# La Convergenza tra OWASP e (ISC)²

## Connubio tra approccio empirico e sistematico


**Paolo Ottolino**

PMP CISSP-ISSAP CISA CISM OPST ITIL

**Claudio Sasso**

CISSP CCSLP CCSK  Auditor ISO27001 ITIL

# Agenda

1) (ISC)$^2$ Chapter Italy
2) (ISC)$^2$ International
3) Convergenza OWASP – (ISC)$^2$
4) CCSLP & OWASP
5) CISSP-ISSAP &OWASP Top Ten

# (ISC)² Italy Chapter – Chi Siamo

www.isc2chapter-italy.it

- Professionisti Certificati e Non - 75-80 soci
- Lavori avviati da un anno, riconoscimento ufficiale da (ISC)² da fine Giugno 2012
- Indipendenza + Supporto da (ISC)²

Cosa facciamo

- Awareness (e Formazione) sulla Sicurezza ICT
- Approfondimenti e Gruppi di Lavoro
- Iniziative di approfondimento per CPE
- Networking

http://www.linkedin.com/company/-isc-2-italy-chapter

info@isc2chapter-italy.it

# (ISC)² Italy Chapter – Iniziative

www.isc2chapter-italy.it

- Iniziative per i soci
  - Guide / Informazioni
  - Seminari per CPE
  - Pillole CISSP
  - Incontri ed Eventi con gli altri Chapter
    - Svizzera, Inghilterra, Germania,…
- Iniziative verso l'esterno
  - Awareness e Formazione nelle Scuole
  - Security Convergence - ASIS
  - (Formazione CISSP & Clusit)

# (ISC)² International

- Established in 1989 – Non-profit consortium
- CISSP è ISO/IEC 17024 / Circa 300 certificati in Italia
  - 80.000 Certified Professionals more than 135 countries
- Many different areas:
  - (ISC)² e-Symposia, (ISC)² Think Tank One-day Security Leadership Series workshops, SecurityTALK
  - Global Information Security Workforce Study
  - Advocacy for the profession
    - Industry, government, academic alliances
  - Awards Programs
    - Americas and Asia-Pacific ISLA / and U.S. GISLA
  - …

# (ISC)² CSSLP


- "Nuova" Certificazione
  - Pochi certificati in Italia
- Aree di sovrapposizione
- Approcci:
  - OWASP – Deep Insight & Guide/Howto/Tools (approccio empirico)
  - (ISC)2 – Visione orizzontale e metodologica (approccio "sistematico")

**Sempre Maggiore Convergenza**

# OWASP Top Ten & (ISC)$^2$ CSSLP

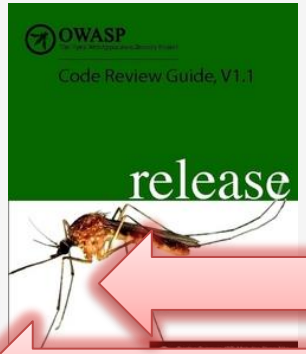
## OWASP Top Ten – Un esempio di convergenza:

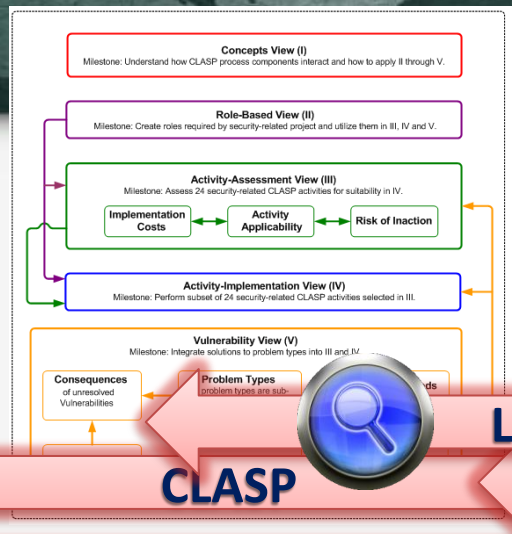
- ✓ A1 - Injection
- ✓ A2 - XSS (Cross Site Scripting)
- ✓ A3 – Broken Authentication and Session Management
- ✓ A4 – Insecure Direct Object References
- ✓ A5 – CSRF (Cross Site Request Forgery)
- ✓ A8 – Failure to Restrict URL Access
- ✓ A10 – Unvalidated Redirects and Forwards

