
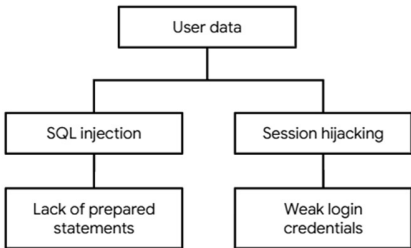


PASTA worksheet

Stages	Sneaker company
I. Define business and security objectives	<p>Make 2-3 notes of specific business requirements that will be analyzed.</p> <ul style="list-style-type: none">● <i>The app will process financial transactions, potentially using many payment options.</i>● <i>Users can create member profiles internally or by connecting external accounts.</i>● <i>The industry regulations that need to be considered are with regard to customer data storage and payment processes, the app should be in compliance with PCI-DSS.</i>
II. Define the technical scope	<p>List of technologies used by the application:</p> <ul style="list-style-type: none">● <i>Application programming interface (API):</i>● <i>Public key infrastructure (PKI)</i>● <i>SHA-256</i>● <i>SQL</i> <p>Write 2-3 sentences (40-60 words) that describe why you choose to prioritize that technology over the others.</p> <p><i>APIs should be prioritized as it facilitates the exchange of data between customers, partners, and employees. They handle a lot of sensitive data while they connect various users and systems together, determining how the software components interact with each other. 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.</i></p>

III. Decompose application	<p style="text-align: center;">Data flow diagram</p> <p>Note: This data flow diagram represents a single process. Data flow diagrams for an application like this are normally much more complex.</p>  <pre> graph LR User[User] -- "Searching for sneakers for sale." --> Process((Product search process)) Process -- "Listings of current inventory." --> Database[Database] </pre>
IV. Threat analysis	<p>List 2 types of threats in the PASTA worksheet that are risks to the information being handled by the application.</p> <ul style="list-style-type: none"> ● <i>Injection</i> ● <i>Session hijacking</i>
V. Vulnerability analysis	<p>List 2 vulnerabilities in the PASTA worksheet that could be exploited.</p> <ul style="list-style-type: none"> ● <i>Lack of prepared statements</i> ● <i>Broken API token</i>
VI. Attack modeling	<p style="text-align: center;">Attack tree diagram</p> <p>Note: Applications like this normally have large, complex attack trees with many branches.</p>  <pre> graph TD A[User data] --> B[SQL injection] A --> C[Session hijacking] B --> D[Lack of prepared statements] C --> E[Weak login credentials] </pre>
VII. Risk analysis and impact	<p>List 4 security controls that you've learned about that can reduce risk.</p> <ul style="list-style-type: none"> -SHA-256 -Incident response procedures -Password policy -Principle of least privilege