

# Introduzione allo sviluppo sicuro delle applicazioni

Approfondimento

Interaziendale

## Presentazione

Il problema della sicurezza del software è probabilmente la più importante sfida del nostro tempo nel campo dell'information security. Lo sviluppo di un applicativo di qualità comporta un buon progetto e pratiche di ingegnerizzazione del software. La pressione per ridurre il time-to-market dell'applicazione rende nella maggior parte dei casi la sicurezza un item a bassa priorità rispetto ad altri fattori. Purtroppo l'esperienza dimostra che la sicurezza non è un add-on che possa essere integrato facilmente a un software già sviluppato.

Il concetto di security-by-design consente di focalizzare l'attenzione verso le problematiche di sicurezza in ogni fase del ciclo di vita del software.

Il corso si propone di approfondire le più comuni vulnerabilità e gli attacchi alle applicazioni con esempi di casi reali e di fornire le linee guida di design architetturale e i principi di sicurezza per implementare un ciclo di vita del software in maniera sicura.

## Obiettivi

Il partecipante sarà in grado di:

- ◆ identificare le basi di implementazione di un processo di sviluppo sicuro del software all'interno della propria organizzazione;
- ◆ applicare i concetti chiave dell'application security: rischi, minacce e strategie di difesa;
- ◆ riconoscere vantaggi e svantaggi di modalità differenti per approcciare il problema della verifica del software: secure code review e penetration test applicativo, tools automatici e attività manuali.

## Target di riferimento

IT manager, security manager, security officer, auditor, responsabili dei team di sviluppo software, sviluppatori.

## Prerequisiti

Conoscenza delle linee guida OWASP.

## Metodologia didattica

ESPOSIZIONE DEL DOCENTE		60%
ATTIVAZIONE INDIVIDUALE		20%
STUDIO DI CASI		20%

## Durata

2 giorni

## Prezzo

€ 1.300,00 + IVA

# Introduzione allo sviluppo sicuro delle applicazioni

Interaziendale | 2 giorni

## Giorno 1

### Il cambiamento organizzativo dei sistemi complessi

- ◆ Introduzione alla Web application security
- ◆ Cos'è la Web application security
- ◆ Quali sono i rischi a cui è esposto un servizio web
- ◆ Quale modello di sicurezza è adottato oggi

### Le minacce e gli impatti

- ◆ Vulnerabilità delle applicazioni web: esempi e casi reali
- ◆ Valutazione degli impatti
- ◆ La OWASP top 10 vulnerabilities
- ◆ Esempi e casi reali

### Le strategie di difesa

- ◆ Il ciclo di vita di sviluppo del software
- ◆ Quali processi implementare per sviluppare un software più sicuro
- ◆ Linee guida, strumenti e metodologie per lo sviluppo sicuro

## Giorno 2

### Introduzione alla verifica di sicurezza delle applicazioni web

- ◆ Cos'è un Web Application Penetration Testing (WAPT)
- ◆ La metodologia OWASP per il WAPT
- ◆ WAPT, code review e training
- ◆ Strumenti open source e commerciali

### Come eseguire un'analisi di sicurezza di un applicativo web

- ◆ Metodologia e strumenti per l'analisi
- ◆ Studio di casi applicativi web vulnerabili: quali soluzioni per la messa in sicurezza

### Come sviluppare applicazioni web sicure: linee guida ed esempi

- ◆ Le linee guida OWASP per lo sviluppo sicuro
- ◆ Esempi e studio di casi
- ◆ Implementazione dei controlli di sicurezza