Threat Modeling Practice

Applying the PASTA Threat Model Framework

Wendy Alayon
13/07/2024 **@syszern**

Threat modeling practice

Scenario

The security team at a company specializing in sneakers for enthusiasts and collectors is conducting a threat model of their upcoming mobile app launch, which facilitates buying and selling shoes. They are using the PASTA framework to systematically go through seven stages to identify security requirements for the new app.

PASTA worksheet

Stages	Sneaker company
I. Define business and security objectives	• *Members have the option to create profiles either internally or by linking external accounts.* • *The application is required to handle financial transactions.* • *It should adhere to PCI-DSS compliance standards.*
II. Define the technical scope	List of technologies used by the application: • *API* • *PKI* • *AES* • *SHA-256* • *SQL* APIs facilitate data exchange among customers, partners, and employees, making prioritization essential. APIs manage sensitive data and integrate diverse users and systems. However, prioritizing technologies should consider specific API usage details to address security vulnerabilities, given the extensive attack surface associated with APIs.
III. Decompose	Data flow diagram

application	The sample data flow diagram illustrates the path of a standard search request as it traverses various layers. An area to consider in this context would involve verifying that the MySQL database employs prepared statements for handling input queries.
IV. Threat analysis	**2 types of threats** in the PASTA worksheet that are risks to the information being handled by the application. • *Injection* • *Session hijacking* SQL injection attacks are a common threat to SQL databases. Session hijacking can occur when cookies are transmitted between multiple layers of the application. It is important to assess the technological attack surface and relevant threats to the product to effectively implement information security responsibilities.
V. Vulnerability analysis	**2 vulnerabilities** in the PASTA worksheet that could be exploited. • *Lack of prepared statements* • *Broken API token* The absence of prepared statements can expose SQL database to injection attacks. Mishandling cookies between input and output sources can lead to potential session hijacking.
VI. Attack modeling	Sample attack tree diagram This sample attack tree illustrates the vulnerabilities of user data identified earlier to specific attacks.
VII. Risk analysis and impact	**4 security controls** that can reduce risk: *SHA-256, incident response procedures, password policy, principle of least privilege* SHA-256, incident response protocols, password policies, and the principle of least privilege are examples of technical, operational, and managerial controls that can be implemented pre-launch to mitigate risks.