## PASTA worksheet

|  |  |
| --- | --- |
| **Stages** | **Sneaker company** |
| **I. Define business and security objectives** | Transaction Processing: The app should efficiently process transactions for buying and selling sneakers.  Back-end Processing: Assess the extent of back-end processing required to ensure smooth operations.  Industry Regulations: Consider any industry-specific regulations that must be adhered to, especially concerning user data and financial transactions. |
| **II. Define the technical scope** | I would prioritize evaluating the "Public Key Infrastructure (PKI)" technology over others because it plays a crucial role in securing the exchange of online information, and the mobile app relies on both AES and RSA encryption algorithms for encrypting sensitive data and exchanging keys. If there are vulnerabilities or misconfigurations in the PKI implementation, it could lead to significant security risks, including data breaches and unauthorized access to sensitive information. |
| **III. Decompose application** | By examining the data flow diagram in detail, security professionals can identify potential security risks and design appropriate security controls to protect user data throughout the process. This analysis helps ensure that sensitive user information is handled securely, minimizing the risk of data breaches and unauthorized access. |
| **IV. Threat analysis** | Internal Threats: Internal threats could include malicious actions by employees or contractors who have access to sensitive data.  External Threats: External threats might involve attacks from cybercriminals, such as phishing, malware, or denial-of-service attacks. |
| **V. Vulnerability analysis** | Codebase Vulnerabilities: The app's codebase might contain vulnerabilities, including input validation issues, authentication flaws, or other coding errors.  Database Weaknesses: Vulnerabilities in the database, such as misconfigured permissions or SQL injection vulnerabilities, could put sensitive data at risk. |
| **VI. Attack modeling** | The complexity of the attack tree emphasizes the need for thorough threat modeling and risk analysis. By understanding the potential attack vectors and associated risks, security professionals can develop and implement appropriate security controls to mitigate these threats and enhance the application's security posture. Additionally, regular updates to the attack tree are necessary to adapt to evolving threats and vulnerabilities. |
| **VII. Risk analysis and impact** | Web Application Firewall (WAF): Implementing a robust WAF can help protect against common web application attacks and provide an additional layer of security.  Penetration Testing and Code Reviews: Regularly conducting penetration testing and code reviews can identify and remediate vulnerabilities in both the application and its codebase.  Strong Encryption Practices: Enforcing strong encryption practices and robust key management for PKI infrastructure can help protect sensitive data.  Employee Training and Awareness: Employee training and awareness programs can mitigate social engineering attacks and improve overall security posture. |