OWASP Foundation Inc.

Tom “jinxpuppy” Brennan
Board Member, OWASP Foundation
tomb@owasp.org

Security Strategist
WhiteHat Security Inc.
www.whitehatsec.com

OWASP

From: http://preview.tinyurl.com/ccxbvg

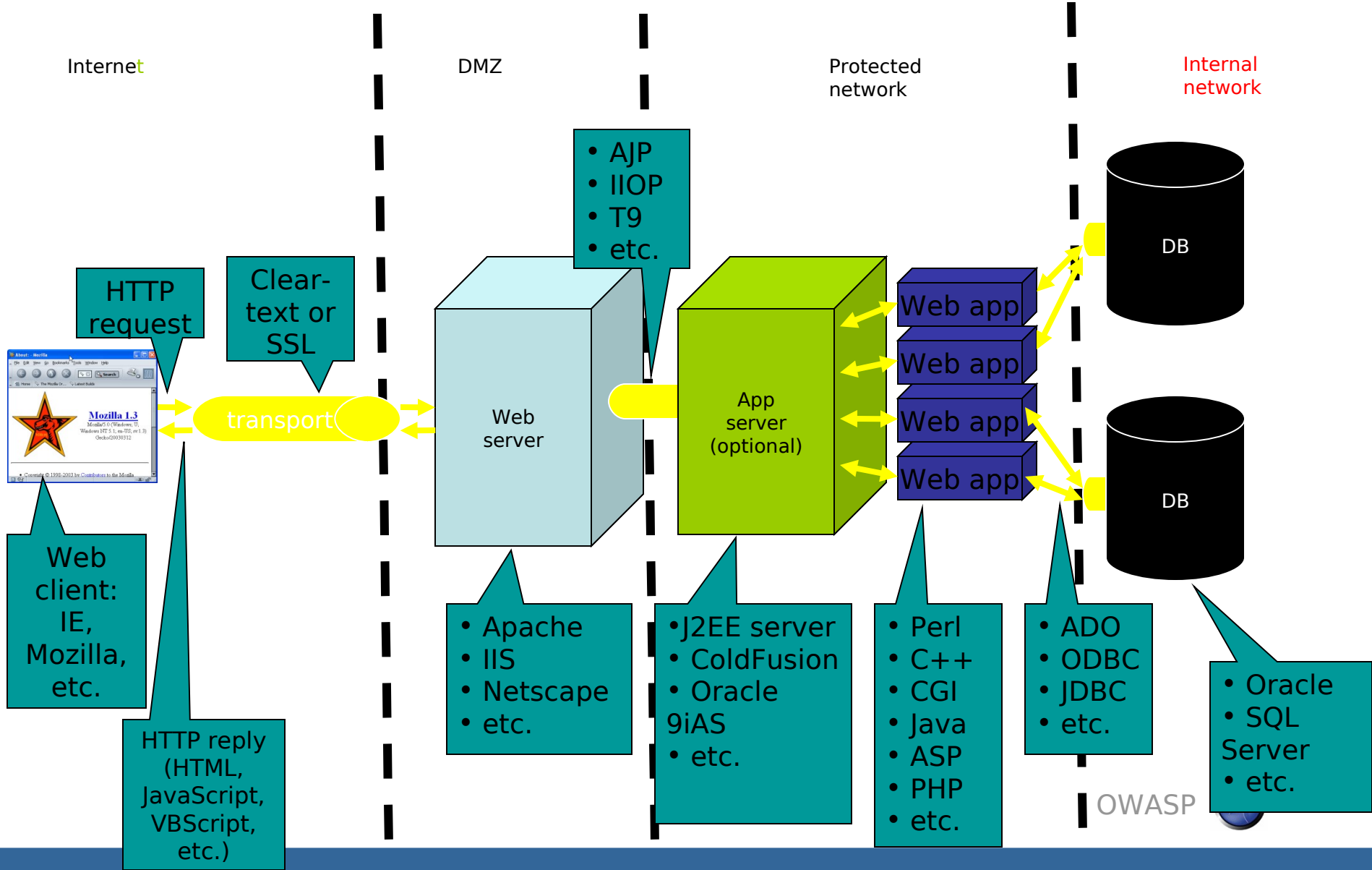
Agenda

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

Agenda

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

Web Applications - 215M/1M *netcraft



OWASP

- **The Open Web Application Security Project (OWASP Foundation Inc.) established 2001'.**
- **Participation in OWASP is free and open to all**
- **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 , 10k members on mailing lists**

