## 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?* * *Does it do a lot of back-end processing?* * *Are there industry regulations that need to be considered?*   Two priorities exist for the company:   * Users can create member profiles internally or by connecting external accounts. * The app must process financial transactions. * The app should comply with PCI-DSS.   Given this it is important to make sure user data (especially passwords, credit card info, PII, SPII) are all encrypted. At the same time, account access control should be convenient but secured with MFA. Payment handling should be prioritised due to legal obligations. |
| **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.  I would evaluate SQL first as it is used to access data regarding the sellers and purchases are processed through SQL. If these queries are not handled properly and are fed straight through the database, there is a high risk of SQL injection.  I would also evaluate the API. This is how the application interfaces with other third-party applications. Having the API token public, for example, would be a critical vulnerability as an attacker could access the application via its API communications. They are more prone to security issues too as there is a larger attack surface. |
| **III. Decompose application** | [Sample data flow diagram](https://docs.google.com/presentation/d/1ol7y79popTFfNHM-90ES-H-i1Lpd0YNvPShxBlXozjg/template/preview?resourcekey=0-DZAkf7Vzh2PXsP-j3oXV-g)  User data should be protected every time a user proceeds with a transaction or queries information regarding a seller. It should be ensured malicious actors are not able to query PII and SPII that are stored in the database. |
| **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?* * *What are the external threats?*   Internal threats are the employees who regularly access the system. If the company isn’t currently enforcing RBAC, unauthorised access could be provided to employees. Social engineering could also be employed to make an employee provide confidential information to a threat actor.  External threats are hackers or other competitors that would benefit from knowing the information from the applciation.  Some threats that could be applied are:   * SQL injection * Session Hijacking |
| **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?*   Vulnerabilities that could be exploited include:   * Direct chat with sellers—this is prime ground for threat actors to obtain information. The employer has to ensure that the conversations held here are encrypted as confidential information could be discussed via chat. * Credit card transactions should not only encrypt data, but they should also protect for SQL injection by sanitising and validating user inputs.   Other vulnerabilities:   * SQL Injection – due to lack of prepared statements * Broken API token |
| **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.  The following controls can be applied:   * Using prepared statements every time an SQL query is carried out. * Sanitising and validating user inputs, especially for financial transactions. * Applying encryption to communications and other confidential information. * Implementing strong password policies (and MFA) would also assist with making sure users can login securely. * Principle of Least Privilege to prevent access from unauthorised users. |