**SAD ASSIGNMENT 1**

1. **What is SDLC and What Are the Phases of SDLC?**

The Software Development Life Cycle (SDLC) is a systematic process used by software developers to design, develop, and test high-quality software. The phases of SDLC include:

* Requirement Gathering and Analysis
* System Design
* Implementation
* Testing
* Deployment
* Maintenance

Each phase is critical to ensure that the final product is efficient, error-free, and meets user requirements. SDLC provides a framework for organizing tasks, improving the development process, promoting collaboration among team members, and reducing risks.

1. **What Are the Key Cybersecurity Threats?**

Key cybersecurity threats include:

**Phishing**: Attackers trick users into providing sensitive information.

**Malware:** Malicious software designed to harm systems or steal data.

**Ransomware:** Malware that locks users out of their system until a ransom is paid.

**Denial-of-Service (DoS) Attacks:** Overwhelm a server to make it unavailable.

**Insider Threats:** Individuals within an organization misuse access.

**Zero-day Vulnerabilities:** Flaws that are exploited before developers can patch them.

1. **What is Meant by Threat Modeling?**

Threat modeling is a structured process used to identify, assess, and prioritize potential security threats to an application or system. It helps developers understand the possible threats early in the design process and how these might affect the system. By performing threat modeling, organizations can better anticipate security issues, allocate resources effectively, and develop stronger defenses against attacks.

1. **Explain SAST Tools in Brief**

Static Application Security Testing (SAST) tools analyze an application's source code or binaries to detect security vulnerabilities. Unlike DAST tools, SAST tools do not require the application to be running, making them useful for identifying issues such as SQL injection, buffer overflows, and cross-site scripting early in the development cycle. These tools help developers fix vulnerabilities before the application goes live, minimizing the risk of security breaches.

1. **What Are OWASP Top 10 Security Risks?**

The OWASP Top 10 is a list of the most critical web application security risks. It includes:

* + Injection
  + Broken Authentication
  + Sensitive Data Exposure
  + XML External Entities (XXE)
  + Broken Access Control
  + Security Misconfiguration
  + Cross-Site Scripting (XSS)
  + Insecure Deserialization
  + Using Components with Known Vulnerabilities
  + Insufficient Logging and Monitoring
  + This list provides guidance on the most prevalent security threats faced by developers.

1. **What Are the Essential Laws of Cybersecurity?**

Essential cybersecurity laws include:

1. The Computer Fraud and Abuse Act (CFAA): Criminalizes unauthorized access to computer systems.
2. The General Data Protection Regulation (GDPR): Governs data privacy and security in the European Union.
3. The Health Insurance Portability and Accountability Act (HIPAA): Protects sensitive health information.
4. The Cybersecurity Information Sharing Act (CISA): Encourages information sharing between government and businesses.
5. The California Consumer Privacy Act (CCPA): Strengthens privacy rights for California residents.