## 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?*   *They would like ways to safely store/collect/use customer’s personal information responsibly. Want proper payment handling to avoid legal issues.* |
| **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.  SHA-256 is important for the way they want to protect passwords and payment information as well as public key infrastructure in order to exchange information securely between customer and seller. These are the main technologies used for security purposes and i think these will be the ones to prioritse if you want the application to be secure. |
| **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 technologies evaluated relate to protecting the user data in this process by when a customer finds a shoe they like they will be securely connected to the seller with encryption and then if the customer decides to buy the shoe their payment information is stored as a hash value 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?*   *External threats can be hackers*  *Internal threats can be employees working at the company*  *Hackers can user social engineering techniques to gain information from an employee which may result in a hacker gaining access to the database.* |
| **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?*   *The database may not store payment information as a hash correctly and the credit card form could fail to encrypt the data. There could also be an underlying vulnerability in the software used to make the application could be an old outdated version and has known vulnerabilities.* |
| **VI. Attack modeling** | [Sample attack tree diagram](https://docs.google.com/presentation/d/1FmWLyHgmq9XQoVuMxOym2PHO8IuedCkan4moYnI-EJ0/template/preview?usp=sharing&resourcekey=0-zYPY7AhPJdcClXamlAfOag)  SQL injection could occur when the form does not sanitise the inputs and doesn't use prepared statements to check the query before sending the request to the server.  Session hijacking could occur when credentials are weak and a strong password policy is not in place; they could brute force their way into someone's account. |
| **VII. Risk analysis and impact** | List **4 security controls** that you’ve learned about that can reduce risk.  **Firewalls**  **Encryption**  **Multi-Factor Authentication (MFA)**  **Regular Software Updates and Patching** |