PASTA worksheet

Stages	Sneaker company
I. Define business and security objectives	Make **2-3 notes** of specific business requirements that will be analyzed. • *The app must ensure the secure handling of customer data, especially personally identifiable information (PII), to protect users' privacy and build trust with customers.* • *The app must support multiple payment options and ensure secure and efficient handling of payment transactions to avoid legal issues.* • *The app should provide an user-friendly interface where customers can sign up, log in, manage their accounts, and communicate with sellers effectively.*
II. Define the technical scope	List of technologies used by the application: • *Application programming interface (API)* • *Public key infrastructure (PKI)* • *SHA-256* • *SQL* **API** and **SQL** should be prioritized, because they are critical components for data interaction and management within the mobile app. APIs facilitate communication between the app and external services, while SQL manages database queries. Ensuring their security is essential to prevent data breaches and unauthorized access, which are key concerns for both user experience and business operations.
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. • *Internal threats:* • *Misconfiguration of security controls within the application, such as improper handling of SQL queries leading to SQL injection risks.* • *Inadequate encryption implementation in the public key*

	infrastructure (PKI), which could compromise the protection of sensitive data. ● *External threats:* ● *Session Hijacking occurs when an attacker intercepts a valid session between a user and the server to gain unauthorized access.* ● *Exploitation of vulnerabilities in the application programming interface (API), allowing attackers to intercept or manipulate data during transit.*
V. Vulnerability analysis	List **some vulnerabilities** in the PASTA worksheet that could be exploited. ● *Weak encryption methods* ● *Lack of prepared statements* ● *Unsanitized inputs* ● *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. **Input Validation**: Implementing strict input validation ensures that data entering the system is sanitized, which helps prevent **SQL injection** and other forms of code injection. **Encryption (PKI and SHA-256)**: Encrypting sensitive data both in transit and at rest using **public key infrastructure (PKI)** and strong algorithms like **SHA-256** can protect data from unauthorized access. **Session Management**: Implementing secure session management techniques, such as **session timeouts** and **regenerating session IDs**, can help prevent **session hijacking**. **Firewalls and Intrusion Detection Systems (IDS)**: Using **firewalls** and **IDS** helps monitor network traffic and block unauthorized access, reducing the risk of external threats like **brute force attacks** or **session hijacking**.