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? yes , with many options of payment* • *Does it do a lot of back-end processing? Sure, massaging, process of purchase, rating* • *Are there industry regulations that need to be considered? Yes, privacy of information, card payments.* *The aim is to keep private customer data safe when making payments, communicating and evaluating sellers. Private personal data will be processed, which must be protected by law*
II. Define the technical scope	List of technologies used by the application: • *Application programming interface (API)* • *Public key infrastructure (PKI)* • *SHA-256* • *SQL* The above technologies were chosen for thorough examination because they are susceptible to the most popular threats and exploitation of vulnerabilities. Hackers try to gain the most benefits at the lowest cost. The above technologies, if not well secured, present such an opportunity.
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?* *An internal threat could be an inadvertent change of permissions or a login screen. Or man in the middle attack, when a customer makes a purchase on public WIFI.*

	An external threat may be a hacker who tries to log into the system using phishing and brute force methods.
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?* *Lack of input validation on user input* *Not closing the database connection properly*
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. The use of data encryption both during storage and transmission to protect against unauthorized access. Establishing strict access policies to ensure only authorized users have access to systems and data Digital Signatures: PKI enables the creation of digital signatures that can confirm the integrity and authenticity of data, helping to prevent tampering and hijacking. Prepared statements helps protect against SQL injection attacks and improves application security