



OWASP Foundation Inc.

Overview Version 2.0
May 25th 2009

OWASP

Copyright © - 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>

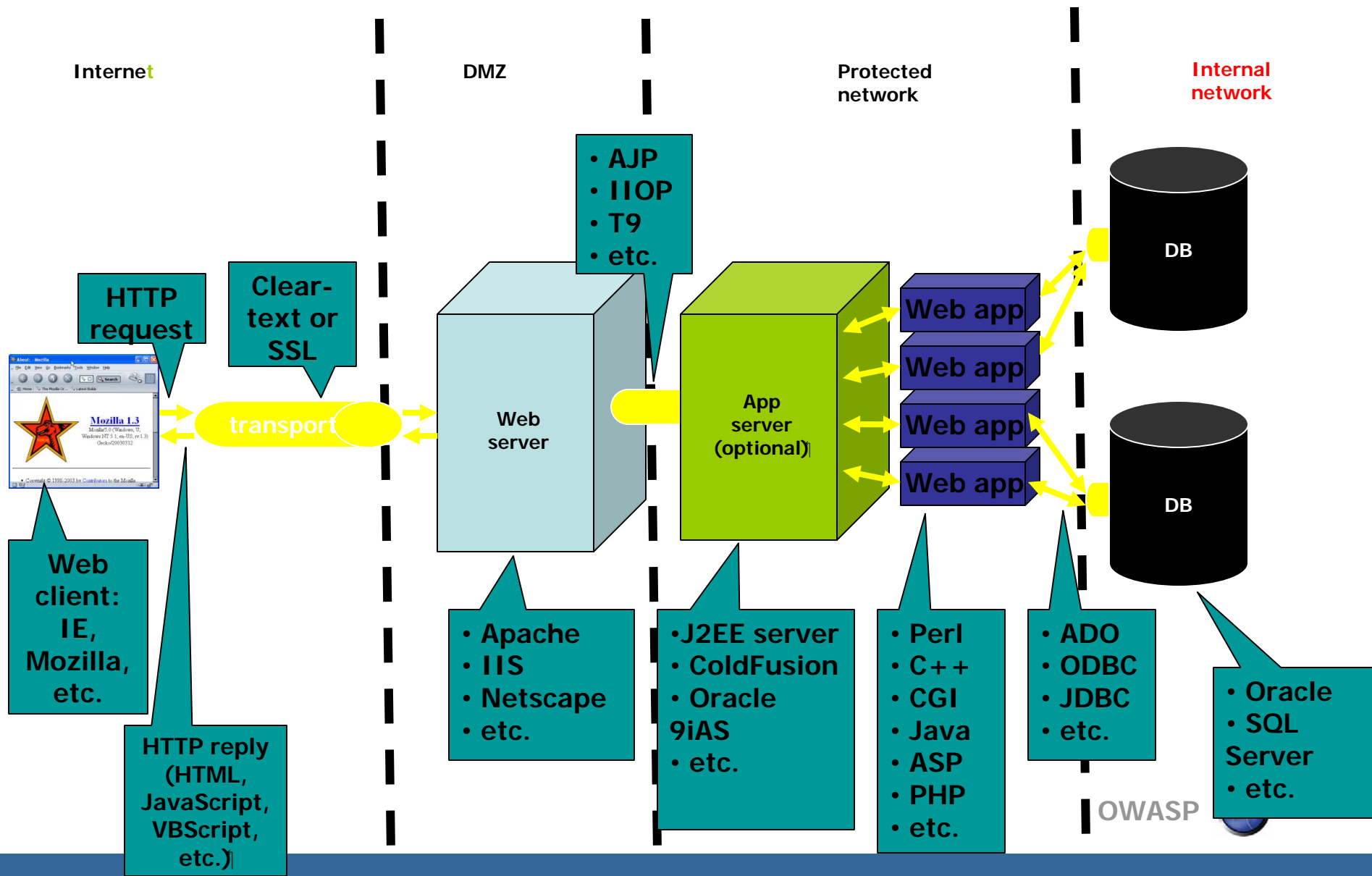
Agenda

- OWASP Introduction
- OWASP Project Parade
- OWASP Near You?

Agenda

- OWASP Introduction
- OWASP Project Parade
- OWASP Near You?

