

OWASP Top 10 - 2013	→	OWASP Top 10 - 2017
A1 – Injection	→	A1-Injection
A2 – Broken Authentication and Session Management	→	A2-Broken Authentication
A3 – Cross-Site Scripting (XSS)	↘	A3-Sensitive Data Exposure
A4 – Insecure Direct Object References [Merged+A7]	U	A4-XML External Entities (XXE) [NEW]
A5 – Security Misconfiguration	↘	A5-Broken Access Control [Merged]
A6 – Sensitive Data Exposure	↗	A6-Security Misconfiguration
A7 – Missing Function Level Access Contr [Merged+A4]	U	A7-Cross-Site Scripting (XSS)
A8 – Cross-Site Request Forgery (CSRF)	⊗	A8-Insecure Deserialization [NEW, Community]
A9 – Using Components with Known Vulnerabilities	→	A9-Using Components with Known Vulnerabilities
A10 – Unvalidated Redirects and Forwards	⊗	A10-Insufficient Logging&Monitoring [NEW,Comm.]

Figura 4 - OWASP Top 10 - 2017

L'adozione di un Secure Software Development Life Cycle (SSDLC) atto a considerare e implementare opportune attività di sicurezza, nel corso di tutte le sue fasi del ciclo di vita del SW (dall'analisi fino alla manutenzione), è una necessità inderogabile per rispondere in modo efficace alle problematiche di sicurezza e per ridurre i costi che comportano trascurarla.

Ripensare alla sicurezza tra responsabilità e consapevolezza, oltre ad essere una buona pratica, è anche un obbligo di legge (Regolamento UE 679/2016).

4.3 Security Tools

Nell'ambito della cybersecurity, Forrester⁸, nel suo report **"Five steps to reinforce and harden application security"**⁹, rileva la necessità di cooperazione tra i team Security & Risk (S&R) e gli IT manager (I&O), ribadendo più volte come i primi non siano in grado, da soli, di coprire tutte le vulnerabilità scaturite dalle nuove esigenze in ambiti IT e digital business. Dal punto di vista dell'analista, infatti, l'IT team deve adottare, attraverso opportuni meccanismi di automazione e integrazione, le **security practices** all'interno di una **'continuous delivery pipeline'**. Questo garantisce una maggiore visibilità nelle interazioni tra hardware, software, servizi web e customer data. I professionisti I&O hanno, quindi, l'obiettivo di creare un ambiente di sicurezza **'responsive'**.

A tal fine, Forrester propone cinque steps per costruire un **responsive security environment**:

Step 1: rimuovere le 'inconsistenze' e creare un 'conto' dei materiali

Innanzitutto è necessario eliminare tutte le problematiche di sicurezza spesso derivanti da vulnerabilità riconducibili a servizi non più utilizzati e non più mantenuti o una cattiva gestione degli accessi e delle autorizzazioni. Tale attività deve essere svolta attraverso la collaborazione tra i team dedicati (I&O e S&R).

⁸ <https://www.forrester.com/>

⁹ <https://www.forrester.com/report/Five+Steps+To+Reinforce+And+Harden+Application+Security/-/E-RES127875>