Principles

- Free & Open
- Governed by rough consensus & running code
- Abide by a code of ethics (see ethics)
- Not-for-profit
- Not driven by commercial interests
- Risk based approach

Code of Ethics

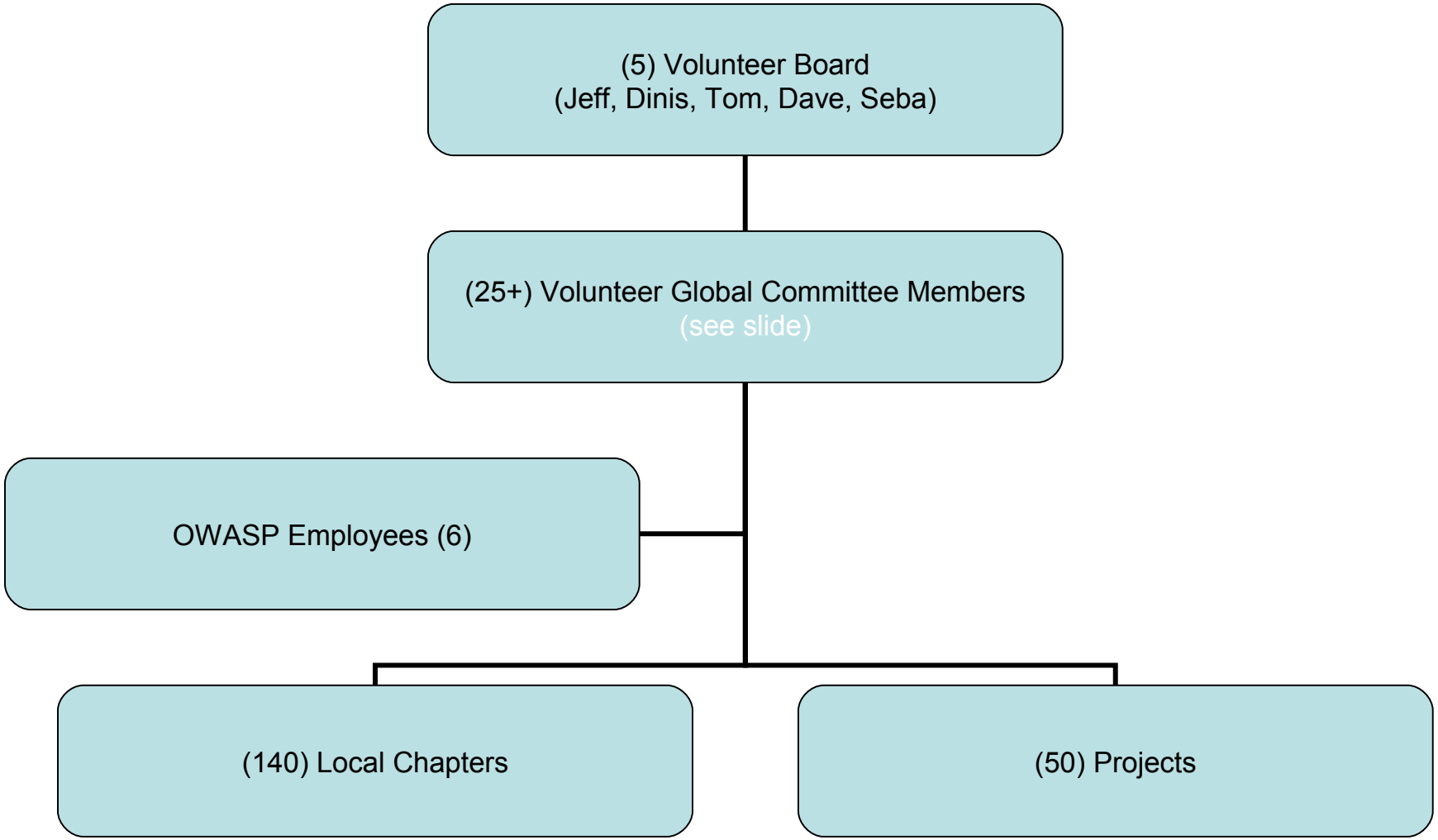
• Perform all professional activities and duties in accordance with all applicable laws and the highest ethical principles;

