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