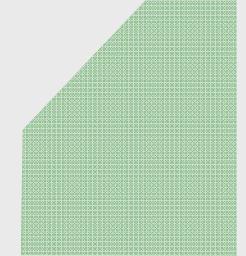




OWASP Day IV: introduzione

Matteo Meucci

OWASP-Italy Chair
CEO Minded Security



OWASP-Italy Day IV
Milan
6th, November 2009

Copyright © 2008 - The OWASP Foundation
Permission is granted to copy, distribute and/or modify this document
under the terms of the GNU Free Documentation License.

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
- ▶ 8+ years on Information Security focusing on Application Security



Minded
— security —

OWASP Day per la PA 2009



consip



OWASP
Italian Chapter

Primo OWASP day per la PA

La sicurezza applicativa come motore per l'e-Gov

Roma 5 novembre 2009, ore 9.30

Auditorium, Via Rieti 13
Roma

Si prega di confermare la propria partecipazione a:
corporateidentity.consip@tesoro.it



La sicurezza applicativa come motore per l'e-Gov

Consip, tramite l'Unità Locale di Sicurezza MEF/Consip ed in collaborazione con OWASP Italy, organizza un evento dedicato alla Pubblica Amministrazione Italiana per discutere delle tematiche di Application Security legate alle iniziative di e-Government. L'importanza dell'evento nasce dalla consapevolezza che senza la garanzia del rispetto di adeguati livelli di sicurezza non è possibile trasferire nel mondo virtuale i processi 'core' per un nuovo rapporto tra PA e utenti.

PROGRAMMA

Chairman: R. Flamini, Direttore Infrastrutture IT
Consip

- | | |
|-------|---|
| 9.30 | <i>Introduzione all'evento</i>
D. Broggi, Amministratore Delegato - Consip |
| 9.45 | <i>OWASP e gli standard per la sicurezza delle applicazioni</i>
M. Meucci - OWASP - Italy Chair, OWASP Testing Guide Lead |
| 10.15 | <i>L'approccio di Consip alla sicurezza applicativa</i>
M. Cavallini - Responsabile Struttura Operativa ULS MEF/Consip |
| 10.45 | Coffee Break |
| 11.00 | <i>How to start a software security initiative within your organization: a maturity based and metrics driven approach</i>
M. Morana - TISO Citigroup |
| 11.30 | <i>L'analisi di sicurezza delle applicazioni web: come realizzare un processo nella PA</i>
S. Di Paola - R&D Director OWASP-Italy |
| 12.00 | <i>Le nuove sfide per la sicurezza applicativa in scenari federati</i>
M. Fontana - Responsabile Sicurezza Applicativa Microsoft Italia |
| 12.30 | <i>La criminalità su Internet e la sicurezza applicativa</i>
T. Palumbo - Responsabile CNAIPIC |



OWASP - Italy Day IV

"Secure Software Initiatives"

6th NOVEMBER 2009, MILAN

9:00	Registration
9:30	"Introduction to the OWASP-Day" Matteo Meucci - OWASP-Italy Chair
9:50	"How to Create Business cases for Your Software Security Initiative" Marco Morana — CISO, Citigroup
10:30	"OWASP SAMM / Open Software Assurance Maturity Model" Claudio Merloni — Software Security Consultant, Fortify Software
11:10	Coffee break
11:40	"From Web Attacks to Malware. Can Secure Software Development Help Internet Banking Security?" Giorgio Fedon — COO, Minded Security
12:20	"Usability versus security: securing Internet facing applications while keeping them highly attractive for everybody" (ENG) Tobias Christen — CTO, DSwiss Ltd
13:00	Business Lunch
14:00	"NoScript, CSP and ABE: When the Browser Is Not Your Enemy" Giorgio Maone — CTO, InformAction
14:40	"Building Security In Maturity Model: A Review of Successful Software" (ENG) Gabriele Giuseppini — Technical Manager, Digital
15:20	"The art of code reviewing" Paolo Perego — Senior Consultant, Spike Reply
16:00	Round Table: Why Software Security is not a priority in our digital world? M. Morana, C. Merloni, G. Giuseppini, S. Di Paola, M.Bregolin — Keynote R. Chiesa



Certificazione CSSLP di ISC²

(ISC)² Security Transcends Technology - Mozilla Firefox

File Modifica Visualizza Cronologia Segnalibri Strumenti Ajuto

http://www.isc2.org/csslp-register

Più visitati Ultime notizie AppSec Feed My Security Planet OWASP Security Podc... Twitter / OWASPItaly Phoenix/Tools - OWASP SANS SANS: The Top Cyber ... Flight search re

(ISC)² Security Transcends Technolo...

