## 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? Of course, it would.* * *Does it do a lot of back-end processing? Maybe, it could be offloaded to the server though.* * *Are there industry regulations that need to be considered? Yes, PII security standards, Payment Security Compliance, Application communication protection etc.* |
| **II. Define the technical scope** | List oftechnologies used by the application:   * *Application programming interface (API)* * *Public key infrastructure (PKI)* * *SHA-256* * *SQL*   These are the bare-bones without which the app wouldn’t function securely, or function at all for that matter. The basic work of fetching required info from the server requires the help of these technologies. For the Application to interact with the server, and fetch & put info, API calls are necessary, both 1st party & 3rd party for logins & payments.  PKI ensures that communication over the Internet is secure through asymmetric key encryption, from the server to the client app & vice-versa.  SHA 256 is a good method to store passwords & other credentials that would need integrity checks, like the app itself, after being downloaded, before installation. SQL, to fetch the required data according to the filters applied by the customer in the app to search for a certain type. |
| **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? Server downtime, Rogue Employees, Supply Chain Attacks, etc.* * *What are the external threats? Competitors & Hackers, Network failure etc.* |
| **V. Vulnerability analysis** | List **2 vulnerabilities** in the PASTA worksheet that could be exploited.   * *Could there be things wrong with the codebase? Yes, not escaping characters properly may lead to SQL injection, XSS etc.* * *Could there be weaknesses in the database? Yes, improper access control can lead to data leaks.* * *Could there be flaws in the network? Yes, MITM attacks, and DDOS attacks protection need to be taken care of.* |
| **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.   * IAM Controls * Defence in depth * MFA * Segregation of Duties |