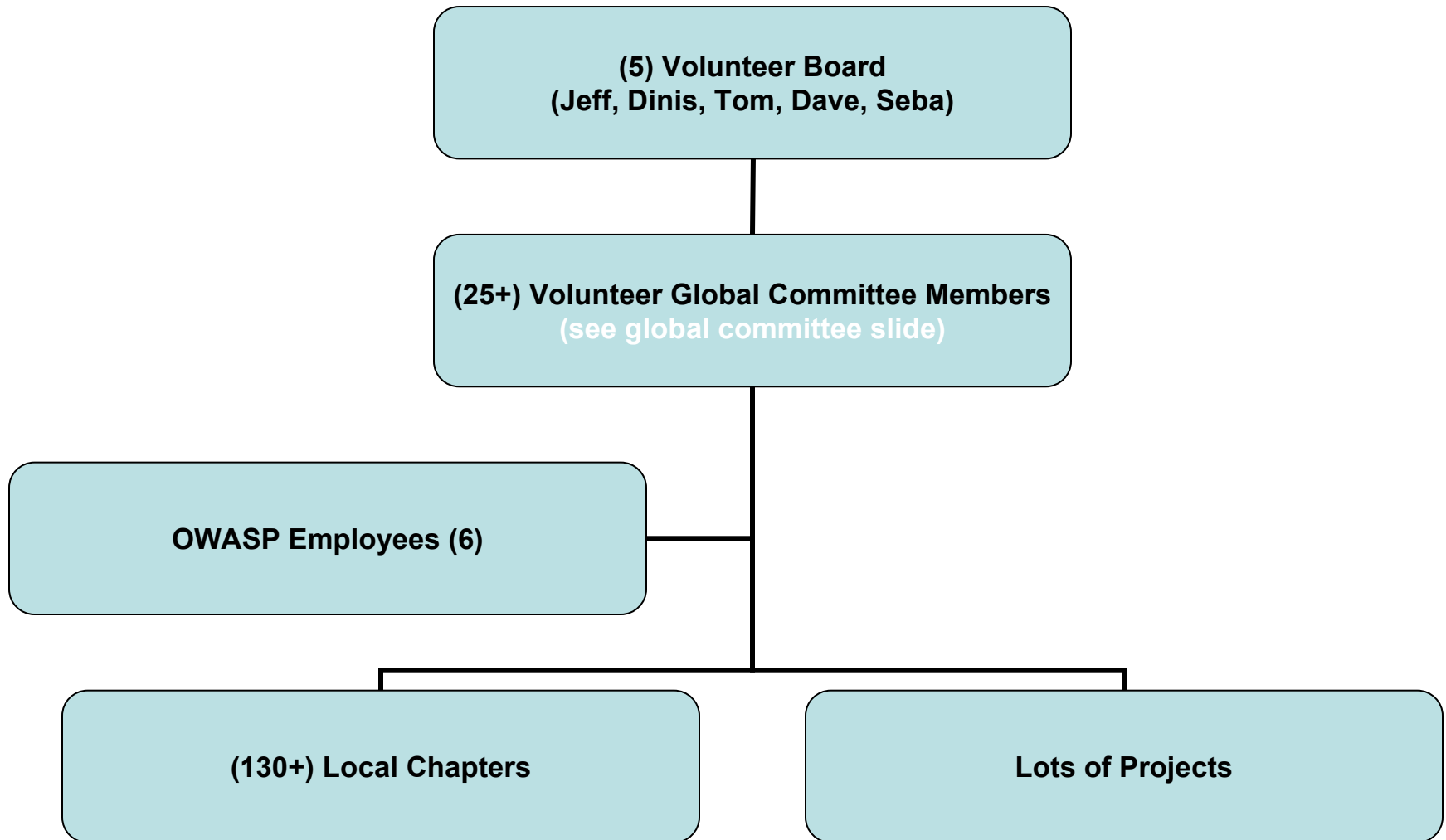
Web Applications



OWASP

- The Open Web Application Security Project (OWASP Foundation Inc.) established 2001'. The vision is a software market that produces code that's secure enough to rely on.
- The mission (to achieve that vision) is to make security visible (or transparent) so that software buyers and sellers are on equal footing and market forces can work.
- International not-for-profit charitable organization funded primarily by volunteers time, OWASP Memberships (\$50 Individuals, \$5k Supporters), and OWASP Conference fees
- **Website: 6,464 registered users, 21,552,771 page views, and 55,941 page edits**
- Participation in OWASP is free and open to all

OWASP FOUNDATION INC. - 501(3)c



Global Committee

OWASP GLOBAL COMMITTEES					
Projects	Membership	Education	Conferences	Industry	Chapters
<ul style="list-style-type: none"> ▪ Dinis Cruz ▪ Jason Li ▪ Matt Tesauro ▪ Leo Cavallari ▪ Pravir Chandra 	<ul style="list-style-type: none"> ▪ Tom Brennan ▪ Dan Cornell ▪ Michael Coates 	<ul style="list-style-type: none"> ▪ Seba Deleersnyder ▪ Martin Knobloch <ul style="list-style-type: none"> ▪ Mano Paul ▪ Eduardo Neves ▪ Kuai Hinjosa <ul style="list-style-type: none"> ▪ Cecil Su ▪ Fabio Cerullo ▪ Andrzej Targosz 	<ul style="list-style-type: none"> ▪ Kate Hartmann ▪ Wayne Huang ▪ Steve Antoniewicz <ul style="list-style-type: none"> ▪ Dhruv Soi ▪ Mark Bristow 	<ul style="list-style-type: none"> ▪ Tom Brennan ▪ Rex Booth ▪ Georg Hess ▪ Eoin Keary ▪ David Campbell ▪ Colin Watson 	<ul style="list-style-type: none"> ▪ Seba Deleersnyder ▪ Puneet Mehta ▪ Ofer Shezaf ▪ Justin Derry

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

2009 Supporters

 acunetix

 ascure

 ASPECT SECURITY
Application Security Specialists

 art defence

 BEST BUY

Booz | Allen | Hamilton

 BREACH

 CENZIC

 cigital

 City Guilds

 CorporateOne

 DENIM GROUP

 denyall
SECURITY SOLUTIONS

 ETS
Listening. Learning. Leading.®

 fishnet
SECURITY

 GOTHAM
DIGITAL SCIENCE

 HARRIS CONNECT

 hp
invent

 Hurricane
LABS

 IMPERVA

 INFOVISION

 (ISC)²

 Microsoft

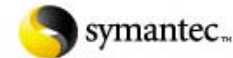
 mnemonic

 NOKIA

 protiviti
Independent Risk Consulting

 SECURE SOLVE

 SOGETI

 symantec™

Educational Supporters of OWASP's mission

 GEORGIA TECH INFORMATION SECURITY CENTER

 THE UNIVERSITY OF TEXAS
HEALTH SCIENCE CENTER AT HOUSTON



 NKU NORTHERN
KENTUCKY
UNIVERSITY

 NORTH TEXAS

 THE GEORGE
WASHINGTON
UNIVERSITY
WASHINGTON DC

 FACULTAD
DE INGENIERIA
Universidad de Buenos Aires

 UCLA



OWASP Mission

The mission is to make security visible (or transparent) so that software buyers and sellers are on equal footing and market forces can work.



OWASP Resources and Community

Documentation (Wiki and Books)

- Code Review, Testing, Building, Legal, more ...

Code Projects

- Defensive, Offensive (Test tools), Education, Process, more ...

Chapters

- Over 130 and growing

Conferences

- Major and minor events all around the world



navigation

- [Home](#)
- [News](#)
- [OWASP Projects](#)
- [Downloads](#)
- [Local Chapters](#)
- [Global Committees](#)
- [AppSec Job Board](#)
- [AppSec Conferences](#)
- [Presentations](#)
- [Video](#)
- [Get OWASP Books](#)
- [Get OWASP Gear](#)
- [Mailing Lists](#)
- [About OWASP](#)
- [Membership](#)

reference

- [How To...](#)
- [Principles](#)
- [Threat Agents](#)
- [Attacks](#)
- [Vulnerabilities](#)
- [Controls](#)
- [Activities](#)
- [Technologies](#)
- [Glossary](#)
- [Code Snippets](#)
- [.NET Project](#)
- [Java Project](#)

language

- [English](#)
- [Español](#)

[article](#) [discussion](#) [view source](#) [history](#)

Main Page



Ad Space Available for 2009

Welcome to OWASP

the free and open application security community

- | | | | |
|-----------------------------|----------------------------|-------------------------------------|-------------------------------|
| ■ Top Ten | ■ ESAPI | ■ Development Guide | ■ CLASP |
| ■ WebGoat | ■ ASVS | ■ Code Review Guide | ■ Contracting |
| ■ WebScarab | ■ AntiSamy | ■ Testing Guide | ■ More... |

[About](#) · [Searching](#) · [Editing](#) · [New Article](#) · [OWASP Categories](#)

[Statistics](#) · [Recent Change](#)

The Open Web Application Security Project (OWASP) is a worldwide free and open community focused on improving the security of application software. Our mission is to make application security "visible," so that people and organizations can make informed decisions about application security risks. Everyone is free to participate in OWASP and all of our materials are available under a free and open software license. The OWASP Foundation is a 501c3 not-for-profit charitable organization that ensures the ongoing availability and support for our work.



You'll find everything [about OWASP](#) here on our wiki. Please feel free to make changes and improve our site. There are hundreds of people around the globe who review the

Special Announcements

- Feb 24 OWASP Software Assurance Day is free! March 13th at DHS Forum in Northern Virginia..
- Feb 23 OWASP traffic is steadily increasing. Our biggest one day in history on 2/10/2009. Fast approaching 500,000 page views a month.
- Feb 23 OWASP Podcast #8 and #9 are live! Two-part appsec newscast.
- Feb 19 OWASP France Call for Papers (CFP).
- Feb 13 OWASP Podcast #7 - Jeff talks about OWASP, ESAPI, XSS prevention, and responds to McGraw.
- Feb 10 Jeff Williams just wrote ClickjackFilter. A Java EE filter to protect against clickjacking using X-FRAME-OPTIONS.
- Feb 07 Aspect just donated a new tool "Scrubbr" to OWASP. Check your databases for XSS stored in there and clean it up.
- Feb 06 ModSecurity Core Rule Set is moving to OWASP! Let's grow an awesome set of rules!



