## PASTA worksheet

| **Stages** | **Sneaker company** |
| --- | --- |
| **I. Define business and security objectives** | * The app must process transactions securely. * Data privacy and responsible handling of user information are top priorities. * Proper payment handling is crucial 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*   *I would prioritize evaluating the "Public key infrastructure (PKI)" technology. It involves the encryption of sensitive data and the exchange of keys, which are essential components for protecting user information and ensuring secure transactions in the mobile app. The use of symmetric and asymmetric encryption algorithms (AES and RSA) for data protection is a critical security consideration.* |
| **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.   * *Threat: Malware infection on the authentication system.* * *Threat: Social engineering attacks targeting employees involved in the authentication process.* |
| **V. Vulnerability analysis** | List **2 vulnerabilities** in the PASTA worksheet that could be exploited.   * *Vulnerability: Inadequate encryption of credit card information in the payment system.* * *Vulnerability: Insufficient input validation leading 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** | Implement multi-factor authentication (MFA) to enhance user account security.  Conduct regular code reviews and penetration testing to identify and address vulnerabilities.  Implement data encryption for credit card information using strong encryption algorithms.  Employ web application firewalls (WAFs) to protect against SQL injection and other web-based threats. |