



Secure Coding

Il corso tratta i concetti generali del secure coding che possono essere adatti per vari linguaggi; i laboratori pratici dimostrativi sono svolti in ASP.NET con C#.

Informatica



Obiettivi

Il corso è indicato per programmatori, project manager o software architect e fornisce indicazioni sulle basi metodologiche, gli standard (ad esempio Owasp) e gli strumenti per sviluppare codice sicuro, evitando di inserire nei programmi bugs o vulnerabilità. Vengono svolti svariati laboratori pratici in linguaggio C# a supporto della trattazione teorica, che mostrano l'uso degli strumenti e la mitigazione di alcune delle vulnerabilità che più frequentemente si riscontrano nelle applicazioni web o desktop

Argomenti

Introduzione alla scrittura di codice sicuro

- Introduzione
- Statistiche sugli scenari di attacco nel mondo IT

Metodologie per lo sviluppo di codice sicuro

- Ciclo di vita dello sviluppo di software
- Analisi dei rischi
- Threat Modeling
- La Community OWASP
- Linee guida per il Secure Coding
- SAST (Static Application Security Testing) tools pag. 2

DURATA TOTALE:
16 ore

**NUMERO
PARTECIPANTI:**
8

CALENDARIO:
dal: 07/05/2025
al : 29/05/2025

**TERMINE
ISCRIZIONI:**
28/04/2025

**MODALITÀ DI
SVOLGIMENTO:**
WEBINAR

**REFERENTE DEL
CORSO:**
Dino Scartozzi
dino.scartozzi@formart.it
338 / 1066274

**QUOTA DI
PARTECIPAZIONE:**
290.00 € + IVA

Il corso sarà realizzato solo al raggiungimento del numero minimo di iscritti. Le date potrebbero subire variazioni.



Confartigianato

FORMart sede di BOLOGNA, Bologna, Via Ronco, 3 - Castel Maggiore (BO)

T. 051-7094911 - info.bologna@formart.it - www.formart.it



Cercaci su



VAPT (Vulnerability Assessment e Penetration Test) di applicazioni

- Introduzione al protocollo HTTP
- OWASP Penetration Testing Guide
- Tools di ausilio per attività di VAPT

La Validazione dell'Input

- Linee guida di Secure Coding per la validazione dell'Input
- Vulnerabilità da Injection
- SQL-Injection, Cross-Site Scripting, LFI/RFI, etc
- Laboratori pratici con applicazioni sviluppate in .NET

L'Autenticazione delle applicazioni

- Meccanismi di autenticazione
- Linee guida per autenticazione e gestione password
- Attacchi all'autenticazione: attacchi brute force e Man-in-the-middle

Sicurezza nella gestione delle sessioni

- Introduzione alla gestione delle sessioni nelle applicazioni web
- Linee guida per la gestione sicura delle sessioni
- Attacchi di tipo XSRF (Cross-site Request Forgery)

Linee guida di Secure Coding per la crittografia

- Introduzione alla crittografia e linee guida per l'uso della crittografia
- Algoritmi di Hashing
- Crittografia Simmetrica e Asimmetrica
- Crittografia Custom

Destinatari



 Confartigianato

FORMart sede di BOLOGNA, Bologna, Via Ronco, 3 - Castel Maggiore (BO)

T. 051-7094911 - info.bologna@formart.it - www.formart.it



Cercaci su



Sviluppatori, Analisti programmatori, Progettisti di Software, IT Managers.

**Dotazioni
richieste per lo
svolgimento dei
laboratori**

Visual Studio Community Edition 2019 con installazione dei template per lo sviluppo di applicazioni desktop ed applicazioni web.

Calendario

Il corso si terrà in modalità webinar nelle seguenti date:

5/05/2025 dalle 9,00-13,00 e dalle 14,00-18,00

6/05/2025 dalle 9,00-13,00 e dalle 14,00-18,00

Docenti

Gianluca Golinelli

Ingegnere elettronico, dal 2001 si occupa di sicurezza informatica per aziende ed enti, per cui svolge attività di formazione e consulenza. Svolge inoltre attività di informatica forense in qualità di Consulente Tecnico di Parte e Consulente Tecnico d'Ufficio. Certificato CEH, CHFI, CompTiA Security+, Case.NET, ISACA CSX-P.

Requisiti

Buona conoscenza di linguaggi di programmazione a oggetti.



FORMart sede di BOLOGNA, Bologna, Via Ronco, 3 - Castel Maggiore (BO)

T. 051-7094911 - info.bologna@formart.it - www.formart.it



Cercaci su