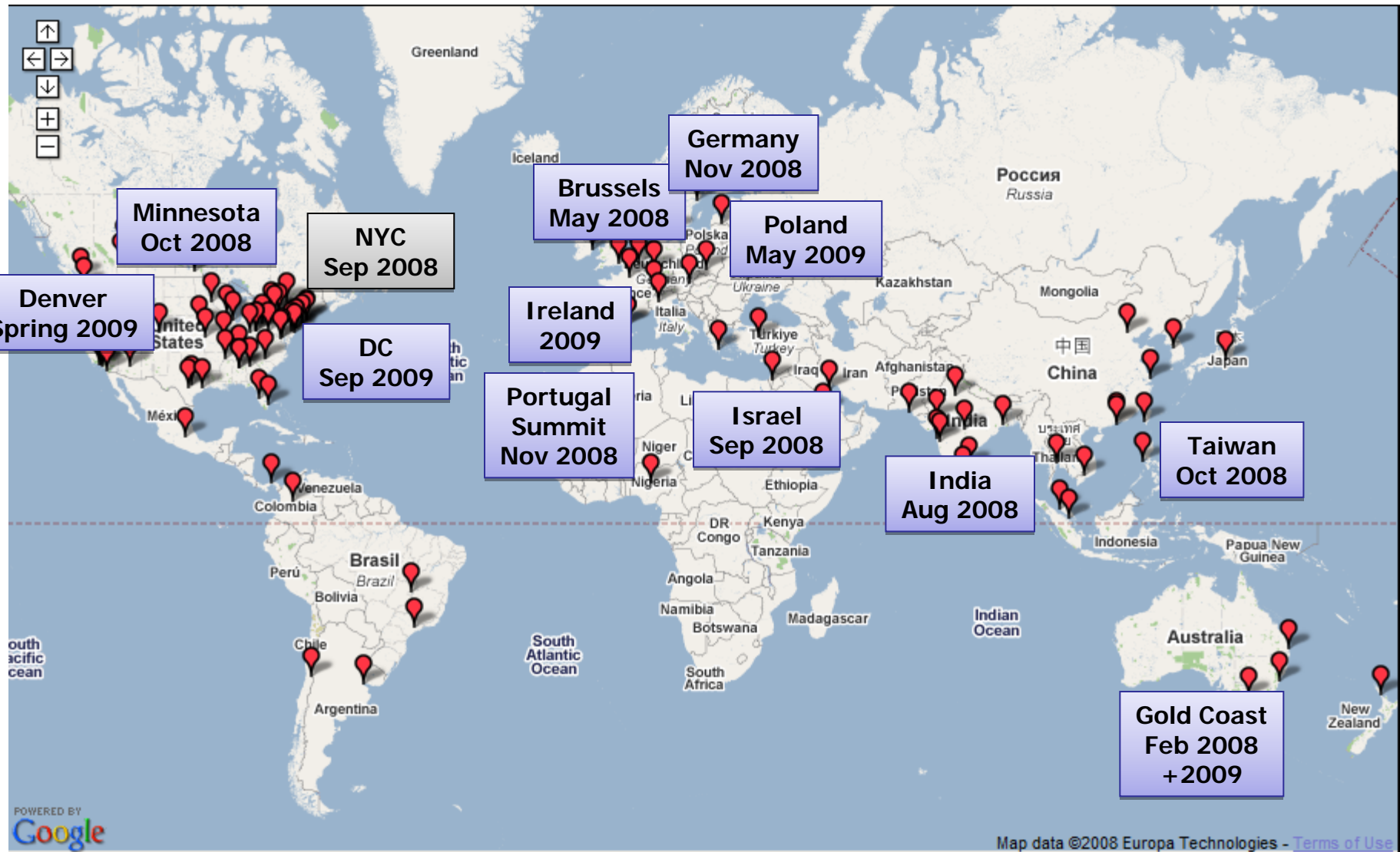
Special

OWASP Application Security Research Grants

130+ Chapters Worldwide



OWASP Conferences (2008-2009)



POWERED BY
Google

Map data ©2008 Europa Technologies - [Terms of Use](#)



Summit Portugal



■ 2009 Focus

- ▶ 80+ application security experts from 20+ countries

■ New Free Tools and Guidance (SoC08)

■ New Outreach Program

- ▶ technology vendors, framework providers, and standards bodies
- ▶ new program to provide free one- day seminars at universities and developer conferences worldwide

■ New Global Committee Structure

- ▶ Education, Chapter, Conferences, Industry, Projects, Membership

Agenda

- OWASP Introduction
- OWASP Project Parade
- OWASP Near You?

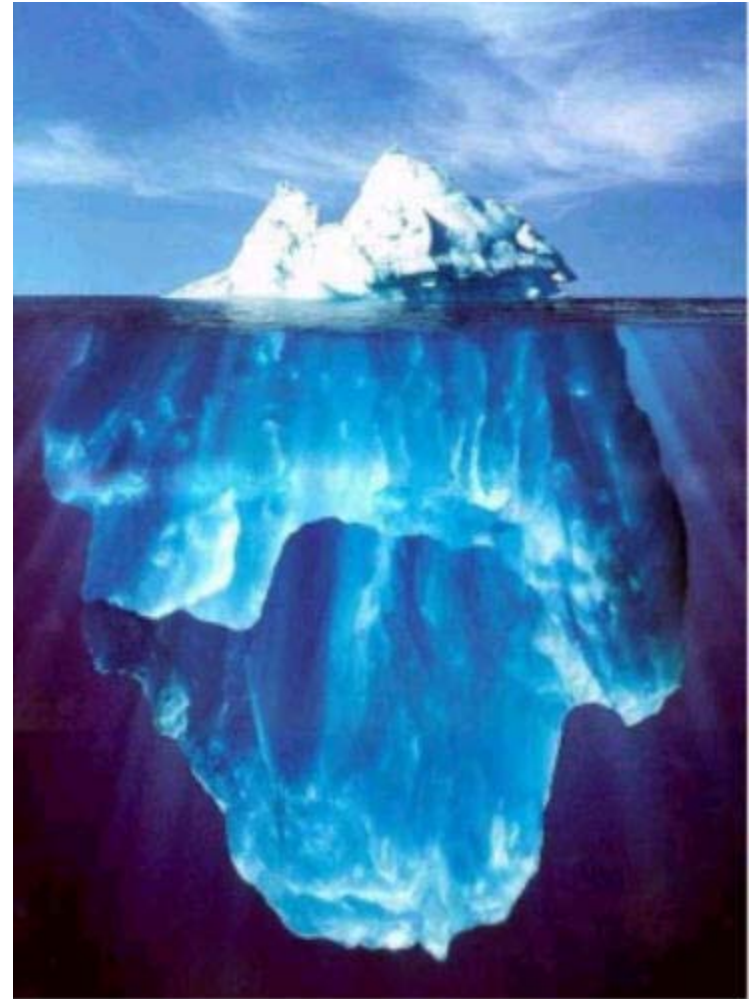
OWASP Projects: Improve Quality and Support

