PASTA worksheet

Stages	Sneaker company
I. Define business and security objectives	● *The app will be making transactions regularly.* ● *The app will be doing a lot of processing on the backend.* ● *An industry regulation that needs to be considered here is PCI-DSS for transactions and GDPR for international users.*
II. Define the technical scope	List of technologies used by the application: ● *API* ● *PKI* ● *AES* ● *RSA* ● *SHA-256* ● *SQL* APIs are used to facilitate the exchange of data and should be prioritized because they will be handling a lot of sensitive data. APIs because of this are prone to attacks and any 3rd party APIs used in the app may have underlying vulnerabilities posing a threat to the organization.
III. Decompose application	Sample data flow diagram
IV. Threat analysis	● *Injection* ● *XSS*
V. Vulnerability analysis	List **2 vulnerabilities** in the PASTA worksheet that could be exploited. ● *Codebase does not properly use sanitation to properly protect against injection attacks.* ● *Database not using prepared statements to protect against SQL injections.* ● *Proper network firewalls, IDS, IPS, etc.... to protect against network attacks.*
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. 1.) Input Sanitation 2.) Prepared Statements 3.) Strong password policies 4.) WAF or Web application Firewalls

---