Lo stato dell'arte dei progetti OWASP ed i falsi miti sull'uso dei tool

Matteo Meucci

Paolo Perego

Giorgio Fedon

Security Summit 2011

Milan – 15th March, 2011

The OWASP Foundation

http://www.owasp.org

Agenda del seminario

- "OWASP 2010 e nuovi progetti 2011: cosa offre ad oggi OWASP per le aziende e dove stiamo puntando per il futuro"
- "Linee guida OWASP per la sicurezza del software"
  - OWASP Top 10
  - OWASP Building, Code Review e Testing Guide
  - OWASP SAMM e ASVS

Matteo Meucci

- "I tool OWASP per la sicurezza del software"
  - OWASP ESAPI
  - OWASP WebScarab e WebGoat
  - OWASP Jbrofuzz, LiveCD
  - OWASP Orizon e O2

Paolo Perego

- "Myth Busting Automatic Code Review tools"

Giorgio Fedon

Who am I?

- Research
  - OWASP-Italy Chair
  - OWASP Testing Guide Lead
  - OWASP SAMM contributor
  - OWASP Common numbering list contributor
- Work
  - 10+ years on Information Security

  focusing on Application Security
  - www.mindedsecurity.com

www.owasp.org

(VIDEO)

Linee guida OWASP

Progetti 2011: OWASP Common Vulnerability List

We need a common vulnerability list

Manager

Governance

OWASP SAMM è il primo maturity model?

eSourcing Capability Model for Client Organizations (eSCM-CL)

eSourcing Capability Model (eSCM)

Data Management Maturity Model (DMMM)

Capability Maturity Model Integration (CMMI)

Building Security In Maturity Model (BSIMM)

Service Integration Maturity Model (SIMM)

Organizational Project Management Maturity Model: (OPM3)

Information Security Management Maturity Model (ISM3)

E-Learning Maturity Model (eMM)

Progressive HR Business Integrated Model (ProBIM)

Open Source Maturity Model (OSMM)

Systems Security Engineering Capability Maturity Model (SSE-CMM)

Self-Assessment Maturity Model (SAMM)

Usability Maturity Model (UMM)

Enterprise Data Management Maturity Model (DMM)

IDEAL

Enterprise Data Management Model Integration (EDMMI)

Web Site Maturity Model

IT Service Capability Maturity Model (IT Service CMM)

Capability Maturity Model (CMM)

Software Reliability Engineering Maturity Model

Testing Maturity Model (TMM)

Software Acquisition Capability Maturity Model (SA-CMM)

People Capability Maturity Model (PCMM)

Portfolio, Programme and Project Management Maturity Model (P3M3)

eSourcing Capability Model for Service Providers (eSCM-SP)

Outsourcing Management Maturity Model

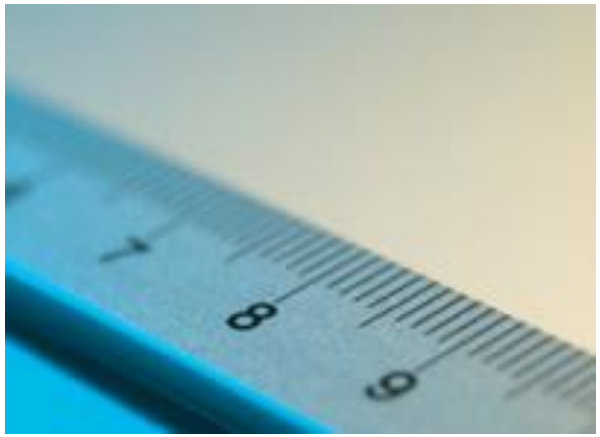
eGovernment Maturity Model (eGMM)

OWASP SAMM e BSIMM

- BSIMM: Lo scopo del BSIMM è quello di documentare le attività comuni a tutte le più importanti attività di software security. Modello descrittivo: a posteriori il modello riflette un insieme di realtà.

- OWASP SAMM: I modelli precedenti sono buoni per gli esperti da utilizzare come una guida, ma difficile per le aziende da utilizzare per migliorare i propri obiettivi. Modello prescrittivo: mostra un percorso comune da seguire.

OWASP SAMM: obiettivi



OWASP SAMM: il modello

SAMM: 4 Funzioni di business critiche

Governance

Software development management activities and organisation-wide business processes

Construction

Goal definition and software creation processes

Verification

Checking, evaluation and testing of software development artifacts

Deployment

Software release management and normal operational management

- Si inizia con le 4 attività di base legate ad ogni azienda che sviluppa o acquista software
- Nomi generici delle funzioni ma dovrebbero essere compresi dagli sviluppatori e manager

Ciascuna area ha 3 Security Practices

Governance	Construction	Verification	Deployment
			
Security & Metrics	Threat Assessment	Design Review	Vulnerability Management
Policy & Compliance	Security Requirements	Code Review	Environment Hardening
Education & Guidance	Secure Architecture	Security Testing	Operational Enablement

Ad esempio: BF Governance, SP Education

Governance

- Security & Metrics
- Policy & Compliance
- Education & Guidance

Obiettivi →

Attività →

EG1	EG2	EG3
Offrire allo staff di sviluppo l'accesso alle risorse di sviluppo sicuro	Educare tutto il personale nel SDLC in base al proprio ruolo nello sviluppo sicuro	Training sulla sicurezza mandatori e completi. Personale certificato
A. Condurre Training tecnici su Security Awareness B. Costruire e mantenere linee guida tecniche	A. Condurre training specifici in base al ruolo B. Utilizzare i trainer per migliorare i team di progetto	A. Creare un supporto formale per la application security B. Stabilire esami in base ai ruoli aziendali