(ISC)² SECURITY TRANSCENDS TECHNOLOGY®

Username: Password:

Forgot Password? Login Help Sign In

Home Education Certification Programs Career Tools Events Industry Resources About (ISC)² Blog

Official (ISC)² Review Seminars CSSLP Education Program Live OnLine Candidate Information Bulletin Education Affiliates Learning Tools Voucher

I am interested in: select below Site Search Search

Home ▶ Education ▶ CSSLP Education Program ▶ Register for CSSLP

Register for CSSLP Education Seminar:

1. Select Seminar location & date (Contact us if there's not a location convenient for you.)
2. Create your (ISC)² account
3. Agree to Terms & Conditions
4. Submit payment

Seminar Pricing
Seminar pricing is based on the location of the actual event site. Download the Seminar Pricing List for details.

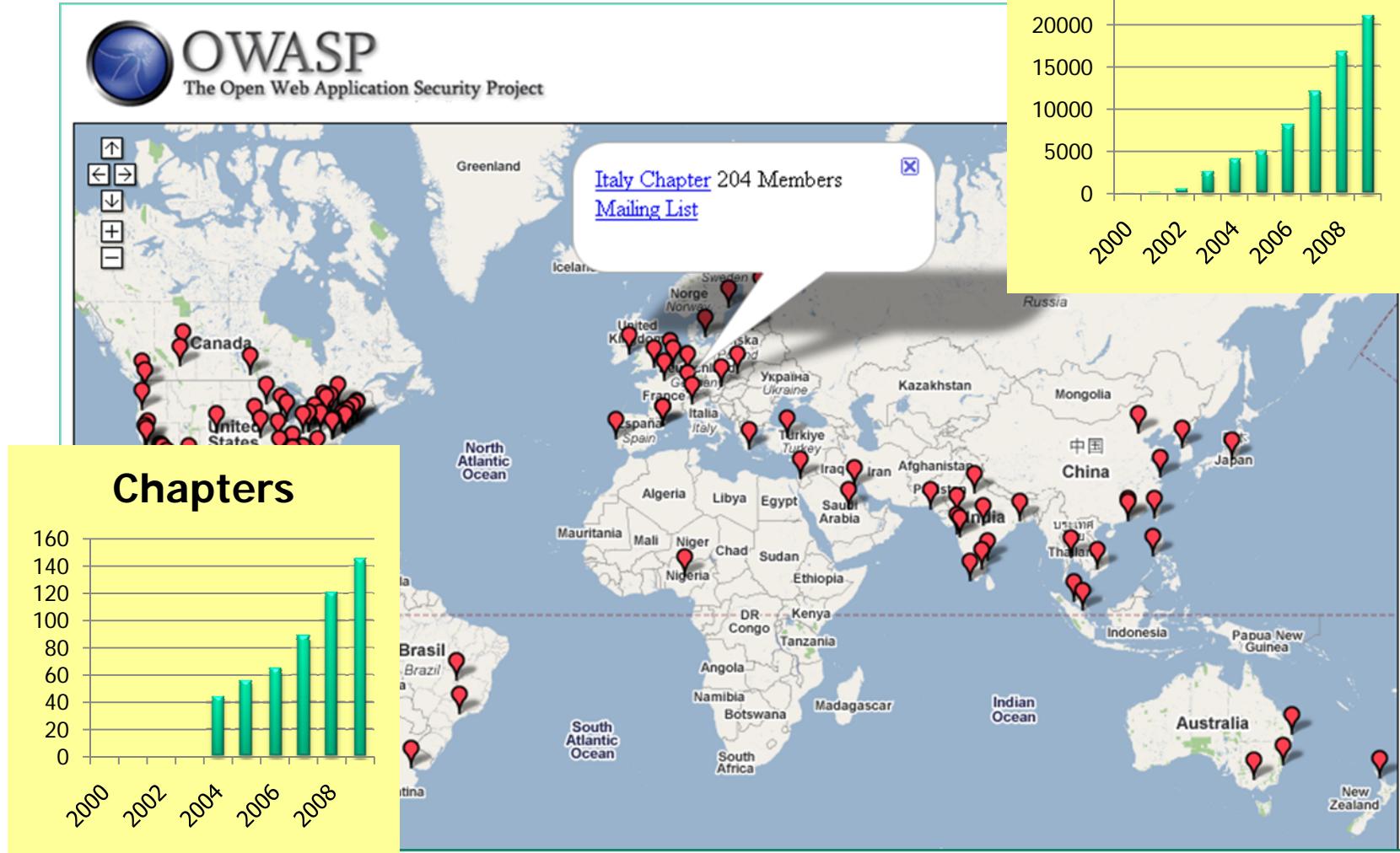
To Pay by Check or Money Order:

