

**INNOVAFORMAZIONE**  
Tecnologia e Formazione



Corso erogato solo su richiesta, preventivo personalizzato. Calendario da concordare. Modalità online classe virtuale o frontale in sede.

rogramma Corso OWASP Sicurezza nello Sviluppo delle Applicazioni Web

Requisiti degli studenti: consigliate basi di programmazione e sviluppo applicazioni front-end e/o backend

Obiettivi del corso: fornire allo studente indicazioni, suggerimenti teorici e pratici, tecniche e risorse per simulare i rischi di vulnerabilità e per implementare software 'più sicuri' tramite le linee guida di OWASP

Programma (32 ore) :

## OWASP Top 10

1. Introduzione
2. Risk management
3. PCI Security Council & OWASP
4. Classificazione delle vulnerabilità e rischi con esempi di casi reali di attacchi e vulnerabilità riscontrate

fino ad oggi

fino ad oggi		
		
2. Sicurezza e Sicurezza nello Sviluppo Web Application		
1. General Painted		
2. Sink and Sinks		
3. Funzioni di Validazione		

Injection

- 1 Interpret
- 2 OS Commanding
- 3 SQL Injection
- 4 Login Bypass



Corso OWASP Sicurezza  
Web App per aziende  
<https://www.annunci.it/x-35907-z>



Corso OWASP Sicurezza  
Web App per aziende  
<https://www.annunci.it/x-35907-z>



Corso OWASP Sicurezza  
Web App per aziende  
<https://www.annunci.it/x-35907-z>



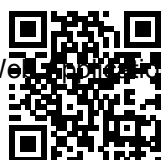
Corso OWASP Sicurezza  
Web App per aziende



Injection  
1 Interpreti  
2 OS Com  
3 SQL Inje  
4 Login By



Corso OWASP Sicurezza  
Web App per aziende  
<https://www.annunci.it/x-35907-z>



Corso OWASP Sicurezza  
Web App per aziende  
<https://www.annunci.it/x-35907-z>



<https://www.annunci.it/x-35907-z>



Web App per aziende

<https://www.annunci.it/x-35907-z>



Web App per aziende

<https://www.annunci.it/x-35907-z>

- 
5. Blind SQL Injection
  6. SQL Injection Countermeasures
  7. LDAP Injection
  8. XPath / JSON Injection

#### Cross-site Scripting (XSS)

1. Reflessivo e persistente
2. Tecniche Avanzate di Cross Site Scripting

#### Broken Authentication & Session Management

1. Cookies
2. Attacking Session
3. Session Fixation
4. Session Prediction

#### Insecure direct object reference

1. Controllo Autorizzazioni negli Oggetti
2. Path Traversal
3. Null byte

#### Cross-site Request Forgery (XSRF)

#### Security Misconfiguration

1. Backup files
2. Local databases
3. Cmapr Hidden HTML
4. Directory Enumeration
5. Directory Indexing

#### Insecure Cryptographic Storage

1. Cenni teorici sulla crittografia e tipi di algoritmi esistenti

#### Errore di Limitazione di Accesso URL

#### Insufficient Transport Layer Protection

1. Digital Certificates
2. HTTPS Protocol
3. Introduzione alla prevenzione attacchi di tipo DDos

#### Unvalidated Redirects and Forwards

---

Vulnerabilità e rischi nell'ambito mobile (Android/iOS)

Caso di studio con simulazione delle vulnerabilità ed esempi di implementazioni più sicure

Corso attivabile on demand e su richiesta, eventualmente individuale.

INFO: tel. 347 75