## 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 process transactions securely. * Users can log-in, sign-up, and manage accounts with data privacy and responsibility for handling user data is a priority. * Proper payment handling to avoid legal issues. |
| **II. Define the technical scope** | List oftechnologies used by the application:   * Application programming interface (API) * Public key infrastructure (PKI) * SHA-256 * SQL   Write **2-3 sentences** (40-60 words) that describe why you choose to prioritize that technology over the others.  API and Public Key Infrastructure should be prioritized. APIs are commonly used to add functionality without having to program it from scratch for example Payment Gateway such as mastercard API or VISA API to handle the proper payment to avoid legal issues. However the use of this API has to be compared with secure sensitive data handling, because of that the Public key infrastructure will be prioritized too. Public key infrastructure will encrypt and secure 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. |
| **III. Decompose application** | [Sample data flow diagram](https://docs.google.com/presentation/d/1ol7y79popTFfNHM-90ES-H-i1Lpd0YNvPShxBlXozjg/template/preview?resourcekey=0-DZAkf7Vzh2PXsP-j3oXV-g) |
| **IV. Threat analysis** | List **2 types of threats** in the PASTA worksheet that are risks to the information being handled by the application.   * SQL Injection * Session Hijacking |
| **V. Vulnerability analysis** | List **2 vulnerabilities** in the PASTA worksheet that could be exploited.   * Weak encryption of sensitive user data such as the user credit card or debit card data for the information in the payment term * Insufficient input validation could lead to potential SQL injection vulnerabilities. |
| **VI. Attack modeling** | [Sample attack tree diagram](https://docs.google.com/presentation/d/1FmWLyHgmq9XQoVuMxOym2PHO8IuedCkan4moYnI-EJ0/template/preview?usp=sharing&resourcekey=0-zYPY7AhPJdcClXamlAfOag) |
| **VII. Risk analysis and impact** | List **4 security controls** that you’ve learned about that can reduce risk.   * Implement Multi-factor authentication to enhance user authentication. * Implement regular code reviews and penetration test to test the security system capability * Implement data encryption for payment cards such as credit card or debit card using Public key infrastructure to encrypt and secure the exchange of online information. * Implement Input validation to prevent SQL injection. * Implement WAF/Web Application Firewall to filter, monitor, and block suspicious HTTP traffic to and from a web site service. |