**Secure Development**

**Course 7564 – 40 Hours**



The Course will present security Guidelines, consideration and techniques for developing secure application, alongside explanations and demonstration of application specific attacks.   
Participant will learn and understand the different application security threats, and the right technique for mitigating each possible threat.

The course is not focused on a specific development or deployment environment, and all principles and concept demonstrated throughout the course are relevant to all applications.

The training includes demonstrations of web security threats using simulated web application and allows understanding of the problems through live demonstration and exercises.



* Developers and team leaders who wish to improve their security skills and awareness.
* System architects wishing to be able to assist the developers in creating a secure application
* Application Security personnel who wish to be able to guide developers and recommend the right way of dealing with application security flaws discovered in the organization.



* Experience in developing Web Applications using modern programming languages
* Recommended: Familiarity with the HTTP protocol
* Recommended: Familiarity with HTML
* Recommended: Familiarity with the SQL Language



**Introduction to Information Security**

* Information Security Principles
* Governance, Risk Management and Compliance
* Protecting and Defending Assets
* Security Management Plans
* Managing Incidents and Operations

**Principles of Secure Development**

* Security by Design
* Identity and Access Control
* Secrets Management
* Error Handling
* Logging and Monitoring
* System Configuration
* Cryptographic Practices
* Input Validation and Output Encoding
* Threat Modeling

**Security Design Principles**

* Defense-in-Depth
* Fail Safe
* Least Privilege
* Separation of Duties
* Economy of Mechanism
* Complete Mediation
* Open Design
* Least Common Mechanism
* Psychological acceptability
* Weakest Link
* Leveraging Existing Components

**Input Validation and Output Sanitization**

* Input Validation Goals
* Input Validation Strategies
* Implementing Input Validation
* Output Sanitization

**Errors and Exceptions Handling**

* Expectation Handling Overview
* Error Messages and Status Codes
* Global Error Handling

**Logging and Monitoring**

* Application Logs Overview
* What should and should not be logged
* Monitoring and Alerts

**Cryptography Fundamentals**

* Cryptography Basic Concepts
* Symmetric Key Cryptography
* Asymmetric Key Cryptography
* Hashing Functions
* Public Key Infrastructure (PKI)
* Digital Signatures and Certificates

**Protect Data in Transit**

* Transport Security Overview
* SSL vs TLS
* The TLS Handshake
* Certificates
* SSL Offloading and SSL Termination
* HTTP Strict Transport Security (HSTS)

**Protect Data at Rest**

* Database Security Overview
* Database Connection
* Managing Logins
* Storing Sensitive Data
* Database Configuration and Hardening

**Secrets Management**

* Understanding Application Secrets
* Safely Store Secrets in Development
* Protecting Production Secrets

**Identity and Access Management**

* What is Identity and Access Management (IAM)
* Authentication
* Authorization
* OAuth 2.0
* OpenID Connect (OIDC)
* JSON Web Token (JWT)
* JSON Object Signing and Encryption (JOSE)
* Bearer Tokens

**Introduction to Threat Modeling**

* What is Threat Modeling
* Threat Modeling Approaches
* Threat Modeling Methodologies
* Improve Application Security with Threat Modeling

**OWASP Top 10 Application Security Risks and Mitigations**

* Injection
* Broken Authentication
* Sensitive Data Exposure
* XML External Entity (XXE) Vulnerabilities
* Broken Access Control
* Security Misconfiguration
* Cross Site Scripting (XSS)
* Insecure Deserialization
* Using Components with Known Vulnerabilities
* Insufficient Logging and Monitoring

**Using Security Analysis Tools**

* Applying Static Code Analysis (SCA)
* Detecting Vulnerable Libraries
* Adding SCA and Vulnerable Library Detection to Build Pipelines

**Secure Application Development Processes**

* Security and Agile
* Secure DevOps (DevSecOps)
* Systems Development Life-Cycle (SDLC)
* Secure SDLC