Introduzione all'OWASP-Day II

Matteo Meucci

OWASP-Italy Chair
CEO Minded Security

matteo.meucci@owasp.org

OWASP-Day
Università La Sapienza
Rome
31st March, 2008

The OWASP Foundation
http://www.owasp.org

Who am I?

- Research
  - OWASP-Italy Chair
  - OWASP Testing Guide Lead

- Work
  - CEO @ Minded Security
    Application Security Consulting
  - 7+ years on Information Security
    focusing on Application Security

OWASP-Day II: Stato dell'arte della Web Application Security e OWASP Guideline nelle aziende

- L'OWASP Day:
  - Parte del Global Security Week
  - 19/104 Chapters nel mondo
  - Focus su Application Security

- Quali argomenti?
  - Mostrare i nuovi problemi di sicurezza delle applicazione e come risolverli (Technical)
  - Discutere di come implementare un ciclo di vita del software con controlli di sicurezza (Divulgative)

OWASP Day II: Technical speeches

10.30h	**"SQL Injection tricks: building the bridge between the Web App and the Operating System"** Alberto Revelli - Portcullis Computer Security
11.30h	**"OWASP Backend Security Project"** Carlo Pelliccioni - Spike Reply
14.00h	**"Web Services and SOA Security " (ENG)** Laurent Petroque - F5
15.00h	**"Secure Programming with Static Analysis" (ENG)** Jacob West - Head of Fortify Software's Security Research Group
15.30h	**"The Owasp Orizon project: internals and hands on"** Paolo Perego - Spike Reply

OWASP Day II: Divulgative speeches

10.00h	**"L'approccio di Telecom Italia allo sviluppo sicuro delle applicazioni"** Marco Bavazzano - CISO TELECOM Italia
11.00h	**"Le problematiche di Web Application Security: la visione di ABI Lab"** Matteo Lucchetti - ABI Lab
14.30h	**"How to start a software security initiative within your organization: a maturity based and metrics driven approach."** Marco Morana - OWASP USA Chapter Lead, TISO Citigroup
16.30h	**"Internet Banking and Web Security"** Giorgio Fedon - Minded Security

OWASP Day II: Tavola rotonda

17:00h **Raoul Chiesa** - CTO @ MediaService.net,

Matteo Flora - Security Evangelist,Direttore OPSI,

Marco Morana - OWASP USA Chapter Lead, TISO Citigroup,

Stefano Di Paola - CTO Minded Security,

Paolo Cravino - Senior IT Specialist Rational Software IBM Software Group.

Keynote: **Matteo Meucci**

- La sensibilizzazione degli utenti: leva fondamentale al fine di implementare controlli di sicurezza?
- Come si può implementare un ciclo di vita del software con processi di sicurezza garantendo un adeguato ROSI?

Secure software: sensibilità degli utenti

Software Facts

Expected Number of Users 15
Typical Roles per Instance 4

Amount Per Serving

Modules 155 Modules from Libraries 120

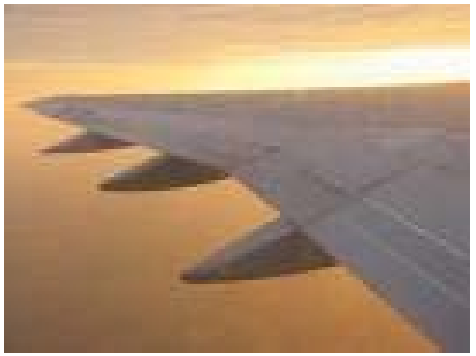
	% Vulnerability*
Cross Site Scripting 22	65%
Reflected 12	15%
Stored 10	
SQL Injection 2	10%
Buffer Overflow 5	95%
Total Security Mechanisms 3	10%
Modularity .035	0%
Cyclomatic Complexity 323	
Encryption 3	
Authentication 15	4%
Access Control 3	2%
Input Validation 233	20%
Logging 33	4%

* % Vulnerability values are based on typical use scenarios for this product. Your Vulnerability Values may be higher or lower depending on your software security needs:

	Usage	Intranet	Internet
Cross Site Scripting	Less Than	10	5
Reflected	Less Than	10	5
Stored	Less Than	10	5
SQL Injection	Less Than	20	2
Buffer Overflow	Less Than	20	2
Security Mechanisms		10	14
Encryption		3	15

Ingredients: Sun Java 1.5 runtime, Sun J2EE 1.2.2, Jakarta log4j 1.5, Jakarta Commons 2.1, Jakarta Struts 2.0, Harold XOM 1.1rc4, Hunter JDOMv1

