


## PASTA worksheet

Stages	Sneaker company
<b>I. Define business and security objectives</b>	<p>Make <b>2-3 notes</b> of specific business requirements that will be analyzed.</p> <ul style="list-style-type: none"> <li>- According to the business description, The owner wants a seamless connection between sellers and shoppers with robust data privacy mechanisms along with being able to process payment transactions. Taking note of these descriptions involve a lot of server processing. One industry standard for payment process is PCI DSS</li> </ul>
<b>II. Define the technical scope</b>	<p>List of technologies used by the application:</p> <ul style="list-style-type: none"> <li>• Application programming interface (API)</li> <li>• Public key infrastructure (PKI)</li> <li>• SHA-256</li> <li>• SQL</li> <li>- If Data privacy is the concern, we may want to prioritize PKI for encryption of customer data and along with hashing as these technologies will securely guarantee the privacy of customers. Then moving to SQL to third as we won't or atleast in description this mentioned user inputs then last is the API since we are using 3rd party for it.</li> </ul>
<b>III. Decompose application</b>	 <pre> graph LR     User[User] -- "Contacting seller for products" --&gt; Seller((Seller))     Seller -- "Listings of current inventory." --&gt; Database[Database] </pre>
<b>IV. Threat analysis</b>	<p>List <b>2 types of threats</b> in the PASTA worksheet that are risks to the information being handled by the application.</p> <ul style="list-style-type: none"> <li>• What are the internal threats?</li> <li>• What are the external threats?</li> <li>- Internal threats would be a disgruntled employee or employee that might cause unintentional accidents like data leaks, Other factors like physical server might malfunction. External threats like competitors or malicious</li> </ul>

	<i>hackers that might attack our database to steal information</i>
<b>V. Vulnerability analysis</b>	<p>List <b>2 vulnerabilities</b> in the PASTA worksheet that could be exploited.</p> <ul style="list-style-type: none"> <li>• <i>Could there be things wrong with the codebase?</i></li> <li>• <i>Could there be weaknesses in the database?</i></li> <li>• <i>Could there be flaws in the network?</i></li> <li>- <i>We may might to look out for SQLi attacks if user inputs are not sanitize or lack of prepared statements, other would be Hash collisions for SHA256, ensure that the secret key is strong and should be securely stored somewhere safe for PKI</i></li> </ul>
<b>VI. Attack modeling</b>	<pre> graph TD     A[User data] --&gt; B[SQL injection]     A --&gt; C[Session hijacking]     A --&gt; D[Hash Collision]     B --&gt; E[Unsanitized Inputs]     B --&gt; F[Lack of prepared statements]     C --&gt; G[Weak login credentials]     C --&gt; H[XSS]     D --&gt; I[Weak Hash Algo] </pre>
<b>VII. Risk analysis and impact</b>	<p>List <b>4 security controls</b> that you've learned about that can reduce risk.</p> <ul style="list-style-type: none"> <li>- Encryption</li> <li>- Least Privilege</li> <li>- Separation of Duties</li> <li>- And Firewalls</li> </ul>