- Define Criteria for Quality Levels
 - ▶ Alpha, Beta, Release
- Encourage Increased Quality
 - ▶ Through Season of Code Funding and Support
 - ▶ Produce Professional OWASP books
- Provide Support
 - ▶ Full time executive director (Kate Hartmann)
 - ▶ Full time project manager (Paulo Coimbra)
 - ▶ Half time technical editor (Kirsten Sitnick)
 - ▶ Half time financial support (Alison Shrader)
 - ▶ Looking to add programmers (Interns and professionals)



OWASP Top 10

- The Ten Most Critical Web Application Security Vulnerabilities
 - Vulnerabilities
- 2007 Release
- A great start, but not a standard
- 3rd version of the Top 10 2009 coming soon
 - *HelpWanted*



Key Application Security Vulnerabilities

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>

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



The 'Big 4' Documentation Projects

**Building
Guide**

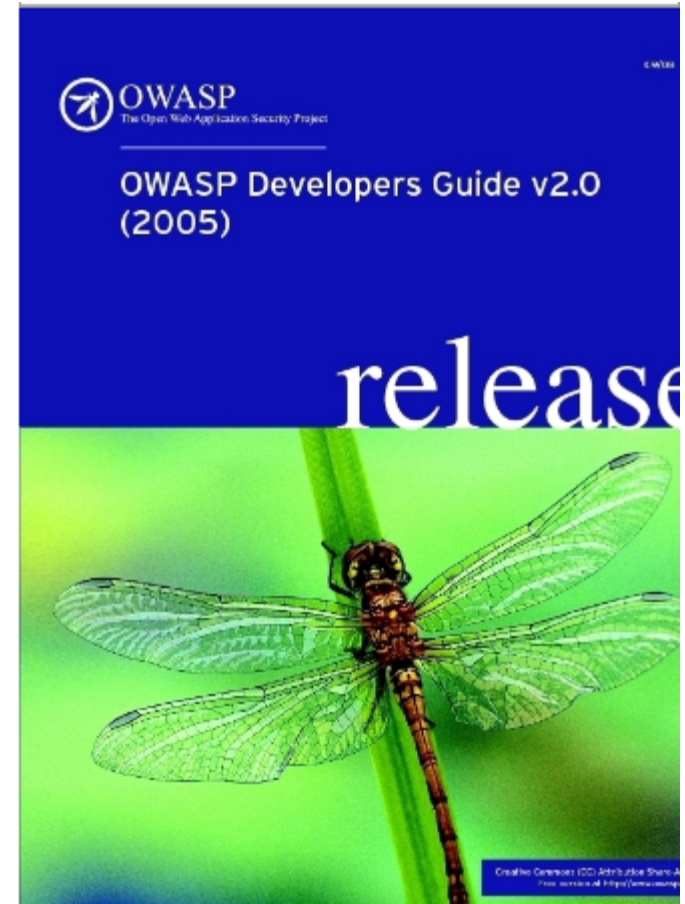
**Code
Review
Guide**

**Testing
Guide**

**Application Security Desk Reference
(ASDR)**

The Guide

- Complements OWASP Top 10
- 310p Book
- Free and open source
 - ▶ Gnu Free Doc License
- Many contributors
- Apps and web services
- Most platforms
 - ▶ Examples are J2EE, ASP.NET, and PHP
- Comprehensive
- Project Leader and Editor
 - ▶ Andrew van der Stock,
vanderaj@owasp.org



Uses of the Guide

■ Developers

- ▶ Use for guidance on implementing security mechanisms and avoiding vulnerabilities

■ Project Managers

- ▶ Use for identifying activities (threat modeling, code review, penetration testing) that need to occur

■ Security Teams

- ▶ Use for structuring evaluations, learning about application security, remediation approaches

Each Topic

- Includes Basic Information (like OWASP T10)

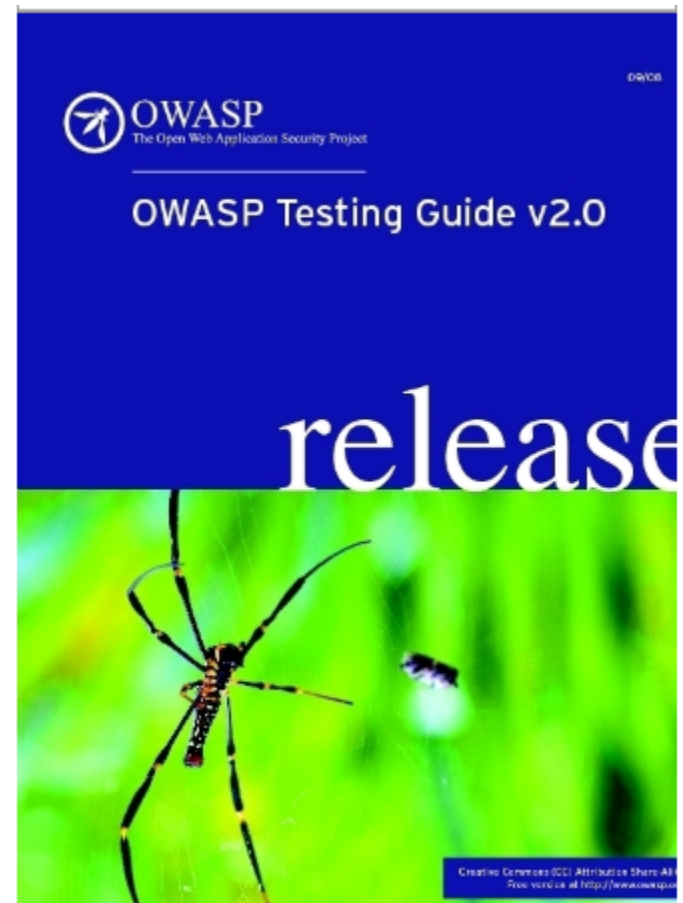
- ▶ How to Determine If You Are Vulnerable
- ▶ How to Protect Yourself

- Adds

- ▶ Objectives
- ▶ Environments Affected
- ▶ Relevant COBIT Topics
- ▶ Theory
- ▶ Best Practices
- ▶ Misconceptions
- ▶ Code Snippets


Testing Guide v2: Index (NOW AT VERSION 3.0)

- 1. Frontispiece
- 2. Introduction
- 3. The OWASP Testing Framework
- 4. Web Application Penetration Testing
- 5. Writing Reports: value the real risk
- Appendix A: Testing Tools
- Appendix B: Suggested Reading
- Appendix C: Fuzz Vectors



What Is the OWASP Testing Guide?