SDLC, costi e testing



```
public class HelloWorld extends HttpServlet {

    public void doGet(
            HttpServletRequest request,
            HttpServletResponse response)
                    throws IOException, ServletException
    {
            response.setContentType("text/html");
            PrintWriter out = response.getWriter();
            out.println("<HTML><HEAD>");
            out.println("<TITLE>Hello World</TITLE>");
            out.println("</HEAD><BODY>");
            out.println("Hello, " +
    request.getParameter("name"));
            out.println("</BODY></HTML>");
    }

}
```

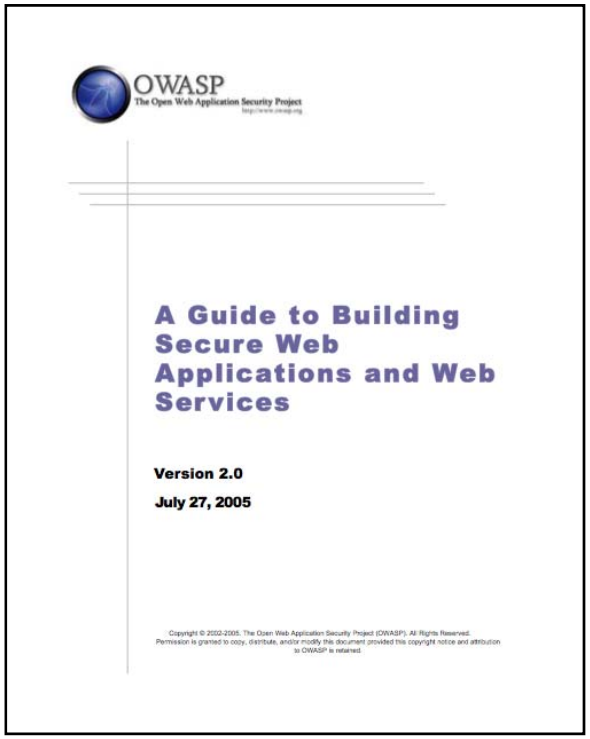
?

SDLC nelle aziende

- A che punto sono la maggioranza delle aziende?
- Quali sono i passi da compiere per migliorare l'aspetto di sicurezza del software
- Usabilità, qualità, sicurezza
- Come può un utente essere certo della sicurezza del proprio servizio di home-banking?
- Cultura, cultura, cultura → sensibilizzazione → richiesta di sicurezza → secure code?

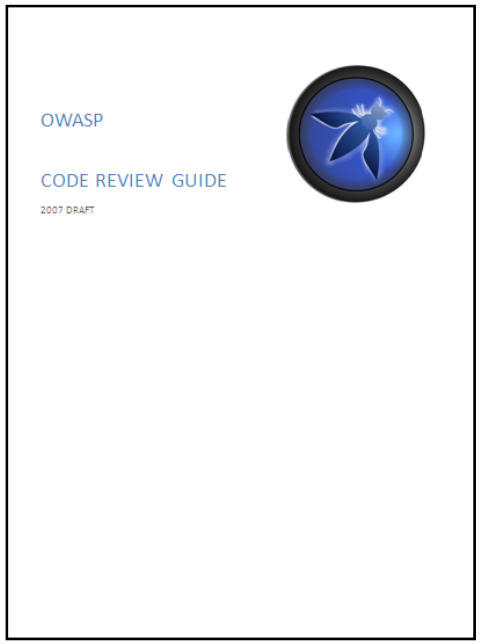
OWASP Building Guide

- 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;



