

SECURE CODING

Presentazione del corso

Il percorso di formazione ha il compito di formare tecnici che siano capaci sia di esaminare approfonditamente la sicurezza di un sistema che di proteggerlo contro minacce esterne.

Destinatari

Sviluppatori

Gli obiettivi

Al termine del corso i partecipanti saranno in grado di:

- Comprendere i concetti base di sicurezza IT
- Individuare le conseguenze della mancata protezione
- Capire le tecniche di protezione architetturale e le loro debolezze
- Scoprire gli errori di codifica e saperli evitare
- Ottenere fonti e ulteriori letture sulle pratiche di codifica sicura

Contenuti

Introduzione alla scrittura di codice sicuro

- Robustezza, Performance e Sicurezza del Software
- Cause delle vulnerabilità
- Costi dei Bugs di sicurezza
- Tipologie di vulnerabilità
- Ciclo di scrittura codice sicuro
- Sicurezza Architetturale e By-Design
- Tipologie di sicurezza
- Sicurezza per le applicazioni Web
- Sicurezza per le applicazioni Desktop
- Sicurezza per le applicazioni Mobile
- Validazione Input utente
- Buffer Overflow
- Cross-Site Scripting • SQL-Injection
- Canonicalizzazione
- Autenticazione
- Men in the middle
- Attacchi di Brute-Force
- Attacchi di dizionario
- Vulnerabilità dei Cookies
- Autorizzazione
- Implementazione dei ruoli
- Data disclosure
- Aumento dei privilegi
- Web Security
- Gestione delle query string
- Dati relativi ai form
- Gestione dei Cookies

- Gestione degli Header http
- Uso di HTTPS
- Web Service Security
- Gestione degli Header SOAP
- Passaggio di dati sensibili
- Invocazione dei servizi per ruolo
- Denial Of Service
- Sicurezza dell'oggetto Session
- Sicurezza dei REST Service
- AJAX security
- Crittografia
- Crittografia Simmetrica e Asimmetrica
- Gestione dell'Hash
- Generazione (debole) delle chiavi
- Crittografia Custom
- Framework Security
- Code Acces Security in .NET
- Implementazione della sicurezza nella JVM
- Crittografia in .NET e le JCA in JAVA
- Secure Communication Platform
- Gestione Assembly firmati in .NET
- JAVA e .NET Code Permissions
- Mobile Security (Android, iOS , Windows Phone)
- Attacchi, Virus e vulnerabilità dei dispositivi
- Autenticazione e Autorizzazione sui dispositivi
- Criptazione dei dati in locale
- Sandboxing delle applicazioni
- Autorizzazioni dell'applicazione

Durata

2 giornate

Metodologia didattica utilizzata

Il corso si costituirà di momenti d'aula interattivi con esplicazione di esempi e casistiche.