

# OSCS-6 - SICUREZZA DELLE APPLICAZIONI WEB

Categoria: **Cyber Security**

## INFORMAZIONI SUL CORSO



**Durata:**  
5 Giorni



**Categoria:**  
Cyber Security



**Qualifica Istruttore:**  
Docente Senior (min.  
5 anni)



**Dedicato a:**  
Sviluppatore



**Produttore:**  
PCSNET

## OBIETTIVI

Al termine del corso i partecipanti saranno in grado di comprendere e distinguere le vulnerabilità del codice e le criticità logiche connesse allo sviluppo delle Applicazioni Web.

Gli sviluppatori acquisiranno le basi per sviluppare in modo sicuro.

Il personale coinvolto nel ciclo di sviluppo del software sarà in grado di interagire correttamente con gli sviluppatori per correggere le vulnerabilità individuate e/o per richiedere l'implementazione sicura sin dalla fase di progettazione.

L'obiettivo del corso consiste nel fornire ai partecipanti le conoscenze necessarie alla comprensione delle problematiche legate alla realizzazione di Applicazioni Web sicure. Inoltre il corso fornirà gli strumenti per riconoscere le vulnerabilità comunemente sfruttate da un agente di minaccia per ottenere un accesso illecito alle risorse ed ai sistemi che erogano le Applicazioni Web.

Il percorso formativo prende spunto dai progetti internazionali legati alla sicurezza dell'ambiente delle Applicazioni Web OWASP (Open Web Application Security Project - [www.owasp.org](http://www.owasp.org)) e WASC (Web Application Security Consortium - [www.webappsec.org](http://www.webappsec.org)), e dal progetto CWE (Common Weakness Enumeration - [cwe.mitre.org](http://cwe.mitre.org)) per la classificazione e descrizione delle vulnerabilità applicative non legate a particolari infrastrutture o linguaggi.

Illustrando e simulando le metodologie di attacco si intende sensibilizzare i partecipanti istruendoli sulle tecniche da applicare al fine di mitigare i rischi connessi alla realizzazione di una Applicazione Web.

## PREREQUISITI

Per gli sviluppatori: conoscenza base di htm, di uno fra i principali linguaggi di programmazione web (ASP, PHP, Java, ...) e di uno fra i principali web server (Microsoft IIS, Apache, JBoss, ...).

Per tutte le altre figure professionali: conoscenza base sul design, l'analisi, lo sviluppo e le altre fasi di vita di una Applicazione Web.

## CONTENUTI

**Applicazioni Web: architetture, strutture ed evoluzione**

**Minacce ed attacchi alle Applicazioni Web: obiettivi di un attacco, differenza fra attacchi e vulnerabilità, falsi miti**

**Application Security: confidentiality, integrity, availability, traceability, privacy, compliance, reputation**

**Attacchi ai client**

Progetti sulla sicurezza delle Applicazioni Web: OWASP, WASC, CWE/SANS, SAFECode.org

**Attacchi, problematiche e vulnerabilità delle Applicazioni Web**

Trovare le vulnerabilità attraverso la OWASP Testing Guide e correggere ed evitare le problematiche attraverso la OWASP Development Guide

**Assessment e secure coding (sessioni teoriche ed esercitazioni)**

Injection

Cross site scripting

Autenticazione, autorizzazione e gestione delle sessioni

Insecure direct object reference

Cross site request forgery

Problemi di configurazione

Memorizzazione delle informazioni criptate

Restrizione di accesso alle URL

Protezione insufficiente del layer di trasporto

Redirect e forwards

**Secure SDLC**

**Web Application Security Tools**

## INFO

**Manuale:** Materiale didattico e relativo prezzo da concordare

**Prezzo manuale:** NON incluso nel prezzo del corso

**Natura del corso:** Operativo (previsti lab su PC)