## PASTA worksheet

| **Stages** | **Sneaker company** |
| --- | --- |
| **I. Define business and security objectives** | Make **2-3 notes** of specific business requirements that will be analyzed.   * *The transactions need to be processed securely among the buyers and the sellers.* * *The user’s data should be handled carefully, they should feel comfortable with their privacy.* * *Since, the app features transactions, proper rules and regulations and security features should be set in place.* |
| **II. Define the technical scope** | List oftechnologies used by the application:   * *Application programming interface (API)* * *Public key infrastructure (PKI)* * *SHA-256* * *SQL*   *The application is to be used for various online transactions. PKI should be of the first focus as ES 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** |  |
| **IV. Threat analysis** | List **2 types of threats** in the PASTA worksheet that are risks to the information being handled by the application.   * *Mishandling of user’s private transaction data* * *SQL Injection* |
| **V. Vulnerability analysis** | List **2 vulnerabilities** in the PASTA worksheet that could be exploited.   * *The application might fail to encrypt the data correctly.* * *PTP protocol can be hacked.* |
| **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** | SHA-256, incident response procedures, password policy,  principle of least privilege |