Applicare il modello

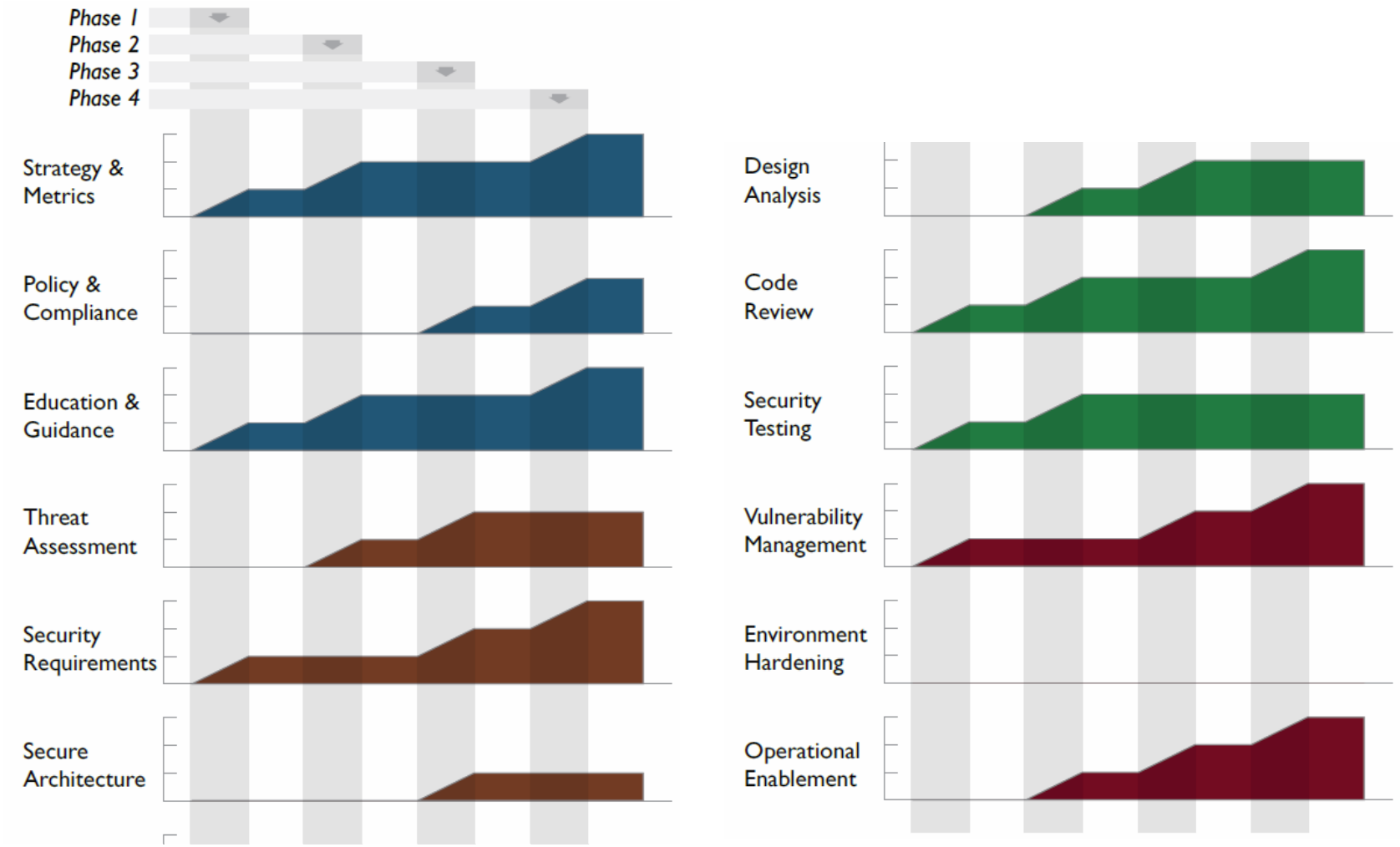
Procedura di assessment

- Condurre un assessment
- Creare uno score card
- Costruire un programma di assurance
  - Metriche
  - Road map
- Implementare gli obiettivi e condurre nuovamente un assessment

Assessment

Education & Guidance	Yes/No	
✦ Have most developers been given high-level security awareness training?		
✦ Does each project team have access to secure development best practices and guidance?		EG 1
✦ Are most roles in the development process given role-specific training and guidance?		
✦ Are most stakeholders able to pull in security coaches for use on projects?		EG 2
✦ Is security-related guidance centrally controlled and consistently distributed throughout the organization?		
✦ Are most people tested to ensure a baseline skill-set for secure development practices?		EG 3

Roadmap


Phase 1
Phase 2
Phase 3
Phase 4
Strategy & Metrics
Policy & Compliance
Education & Guidance
Threat Assessment
Security Requirements
Secure Architecture
Design Analysis
Code Review
Security Testing
Vulnerability Management
Environment Hardening
Operational Enablement

Manager

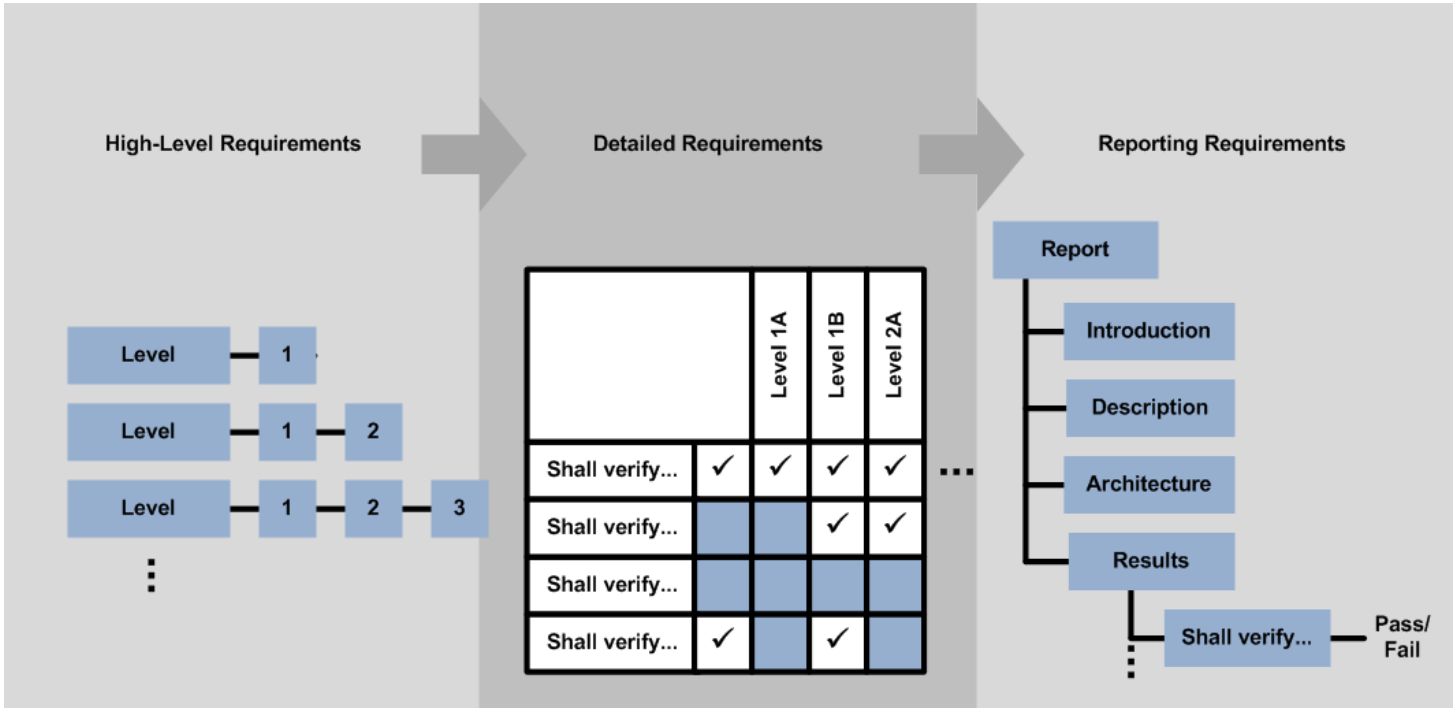
Verification

A quali domande ASVS risponde?

