

# Secure Coding per Sviluppatori

## CODICE

CSSCD

## DURATA

2 Giorni

## PREZZO

900,00€ (iva escl.)

## LINGUA

Italiano

## MODALITÀ

Virtual Classroom  
Corso in aula

## SCHEDULAZIONE

- A Richiesta

Il corso ha come obiettivo lo sviluppo di applicazioni sicure che utilizzino la tecnologia Microsoft ASP.NET o Java e il framework Spring.

Partendo dal concetto di Information Security e di Web Application Security, il corso descriverà i rischi di sicurezza più comuni per le applicazioni web (OWASP Top 10) fornendo, per ogni problematica, una mappa dettagliata ed esaustiva degli aspetti teorici e delle tipiche implementazioni vulnerabili.

Il metodo sicuro e corretto di scrittura è quindi spiegato in modo estensivo.

I partecipanti al corso impareranno come scrivere un codice sicuro per sviluppare applicazioni solide e sicure.

Sulla base delle esigenze del cliente, Secure Network adatterà il corso indirizzando gli stessi argomenti per le diverse tecnologie e framework.

## OBIETTIVI

Il corso ha come obiettivo lo sviluppo di applicazioni sicure che utilizzino la tecnologia Microsoft ASP.NET o Java e il framework Spring.

Partendo dal concetto di Information Security e di Web Application Security, il corso descriverà i rischi di sicurezza più comuni per le applicazioni web (OWASP Top 10) fornendo, per ogni problematica, una mappa dettagliata ed esaustiva degli aspetti teorici e delle tipiche implementazioni vulnerabili.

Il metodo sicuro e corretto di scrittura è quindi spiegato in modo estensivo. I partecipanti al corso impareranno come scrivere un codice sicuro per sviluppare applicazioni solide e sicure.

Sulla base delle esigenze del cliente, NovaNext adatterà il corso indirizzando gli stessi argomenti per le diverse tecnologie e framework.

## DESTINATARI

Sviluppatori, Consulenti di Sicurezza Junior.

## CONTENUTI

**Versioni disponibili:**

- Microsoft ASP.NET
- Java Spring



**Agenda Sintetica del corso:**

- Principi dell'Information Security
- Introduzione alla Web Application Security
- OWASP Top 10 Web Application Security Risks
  - A1 – Injection
  - A2 – Broken Authentication
  - A3 – Sensitive Data Exposure
  - A4 – XML External Entities (XXE)
  - A5 – Broken Access Control
  - A6 – Security Misconfiguration
  - A7 – Cross-Site Scripting (XSS)
  - A8 – Insecure Deserialization
  - A9 – Using Components with Known Vulnerabilities
  - A10 – Insufficient Logging & Monitoring
- Input Data Validation Theory

*Prezzi e corsi potrebbero subire variazioni; si consiglia di verificare sul sito [www.novanext.it/training](http://www.novanext.it/training).*