• Promote the implementation of and promote compliance with standards, procedures, controls for application security; Maintain appropriate confidentiality of proprietary or otherwise sensitive information encountered in the course of professional activities;

• Discharge professional responsibilities with diligence and honesty; Refrain from any activities which might constitute a conflict of interest or otherwise damage the reputation of employers, the information security profession, or the Association; and

• Not intentionally injure or impugn the professional reputation of practice of colleagues, clients, or employers.

OWASP FOUNDATION INC. - Structure



Global Committee

OWASP GLOBAL COMMITTEES					
Projects	Membership	Education	Conferences	Industry	Chapters
▪ Dinis Cruz ▪ Jason Li ▪ Matt Tesauro ▪ Leo Cavallari ▪ Pravir Chandra	▪ Tom Brennan ▪ Dan Cornell ▪ Michael Coates	▪ Seba Deleersnyder ▪ Martin Knobloch ▪ Mano Paul ▪ Eduardo Neves ▪ Kuai Hinjosa ▪ Cecil Su ▪ Fabio Cerullo ▪ Andrzej Targosz	▪ Kate Hartmann ▪ Wayne Huang ▪ Steve Antoniewicz ▪ Dhruv Soi ▪ Mark Bristow	▪ Tom Brennan ▪ Rex Booth ▪ Georg Hess ▪ Eoin Keary ▪ David Campbell ▪ Colin Watson	▪ Seba Deleersnyder ▪ Puneet Mehta ▪ Ofer Shezaf ▪ Justin Derry

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

2009 Organization Supporters

2009 Educational Supporters

OWASP Mission

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.

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

www.owasp.org

article | discussion | view source | history

Main Page

Ad Space Available for 2009

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

Welcome to OWASP
the free and open application security community

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

About · Searching · Editing · New Article · OWASP Categories

Statistics · Recent Chang

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

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!

OWASP Application Security Research Grants

130+ chapters

Mailing Lists

- 100+ Mailing Lists
- Local Chapters
- Projects
- Regional/Global Committees

- LinkedIn Group too… 2700+ members

OWASP Conferences (2008-2009)

Summit Portugal

- 2009 Focus
  - 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?

Industry Committee

- Start outreach to critical infrastructures worldwide such as:
  - electricity generation, transmission and distribution; gas production, transport and distribution;
  - oil and oil products production, transport and distribution;
  - telecommunication;
  - water supply (drinking water, waste water/sewage, stemming of surface water (e.g. dikes and sluices));
  - agriculture, food production and distribution;
  - heating (e.g. natural gas, fuel oil, district heating);
  - public health (hospitals, ambulances);
  - transportation systems (fuel supply, railway network, airports, harbors, inland shipping);
  - financial services (banking, clearing);
  - security services (police, military).

Industry - Accomplishments

1. Has submitted RFC feedback for both British and US/NIST 800-53 rev 3 standards

2. Have been promoting supporter membership to raise awareness in industry verticals

3. Have established working relationships with ISSA & ISACA to assist with industry focused outreach and international insight