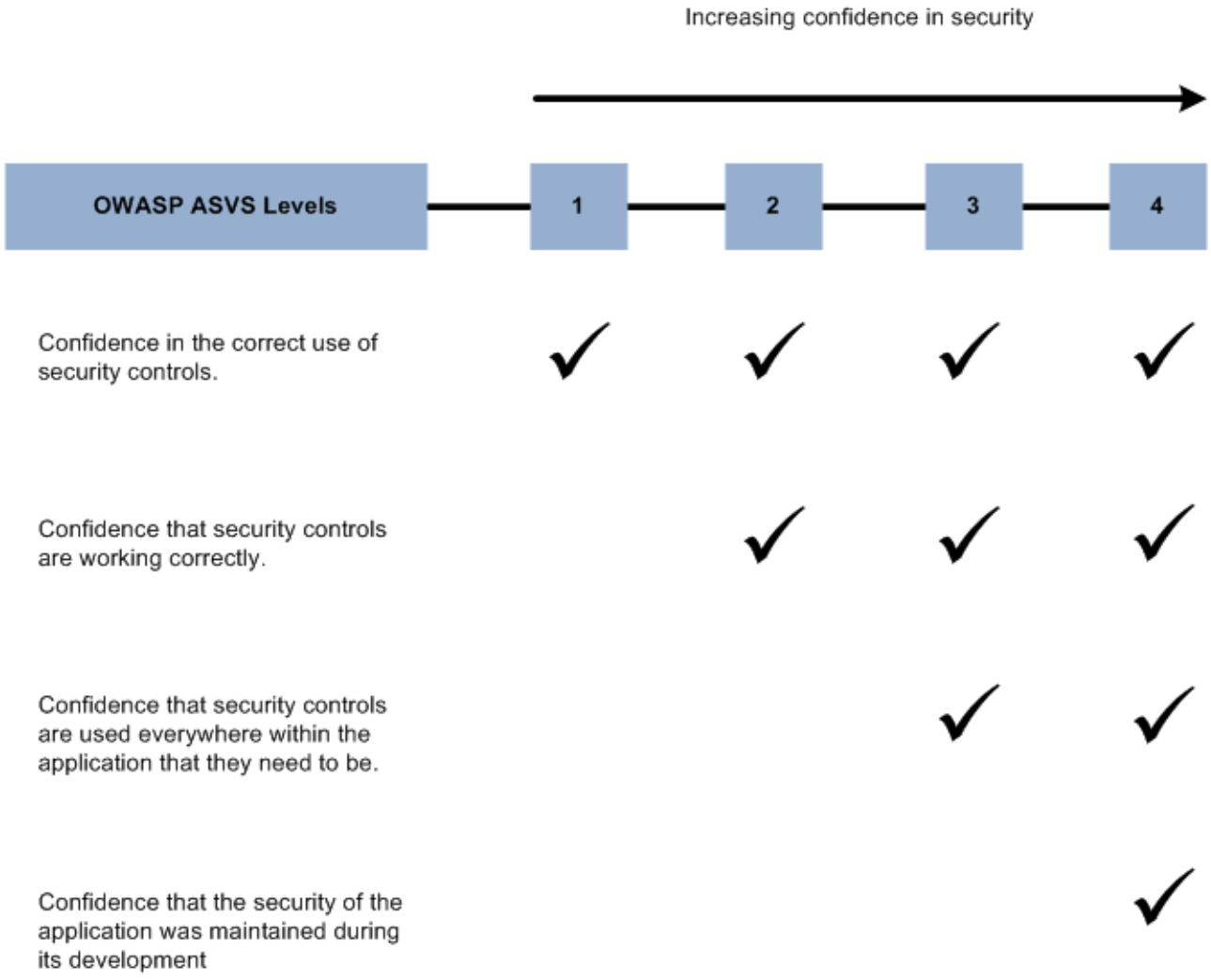
- Come posso comparare le attività di verifica?
- Quali caratteristiche di sicurezza dovrebbero essere implementate nell'insieme di controlli di sicurezza richiesti?
- Quali sono gli aspetti da migliorare nella verifica della sicurezza di una applicazione web?
- Quanta fiducia posso dare alla mia applicazione web?

Overview di ASVS

- "Verification Levels" section
- "Verification Requirements" section
- "Verification Reporting Requirements" section



Quali sono i livelli di verifica proposti da ASVS ?



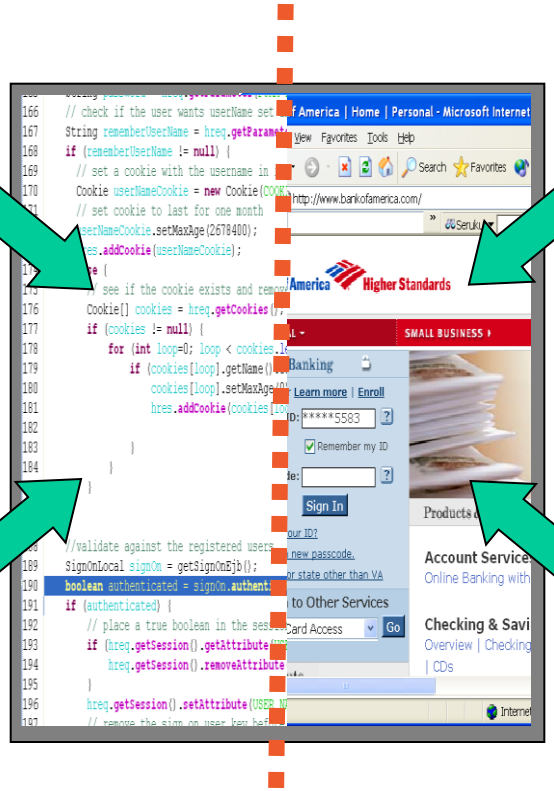
Security Analysis Techniques:

Trovare vulnerabilità nel Codice Sorgente (White Box Testing)

Trovare vulnerabilità nelle applicazioni sviluppate (Black Box Testing)