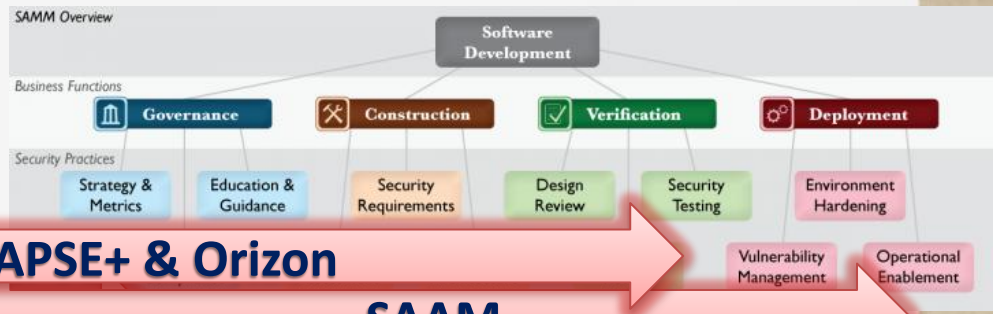
## …ma anche…

- ✓ A7-Insecure Cryptographic Storage
- ✓ A6-Security Misconfiguration
- ✓ A9-Insufficient Transport Layer Protection

# Progetti OWASP e Convergenza




LAPSE+ & Orizon

CLASP

SAAM

Code Review Guide

Requir. → Design → Coding → Testing → Accept. → Operat. &Assu

Top 10

OWASP Testing Guide

A1: Injection

A2: Cross Scripting (X

anagement

References

A5: Cross Site Request Forgery (CSRF)

A6: Security Misconfiguration

A7: Insecure Cryptographic Storage

A8: Failure to Restrict URL Access

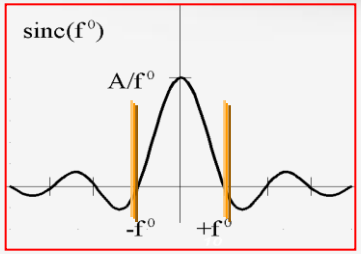
A9: Insufficient Transport Layer Protection

A10: Unvalidated Redirects and Forwards

# Convergenza OWASP - (ISC)²

**Antinomia Stateless – Statefull:**

**Web 2.0 crea un client (intrinsecamente statefull) su piattaforma "Request-Response OneShot" (stateless "by design") - simile ad antinomia Delimitazione della Banda per Trasmissione Radio**

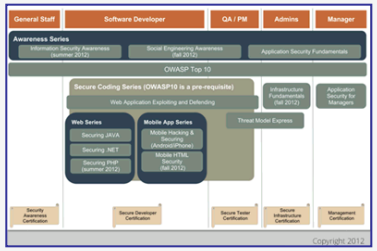



**ISO/OSI (Ultimi 2 Layer):**

**Web 2.0 crea Application e Presentation. Viceversa si affida ai sottostanti 5 Layer (Session, Transport, Network, Data-Link e Physical) che ne realizzano le fondamenta**

