mediaservice.net
CORPORATE SECURITY & IMAGE

Sicurezza delle Applicazioni Web

Executive Summary

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) e **WASC** (Web Application Security Consortium - www.webappsec.org), e dal progetto **CWE** (Common Weakness Enumeration - cwe.mitre.org) per la classificazione e descrizione delle vulnerabilità applicative non legate a particolari infrastrutture o linguaggi.

Illustrando 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. Le metodologie e le tecniche illustrate sono volontariamente generiche e non specifiche per una singola piattaforma o linguaggio di programmazione.

Audience

Il corso è rivolto agli sviluppatori e agli analisti che si occupano di realizzare e gestire le applicazioni web.

Il corso è altresì indicato per tutte le figure coinvolte nel ciclo di sviluppo del software, quali ad esempio i responsabili dei gruppi preposti allo sviluppo, i Security Officer o il personale che si occupa di sicurezza dell'infrastruttura di rete

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.

OWASP

Open Web Application Security Project

E' una comunità internazionale di ricerca senza scopo di lucro, fondata nel 2001 al fine di aumentare la robustezza del software applicativo, promuovendo lo sviluppo ed il mantenimento di Applicazioni Web sicure.

E' impegnata su diverse linee, dalla definizione dei criteri di progettazione ed analisi del software, alla creazione di tool per il vulnerability assessment e l'analisi del codice.

www.owasp.org

WASC

Web Application Security Consortium

E' una comunità internazionale di ricerca, senza scopo di lucro, che produce una serie di best-practice security standards open source per lo sviluppo ed il mantenimento di Applicazioni Web sicure.

www.webappsec.org

CWE

Common Weakness Enumeration

E' un progetto pubblico creato da una comunità internazionale che produce una classificazione di tutte le vulnerabilità e le debolezzoe note del software.

cwe.mitre.org

Capacità e Competenze Acquisite

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.

Programma (3 Giorni)

Il corso si articola su 3 giorni. Vengono adottati entrambi gli approcci: quello tradizionale, nel quale i discenti si focalizzano sulle principali tecniche di difesa e di sviluppo di codice sicuro, quello "out of the box", nel quale i discenti impersonano un agente di minaccia. Al fine di ottenere i migliori risultati, sarà predisposto un apposito test-lab dove saranno simulate le principali vulnerabilità illustrate durante il corso e tramite il quale gli studenti potranno interagire sotto la guida del docente.
I contenuti sono divisi in 9 moduli qui di seguito schematizzati:

- **Le Applicazioni Web**, architetture, strutture e evoluzione.
- **Minacce, attacchi e attaccanti sulle Applicazioni Web**, obiettivi di un attacco, differenza fra attacchi e vulnerabilità, falsi miti.
- **Application Security** (confidentiality, integrity, availability, traceability, privacy, compliance, reputation)
- **Progetti sulla sicurezza delle Applicazioni Web** (OWASP, WASC, CWE/SANS, SAFECode.org)
- **Attacchi, problematiche e vulnerabilità sulle Applicazioni Web**, trovare le vulnerabilità attraverso la OWASP Testing Guide Correggere e evitatare le problematiche attraverso la OWASP Development Guide
- **Linee guida e principi del Security Design.**
- **Introduzione al Secure SDLC.**
- **Attacchi ai client.**
- **Web Application Security Tools**, installazione e utilizzo di alcuni tool fondamentali per la sicurezza delle Applicazioni Web.

Riferimenti e Partnership

@ Mediaservice.net, grazie alla sua decennale esperienza nel campo della sicurezza, può supportare in modo unico l'esecuzione di ogni progetto, basandosi su metodologie e standard internazionali riconosciuti, quali:

- PCI - DSS (QSA e ASV)
- ISO/IEC 27001
- OSSTMM
- OWASP
- ITIL
- COBIT

@ Mediaservice.net può vantare inoltre conoscenze acquisite attraverso partnership strategiche con le principali associazioni professionali e con i centri di competenza nazionali e internazionali.

Costi

Prezzo di listino	1.950 € + iva per partecipante
Sconti	5% se si effettua il pagamento almeno 10 giorni prima della scadenza delle iscrizioni
	10% Soci Clusit, Forze dell' ordine e Studenti Universitari

Compreso nel prezzo:

- aula attrezzata e materiale didattico del corso in formato digitale
- server di laboratorio virtualizzati sul client del docente
- un pasto e due coffee break al giorno
- attestato di frequenza

mediaservice.net
CORPORATE SECURITY & IMAGE

@ Mediaservice.net S.r.l. con Socio Unico
Via Santorelli, 15 - 10095 Grugliasco (TO)
Tel +39 011-3272100 - Fax +39 011-3246497
info@mediaservice.net - **www.mediaservice.net**