## 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?* ***Secure Transaction Processing****: Ensure that all transactions processed through the app are secure, preventing unauthorized access and fraud.* * *Does it do a lot of back-end processing?* ***User Engagement and Retention****: Create a user-friendly interface that encourages repeated use and engagement, boosting sales and user satisfaction.* * *Are there industry regulations that need to be considered?* ***Compliance with Industry Regulations****: Adhere to relevant e-commerce and data protection regulations to avoid legal issues and build trust with users.* |
| **II. Define the technical scope** | List oftechnologies used by the application:   * *API-are prioritized for their essential role in integrating various components of the app, facilitating user interactions and backend communications. This ensures a seamless and responsive user experience.* * *PKI-****(Public Key Infrastructure)*** *is vital for securing communications between the app and its users. By enabling secure data exchange through encryption and digital signatures, PKI helps in authenticating users and preventing unauthorized access, which is fundamental for transactions and data privacy.* * *AES-****(Advanced Encryption Standard)*** *is chosen for its robustness in encrypting sensitive data at rest, such as stored user information and transaction details. AES provides a high level of security against data breaches, making it indispensable for protecting user data.* * *SHA-256-is used for ensuring data integrity and security. It generates unique hash values for data, which helps in verifying the authenticity of the data without exposing the actual data. This is particularly useful in safeguarding passwords and other sensitive data against tampering and corruption.* * *SQL-is critical for efficient data management, handling the large volumes of transaction and user data. It supports complex queries and ensures data integrity, which is crucial for the app's operations.*   Write **2-3 sentences** (40-60 words) that describe why you choose to prioritize that technology over the others.  For the new sneaker company app, prioritizing **APIs** and **SQL** is essential due to their critical roles in the application's functionality. **APIs** facilitate seamless communication between the app's front end and various services, which is vital for a dynamic, responsive user experience. **SQL**, on the other hand, is crucial for efficiently managing the large volumes of data involved in transactions and user interactions, ensuring robust and scalable database operations. These technologies are foundational to supporting the app's performance and security requirements. |
| **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?* ***Internal Threats*** * ***Insider Misuse****: Employees or insiders with access to the backend systems could misuse their privileges to manipulate or steal sensitive user data or transaction details.* * ***Accidental Data Leaks****: Unintentional actions by employees, such as misconfiguring database permissions or losing devices containing sensitive information, could lead to significant data breaches.* * *What are the external threats?* ***SQL Injection Attacks****: Given the use of SQL databases, the app is at risk from attackers who could exploit vulnerabilities in the app's SQL database to inject malicious code, potentially accessing or manipulating user data and other sensitive information.* * ***Phishing Attacks****: Attackers could target users of the app with phishing schemes to steal login credentials, thereby gaining unauthorized access to user accounts and sensitive personal and financial data.* |
| **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?*  1. ***Codebase Vulnerabilities****:*    * ***Injection Flaws****: The codebase might contain vulnerabilities such as SQL injection points where user inputs are not properly sanitized. This can allow attackers to insert malicious SQL statements that are executed by the database, potentially leading to unauthorized data access or manipulation.* 2. ***Database Security Weaknesses****:*    * ***Inadequate Access Controls****: If the database does not implement strict access controls and permissions, unauthorized users or even low-privileged users might gain access to sensitive data that they should not be able to view or alter. This can include personal user information, payment details, and transaction records.* |
| **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.   1. **Input Validation and Sanitization**: Implement rigorous input validation to prevent SQL injection and other forms of attacks where malicious data is inserted into the app. 2. **Access Controls and Role Management**: Establish strict access controls and role-based access management to ensure that only authorized personnel have access to sensitive data and operations. 3. **Regular Security Audits**: Conduct frequent security audits and code reviews to identify and rectify vulnerabilities in the app’s codebase and infrastructure. 4. **User Education and Phishing Prevention**: Educate users about security best practices and common phishing tactics through regular communications and secure login alerts. |