Manual Code Review

Manual Penetration Testing



Automated Static Code Analysis

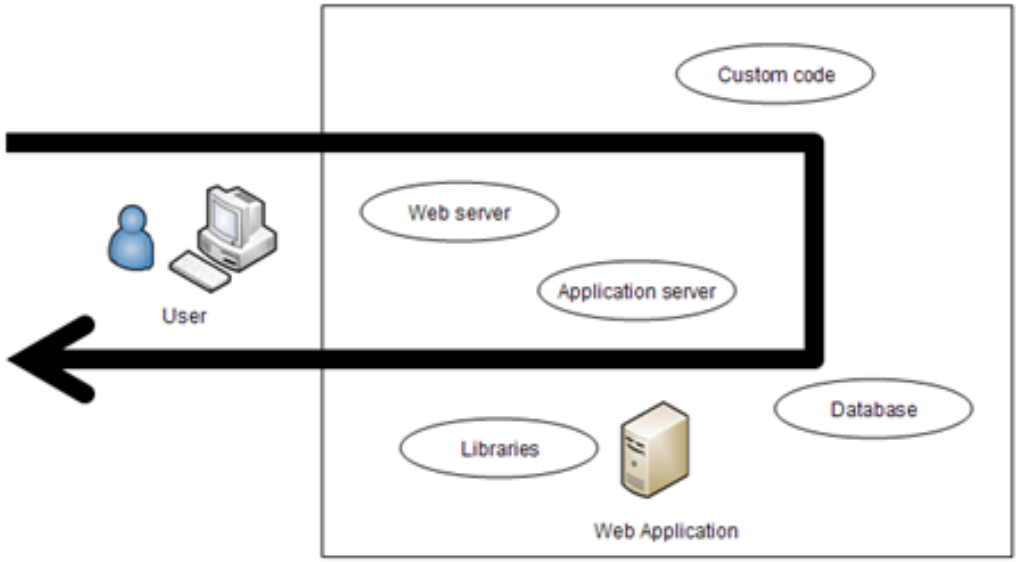
Automated Vulnerabilty Scanning

Definizione dei livelli in ASVS

- Level 1 – Automated Verification
  - Level 1A – Dynamic Scan (Partial Automated Verification)
  - Level 1B – Source Code Scan (Partial Automated Verification)
- Level 2 – Manual Verification
  - Level 2A – Penetration Test (Partial Manual Verification)
  - Level 2B – Code Review (Partial Manual Verification)
- Level 3 – Design Verification
- Level 4 – Internal Verification

Livello 1

- Verifiche automatizzate di una applicazione vista come un gruppo di componenti con entità singole monolitiche.



Opzioni del livello 1

- Level 1A

  Dynamic Scan (Partial Automated Verification)

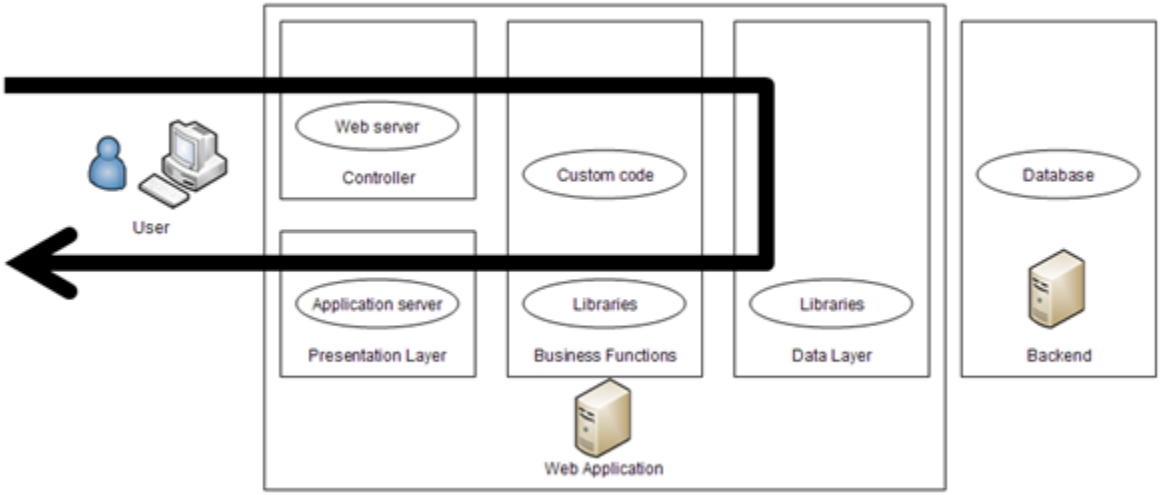
- Level 1B

  Source Code Scan (Partial Automated Verification)

Sono necessarie entrambe per raggiungere un pieno livello 1…

Livello 2

- Verifica manuale di una applicazione web organizzata in una architettura di alto livello.