1. Download one of the following Seminar Forms:
■ 2009 US Seminar Form (PDF)
■ 2009 Non-US Seminar Form (PDF)

OWASP: The Open Web Application Security Project

- Il progetto Open Web Application Security Project (OWASP) è una organizzazione Open Source dedicata alla creazione e alla diffusione di una cultura per quanto riguarda la sicurezza delle applicazioni web
- Progetto free, come il materiale disponibile sul portale www.owasp.org
- Migliaia di membri, +100 capitoli locali e altri partecipanti ai progetti. Milioni di hit su www.owasp.org al mese
- Defense Information Systems Agency (DISA) , US Federal Trade Commission (FTC), VISA, Mastercard, American Express e molte aziende in Italia hanno adottato la documentazione OWASP nei loro standard e linee guida

OWASP Worldwide Community

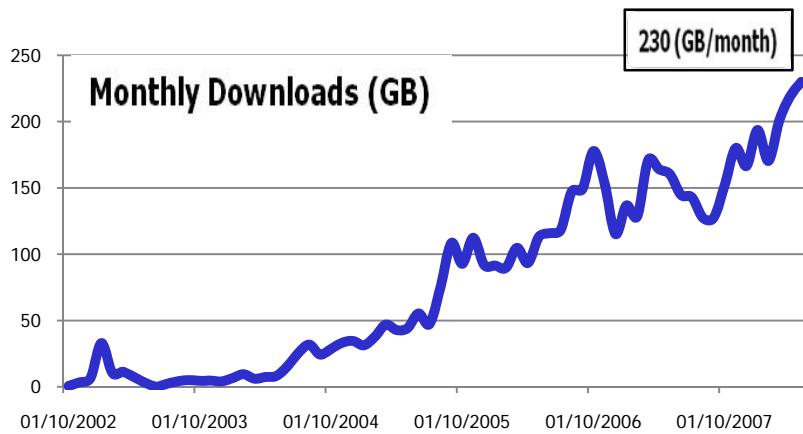


OWASP Dashboard

Worldwide Users



Most New Visitors



La base di conoscenza di OWASP



- 6,381 Articoli
- 427 presentazioni
- 200 aggiornamenti/giorno
- 271 mailing lists
- 180 blog monitorati



OWASP-Italy Day IV - Oct, Nov 09

OWASP



OWASP Top Ten

www.owasp.org/index.php?title=Top_10_2007

A1: Cross Site Scripting (XSS)

A2: Injection Flaws

A3: Malicious File Execution

A4: Insecure Direct Object Reference

A5: Cross Site Request Forgery (CSRF)

A6: Information Leakage and Improper Error Handling

A7: Broken Authentication and Session Management

A8: Insecure Cryptographic Storage

A9: Insecure Communications

A10: Failure to Restrict URL Access



OWASP

The Open Web Application Security Project
<http://www.owasp.org>



OWASP-Italy Day 11 – 6th, Nov 09



Linee Guida OWASP

- Gratuite e open source
- Libri a basso costo
- Coprono tutti i controlli di sicurezza
- Centinaia di esperti
- Tutti gli aspetti di sicurezza applicativa