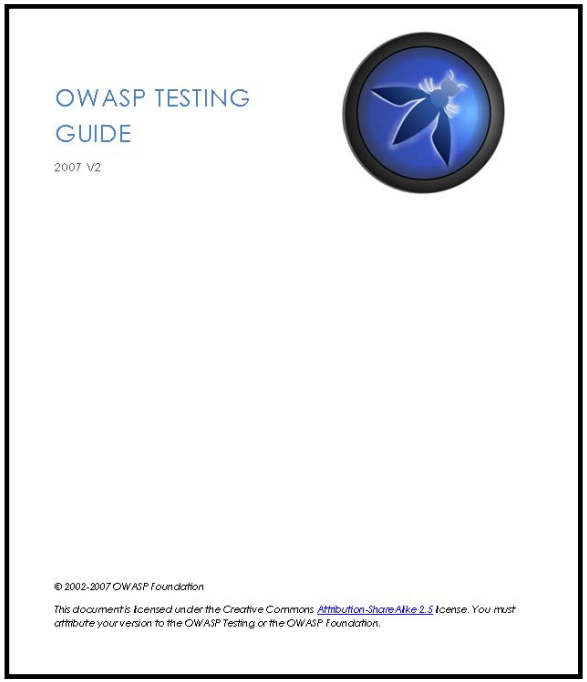
OWASP Code Review Guide

- Descrive la metodologia OWASP per testare il codice di un'applicazione (white box testing)
- Reviewing Code for:
  - Buffer Overruns and Overflows
  - OS Injection
  - SQL Injection
  - Data Validation
  - XSS issues
  - Cross-Site Request Forgery issues
  - Error Handling
  - Logging Issues
  - Secure Code Environment
  - Authorization Issues
  - Authentication
  - Session Integrity issues



OWASP Testing Guide v2

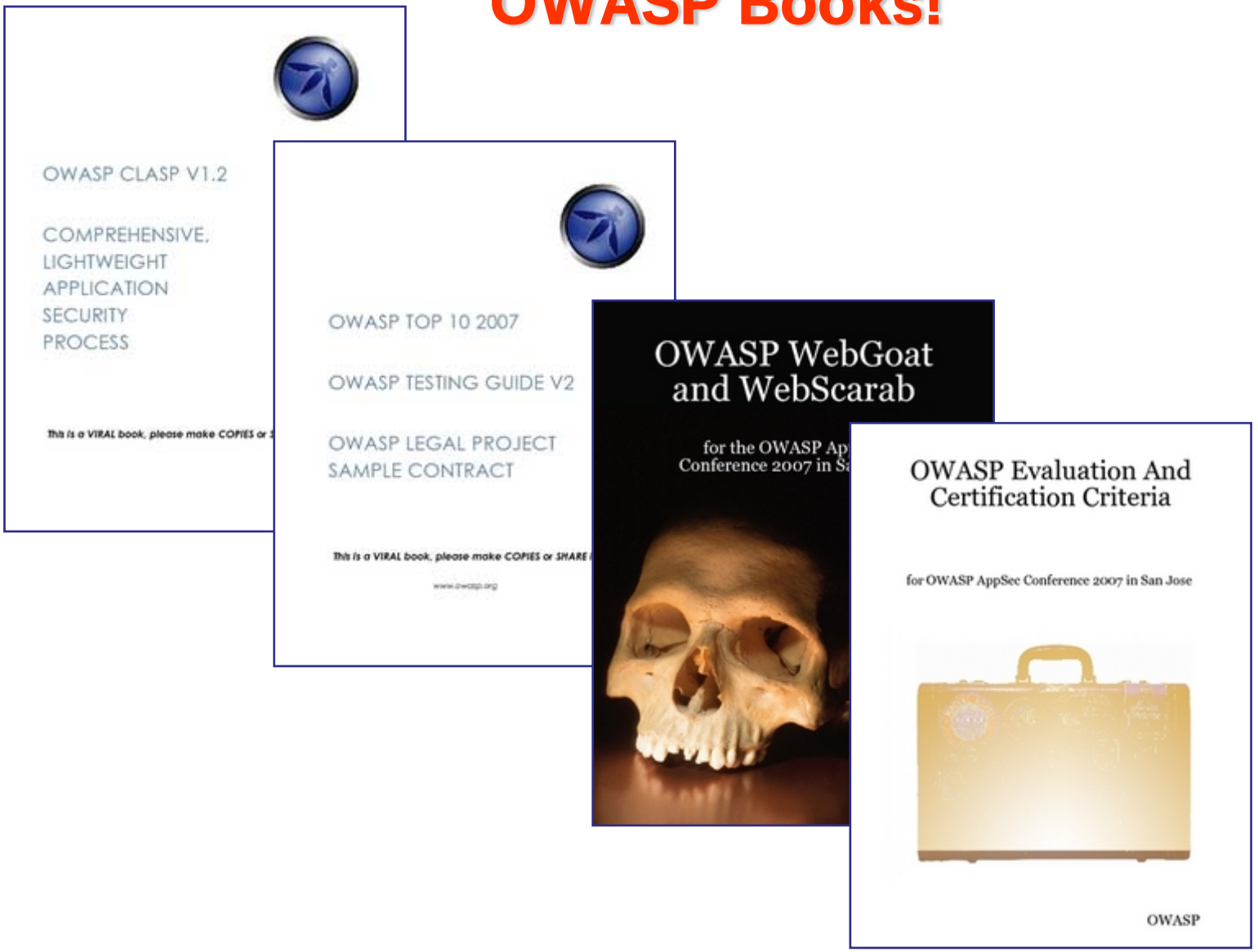
- Descrive la metodologia OWASP per testare un applicativo web
- 272 pagine, 48 controlli
- Approccio della metodologia:
  - Definita
  - Consistente
  - Ripetibile
  - Di qualità