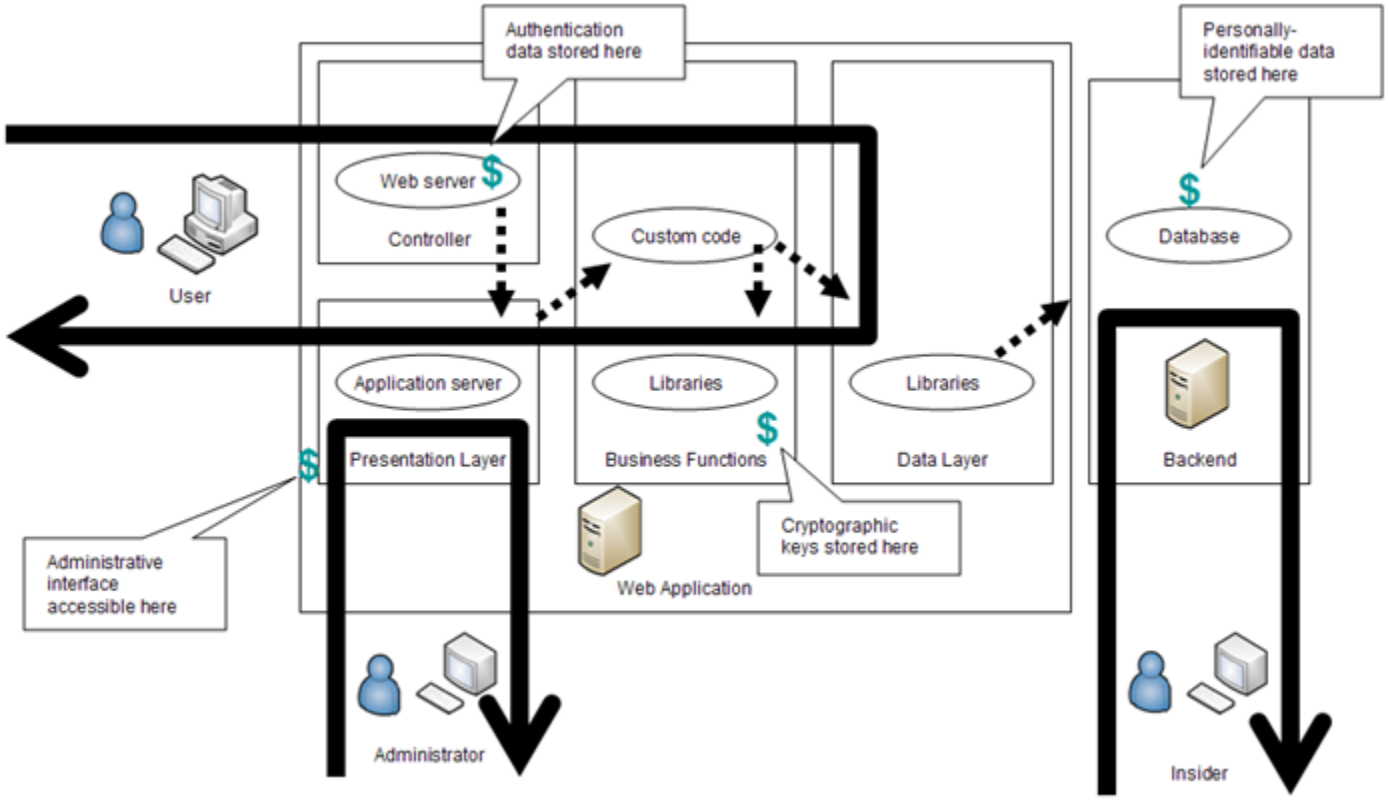
Level 2 Options

- Level 2A
  Manual Penetration Test
- Level 2B
  Manual Code Review

Sono necessarie entrambe per raggiungere un pieno livello 2…

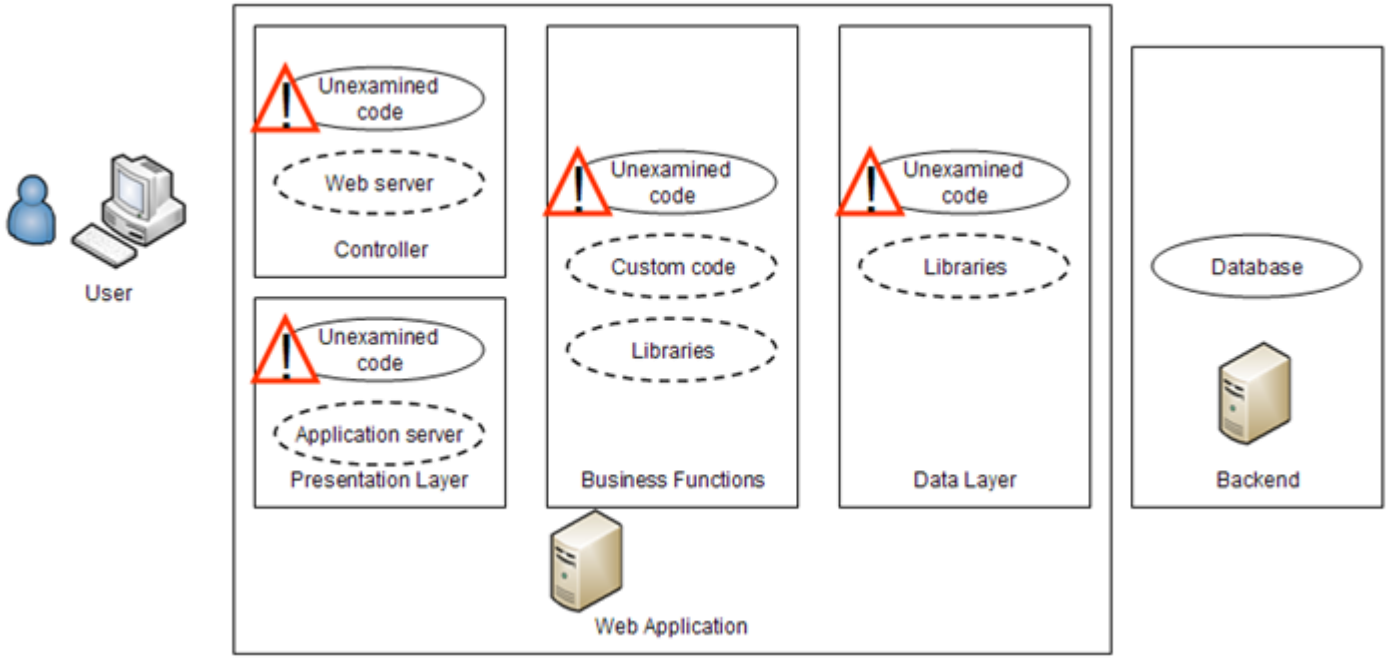
Livello 3

- Verifica del design dell'applicazione organizzata in un'architettura di alto livello (Threat modeling e design review).



Livello 4 in dettaglio

- Verifica interna dell'applicazione web ed esame di come funzionano i controlli di sicurezza.



Quali sono i requisiti di verifica nel ASVS ?

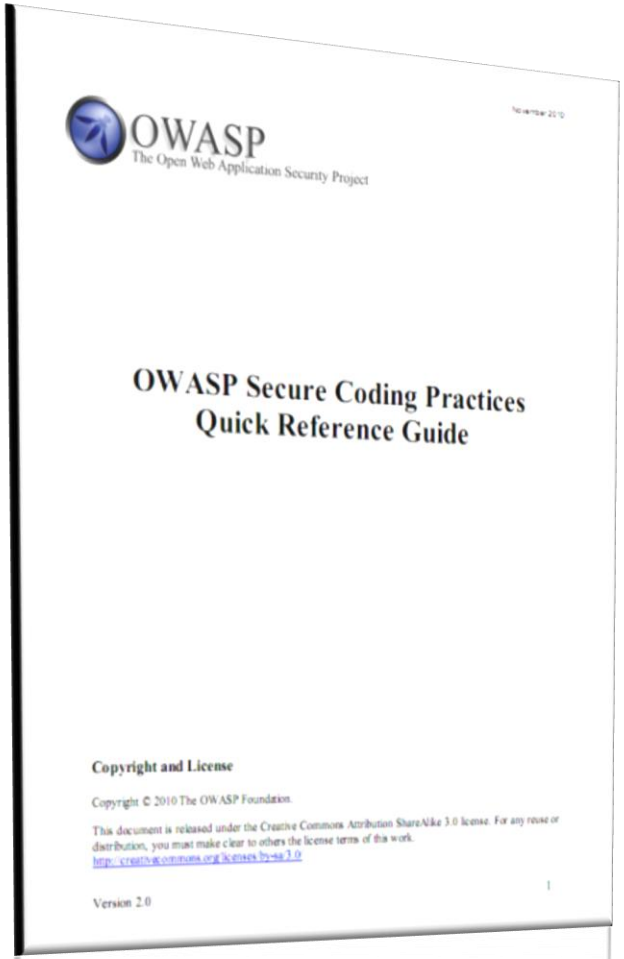
- V1. Security Architecture
- V2. Authentication
- V3. Session Management
- V4. Access Control
- V5. Input Validation
- V6. Output Encoding/Escaping
- V7. Cryptography
- V8. Error Handling and Logging
- V9. Data Protection
- V10. Communication Security
- V11. HTTP Security
- V12. Security Configuration
- V13. Malicious Code Search
- V14. Internal Security

V3 - Session Management Verification Requirements

The Session Management Verification Requirements define a set of requirements for safely using HTTP requests, responses, sessions, cookies, headers, and logging to manage sessions properly. The table below defines the corresponding verification requirements that apply for each of the four verification levels.

