Sicurezza delle web application
200 ore

Descrizione del profilo in uscita:
il profilo in uscita dal corso “Sicurezza delle web application” saprà scrivere codice pulito, in modo che i rilasci software siano sicuri dal punto di vista della sicurezza.
Verranno analizzati i principali attacchi, come prevenirli analizzando le principali vulnerabilità, fino ad implementare i buoni principi per la scrittura di un listato “pulito” e, per quanto più possibile, riducendo le vulnerabilità.
Il discente saprà, alla fine del corso, distinguere eventuali falle nel codice per poter apportare le opportune modifiche.

Modulo 1 - Applicazioni Web: architetture, strutture ed evoluzione

Modulo 2 - Minacce ed attacchi alle Applicazioni Web: obiettivi di un attacco, differenza fra attacchi e vulnerabilità, falsi miti

Modulo 3 - Application Security: confidentiality, integrity, availability, traceability, privacy, compliance, reputation, attacchi ai client

Modulo 4 - Progetti sulla sicurezza delle Applicazioni Web: OWASP, WASC, CWE/SANS, SAFECode.org, attacchi, problematiche e vulnerabilità delle Applicazioni Web

Modulo 5 - Trovare le vulnerabilità attraverso la OWASP Testing Guide e correggere ed evitare le problematiche attraverso la OWASP Development Guide

Modulo 6 - Assessment e secure coding
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