## 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?*   The app will process transactions for the sale of sneakers and will have many different methods of payment for a smooth checkout process.   * *Does it do a lot of back-end processing?*   There isn’t too much back-end processing mentioned, there might be a possibility that the app would store customer information or payment details.   * *Are there industry regulations that need to be considered?*   Because payment methods would include credit cards or debit cards the PCI DSS standard needs to be considered in terms of storing customer payment details. |
| **II. Define the technical scope** | List oftechnologies used by the application:   * *API* * *PKI* * *AES* * *SHA-256* * *SQL*   I would first investigate SQL because of the SQL injection attacks that could be done through the user login page, and to mitigate SQL injections you would have to implement prepared statements, input validation, stored procedures, etc.  Write **2-3 sentences** (40-60 words) that describe why you choose to prioritize that technology over the others. |
| **III. Decompose application** | [Sample data flow diagram](https://docs.google.com/presentation/d/1ol7y79popTFfNHM-90ES-H-i1Lpd0YNvPShxBlXozjg/template/preview?resourcekey=0-DZAkf7Vzh2PXsP-j3oXV-g)   * APIs can be used to restrict access to sensitive data by requiring users to authenticate before they can access the data. * PKI can be used to ensure that only authorized users can access data by verifying the identity of the user or device before they are granted access. * AES can be used to protect sensitive data by encrypting the data before it is stored or transmitted. * SHA-256 can be used to verify the authenticity of data by creating a unique fingerprint of the data and comparing it to a known fingerprint. * SQL can be used to control who has access to data by creating user accounts and assigning permissions to those accounts. |
| **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?*   Internal threats are threats that can come from within the organization from employees, contractors, or other people who have access to the organization’s system and data. This could include a data breach from an authorized personal within the organization who accesses unauthorized customer data.   * *What are the external threats?*   External threats are threats that come from outside the organization from malicious actors. This could be a SQL injection since the app uses a SQL database, or it could be some sort of social engineering attack targeting employees of the organization. |
| **V. Vulnerability analysis** | List **2 vulnerabilities** in the PASTA worksheet that could be exploited.   * *Could there be things wrong with the codebase?*   The codebase is the collection of source code files that make up a software application. Codebase vulnerabilities can be exploited by attackers to gain unauthorized access to a system or to modify or delete data.   * *Could there be weaknesses in the database?*   Database vulnerabilities can be exploited by attackers to gain unauthorized access to data, to modify or delete data, or to disrupt the availability of the database.   * *Could there be flaws in the network?*   Network vulnerabilities can be exploited by attackers to gain unauthorized access to a system, to modify or delete data, or to disrupt the availability of the system. |
| **VI. Attack modeling** | [Sample attack tree diagram](https://docs.google.com/presentation/d/1FmWLyHgmq9XQoVuMxOym2PHO8IuedCkan4moYnI-EJ0/template/preview?usp=sharing&resourcekey=0-zYPY7AhPJdcClXamlAfOag)  2 types of vulnerabilities that could be exploited are SQL injections and session hijacking. One reason why SQL injections occur is the lack of prepared statements. Prepared statements are a way of preventing SQL injection attacks. When using prepared statements, the SQL code is stored in the database and the values are passed to the database at runtime. This prevents the attacker from injecting malicious SQL code into the database.  One reason why session hijacking occurs is the use of weak login credentials. If a user uses weak passwords or reuses passwords across multiple websites, an attacker can easily crack the password and hijack the session. |
| **VII. Risk analysis and impact** | List **4 security controls** that you’ve learned about that can reduce risk.   * Multi-factor authentication (MFA) adds an extra layer of security for the customer by requiring users to provide two or more forms of authentication, such as a username and password, plus a code from a mobile device, to gain access to a system or service. * Data encryption is the process of converting data into an unreadable format. This can help to protect data such as credit card information from unauthorized access, even if it is intercepted in transit or stored on a compromised system. * Vulnerability scanning: Vulnerability scanning is the process of identifying vulnerabilities in software and systems. Vulnerability scanning can help to identify potential security risks before they are exploited by attackers. * Access control: Access control is the process of restricting who has access to data and systems. This can help to prevent unauthorized users from accessing sensitive data or systems. |