PASTA worksheet

Stages	**Sneaker company**
I. Define business and security objectives	Make **2-3 notes** of specific business requirements that will be analyzed. *One business requirement is for users to have a secured account because payment transactions will be used. Since there are lots of different data being sent/used by this website like buyers being able to message sellers, users making accounts, etc, those would need to be encrypted. Industry regulations require them to be encrypted like FIPS 140-3 and GDPR.*
II. Define the technical scope	List of technologies used by the application: ● *Application programming interface (API)* ● *Public key infrastructure (PKI)* ● *SHA-256 - This technology would be the top priority for security. Since the company wants users to feel the most secure this would be where that would happen, since SHA-256 protects all user sensitive data, without this the users would not be protected at all.* ● *SQL - This application would require the second security out of the rest so high priority. Important data would be stored in a MySQL database so securing SQL would be top priority. If they break through they would be able to access information about the seller and the data during a purchase.*
III. Decompose application	The dataflow diagram shows how a user can search for sneakers on the site by accessing the database. Make sure the database portion of the MySQL portion of it is secured because sensitive information can be accessed from there.
IV. Threat analysis	List **2 types of threats** in the PASTA worksheet that are risks to the information being handled by the application. ● *Internal threats can be customer service employees, who can leak valuable information.* ● *Malicious hacker is an external threat, they can utilize SQL injections since the business utilizes SQL.*

V. Vulnerability analysis	List **2 vulnerabilities** in the PASTA worksheet that could be exploited. ● *Since the database lacks prepared statements, hackers can use SQL injection attacks.* ● *The application communicates with cookies between multiple layers, so session hijacking is possible if the cookies are used incorrectly.*
VI. Attack modeling	Attack tree shows that user data is vulnerable to SQL injections because of lack of prepared statements, and session hijacking because of weak login credentials.
VII. Risk analysis and impact	List **4 security controls** that you've learned about that can reduce risk. ● SHA-256 ● MFA ● HASH ● Least privilege