PASTA worksheet

Stages	Sneaker company
I. Define business and security objectives	The application should : • *Protect buyer and seller information* • *Process transactions efficiently, securely and safely* • *Follow the PCI DSS standards to avoid any potential issues*
II. Define the technical scope	List of technologies used by the application: • *Application programming interface (API)* • *Public key infrastructure (PKI)* • *SHA-256* • *SQL* *APIs facilitate the exchange of data between customers, partners, and employees, so they should be prioritized. They handle a lot of sensitive data while they connect various users and systems together. However, details such as which APIs are being used should be considered before prioritizing one technology over another. So, they can be more prone to security vulnerabilities because there's a larger attack surface.* SHA–256 will be prioritized, due to it being responsible for protecting the data and sensitive information that is available on the website, which includes passwords, credit cards, and addresses.
III. Decompose application	Sample data flow diagram SQL is responsible for providing the search forum, and by giving the information queried only it allows for protection of database information. SHA-256 and PKI protect sensitive information like user name and credit cards. API ensures that the information requested is presented back to the user accurately, and that the database receives the request and processes it correctly.
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 i.e employees which could succumb to social engineering*

	• *External threats which could perform attacks such as SQL injection*
V. Vulnerability analysis	List **2 vulnerabilities** in the PASTA worksheet that could be exploited. • *Form for input of credit card information could be accessed when SQL injection is carried out* • *Failure to encrypt all information in the database could give rise to leaks*
VI. Attack modeling	Sample attack tree diagram Threat actors could use SQL injection to protect the query form and database. They could also attempt brute force attacks for weak login credentials associated with accounts on the application.
VII. Risk analysis and impact	4 security controls to reduce risk: 1. Input sanitization 2. Strong password policy 3. Prepared statements 4. Multi factor authentication