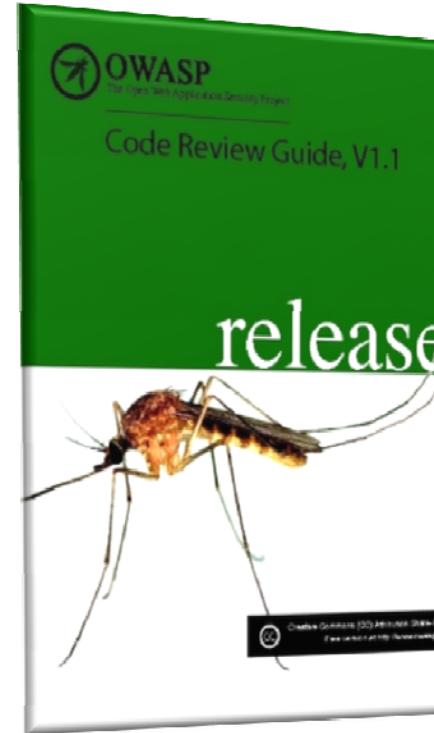
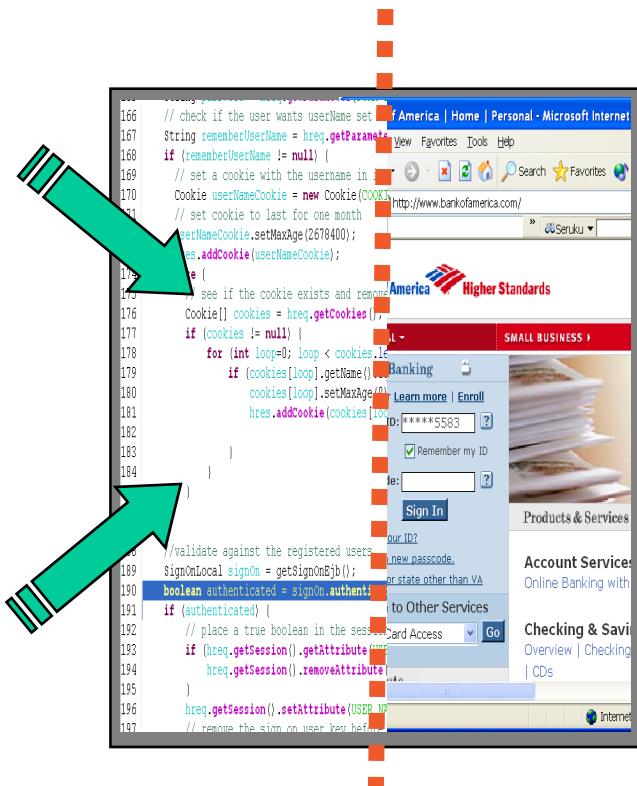
OWASP Building Guide

- 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;



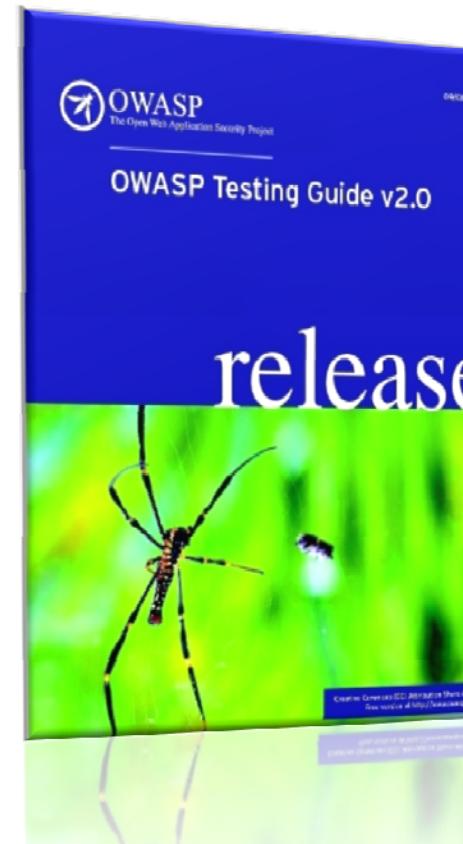
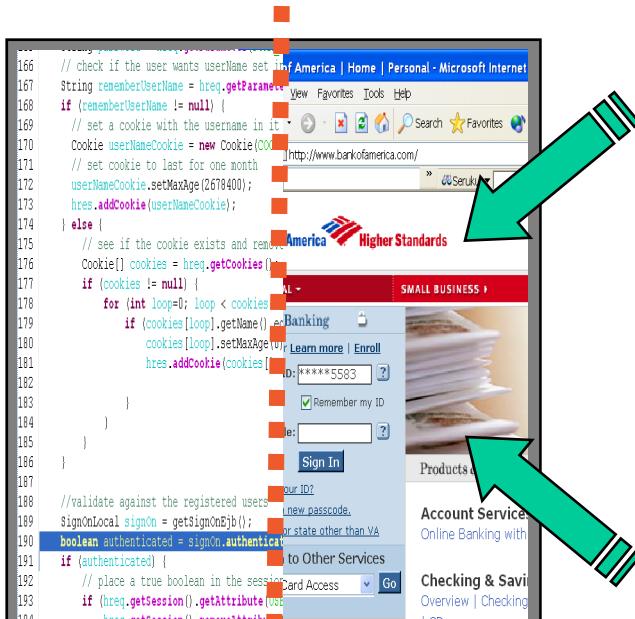
OWASP Code Review Guide

