# PASTA worksheet

---

| Stages | Sneaker company |
| --- | --- |
| **I. Define business and security objectives** | Make **2-3 notes** of specific business requirements that will be analyzed.<br>• *According to the business statement from the company, there will be several different forms of payment options, ensuring that they are secure and reliable is paramount.*<br>• *Due to the nature of this site(Online customer-to-buyer), backend processing is going to be quite intensive. Sign-in/login portals, account management, internal messaging server+database, photo display(possibly), payment handling and processing(PCI DSS),and customer PII database(location, phone number, payment info, past transactions, names, email)*<br>• *Since the company is dealing with multiple online payment options and personal information, it's best to adhere to the PCI DSS and GDPR regulations.(Payment Card Industry Data Security Standards and General Data Protection Regulation)* |
| **II. Define the technical scope** | List of technologies used by the application:<br>• *Application programming interface (API)*<br>• *Public key infrastructure (PKI)*<br>• *SHA-256*<br>• *SQL*<br><br>Write **2-3 sentences** (40-60 words) that describe why you choose to prioritize that technology over the others.<br>• A solid and secure API is needed to ensure the data exchange between all parties is effective, seamless and secure, making it a top priority.<br>• Ensuring that the SQL component is secure is paramount to the overall security of the web site. If SQL statements and queries are not securely programmed, a large and disastrous data breach may occur. This makes it a top priority. |
| **III. Decompose** | Sample data flow diagram |

| | |
|---|---|
| **application** | |
| **IV. Threat analysis** | List **2 types of threats** in the PASTA worksheet that are risks to the information being handled by the application.<br>● *There is a potential for several internal threats, the most common and dangerous is the SQL injection or inferential SQL injections since they focus on the database which could hold PII and payment card information.*<br>● *A potential external threat would most likely come from a social engineering standpoint, usually in the form of phishing and vishing.* |
| **V. Vulnerability analysis** | List **2 vulnerabilities** in the PASTA worksheet that could be exploited.<br>● *An error or weakness in the API codebase could allow a malicious actor to exploit a flaw and gain access to data and resources they have no authorization to access.*<br>● *The database may be vulnerable due to no prepared statements or sanitize inputs*<br>● *Since the web application is connected to the internet and thus has network functionalities, it is best to assume that the server may be vulnerable to XSS attacks(Cross-Site Scripting).* |
| **VI. Attack modeling** | Sample attack tree diagram |
| **VII. Risk analysis and impact** | List **4 security controls** that you've learned about that can reduce risk.<br>● Data encryption(At rest or In Transit)<br>● Password policy with salted hashes(SHA-256)<br>● MultiFactor Authorization<br>● Input sanitation<br>● Web application firewall(WAF) |