## PASTA worksheet

| **Stages** | **Sneaker company** |
| --- | --- |
| **I. Define business and security objectives** | *The primary business objective for the product search process is to enable users to quickly and efficiently find shoes listed by sellers. From a security perspective, this process must securely handle search queries and return accurate results to maintain user trust and prevent data manipulation.* |
| **II. Define the technical scope** | *Focusing on API OWASP compliance ensures that the backend reaches a good level of security and data integrity.*  *SQL queries must be meticulously reviewed for unescaped entry data that could return unauthorized data.* |
| **III. Decompose application** | [Sample data flow diagram](https://docs.google.com/presentation/d/1ol7y79popTFfNHM-90ES-H-i1Lpd0YNvPShxBlXozjg/template/preview?resourcekey=0-DZAkf7Vzh2PXsP-j3oXV-g) |
| **IV. Threat analysis** | *A threat actor would try to exploit the user’s search form to extract data, or gain access, to the database through SQL injection. Additionally, a threat actor could attempt session hijacking to take control of a legitimate user's session, potentially leading to unauthorized actions or data access within the application.* |
| **V. Vulnerability analysis** | *Lack of prepared statements*  *Weak session management* |
| **VI. Attack modeling** | [Sample attack tree diagram](https://docs.google.com/presentation/d/1FmWLyHgmq9XQoVuMxOym2PHO8IuedCkan4moYnI-EJ0/template/preview?usp=sharing&resourcekey=0-zYPY7AhPJdcClXamlAfOag) |
| **VII. Risk analysis and impact** | *Prepared statements and Input validation can mitigate SQL Injection attacks while TLS cryptography and session timeout can mitigate session hijacking attacks.* |