## PASTA worksheet

| **Stages** | **Sneaker company** |
| --- | --- |
| **I. Define business and security objectives** | * *The app should accept payments, user sessions, messages and a rating system, each one of these should be carefully developed as there is a lot of input required and threat actors could inject SQL code and access a lot of PII* |
| **II. Define the technical scope** | List oftechnologies used by the application:   * *Application programming interface (API)* * *Public key infrastructure (PKI)* * *SHA-256* * *SQL*   Write **2-3 sentences** (40-60 words) that describe why you choose to prioritize that technology over the others.  API and PKI are important parts of encryption, but as they are well established protocols that offer plenty of security, i don’t consider them that important to analyze, the same goes for the hashing protocol.  SQL can be deceptively easy to set up at times, but really hard to secure as people can inject SQL code that can reveal all of the PII and other relevant information |
| **III. Decompose application** | SQL can be dangerous as the processes the user does are directly passed to the database which then processes the data the user passes, but the user can pass along sql code and then the DB execute said code without restrictions, unless we make those restrictions real.  Things like the API and the PKI are also really important as they are how one interacts with the web page.  How passwords are encrypted is also important, as a weak hashing can lead to easily hackable passwords. |
| **IV. Threat analysis** | List **2 types of threats** in the PASTA worksheet that are risks to the information being handled by the application.   * *An internal threat could be a threat actor disguised as an employee and revealing public keys as well as PII of the users that is saved in the DB* * *An external threat could be a threat actor injecting SQL code or social engineering an employee with access to PII due to publicity or other important things.* |
| **V. Vulnerability analysis** | List **2 vulnerabilities** in the PASTA worksheet that could be exploited.   * *Could there be things wrong with the codebase?* * *Could there be weaknesses in the database?* * *Could there be flaws in the network?* * *There could be many vulnerabilities like: bad input sanitization that could lead to SQL injection, multiple admin levels (bad structure), hardcoded passwords (bad code), amongst others.* |
| **VI. Attack modeling** | Attack vectors like lack of prepared statements and weak login credentials can be attacked quite easily, a login with no input sanitization can easily lead to SQL injection, and no input regulation can also lead to users having passwords really easy to guess. |
| **VII. Risk analysis and impact** | List **4 security controls** that you’ve learned about that can reduce risk.  Input sanitization, Input Validation, Access Control, Good Cryptographic Algorithms |