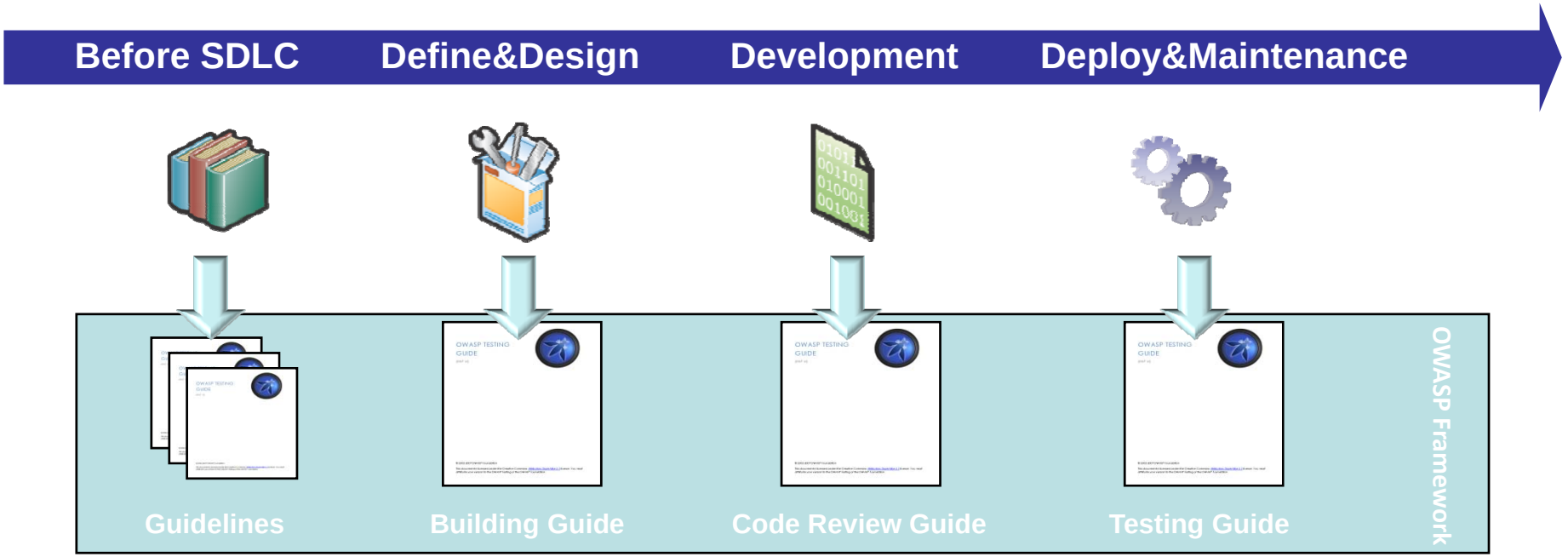
- **SANS Top 20 2007**
- **NIST "Technical Guide to Information Security Testing (Draft)"**

Cita la Testing Guide come referenza per il testing

OWASP Books!


OWASP CLASP V1.2
COMPREHENSIVE, LIGHTWEIGHT APPLICATION SECURITY PROCESS
This is a VIRAL book, please make COPIES or
OWASP TOP 10 2007
OWASP TESTING GUIDE V2
OWASP LEGAL PROJECT SAMPLE CONTRACT
This is a VIRAL book, please make COPIES or SHARE
OWASP WebGoat and WebScarab
for the OWASP Ap
Conference 2007 in S
OWASP Evaluation And Certification Criteria
for OWASP AppSec Conference 2007 in San Jose
OWASP

SDLC & OWASP



OWASP Top10	.NET	Orizon	WebScarab
Web Goat	CSRFGuard	LAPSE	SWF Intruder
	ESAPI		SQL Ninja
			Pantera

Grazie!

Matteo Meucci
matteo.meucci@owasp.org