- Testing Principles
- Testing Process
- Custom Web Applications
 - Black Box Testing
 - Grey Box Testing
- Risk and Reporting
- Appendix: Testing Tools
- Appendix: Fuzz Vectors

- 
- Information Gathering
 - Business Logic Testing
 - Authentication Testing
 - Session Management Testing
 - Data Validation Testing
 - Denial of Service Testing
 - Web Services Testing
 - Ajax Testing

Soc08 version 3



- Improve version 2
 - improved 9 articles
- Total of 10 Testing categories and 66 controls.
- New sections and controls
 - Configuration Management
 - Authorization Testing
 - 36 new articles
- New Encoded Injection Appendix;

How the Guide helps the security industry

Testers

- ✓ A structured approach to the testing activities
- ✓ A checklist to be followed
- ✓ A learning and training tool

Organisations

- ✓ A tool to understand web vulnerabilities and their impact
- ✓ A way to check the quality of security tests

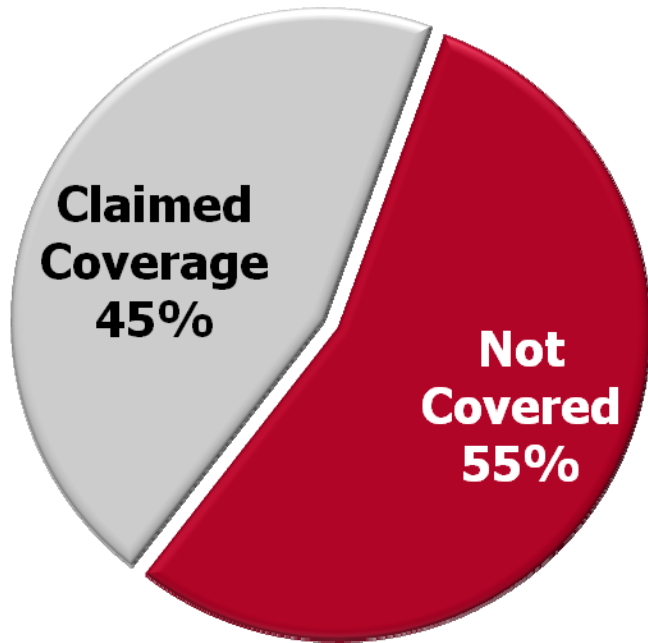
More generally, the Guide aims to provide a pen-testing standard that creates a 'common ground' between the testing groups and its 'customers'.

This will raise the overall quality and understanding of this kind of activity and therefore the general level of security of our applications

Tools

- <http://www.owasp.org/index.php/Phoenix/Tools>
- Best known OWASP Tools
 - ▶ WebGoat
 - ▶ WebScarab
- Remember:
 - ▶ A Fool with a Tool is still a Fool

Tools – At Best 45%



- MITRE found that all application security tool vendors' claims put together cover only 45% of the known vulnerability types (over 600 in CWE)
- They found very little overlap between tools, so to get 45% you need them all (assuming their claims are true)



OWASP WebGoat

Bypass a Path Based Access Control Scheme - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Address <http://localhost/WebGoat/attack?Screen=5&menu=210> Go

Logout ?

Bypass a Path Based Access Control Scheme

OWASP WebGoat V5.1

Hints Show Params Show Cookies Show Java Show Solution Lesson Plans

Admin Functions
General
Code Quality
Concurrency
Unvalidated Parameters
Access Control Flaws

Restart this Lesson

The 'guest' user has access to all the files in the lesson_plans directory. Try to break the access control mechanism and access a resource that is not in the listed directory. After selecting a file to view, WebGoat will report if access to the file was granted. An interesting file to try and obtain might be a file like tomcat/conf/tomcat-users.xml

Current Directory is: C:\WebGoat-5.1\tomcat\webapps\WebGoat\lesson_plans

Choose the file to view:

- 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
- DBSQLInjection.html

View File

Viewing file: C:\WebGoat-5.1\tomcat\webapps\WebGoat\lesson_plans

Local intranet



OWASP WebScarab

The screenshot displays the OWASP WebScarab application window. The title bar reads "WebScarab". The menu bar includes "File", "View", "Tools", and "Help". The toolbar contains buttons for "Summary", "Message log", "Proxy", "Manual Request", "WebServices", "Spider", "Extensions", "SessionID Analysis", "Scripted", "Fragments", "Fuzzer", and "Compare".

The "Summary" tab is active, showing a "Tree Selection filters conversation list". The tree view on the left shows the following structure:

- http://www.owasp.org:80/
 - banners/
 - images/
 - index.php/
 - Main_Page
 - skins/

The main table displays the following data:

Url	Methods	Status	Set-Cookie	Comments	Scripts
http://www.owasp.org:80/	GET	301 Moved ...	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
http://www.owasp.org:80/index.php/Main_Page	GET	200 OK	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Below the tree view, a detailed log table is shown:

ID	Date	Method	Host	Path	Parameters	Status	Origin
5	2006/06/23...	GET	http://www.owasp.org:80	/skins/monobook/main...	??	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

The status bar at the bottom left shows "5.27 / 63.56".

OWASP CSRFTester

The screenshot shows the OWASP CSRFTester application window. The title bar reads "OWASP CSRFTester". Below the title bar is a menu bar with "File" and "Options". The main area has a header "OWASP CSRFTester" and two buttons: "Clear All" and "Stop Recording".

Step	Method	URL	Parameters	Pause
Request 18	GET	http://www.google-anal...		63
Request 19	GET	http://www.owasp.org:...		15
Request 25	GET	http://www.owasp.org:...		125
Request 28	GET	http://www.owasp.org:...		312
Request 29	GET	http://www.owasp.org:...		31
Request 32	GET	http://www.owasp.org:...		62
Request 33	GET	http://www.owasp.org:...		109
Request 34	GET	http://www.owasp.org:...		109
Request 36	GET	http://www.google-anal...		78
Request 37	GET	http://www.google.com...		94
Request 39	GET	http://www.google.com...		109

