

PASTA worksheet

Stages	Sneaker company
I. Define business and security objectives	<p>The app processes a transaction between buyers and sellers. It does a lot of back-end processing where it connects the buyers with the sellers and also allows them to rate the sellers for good service. There are industry regulations that need to be considered as they involve transactions between buyers and sellers.</p>
II. Define the technical scope	<p>List of technologies used by the application:</p> <ul style="list-style-type: none">• Application programming interface (API)• Public key infrastructure (PKI)• SHA-256• SQL <p>Among the list of technologies used by the application, I would like to examine the API because it is informed that third-party APIs may be used to avoid coding from scratch. Since the third-party APIs possess security risks, I would examine them at first then I would examine SQL because it is said that SQL is used to get data while purchasing.</p>
III. Decompose application	<p>The decomposition of application includes one part where user searches for sneakers on sale and the product search process lists the products that are on sale which is pulled from the database upon user requests. It includes others as well but this one is most common.</p> <p>Sample data flow diagram.</p>
IV. Threat analysis	<p>The internal threats includes the data being accessed by SQL because if the command which is used to get the data from the database is sent straight as SQL queries without any encryption then, there is high of an attack could happen. The external threats includes using third-party APIs. As third-party APIs are cannot be trusted all time, they could also possess high risk of a security event.</p>
V. Vulnerability analysis	<p>There could be some wrong with the database because of the use of third-party APIs to avoid coding from scratch. There could be</p>

	also a weakness in the database if the data is not encrypted in it or the SQL query which is used to access data in the database is not encrypted. There could be some flaws in the network if they use weak/incorrect protocols to enable communication.
VI. Attack modeling	Sample attack tree.
VII. Risk analysis and impact	We can implement end-to-end encryption between the user and buyers until the purchase and payment transaction completes. We can also implement encryption in the database, so that the database is kept safe from illegal accessing. We can implement single-sign-on and MFA for authentication purposes. We can also implement secure coding practices while coding the application, which potentially reduces risk of vulnerability to the application.
