PROGRAMMA

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 apposita macchina virtuale di laboratorio dove saranno simulate le principali vulnerabilità illustrate durante il corso e tramite il quale i partecipanti potranno interagire sotto la guida del docente.

I contenuti sono divisi in 11 moduli descritti di seguito:

1. Le Applicazioni Web, architetture, strutture e evoluzione.
2. Minacce, attacchi e attaccanti sulle Applicazioni Web, obiettivi di un attacco, differenza fra attacchi e vulnerabilità, falsi miti.
3. Application Security (confidentiality, integrity, availability, traceability, privacy, compliance, reputation)
4. Progetti sulla sicurezza delle Applicazioni Web (OWASP, WASC, CWE/SANS, SAFECode.org)
5. 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
6. Linee guida e principi del Security Design.
7. Introduzione al Secure SDLC.
8. Attacchi ai client.
9. Alcuni casi di studio
10. Web Application Security Tools, installazione e utilizzo di alcuni tool fondamentali per la sicurezza delle Applicazioni Web.
11. Penetration Testing su Vulnerabilità connesse con piattaforme CMS come Joomla, Wordpress.