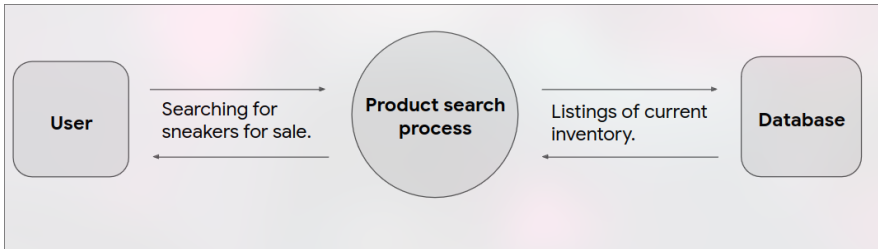
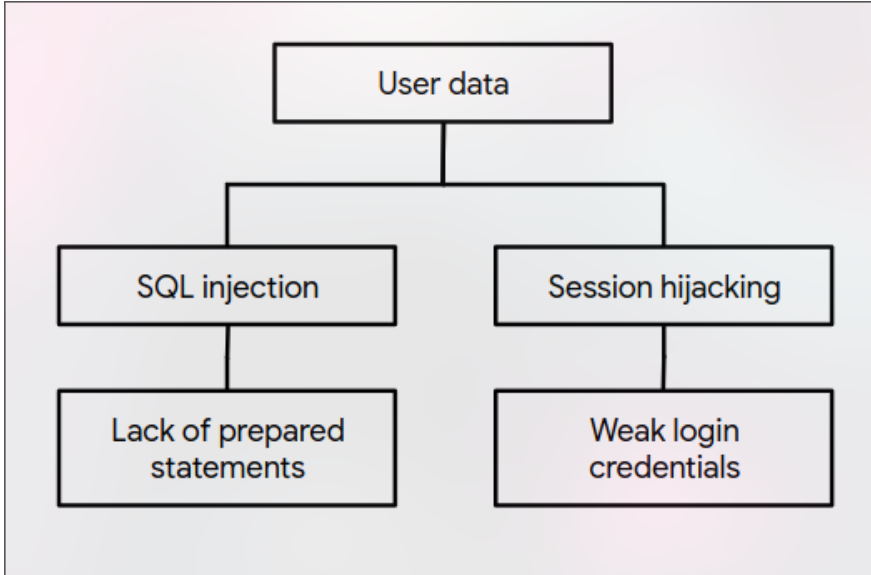


PASTA worksheet

Stages	Sneaker company
I. Define business and security objectives	<ul style="list-style-type: none"> • <i>Will the app process transactions?</i> <i>Yes, since the users can order their pairs from the app.</i> • <i>Does it do a lot of back-end processing?</i> <i>Creating user profiles, adding items to cart, processing transaction etc..</i> • <i>Are there industry regulations that need to be considered?</i> <i>The Privacy Act, 2075, GDPR, 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>APIs are used by the application to interact with other backends that might contain vulnerabilities. Since the API is not under our control, it will have a larger attack surface in our application when compared to others, but the SQL we are using may also be vulnerable to injection attacks, so it should also be thoroughly tested.</p>
III. Decompose application	<p>Sample data flow diagram</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	<ul style="list-style-type: none"> • <i>What are the internal threats?</i> <i>Unaware employees, disgruntled employees, misconfigured elements</i> • <i>What are the external threats?</i> <i>Social engineering, injection attacks, session hijacking</i>

V. Vulnerability analysis	List 2 vulnerabilities in the PASTA worksheet that could be exploited. <ul style="list-style-type: none"> • <i>Vulnerable API</i> • <i>Lack of prepared statements for SQL injection protection</i>
VI. Attack modeling	<p>Sample attack tree diagram</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	List 4 security controls that you've learned about that can reduce risk. <ul style="list-style-type: none"> • <i>Implementing prepared statements</i> • <i>API security checks</i> • <i>Storing usernames and passwords by hashing and salting</i> • <i>Social engineering prevention drills</i>