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? The app will process sneaker sales using several payment options.* ● *Does it do a lot of back-end processing? The app does a lot of back-end processing because it will store customers' log in credentials, seller ratings, and order history.* ● *Are there industry regulations that need to be considered? Industry regulations concerning data privacy and payment processing need 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* Write **2-3 sentences** (40-60 words) that describe why you choose to prioritize that technology over the others. I would evaluate PKI and SHA-256 first. I would prioritize these technologies because they play a large role in keeping the most sensitive customer information, their financial data, secure. These technologies might present risks from a security perspective because if the encryption is not secure enough, the company could be exposed to legal and financial consequences linked to failing to meet regulatory standards.
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? Employees maliciously leaking customer payment information are internal threats.* ● *What are the external threats? Competitors hacking the inventory database to offer more competitive pricing is an*

	external threat.
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? If the saved payment methods aren't properly encrypted, they could be compromised. Reviewer data could become visible to sellers.* ● *Could there be flaws in the network?* *Log in form could be subject to SQL injection* *Email phishing could be used to encourage customers to release their payment information under the guise of updating or confirming their order*
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. Use prepared statements to lessen chances of SQL injection Implement input sanitization Set up automated monitoring for increased CPU usage to check for cryptojacking Disable Javscript