Process for Attack Simulation & Threat Analysis Worksheet

Description: Our application should seamlessly connect sellers and shoppers. It should be easy for users to sign-up, log in, and manage their accounts. Data privacy is a big concern for us. We want users to feel confident that we're being responsible with their information.

Buyers should be able to directly message sellers with questions. They should also have the ability to rate sellers to encourage good service. Sales should be clear and quick to process. Users should have several payment options for a smooth checkout process. Proper payment handling is really important because we want to avoid legal issues.

Stages	Sneaker company
I. Define business and security objectives	*This app will handle sign up & logins, allow users to manage their accounts, facilitate communication & connection between buyers + sellers, as well as have the ability to process transactions. Due to the nature of this application's features, characteristics, abilities, and data handling - there is a substantial amount of back-end processing expected. Because financial transactions are expected, adequate data handling is a strong priority for this company. Regulations, policies, guidelines, and handbooks will be created, modified, and maintained in accordance & alignment with NIST-recommended practices such as ensuring proper encryption, routine risk management, IAM principles, incident response, secure data handling, as well as any local & state-level privacy regulations and laws.*
II. Define the technical scope	List of technologies used by the application ranked by priority: • *Application programming interface (API)* ***4*** • *Public key infrastructure (PKI)* ***1*** • *SHA-256* ***2*** • *SQL* ***3*** The technology I would prioritize is the implementation and use of Public Key Infrastructure. By incorporating this technology within the app we can ensure the secure exchange of information between user, app, and database. This encryption framework uses symmetric & asymmetric encryption to secure any data exchanged within the app.
III. Decompose application	Sample data flow diagram
IV. Threat analysis	*Some internal threats could be unreliable workers attempting to get themselves, their family & friends discounts/free shoes by modifying inventory, price, or transaction fields. Or perhaps a disgruntled employee*

	that was laid off but had administrative access to the application, database, or user data. *An external threat could be a malicious actor attempting to steal credit card information that users have input when making a purchase or that may be saved under their profile.*
V. Vulnerability analysis	List **2 vulnerabilities** in the PASTA worksheet that could be exploited. ● *Data not encrypted properly can pose a grave security threat for our databases and information.* ● *Lack of protections against input manipulation can lead to devastating SQL injections.*
VI. Attack modeling	Sample attack tree diagram
VII. Risk analysis and impact	List **3 security controls** that can reduce risk. - Encryption of data in transit while it is being exchanged as well as at rest can help prevent man in the middle attacks. - Input validation prevents manipulation that can lead to SQL injections and potential data loss. - I would also suggest routine IAM audits to ensure the appropriate users have approved access.