## PASTA worksheet

| **Stages** | **Sneaker company** |
| --- | --- |
| **I. Define business and security objectives** | This app will connect sellers and buyers for sneakers so security and adherence to PCI-DSSis a must.  Ease of use for smooth transactions  Privacy protection |
| **II. Define the technical scope** | List oftechnologies used by the application:   * *Application programming interface (API)* * *Public key infrastructure (PKI)* * *SHA-256* * *SQL*   OWASP’s number two on its top ten is Cryptographic failures and given the nature of this app with its core concept being financial in nature this should be the focus of this threat model. The PKI should be focused on as it poses the biggest risk if not implemented securely and could lead to loss of data, lawsuits, and reputation damage. |
| **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** | Two possible threats here would be:   * Unauthorized access to the company database which includes usernames, passwords, and payment details. * Payment related vulnerabilities such as a weakness in encryption being exploited to start unauthorized payments to or from accounts. |
| **V. Vulnerability analysis** | List **2 vulnerabilities** in the PASTA worksheet that could be exploited.   * ***Broken Access Control*** allows more access than intended. * ***Cryptographic Failures*** allowing SPII and PII to be viewed and stolen |
| **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** | * Least privilege * MFA * RBAC * Prepared statements SQL to help protect against injection attacks * Password complexity requirement in compliance with NIST 800-63B. |