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



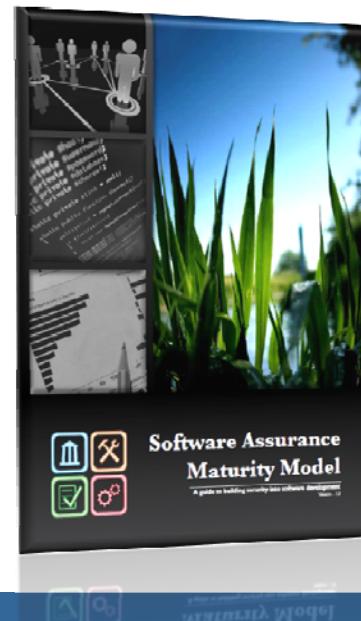
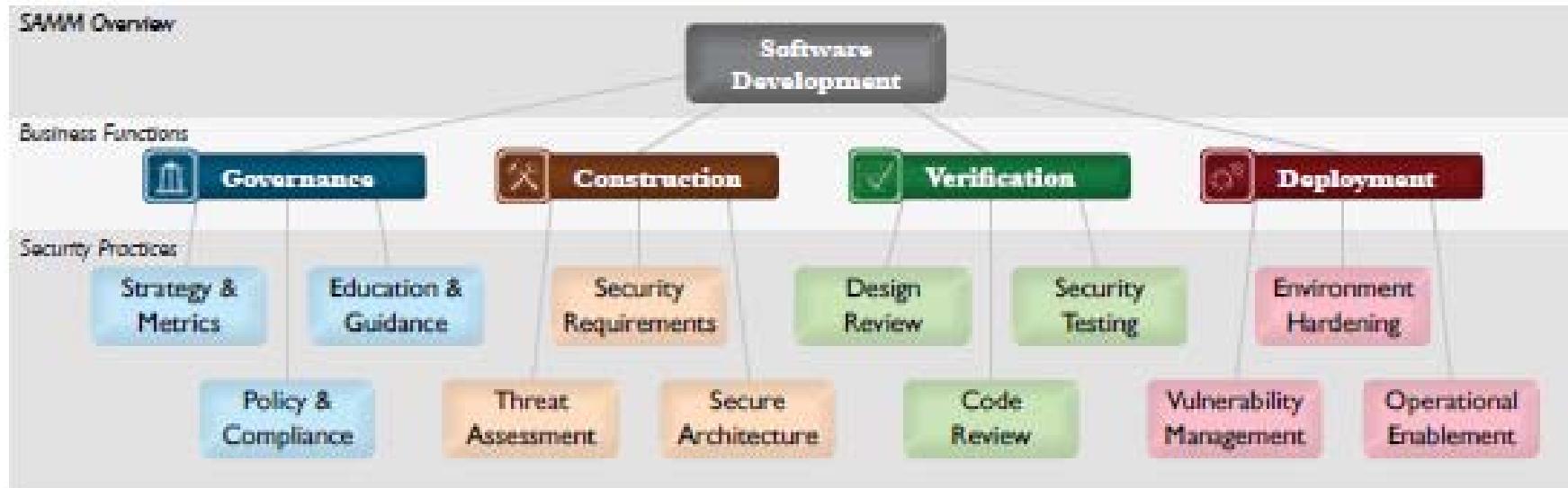
OWASP Testing Guide