Table 3 - OWASP ASVS Session Management Requirements (V3)

Verification Requirement		Level 1A	Level 1B	Level 2A	Level 2B	Level 3	Level 4
V3.1	Verify that the framework's default session management control implementation is used by the application.	✓		✓	✓	✓	✓
V3.2	Verify that sessions are invalidated when the user logs out.	✓		✓	✓	✓	✓
V3.3	Verify that sessions timeout after a specified period of inactivity.	✓		✓	✓	✓	✓
V3.13	Verify that all code implementing or using session management controls is not affected by any malicious code.						✓



Developer

Construction

Secure Coding Practices Checklist

- Input Validation
- Output Encoding
- Authentication and Password Management
- Session Management
- Access Control
- Cryptographic Practices
- Error Handling and Logging
- Data Protection
- Communication Security
- System Configuration
- Database Security
- File Management
- Memory Management
- General Coding Practices

Session Management:

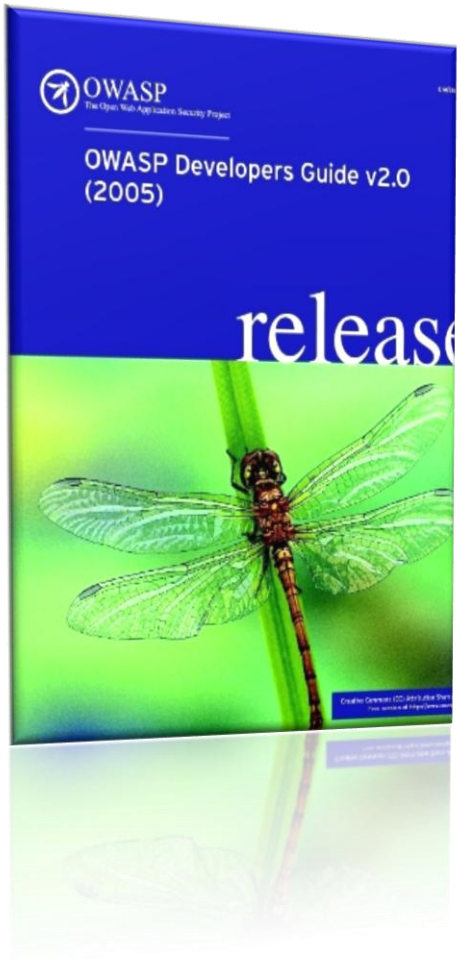
- Use the server or framework's session management controls. The application should only recognize these session identifiers as valid
- Session identifier creation must always be done on a trusted system (e.g., The server)
- Session management controls should use well vetted algorithms that ensure sufficiently random session identifiers
- Set the domain and path for cookies containing authenticated session identifiers to an appropriately restricted value for the site
- Logout functionality should fully terminate the associated session or connection
- Logout functionality should be available from all pages protected by authorization
- Establish a session inactivity timeout that is as short as possible, based on balancing risk and business functional requirements. In most cases it should be no more than several hours
- Disallow persistent logins and enforce periodic session terminations, even when the session is active. Especially for applications supporting rich network connections or connecting to critical systems. Termination times should support business requirements and the user should receive sufficient notification to mitigate negative impacts
- If a session was established before login, close that session and establish a new session after a successful login
- Generate a new session identifier on any re-authentication
- Do not allow concurrent logins with the same user ID
- Do not expose session identifiers in URLs, error messages or logs. Session identifiers should only be located in the HTTP cookie header. For example, do not pass session identifiers as GET parameters
- Protect server side session data from unauthorized access, by other users of the server, by implementing appropriate access controls on the server

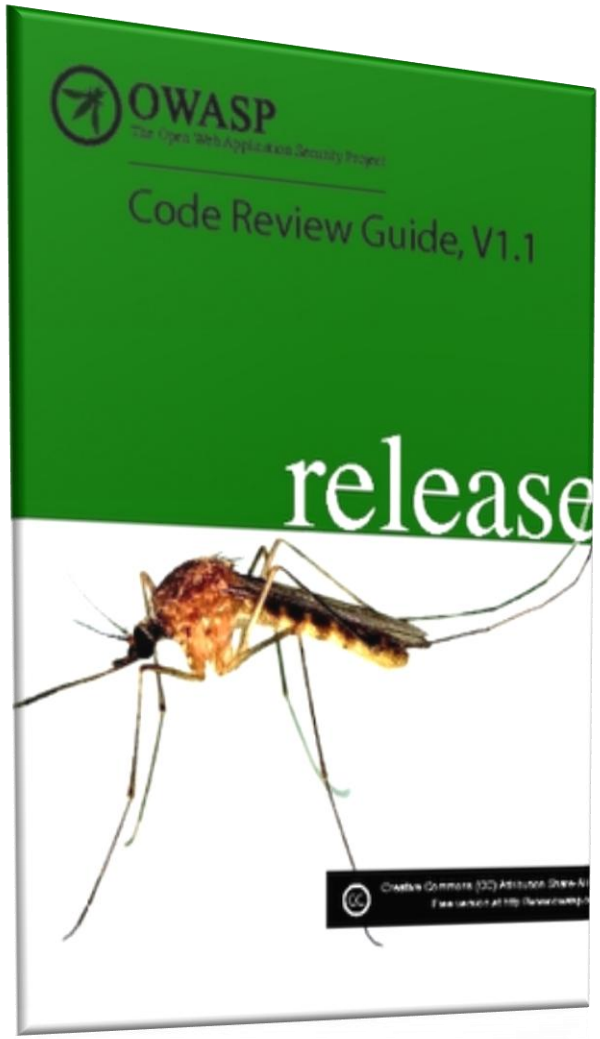
Developer

Construction

OWASP Building Guide

- Al fine di comprendere ed eliminare le cause della "insicurezza" nel software,OWASP ha sviluppato la guida per lo sviluppo delle applicazioni web sicure pensata per:
  - Sviluppatori per implementare i meccanismi di sicurezza ed evitare le vulnerabilità;
  - Project manager che la utilizzano per identificare le attività da svolgere (threat modeling, code review, development);
  - Team di sicurezza che la usano per apprendere le tematiche di application security e l'approccio per la messa in sicurezza;



