance user experience.- Enable multiple payment options to cater to diverse user preferences and avoid legal issues.- Process transactions securely to avoid legal issues.- Comply with industry regulations regarding data privacy and payment processing.
II. Define the technical scope	Technologies Used:- Application Programming Interface (API)- Public Key Infrastructure (PKI)- SHA-256- SQL Prioritized Technology: PKI is prioritized due to its role in encrypting sensitive data and managing key exchanges. Any compromise in PKI can lead to significant data breaches, impacting user trust and legal compliance
III. Decompose application	Sample data flow diagram
IV. Threat analysis	**Internal Threats:**- Insider threats where employees misuse their access to sensitive data.- Misconfigured security settings that allow unauthorized access. **External Threats:**- Phishing attacks targeting users to steal login credentials.- Man-in-the-Middle (MitM) attacks intercepting data transmission.
V. Vulnerability analysis	***Vulnerabilities:****- SQL Injection: If user inputs are not properly sanitized, attackers could exploit SQL injection vulnerabilities to access or manipulate the database.- Weak Encryption Algorithms: Using outdated or weak encryption methods can lead to easy decryption of sensitive data by attackers*
VI. Attack modeling	Sample attack tree diagram
VII. Risk analysis and impact	**Security Controls:**- Use strong encryption (AES, RSA) to protect sensitive data.- Secure APIs by implementing rate limiting, input validation, and proper authentication.- Conduct regular security audits to identify and fix vulnerabilities.- Educate users about phishing attacks and safe practices to protect their credentials.