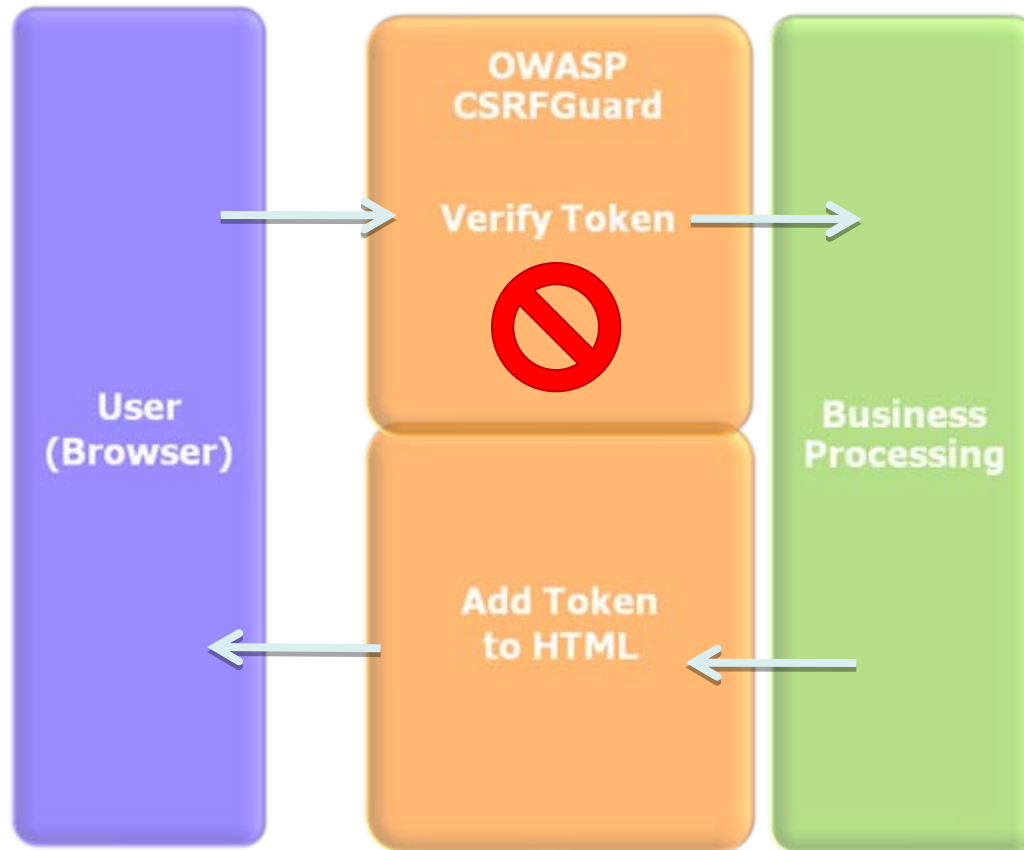
Below the table, the details for "Request 36" are shown. The method is "GET" and the URL is "http://www.google-analytics.com:80/___utm.gif".

Query Parameters	Form Parameters
utmww=1	
utmn=524956485	
utmcs=UTF-8	
utmsr=1280x1024	

At the bottom, there are fields for "Include Regex:" (containing ".") and "Exclude Regex:" (containing ".\\.(gif|jpg|png|css|ico|js|axd|?.*|ico)\$"). There are "Reset" buttons for both. Below these are radio buttons for "Report Type:" with options "Forms" (selected), "iFrame", "IMG", "XHR", and "Link". There is a checked checkbox for "Display in Browser" and a "Generate HTML" button.

Moving to row 21

OWASP CSRFGuard 2.0



■ Adds token to:

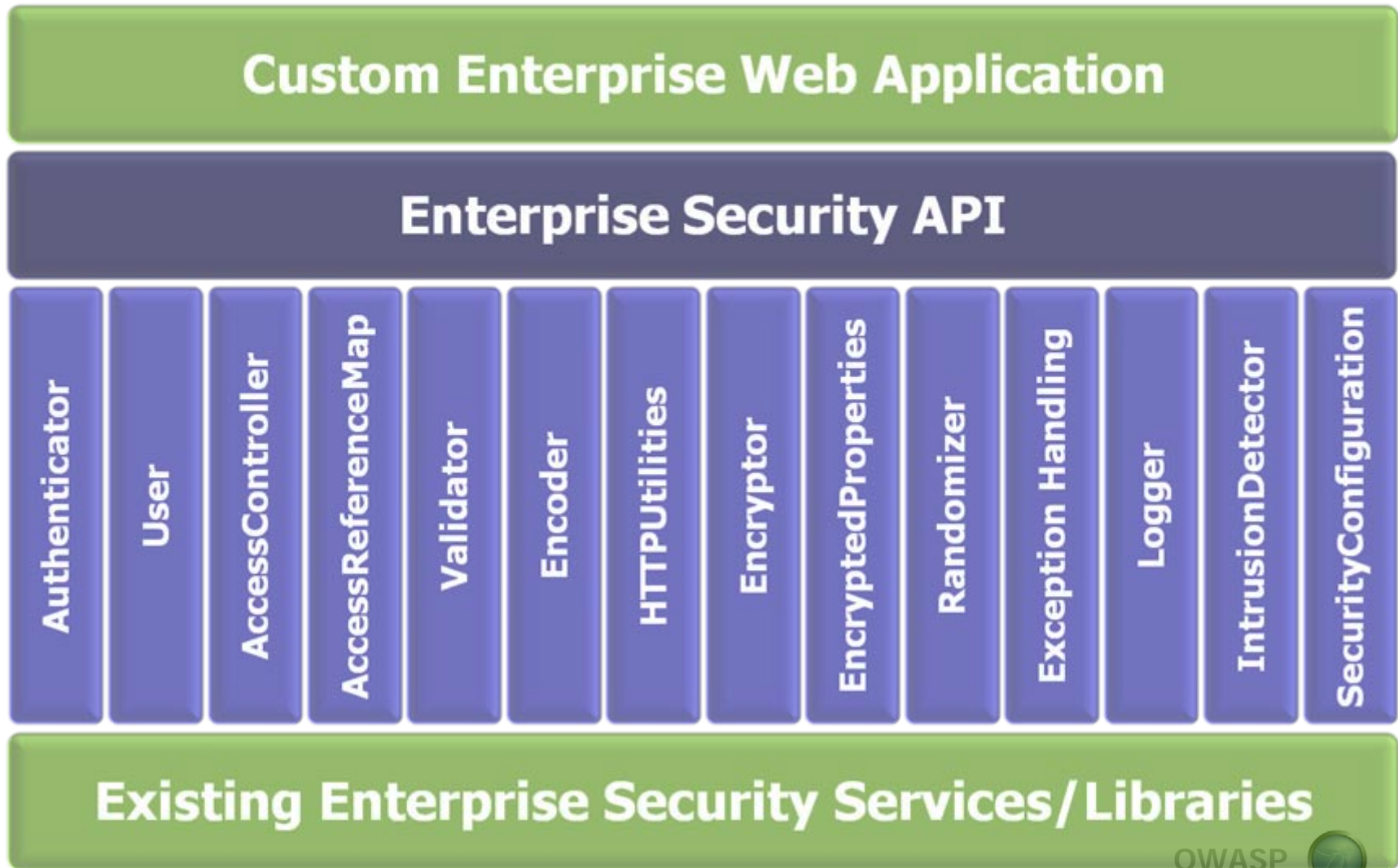
- ▶ href attribute
- ▶ src attribute
- ▶ hidden field in all forms

■ Actions:

- ▶ Log
- ▶ Invalidate
- ▶ Redirect

<http://www.owasp.org/index.php/CSRFGuard>

The OWASP Enterprise Security API



Coverage

OWASP Top Ten

A1. Cross Site Scripting (XSS)

A2. Injection Flaws

A3. Malicious File Execution

A4. Insecure Direct Object Reference

A5. Cross Site Request Forgery (CSRF)

A6. Leakage and Improper Error Handling

A7. Broken Authentication and Sessions

A8. Insecure Cryptographic Storage

A9. Insecure Communications

A10. Failure to Restrict URL Access

OWASP ESAPI

Validator, Encoder

Encoder

HTTPUtilities (upload)

AccessReferenceMap

User (csrftoken)

EnterpriseSecurityException, HTTPUtils

Authenticator, User, HTTPUtils

Encryptor

HTTPUtilities (secure cookie, channel)

