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?* • *The app should allow users to message sellers, process purchase transactions, and user reviews.* • *It should adhere to global regulations for data privacy and financial regulations like GDPR and FFIEC to avoid legal troubles.* • *The app will do a lot of back-end processing because of the different payment options and users' account data.*
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) describing why you prioritize that technology over the others. I would evaluate the app's third-party APIs before the others because it is the most vulnerable technology. The APIs could be susceptible to data breaches caused by SQL injection on the login or search inputs or session hijacking from broken authentication and session management.
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?*

	• *SQL injections* • *Session hijacking*
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?* • *Weak user account passwords* • *Lack of prepared statements or input sanitization*
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. • Add prepared statements before every request to the database • Add input sanitization to database requests • Update and maintain intrusion detection and prevention systems • Add multi-factor authentication(2-factor)