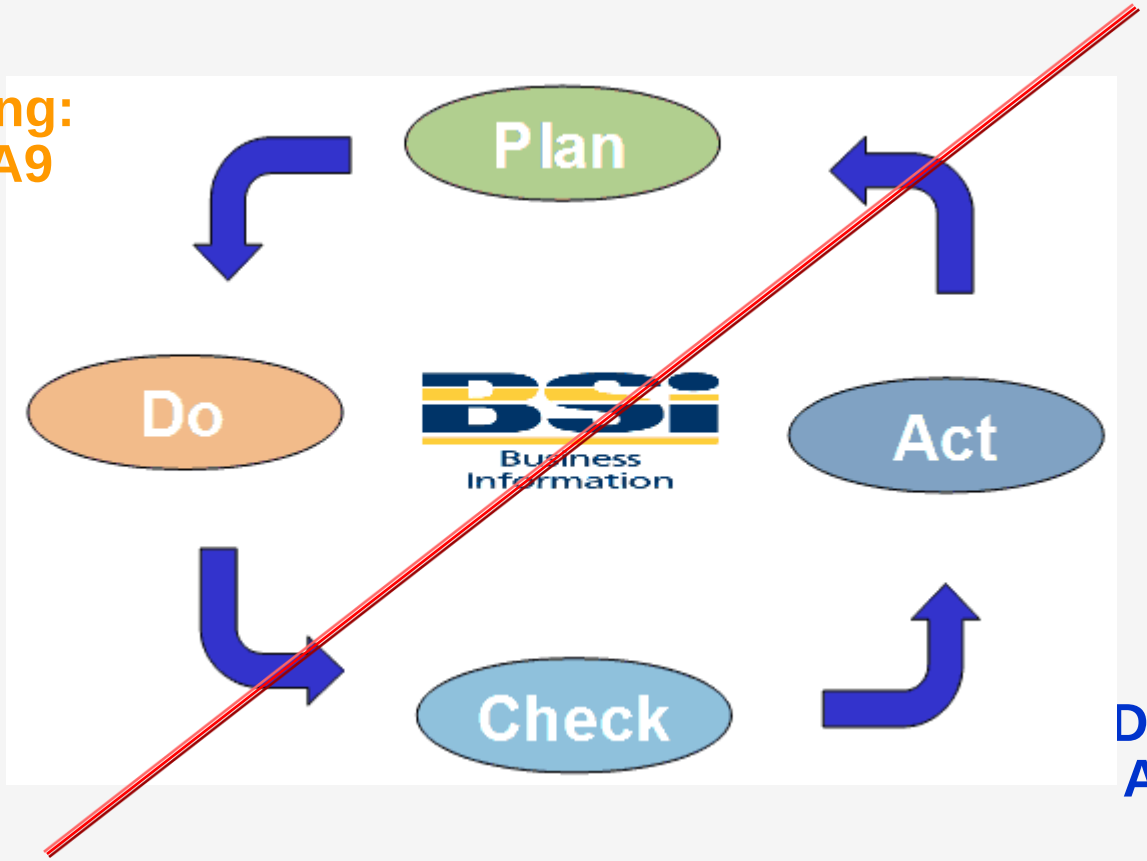

**(ISC)² Training: "OWASP Top 10 Training"**

https://www.isc2.org/owasp.aspx



# CISSP-ISSAP addresses 6/10 OWASP Top Ten 1/4

**Hardening:**
**A6, A7, A9**

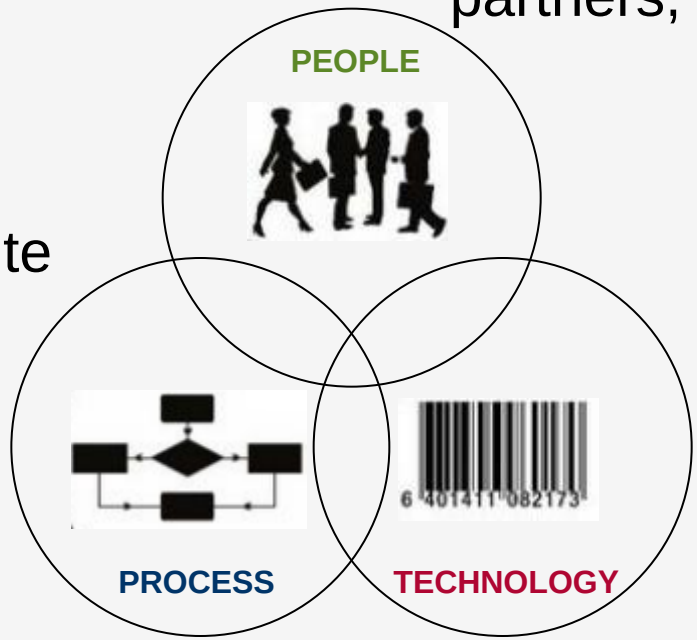



**Detection:**
**A5, A2, A1**

# CISSP-ISSAP addresses 6/10 OWASP Top Ten 2/4

**People:** stakeholders (employees, customers, partners, suppliers, attackers)

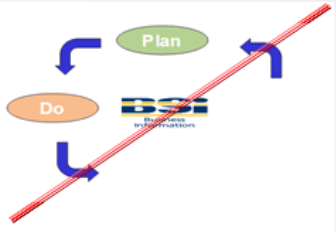
**Process:** action performed to execute business



