## PASTA worksheet

| **Stages** | **Sneaker company** |
| --- | --- |
| **I. Define business and security objectives** | Make **2-3 notes** of specific business requirements that will be analyzed.   * *The app will process several payment options* * *It does a lot of back end processing* * *The app needs to have 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* * *I chose to prioritize SQL because it stores a lot of sensitive data and it is used to access data during a process, this makes it really important to secure.*   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)   1. The database shows what sneakers are for sale and the vendor 2. The user chooses a sneaker 3. The user makes a purchase for it to happen the sql server needs to access sensitive data during the purchase |
| **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 are sql injection and session* |
| **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 network could not have a properly configured firewall with open ports* * *The database could be weak to sql injections* |
| **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.  To avoid a out-of-band injection certain features should be disabled  To avoid a inferential sql injection the system should return only pre set error messages  To avoid sql injection the database should only accept certain parameters of user input  The site should also have prepared statements that executes sql statements before passing them to a database |