## PASTA worksheet

|  |  |
| --- | --- |
| **Stages** | **Sneaker company** |
| **I. Define business and security objectives** | * *The application is a market place application that allows sellers and shoppers a way to connect.* * *Users accessing the site to, sign up, login and manager there accounts should be an easy process.* * *Sales should be a quick and clear process.* |
| **II. Define the technical scope** | List oftechnologies used by the application:   * *API* * *PKI* * *AES* * *SHA-256* * *SQL*   SQL attacks are the simplest attacks to conduct against the website with very little technical information about the site. SQL injection attacks should be the first area evaluated for the new website. Eliminating known SQL injection attacks will dramatically reduce the vulnerability to attacks to the website. |
| **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.  *internal threats- Social engineering to gain access to the admin functions in the website or directly to the database.*   * + *external threats -SQL injection attacks through the website to gain access, delete\change data or for gaining a foothold into the system for future attacks.* |
| **V. Vulnerability analysis** | List **2 vulnerabilities** in the PASTA worksheet that could be exploited.   * *Improper Data Validation*   + [*https://www.cve.org/CVERecord?id=CVE-2024-7456*](https://www.cve.org/CVERecord?id=CVE-2024-7456)   + *https://www.cve.org/CVERecord?id=CVE-2024-24773* * Injection problem   https://www.cve.org/CVERecord?id=CVE-2025-9943 |
| **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. Parameterized Queries/Prepared Statements  2. Input Sanitization  3. stored procedures  4. server side validation  5. least privilege access. |