AccessController



Create Your ESAPI Implementation

■ Your Security Services

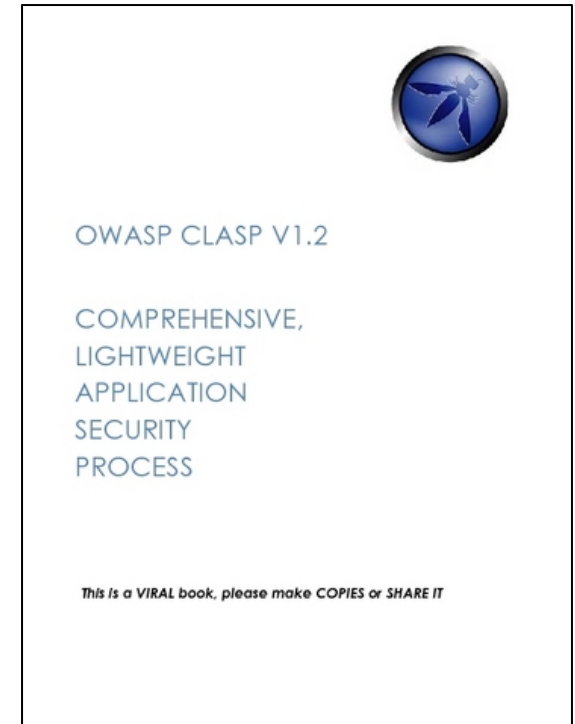
- ▶ Wrap your existing libraries and services
- ▶ Extend and customize your ESAPI implementation
- ▶ Fill in gaps with the reference implementation

■ Your Coding Guideline

- ▶ Tailor the ESAPI coding guidelines
- ▶ Retrofit ESAPI patterns to existing code

OWASP CLASP

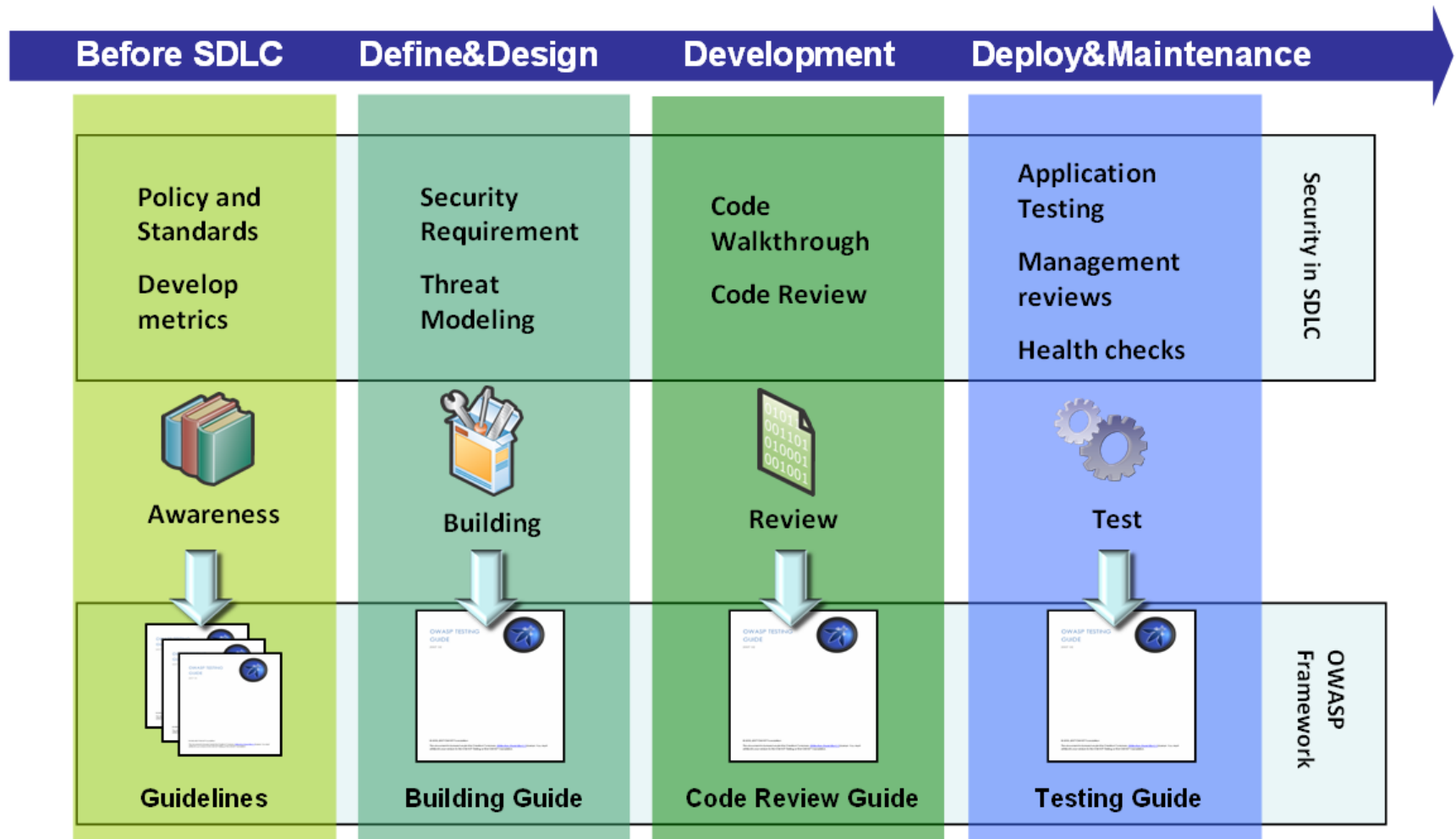
- Comprehensive, Lightweight Application Security Process
 - ▶ Prescriptive and Proactive
 - ▶ Centered around 7 AppSec Best Practices
 - ▶ Cover the entire software lifecycle (not just development)
- Adaptable to any development process
 - CLASP defines roles across the SDLC
 - 24 role-based process components
 - Start small and dial-in to your needs



The CLASP Best Practices

1. Institute awareness programs
2. Perform application assessments
3. Capture security requirements
4. Implement secure development practices
5. Build vulnerability remediation procedures
6. Define and monitor metrics
7. Publish operational security guidelines

SDLC & OWASP Guidelines



Want More ?

