

## ASSIGNMENT 5.

### JMOJREALI' MORE REUBEN.

1. Incorporating security considerations early in software design.

- Proves to be vital for several reasons. It helps to identify potential security vulnerabilities and threats at an early stage, reducing the cost and complexity of addressing them later. Proactive security design contributes to building resilient and trustworthy software systems.

2. Role of threat modeling in software design.

- Threat modeling is a systematic approach used to identify potential security threats and vulnerabilities, assess their likelihood and potential impact and prioritize mitigations. Techniques such as STRIDE or DREAD help in identifying and categorizing threats at the design stage.

3. Principle of defense in depth in software design.

- The principle of defense in depth involves implementing multiple layers of security controls throughout the software to protect against cyber threats.
- This approach recognizes that no single security measure is foolproof and multiple barriers can provide redundancy and mitigate the impact of a control failure.

4. Challenges of designing secure APIs.

- This is due to the complexity of technologies and the evolving nature of cyber threats. Best practices for designing secure APIs include implementing proper authentication and authorization mechanisms, encrypting data in transit and at rest, validating and sanitizing input data to prevent injection attacks, and designing for rate limiting and throttling to mitigate denial of service attacks.

## 5 Secure by design.

- involves integrating security patterns principles and architectural guidance into the SW design process from the outset. Applying principles such as the principle of least privilege where users are given only the permissions they need to perform their tasks and the principle of least astonishment which advocates for security systems behaving in expected ways.

## 6 Trade-offs between security and usability

- Balancing security and usability is one of the significant challenges in software design. Excessive security measures can negatively impact user experience leading to user frustration and potential circumvention of security controls.
- To create software that is both user user friendly and secure designers must integrate UX design principles with security requirements.
- This involves designing intuitive authentication process providing clear security information to users.

## 7 Importance of Secure Coding practices.

- Secure coding practices are crucial in mitigating common security vulnerabilities such as injection attacks and cross-site scripting.
- Education and empowering developers to write secure code involves providing training on secure coding standards encouraging the use of security awareness. Code reviews static and dynamic analysis tools and security testing can also help identify and rectify security issues early in the development process.