


## Process for Attack Simulation & Threat Analysis (PASTA)

Stages	Sneaker Company
<b>I. Define business and security objectives</b>	<p>Specific business requirements:</p> <ul style="list-style-type: none"> <li>• Users can create member profiles internally or by connecting external accounts.</li> <li>• The app must process financial transactions.</li> <li>• The app should be in compliance with 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>• Advanced encryption system (AES)</li> <li>• SHA-256</li> <li>• SQL</li> </ul> <p>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.</p>
<b>III. Decompose application</b>	 <pre> graph LR     User[User] -- "Searching for sneakers for sale" --&gt; Process((Product search process))     Process -- "Listings of current inventory" --&gt; Database[Database]     Database --&gt; Process     Process --&gt; User     </pre>
<b>IV. Threat analysis</b>	<p>2 types of threats that are risks to the information being handled by the application:</p> <ul style="list-style-type: none"> <li>• Injection</li> <li>• Session hijacking</li> </ul>
<b>V. Vulnerability analysis</b>	<p>2 vulnerabilities that could be exploited:</p> <ul style="list-style-type: none"> <li>• Lack of prepared statements in the code</li> </ul>

## Process for Attack Simulation & Threat Analysis (PASTA)

	<ul style="list-style-type: none"><li>• Broken API token</li></ul>
<b>VI. Attack modeling</b>	<pre>graph TD;     A[User data] --- B[ ];     B --- C[SQL injection];     B --- D[Session hijacking];     C --- E[Lack of prepared statements];     D --- F[Weak login credentials];</pre>
<b>VII. Risk analysis and impact</b>	<p>4 security controls that can reduce risk:</p> <ul style="list-style-type: none"><li>• SHA-256</li><li>• Incident response procedures</li><li>• Password policy (MFA)</li><li>• Principle of least privilege</li></ul>