- Descrive la metodologia OWASP per testare la sicurezza di un applicativo web



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

OWASP Software Assurance Maturity Model



OWASP WebGoat

The screenshot shows a Microsoft Internet Explorer window with the title "Bypass a Path Based Access Control Scheme - Microsoft Internet Explorer". The address bar contains "http://localhost/WebGoat/attack?Screen=5&menu=210". The page features a red background with a goat logo on the left. The main content area has a header "Bypass a Path Based Access Control Scheme" and a sub-header "OWASP WebGoat V5.1". Below this are several navigation links: "Admin Functions", "General", "Code Quality", "Concurrency", "Unvalidated Parameters", "Access Control Flaws", "Using an Access Control Matrix", "Bypass a Path Based Access Control Scheme" (which is underlined and bolded), "LAB: Role Based Access Control", "Stage 1: Bypass Business Layer Access Control", "Stage 2: Add Business Layer Access Control", "Stage 3: Bypass Data Layer Access Control", "Stage 4: Add Data Layer Access Control", "Remote Admin Access", "Authentication Flaws", "Session Management Flaws", "Cross-Site Scripting (XSS)", "Buffer Overflows", "Injection Flaws", "Improper Error Handling", "Insecure Storage", "Denial of Service", "Insecure Configuration", and "Web Services". A "Hints" button is also present. To the right, there is a "Logout" link and a "Restart this Lesson" button. The central part of the page displays a list of files in a dropdown menu: "AccessControlMatrix.html", "BackDoors.html", "BasicAuthentication.html", "BlindSqlInjection.html", "BufferOverflow.html", "ChallengeScreen.html", "ClientSideFiltering.html", "ClientSideValidation.html", "CommandInjection.html", "ConcurrencyCart.html", "CrossSiteScripting.html", "CSRF.html", "DangerousEval.html", "DBCrossSiteScripting.html", and "DBSQLInjection.html". A "View File" button is located next to the list. At the bottom, a status bar says "Viewing file: C:\WebGoat-5.1\tomcat\webapps\WebGoat\lesson_plans" and "Local intranet".

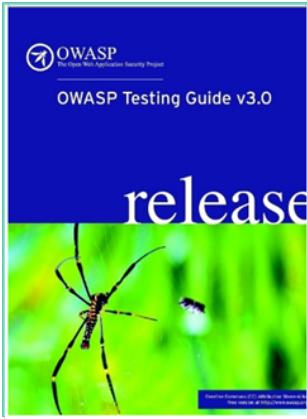
OWASP WebScarab

The screenshot shows the OWASP WebScarab application window. The menu bar includes File, View, Tools, and Help. The toolbar below the menu contains buttons for Summary, Message log, Proxy, Manual Request, WebServices, Spider, Extensions, SessionID Analysis, Scripted, Fragments, Fuzzer, Compare, and a dropdown menu. The main interface has a tab bar with 'Summary' selected, followed by 'Tree Selection filters conversation list'. The 'Summary' tab displays a tree view of URLs under 'http://www.owasp.org:80/'. One entry for 'index.php/Main_Page' is expanded, showing a GET request with status 200 OK. The 'Tree Selection filters conversation list' tab shows a table of network conversations:

ID	Date	Method	Host	Path	Parameters	Status	Origin
5	2006/06/23...	GET	http://www.owasp.org:80/	/skins/monobook/main....?7		200 OK	Proxy
4	2006/06/23...	GET	http://www.owasp.org:80/	/skins/common/IEFixes...		200 OK	Proxy
3	2006/06/23...	GET	http://www.owasp.org:80/	/skins/common/commo...		200 OK	Proxy
2	2006/06/23...	GET	http://www.owasp.org:80/	/index.php/Main_Page		200 OK	Proxy
1	2006/06/23...	GET	http://www.owasp.org:80/	/		301 Moved ...	Proxy

A progress bar at the bottom indicates 5.27 / 63.66.

Principali progetti OWASP



BOOKS

- Owasp top10
- Building guide
- Code review guide
- Testing guide



TOOLS

- WebGoat
- WebScarab
- SQLMap – SQL Ninja
- SWF Intruder
- Orizon
- Code Crawler



Il ciclo di vita del software e la sicurezza

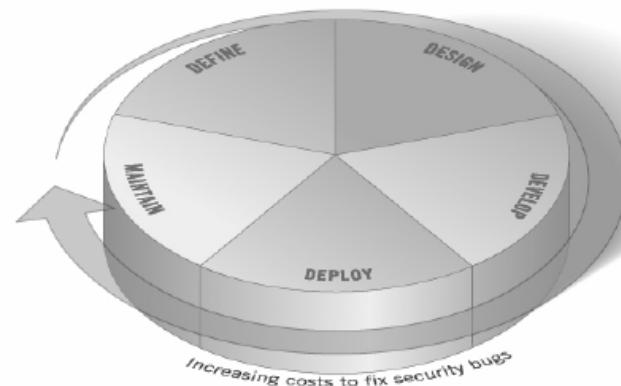
Il ciclo di vita del software

- Il Ciclo di Vita del Software (Software Development Life Cycle, SDLC) comprende :

- ▶ Define
- ▶ Design
- ▶ Develop
- ▶ Deploy
- ▶ Maintain

- Quali processi implementare?

- ▶ Awareness
- ▶ Secure Code Guidelines
- ▶ Code Review
- ▶ Application Testing



SDLC & OWASP Guidelines e tools

