

# OSCS-6 - SICUREZZA DELLE APPLICAZIONI WEB

Categoria: **Cyber Security**

## INFORMAZIONI SUL CORSO



**Durata:**  
4 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.

L'obiettivo 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 e ai sistemi che erogano le Applicazioni Web.

## PREREQUISITI

- Conoscenza di HTML, CSS, JavaScript, di uno fra i principali linguaggi di programmazione web (ASP.NET, PHP, Java, ...) e di uno fra i principali web server (Microsoft IIS, Apache, JBoss, ...).
- Conoscenza base sul design, l'analisi, lo sviluppo e le altre fasi di vita di una Applicazione Web.

## CONTENUTI

### Minacce e Attacchi alle Applicazioni Web

- Introduzione ai concetti fondamentali della sicurezza
- Le architetture di riferimento
- Evoluzione delle applicazioni nel tempo
- Obiettivi di un attacco
- Differenza fra attacchi e vulnerabilità
- Falsi miti

### Breve ripasso di HTML, CSS e JavaScript

- Introduzione
- Struttura di un documento HTML
- CSS
- JavaScript

### Principi della Security

- Least Privilege
- Adopt Industry Supported Standards

- Fail Securely
- Secure Defaults
- Separation of Duties
- Reduce Your Attack Surface
- Defense in Depth
- Reduce Complexity
- Audit Sensitive Events

### **Protocollo http**

- Introduzione
- Stateless
- Request
- Header http
- Response
- https
- http2

### **Same Origin Policy**

- Introduzione SOP
- CORS
- Chiamate su domini
- Finestre correlate cross origine
- JSON
- XSHM

### **Sicurezza e Cookie**

- Introduzione
- Cookie di sessione e permanenti
- Tecniche Cookieless
- Sessioni Stateless
- Cookie di terze parti

### **Session Riding**

- CSRF
- XS-Leaks
- XSSI

### **Cross Site Scripting**

- Introduzione
- XSS Reflected
- XSS Stored
- Attacchi e mitigazioni
- Sanitizzazioni
- Approccio Architetturale
- Content Security Policy

### **Altri tipi di Code Injection**

- SQL Injection
- Prototype Pollution

- HTML Injection
- CSS Injection

#### **Attacchi diversi**

- Clickjacking
- SRI
- Attacco DOS
- txt
- Directory Browsing
- Referral Spam

#### **Login**

- Brute Force
- Biometria
- Phishing
- Web Authentication

#### **Sicurezza delle API**

- Introduzione
- OAuth 2
- JWT
- Insicurezza delle API

## **INFO**

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

**Costo materiale didattico:** NON incluso nel prezzo del corso

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