Foundation of Code Security

Curriculum 4 Days

Day - 1

- **Introduction of Security**
  - Introduction of Agile
  - Introduction of DevOps
  - Introduction of DevSecOps
  - Overview of Security fundamentals
  - Common security threats
  - Attack vectors
  - Potential security impact on applications

Day - 2

- **OWASP Top 10**
  Training Objective: To familiarise developers with most critical risks to the security applications and avoid the risks at the development stage itself.
  - Introduction
  - Broken Access Control
  - Cryptographic Failures
  - Injection
  - Insecure Design
  - Security Misconfiguration
  - Vulnerable and Outdated Components
  - Identification and Authentication Failures
  - Software and Data Integrity Failures
  - Security Logging and Monitoring Failures
  - Server-Side Request Forgery (SSRF)

Day - 3

- **DevOps Specific security topics**

  Objective: To familiarise developers with security best practices specific to Devops

  - Infrastructure as Code (IaC) Security
  - Container Security
  - Continuous Integration/Continuous Deployment (CI/CD) Security
  - Secrets Management (API Keys storage and management)
  - Security Testing Automation (Vulnerability assessments, SAST/DAST)
  - Secure configuration management
  - Authentication and Authorization
  - Monitoring and Logging
  - Patch Management - during maintenance phase
  - Third-Party Code and Integrations - Software bill of material, supply chain security etc.

- **Mobile Application Security**

  Training Objective: To familiarise developers with most critical risks to the security of the mobile applications and avoid the risks at the development stage itself.

  - Insecure Data Storage
  - Unintended data Leakage
  - Broken Cryptography
  - Client-Side Injection
  - Reverse Engineering

Day - 4

- **Common vulnerabilities in the programming languages**

  Training Objective: To familiarise developers with the common vulnerabilities of the programming languages used for development. Customise according to the languages, frameworks and libraries used for development.

  Other secure application design concepts:
  - Security by Design Principles
  - Threat Modelling
  - Data Encryption and Protection
  - Least Privilege
  - Insecure Direct Object References
  - Error Handling
  - Secure File and Resource Handling
  - Session Management
  - Compliance and Regulation (GDPR - Privacy by design principles for data protection)