## PASTA worksheet

|  |  |
| --- | --- |
| **Stages** | **Sneaker company** |
| **I. Define business and security objectives** | Make **2-3 notes** of specific business requirements that will be analyzed.   * *Will the app process transactions?*   *Yes it will process financial transactions.*   * *Are there industry regulations that need to be considered?*   *Yes, it should follow the PCI-DSS regulation model.* |
| **II. Define the technical scope** | List oftechnologies used by the application:   * *API* * *PKI* * *AES* * *SHA-256* * *SQL*   Write **2-3 sentences** (40-60 words) that describe why you choose to prioritize that technology over the others.  From the above list I believe the API technology should be used for this application, as it lays out a set of rules on how the application will interact with other components making it relatively safe to be handling a lot of sensitive data between customers, partners, and employees. |
| **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.   * *What are the internal threats?*   *Injection*   * *What are the external threats?*   *Session hijacking* |
| **V. Vulnerability analysis** | List **2 vulnerabilities** in the PASTA worksheet that could be exploited.  *The things that could be vulnerable with the codebase could be the lack of prepared statements.*  *Another vulnerability could be weak login credentials.* |
| **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.  Principle of the least privileged, incident response procedures, password policy, Multifactor authentication. |