

PASTA worksheet

| Stages | Sneaker company |
|---|---|
| I. Define business and security objectives | <p>Make 2-3 notes of specific business requirements that will be analyzed.</p> <ul style="list-style-type: none">• <i>The application must provide a simple and secure process for user sign-up, login, and account management.</i>• <i>It must ensure strong data privacy and compliance with relevant data protection regulations to build user trust</i>• <i>The app must process financial transactions.</i> |
| II. Define the technical scope | <p>List of technologies used by the application:</p> <ul style="list-style-type: none">• Application programming interface (API)• Public key infrastructure (PKI)• SHA-256• SQL <p>APIs facilitate the exchange of data between customers, partners, and employees, so they should be prioritized. They handle a lot of sensitive data while they connect various users and systems together. However, details such as which APIs are being used should be considered before prioritizing one technology over another. So, they can be more prone to security vulnerabilities because there's a larger attack surface.</p> <p>PKI is an encryption framework that secures the exchange of online information. The mobile app uses a combination of symmetric and asymmetric encryption algorithms: AES and RSA. AES encryption is used to encrypt sensitive data, such as credit card information. RSA encryption is used to exchange keys between the app and a user's device.</p> <p>SHA-256 is a commonly used hash function that takes an input of any length and produces a digest of 256 bits.</p> <p>SQL is a programming language used to create, interact with, and request information from a database</p> |

| | |
|--------------------------------------|--|
| | |
| III. Decompose application | Sample data flow diagram |
| IV. Threat analysis | <p>List 2 types of threats in the PASTA worksheet that are risks to the information being handled by the application.</p> <ul style="list-style-type: none"> • <i>Injection</i> • <i>Session hijacking</i> |
| V. Vulnerability analysis | <p>List 2 vulnerabilities in the PASTA worksheet that could be exploited.</p> <ul style="list-style-type: none"> • <i>Lack of prepared statements</i> • <i>Broken API token</i> |
| VI. Attack modeling | Sample attack tree diagram |
| VII. Risk analysis and impact | <p>List 4 security controls that you've learned about that can reduce risk.</p> <ul style="list-style-type: none"> • SHA-256, • incident response procedures, • password policy, • principle of least privilege |