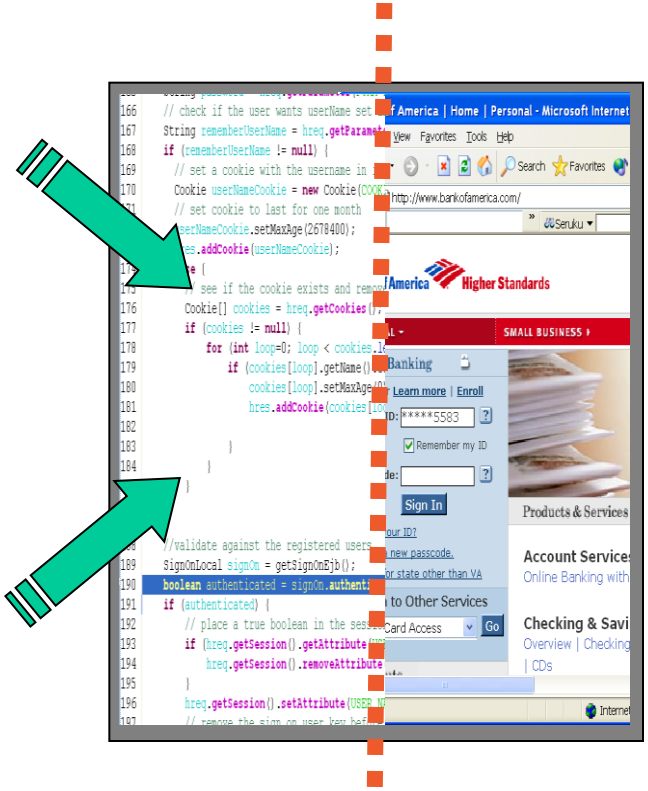


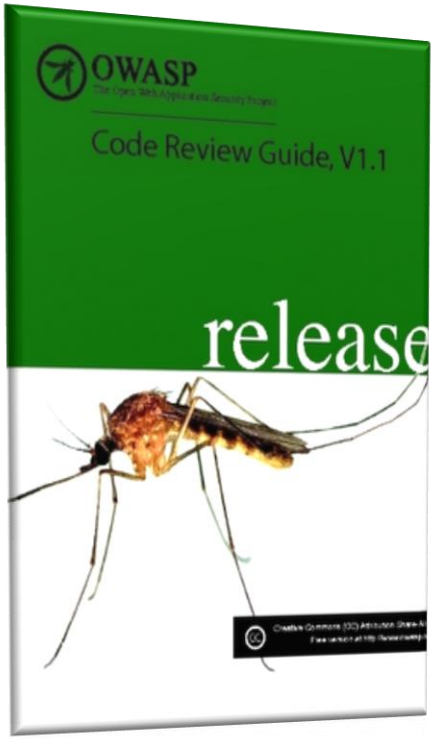
Tester

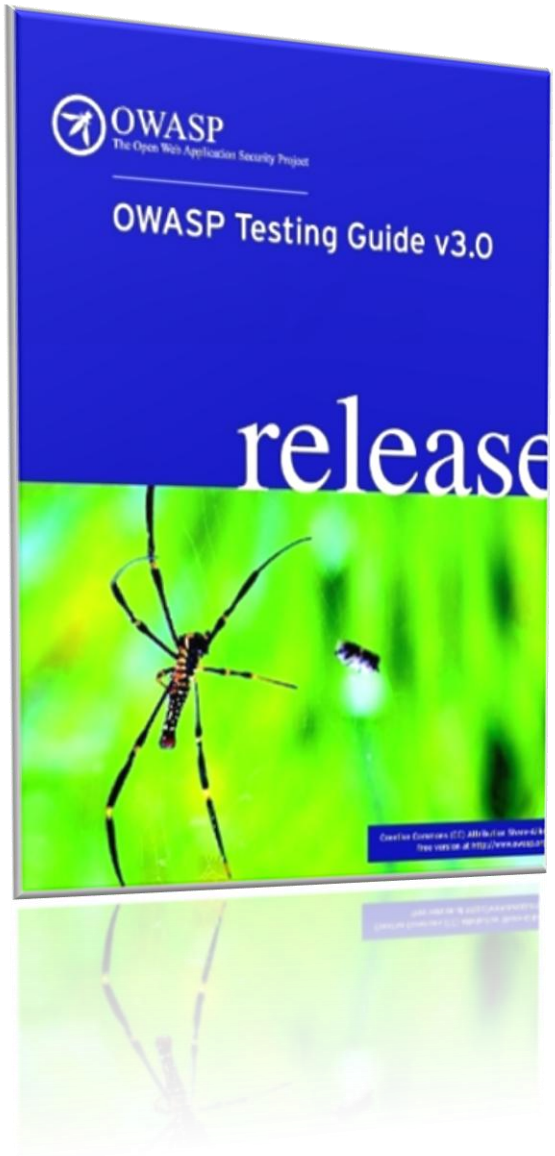
Verification

OWASP Code Review Guide

- Descrive la metodologia OWASP per testare il codice di un'applicazione (white box testing, conoscendo il codice sorgente)