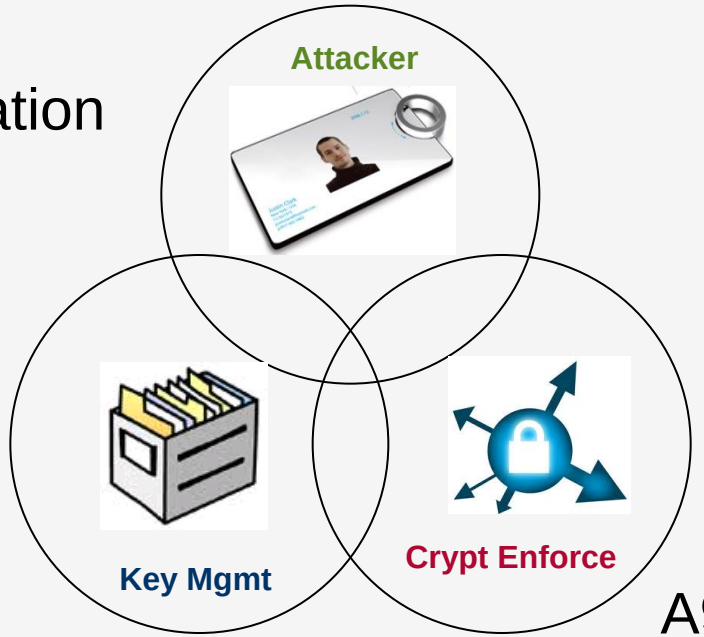

**Technology:** tools used to perform processes by people

# CISSP-ISSAP addresses 6/10 OWASP Top Ten 3/4

## Hardening




**People:**
A6 Security Misconfiguration

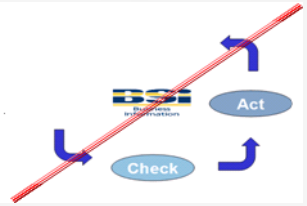



**Process:**
A7 Cryptographic Storage

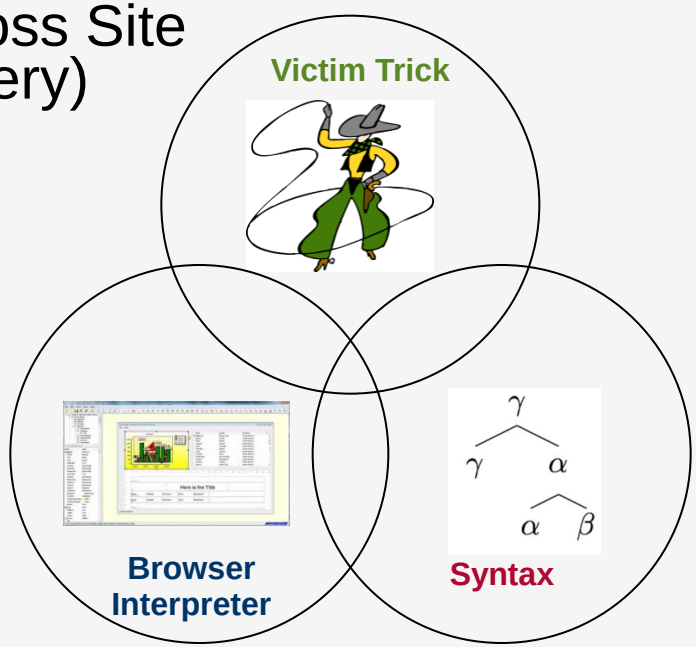
**Technology:**
A9 Transport Layer Protection

# CISSP-ISSAP addresses 6/10 OWASP Top Ten 4/4

## Detection




**People:**
A5 CSRF (Cross Site Request Forgery)




**Technology:**
A1 Code Injection

**Process:**
A2 XSS (Cross Site Scripting)

# Grazie!


http://www.isc2chapter-italy.it

http://www.linkedin.com/company/-isc-2-italy-chapter
http://www.linkedin.com/groups?gid=119039

**Paolo Ottolino**
paolo.ottolino@isc2chapter-italy.it

**Claudio Sasso**
claudio.sasso@isc2chapter-italy.it