PASTA worksheet

Stages	Sneaker company
I. Define business and security objectives	Make **2-3 notes** of specific business requirements that will be analyzed. ● *Will the app process transactions?* ● *Does it do a lot of back-end processing?* ● *Are there industry regulations that need to be considered?* It should be easy for users to sign-up, log in, and manage their accounts. Data privacy is a big concern for us. Users feel confident that we're being responsible with their information. Users should have several payment options for a smooth checkout process. Proper payment handling is really important because we want to avoid legal issues. In compliance with PCI-DSS.
II. Define the technical scope	List of technologies used by the application: ● *Application programming interface (API)* ● *Public key infrastructure (PKI)* ● *SHA-256* ● *SQL* Write **2-3 sentences** (40-60 words) that describe why you choose to prioritize that technology over the others. APIs are prioritized as they enable seamless integration between the application's components and external systems, ensuring efficient communication and scalability while enhancing user experience. Choose because it is specifically an application programming interface that enhances user experience.
III. Decompose application	Sample data flow diagram Single process- when a user looks something up it goes through the database system returns information back to the user.
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?* Injection Attacks

	• ***Description****: Malicious input is sent to the application, exploiting vulnerabilities in how queries are executed.* • ***Impact****: Attackers could gain unauthorized access to sensitive data, manipulate or delete database records, or compromise the entire system.* • ***Mitigation****: Use prepared statements and parameterized queries to sanitize input and prevent malicious code execution.* Data Interception • ***Description****: An attacker intercepts communication between the user and the server to steal sensitive data.* • ***Impact****: Confidential information, such as search queries, authentication tokens, or personal data, could be exposed or tampered with.* • ***Mitigation****: Implement strong encryption protocols (e.g., TLS) and use PKI to authenticate server-client communications.*
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?* *A couple of vulnerabilities the security team found consist of things in the codebase, database, and network. Vulnerabilities in common in codebase as they can be insecure coding practices such as improper spelling, or lack of security checks. Database can also be exploited in several ways, especially if there is a lack of encryption attacks can gain access to the database and steal or leak sensitive data and information. Lastly, the network can also be exploited. Similar to database, a weak encryption can allow an exploitation. However, open ports and unused common network ports can also be exploited by attackers.*
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. Encryption MFA -Multi-Factor Authentication Principle of Least Privilege SHA-256