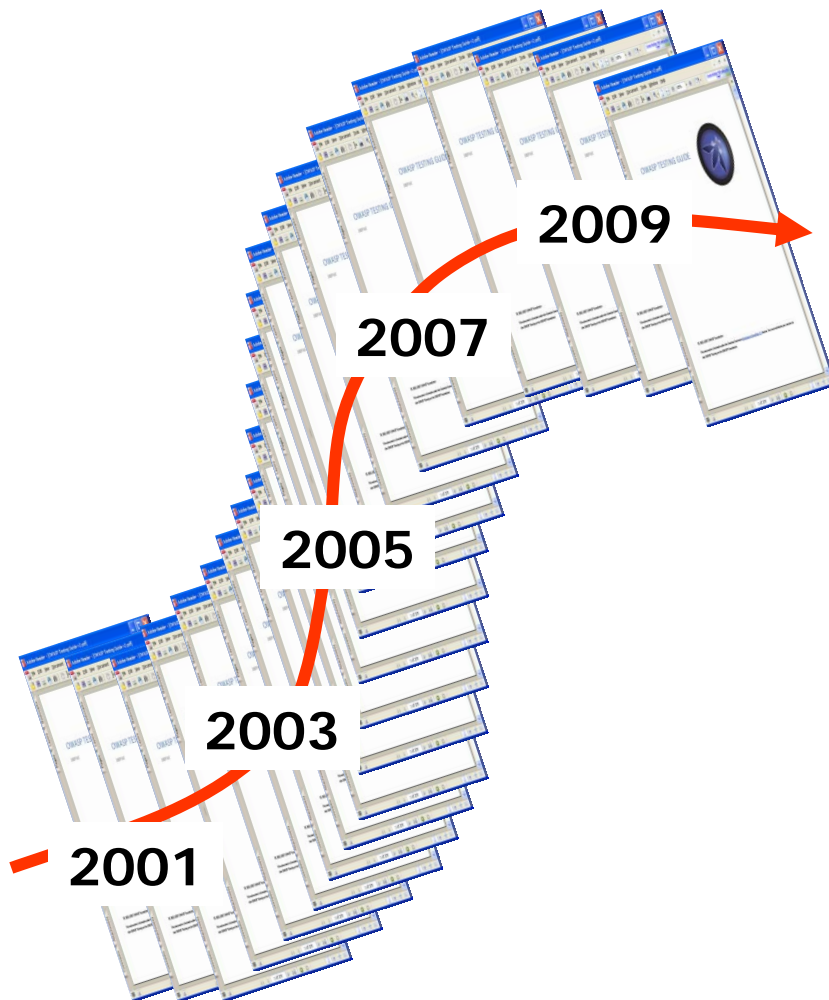
- OWASP .NET Project
- OWASP ASDR Project
- OWASP AntiSamy Project
- OWASP AppSec FAQ Project
- OWASP Application Security Assessment Standards Project
- OWASP Application Security Metrics Project
- OWASP Application Security Requirements Project
- OWASP CAL9000 Project
- OWASP CLASP Project
- OWASP CSRFGuard Project
- OWASP CSRFTester Project
- OWASP Career Development Project
- OWASP Certification Criteria Project
- OWASP Certification Project
- OWASP Code Review Project
- OWASP Communications Project
- OWASP DirBuster Project
- OWASP Education Project
- OWASP Encoding Project
- OWASP Enterprise Security API
- OWASP Flash Security Project
- OWASP Guide Project
- OWASP Honeycomb Project
- OWASP Insecure Web App Project
- OWASP Interceptor Project
- OWASP JBroFuzz
- OWASP Java Project
- OWASP LAPSE Project
- OWASP Legal Project
- OWASP Live CD Project
- OWASP Logging Project
- OWASP Orizon Project
- OWASP PHP Project
- OWASP Pantera Web Assessment Studio Project
- OWASP SASAP Project
- OWASP SQLiX Project
- OWASP SWAAT Project
- OWASP Sprajax Project
- OWASP Testing Project
- OWASP Tools Project
- OWASP Top Ten Project
- OWASP Validation Project
- OWASP WASS Project
- OWASP WSFuzzer Project
- OWASP Web Services Security Project
- OWASP WebGoat Project
- OWASP WebScarab Project
- OWASP XML Security Gateway Evaluation Criteria Project
- OWASP on the Move Project

SoC2008 selection



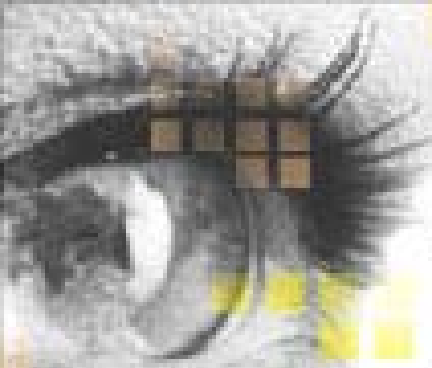
- OWASP Code review guide, V1.1
- The Ruby on Rails Security Guide v2
- OWASP UI Component Verification Project (a.k.a. OWASP JSP Testing Tool)
- Internationalization Guidelines and OWASP-Spanish Project
- OWASP Application Security Desk Reference (ASDR)
- OWASP .NET Project Leader
- OWASP Education Project
- The OWASP Testing Guide v3
- OWASP Application Security Verification Standard
- Online code signing and integrity verification service for open source community (OpenSign Server)
- Securing WebGoat using ModSecurity
- OWASP Book Cover & Sleeve Design
- OWASP Individual & Corporate Member Packs, Conference Attendee Packs Brief
- OWASP Access Control Rules Tester
- OpenPGP Extensions for HTTP - Enigform and mod_openpgp
- OWASP-WeBekci Project
- OWASP Backend Security Project
- OWASP Application Security Tool Benchmarking Environment and Site Generator refresh
- Teachable Static Analysis Workbench
- OWASP Positive Security Project
- GTK+ GUI for w3af project
- OWASP Interceptor Project - 2008 Update
- Skavenger
- SQL Injector Benchmarking Project (SQLIBENCH)
- OWASP AppSensor - Detect and Respond to Attacks from Within the Application
- Owasp Orizon Project
- OWASP Corporate Application Security Rating Guide
- OWASP AntiSamy .NET
- Python Static Analysis
- OWASP Classic ASP Security Project
- OWASP Live CD 2008 Project

OWASP Projects Are Alive!



Agenda

- OWASP Introduction
- OWASP Project Parade
- OWASP Near You?



OWASP USA, NYC

AppSec 2008 Conference

Sept 24th - 25th 2008



Two days of Seminars and Technology Pavilion from the world's best application security technology minds, two days of hardcore hands-on training.



www.owasp.tv

56 videos – 40+ hrs



Upcoming Conferences

- July 2009 - OWASP New Zealand Day 2009 - New Zealand
- July 13th - 2 track conference, University of Auckland, Auckland, New Zealand (Registrations are Open)
- September 2009 - OWASP AppSec Ireland 2009
- September 10th - 1-Day Conference at Trinity College in Dublin
- October 2009 - OWASP AppSec Brazil 2009
- October 7- 27th-30th Conference and tutorials at Câmara dos Deputados, Anexo II, Praça dos Três Poderes
- November 2009 - OWASP AppSec US 2009 - Washington, D.C.
- http://www.owasp.org/index.php/Category:OWASP_AppSec_Conference

Chapter Resources

- Meetings
- Local Mailing List
- Presentations & Groups
- Open forum for discussion
- Meet fellow InfoSec professionals
- Create (Web)AppSec awareness
- Local projects?
- JOBS = http://www.owasp.org/index.php/OWASP_Jobs

TTD Subscribe to local chapter mailing list

- Visit www.owasp.org
- Find your local chapter
- Listen to PodCasts
- Watch Videos
- Read Materials
- Post your (Web)AppSec questions
- Come to a meeting to meet peers
- Contribute to discussions
- Conference

Got Questions?

**Talk to your local chapter leader or
email owasp@owasp.org**