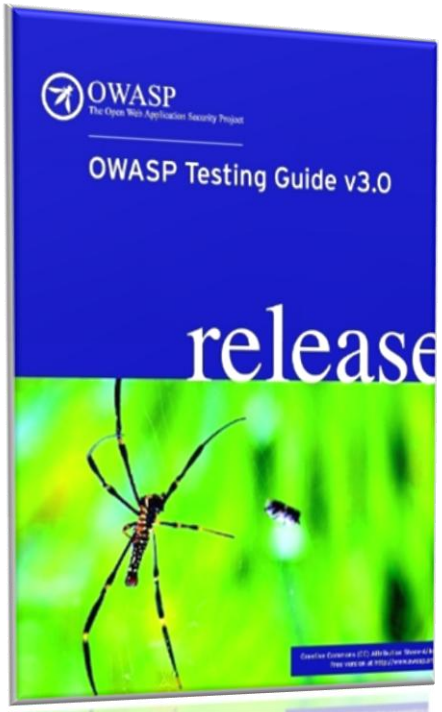


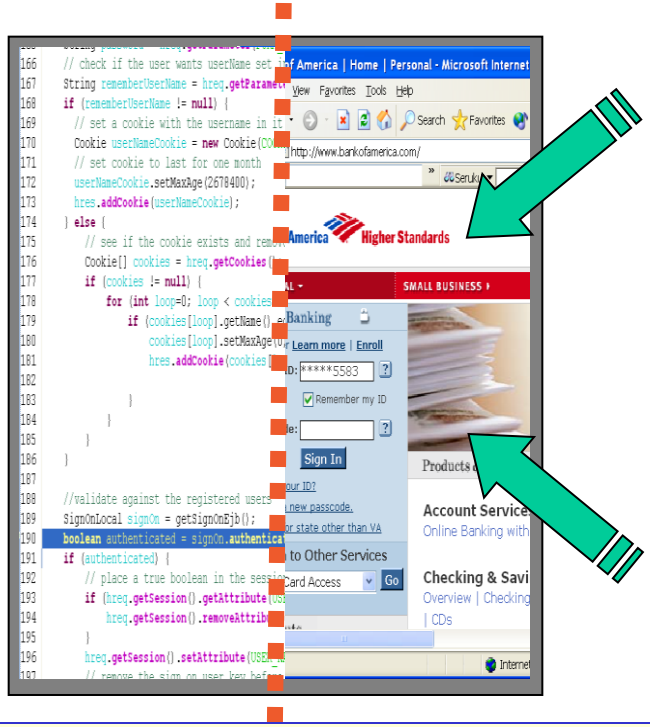


Tester

Verification

OWASP Testing Guide v3





- SANS Top 20 2007
- NIST “Technical Guide to Information Security Testing (Draft)”
- Gary McGraw (CTO Cigital) says: “In my opinion it is the strongest piece of Intellectual Property in the OWASP portfolio” – OWASP Podcast by Jim Manico

Proposed v4 list

Authorization	Path Traversal	TG
	Bypassing authorization schema	TG
	Privilege Escalation	TG
	Insecure Direct Object References	Top10 2010
	Failure to Restrict access to authorized resource	TG
Session Managment	Bypassing Session Management Schema	TG
	Weak Session Token	TG
	Cookies are set not 'HTTP Only', 'Secure', and no time validity	TG
	Exposed sensitive session variables	TG
	CSRF	
	Session passed over http	Vishal
	Session token within URL	Vishal
	Session Fixation	Vishal
	Session token not removed on server after logout	Vishal
	Persistent session token	Vishal
	Session token not restrcited properly (such as domain or path not set properly)	Vishal
Data Validation	Reflected XSS	TG
	Stored XSS	TG - Vishal
	HTTP Verb Tampering	new TG
	HTTP Parameter pollution	new TG
	Unvalidated Redirects and Forwards	T10 2010: new TG
	SQL Injection	TG
	SQL Fingerprinting	
	LDAP Injection	TG
	ORM Injection	TG
	XML Injection	TG
	SSI Injection	TG

Awareness

Governance

I dieci maggiori rischi delle applicazioni web:

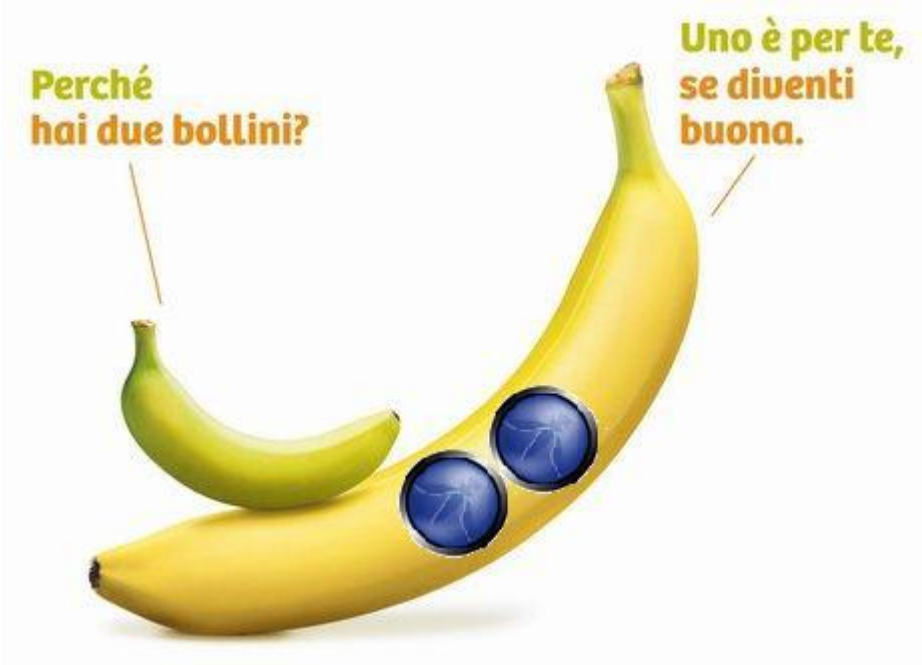
A1: Injection
A2: Cross-Site Scripting (XSS)
A3: Broken Authentication and Session Management
A4: Insecure Direct Object References
A5: Cross-Site Request Forgery (CSRF)
A6: Security Misconfiguration
A7: Insecure Cryptographic Storage
A8: Failure to Restrict URL Access
A9: Insufficient Transport Layer Protection
A10: Unvalidated Redirects and Forwards


OWASP
The Open Web Application Security Project
OWASP Top 10 - 2010
The Ten Most Critical Web Application Security Risks
Versione in Italiano
release

!=

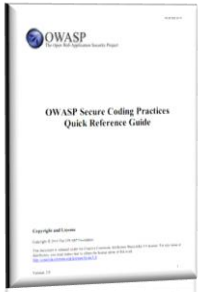

OWASP
OWASP Testing Guide v3.0
release

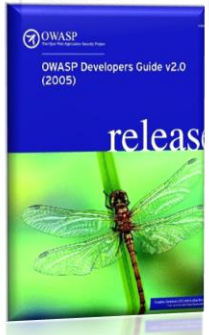
OWASP != Bollini !=certificazioni



Linee guida OWASP nel SDLC

Governance	Construction	Verification	Deployment





OWASP-Italy Next step

- Training, OWASP-Day, AppSec:
  - OWASP Training per luglio 2011
  - OWASP Day per PA Novembre 2011
  - OWASP AppSec 2013
- Iscrivetevi alla mailing list OWASP-it!

http://www.owasp.org/index.php/Italy

- Membership (50$/y)
  - Lista dei membri sul sito OWASP
  - Accesso AppSec (sconto)
  - OWASP Training (free)

Thank you!

http://www.owasp.org
http://www.owasp.org/index.php/Italy
Matteo.meucci@owasp.org