5 ANALISI DELLE INIZIATIVE E DEGLI STANDARD

5.1 Iniziative Internazionali

5.1.1 Open Web Application Security Project (OWASP)

L'Open Web Application Security Project (chiamato semplicemente OWASP) è un progetto open-source per la sicurezza delle applicazioni Web. L'OWASP offre guide con consigli sulla creazione di applicazioni Internet sicure, e indicazioni per i test cui andrebbero sottoposte. È stato, inoltre, pubblicato WebGoat, utile ad apprendere, attraverso esempi concreti, le minacce più diffuse per la sicurezza delle applicazioni web. Nel 2004 è stata istituita una fondazione no-profit che supporta l'OWASP e che persegue l'obiettivo di aumentare la sicurezza delle applicazioni consentendo di prendere le decisioni in base ai rischi. In Europa è un'organizzazione no-profit registrata da giugno 2011 ed è presente anche in Italia.

La filosofia cui si ispira OWASP si può riassumere nei seguenti punti:

- **Apertura**. Tutto in OWASP è aperto e trasparente, dal codice sorgente ai bilanci societari.
- **Innovazione**. OWASP incoraggia e supporta l'innovazione e la sperimentazione per trovare nuove e sempre più efficaci soluzioni alle sfide della sicurezza del software.
- **Universalità**. Chiunque è incoraggiato a partecipare alla comunità OWASP.
- **Integrità**. OWASP è una comunità globale, che si basa sull'onestà e sull'indipendenza.

URL	**https://www.owasp.org/**
Country of HQ location	**US**
Geographic Scope	**International**
Type	**Various Industry (not for profit)**

L'iniziativa è organizzata come una comunità collaborativa che produce tool e documenti nelle seguenti tre aree principali:

- Protection,
- Detection,
- Life-cycle security.

Relativamente a queste tre aree, OWASP ha prodotto:

- un insieme di guide sulle buone pratiche quali: OWASP Testing Guide, OWASP Code Review e Software Assurance Maturity Model;
- il Report' OWASP Top 10' sui rischi per le applicazioni web.

Da considerare inoltre, come attività rilevanti svolte da OWASP, quanto segue:

Good Practice	[Protection Area] OWASP Secure Coding Practices - Quick Reference Guide v2.0 - Un insieme indipendente dalla tecnologia di pratiche di codifica della sicurezza generale del software, in formato checklist, che può essere integrata nel ciclo di vita dello sviluppo del software. [Protection Area] OWASP Developers Guide v2.0 (2005) - Un documento completo che copre tutti gli aspetti della sicurezza delle applicazioni e dei servizi web. [Detection Area] OWASP Code Review Guide v2.0 - Una guida che raccoglie le

	migliori pratiche per la revisione del codice. [Detection Area] OWASP Testing Guide v4.0 - Una guida sulle procedure e checklist di test di sicurezza dell'applicazione. [Detection Area] OWASP Mobile Security Testing Guide (MSTG). Un manuale completo per il test di sicurezza delle applicazioni "mobile" e il reverse engineering per il security testing delle piattaforme iOS e Android.
Standards	[Detection Area] Application Security Verification Standard (ASVS). L'ASVS definisce uno standard internazionale per la valutazione della sicurezza delle applicazioni e copre sia la verifica delle applicazioni automatizzata che quella manuale, utilizzando tecniche di test di sicurezza e di revisione del codice. [Detection Area] OWASP Mobile Application Security Verification Standard (MASVS). Uno standard per la sicurezza delle applicazioni mobili.
Tools (Projects)	[Detection Area] Progetto OWASP Web Testing Environment (WTE). Una raccolta di strumenti di sicurezza delle applicazioni e di documentazione disponibile in diversi formati come VM, pacchetti di distribuzione Linux, installazioni basate su cloud e immagini ISO. Il progetto OWASP WTE è un miglioramento dell'originale OWASP Live CD Project. [Detection Area] Progetto Zed Attack Proxy (ZAP) - Questo progetto di punta di OWASP è tecnicamente uno strumento proxy per intercettare, attraverso il traffico di rete, le vulnerabilità nelle applicazioni web. È stato progettato per essere utilizzato da persone con un'esperienza consolidata in materia di sicurezza e, come tale, è ideale per gli sviluppatori e tester funzionali chiamati a svolgere il penetration testing. Include le caratteristiche dei vecchi progetti WebScarab e DirBuster. [Detection Area] Progetto SWFIntruder. È uno strumento per analizzare e testare la sicurezza delle applicazioni flash in fase di esecuzione. [Life cycle security Area] Progetto OWASP WebGoat. Un'applicazione web insicura per insegnare la sicurezza delle applicazioni web attraverso lezioni pratiche interattive. [Life cycle security Area] Piattaforma OWASP O2. Una raccolta di moduli Open Source a supporto dei professionisti della sicurezza delle applicazioni web per massimizzare i loro sforzi e ottenere rapidamente una significativa conoscenza del profilo di sicurezza di un'applicazione. [Protection Area] OWASP OWASP OWTF. Un altro strumento di punta di OWASP per i pen-test. [Detection Area] OWASP Dependency Check. Strumento per controllare e verificare la vulnerabilità delle librerie di terze parti utilizzate nei progetti di sviluppo software. [Protection Area] OWASP Security Shepherd. Strumento destinato a migliorare la capacità di pen-test del personale di sicurezza. [Protection Area] OWASP DefectDojo. Uno strumento open source di gestione delle vulnerabilità che semplifica il processo di testing, fornendo template, report, metriche e strumenti di base. [Life cycle security Area] OWASP Juice Shop. Un'applicazione web volutamente insicura per i corsi di sicurezza scritta interamente in JavaScript che comprende l'intera Top Ten di OWASP e altri gravi difetti di sicurezza. [Protection Area] OWASP Security Knowledge Framework. Uno strumento che viene utilizzato come guida per la creazione e la verifica di software sicuro; può essere utilizzato anche per formare gli sviluppatori sulla sicurezza delle applicazioni. [Detection Area] OWASP Dependency Track. Una piattaforma di analisi della