PASTA worksheet

Stages	Sneaker company
I. Define business and security objectives	• *Will the app process transactions?* • *Does it do a lot of back-end processing?* • *Are there industry regulations that need to be considered?* The app will process transactions as it will be a platform for sneaker enthusiasts to buy and sell shoes. It will be doing a lot of back-end processing. There will be regulations regarding PII usage such as PCI-DSS and GDPR that needs to be considered.
II. Define the technical scope	List of technologies used by the application: • *Application programming interface (API)* • *Public key infrastructure (PKI)* • *SHA-256* • *SQL* We are using more advanced encryption algorithms such as AES and RSA to make sure data in transit is well protected. The choice of SHA-256 as the hashing algorithm is meant so that the sensitive user data like passwords and credit cards are protected and not easily decrypted.
III. Decompose application	Sample data flow diagram
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?* The internal threats include employees who have access to customer information that can be compromised if their credentials are stolen. The external threats include any rival businesses or hackers that would want to steal any proprietary information. Injection and session hijacking are threats that can occur.
V. Vulnerability	• *Could there be things wrong with the codebase?*

analysis	• *Could there be weaknesses in the database?* • *Could there be flaws in the network?* Some vulnerabilities that could happen are the lack of input validation and sanitization and prepared statements, which could result in injection vulnerabilities. The database can also be injected if not properly protected. There could also be issues regarding any weak login credentials.
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. SHA-256 hashing, incident response playbook, well-kept password policy, the principle of least privilege

---