PASTA worksheet

Stages	Sneaker company
I. Define business and security objectives	Make **2-3 notes** of specific business requirements that will be analyzed. • *App would allow customers to make transctions* • *App would need back-end processing for managing user's accounts* • *App should consider the regulations to protect customers' PII or SPII. App should comply to GDPR (for European customers), PSI DSS (protecting payments) etc.*
II. Define the technical scope	List of technologies used by the application: • *Application programming interface (API)* • *Public key infrastructure (PKI)* • *SHA-256* • *SQL* Team chose to priortize PKI component of the app first. We did so determine if the app is using asymmetric encryption when customer tries to establish connection with a seller using log in credentials as it provides more secure communication.
III. Decompose application	Sample data flow diagram Customer looks for the shoes of his choice by searching. By searching, the user is utilizing the SQL technology as he query's the company's database. In response to customer's query the company's data outputs the collection of shoes that matches customer's search criteria
IV. Threat analysis	List **2 types of threats** in the PASTA worksheet that are risks to the information being handled by the application. • *Employee could be targeted with social engineering to reveal information about the company that could grant unauthorized access* • *Hacker targeting servers using stored XSS attack*
V. Vulnerability analysis	List **2 vulnerabilities** in the PASTA worksheet that could be exploited.

	• *Vulnerableto SQL injection as its being used during purchase.* • *Lacks MFA, Salting etc.* • *Could there be flaws in the network?*
VI. Attack modeling	Sample attack tree diagram Threat actors could use SQL injection steal PII due to lack of prepared statements. SSO or weak password could be target of attacks for session hijacking by the threat actors
VII. Risk analysis and impact	- Use of MFA - Prepared statements to execute Sql statements before passing them to the database. - Salting the hash values to render rainbow tables useless - Antiviruses

---