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* * *Does it do a lot of back-end processing?* * *Are there industry regulations that need to be considered?*   *A shopping application like this will need to process payments. Based on this description, we know certain technologies are required to keep information private and secure and that everything will need to be compliant with PCI-DSS.* |
| **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.  APIs facilitate the exchange of data between customers, partners, and employees, so they should be prioritized. They handle a lot of sensitive data while they connect various users and systems together. However, details such as which APIs are being used should be considered before prioritizing one technology over another. So, they can be more prone to security vulnerabilities because there’s 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)  The sample data flow diagram shows how a typical search request passes through multiple layers. One thing you might review here would be to ensure the MySQL database is using prepared statements when queries are input. |
| **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? Employees* * *What are the external threats? Competitor*   *Injection attacks are common for SQL databases. Session hijacking is possible because the app communicates cookies between multiple layers.  It's important to consider your technological attack surface and any relevant threats to your product to effectively implement your information security responsibilities* |
| **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?*   *A lack of prepared statements can make our SQL database vulnerable to injection attacks. And session hijacking is possible if cookies are mishandled between input and output sources.* |
| **VI. Attack modeling** | [Sample attack tree diagram](https://docs.google.com/presentation/d/1FmWLyHgmq9XQoVuMxOym2PHO8IuedCkan4moYnI-EJ0/template/preview?usp=sharing&resourcekey=0-zYPY7AhPJdcClXamlAfOag)  This sample attack tree models how user data is vulnerable to the attacks that were identified earlier. Like the sample data flow diagram, an actual attack tree for a mobile application would be much more complex than this. |
| **VII. Risk analysis and impact** | List **4 security controls** that you’ve learned about that can reduce risk.  SHA-256, incident response procedures, password policy, and principle of least privilege are a few examples of technical, operational, and managerial controls that can be implemented before launch to reduce risk. |