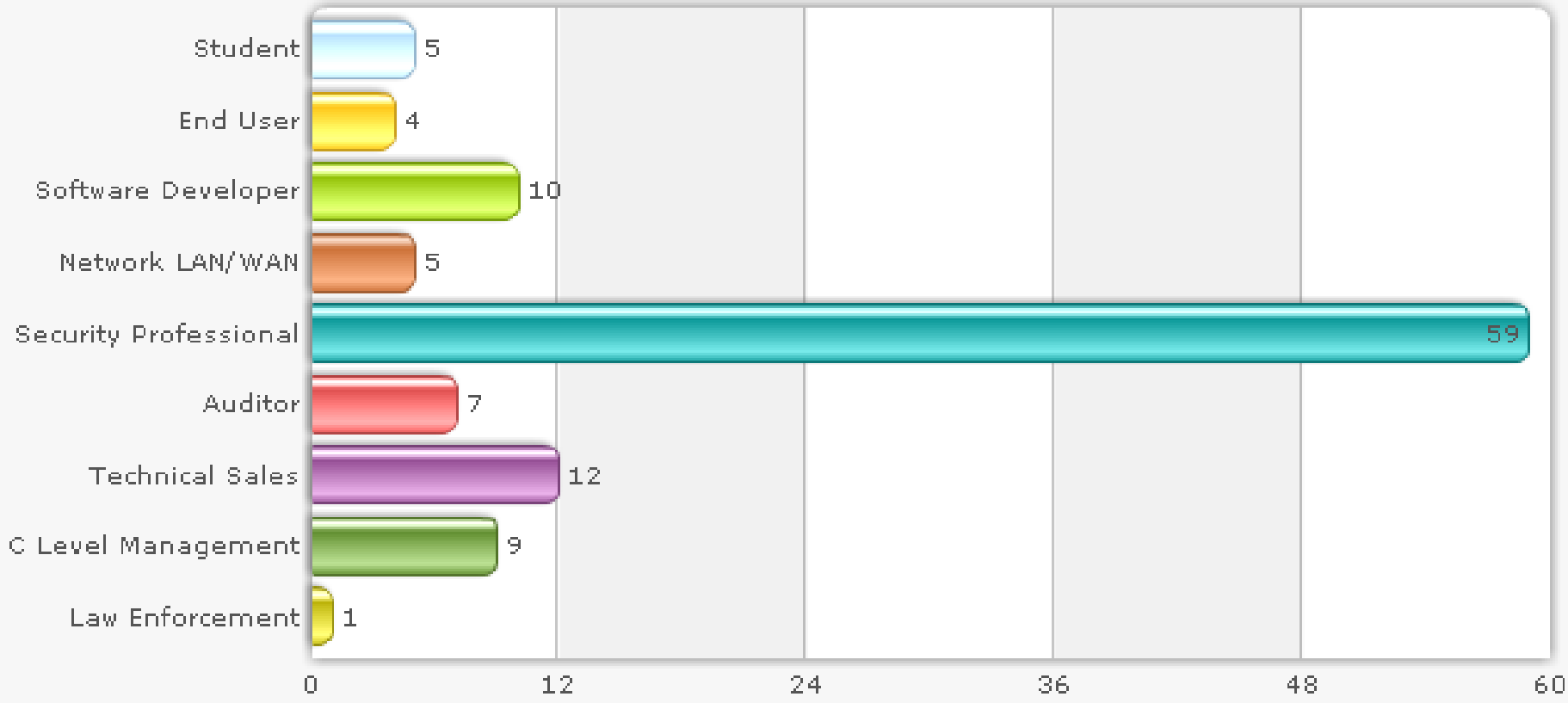
Membership Committee

- Increase individual membership 100% in 18 months (Individuals)
- Increase organizational supporters 100% in 18 months (Supporters)
- Increase university supporters 100% in 18 months

1. Has created and launched a new membership model
2. Has created and launched Membership drive to support our efforts
3. Has created video to promote/explain (tbd)

Chapters Committee

What BEST describes your role in Information Security today?



Total Number of Responses for this Item: 114

Education Committee

- Establish a adoptable program that can be incorporated into Univ., and technical education programs that leverages the efforts of many at OWASP to raise the level of awareness to secure software.
- Training at Conferences
- Obtain grants to further our work

Projects Committee

1. Organizing the next OWASP Season of Code

3. Drafting proposals for standardization and organization of the OWASP Projects page

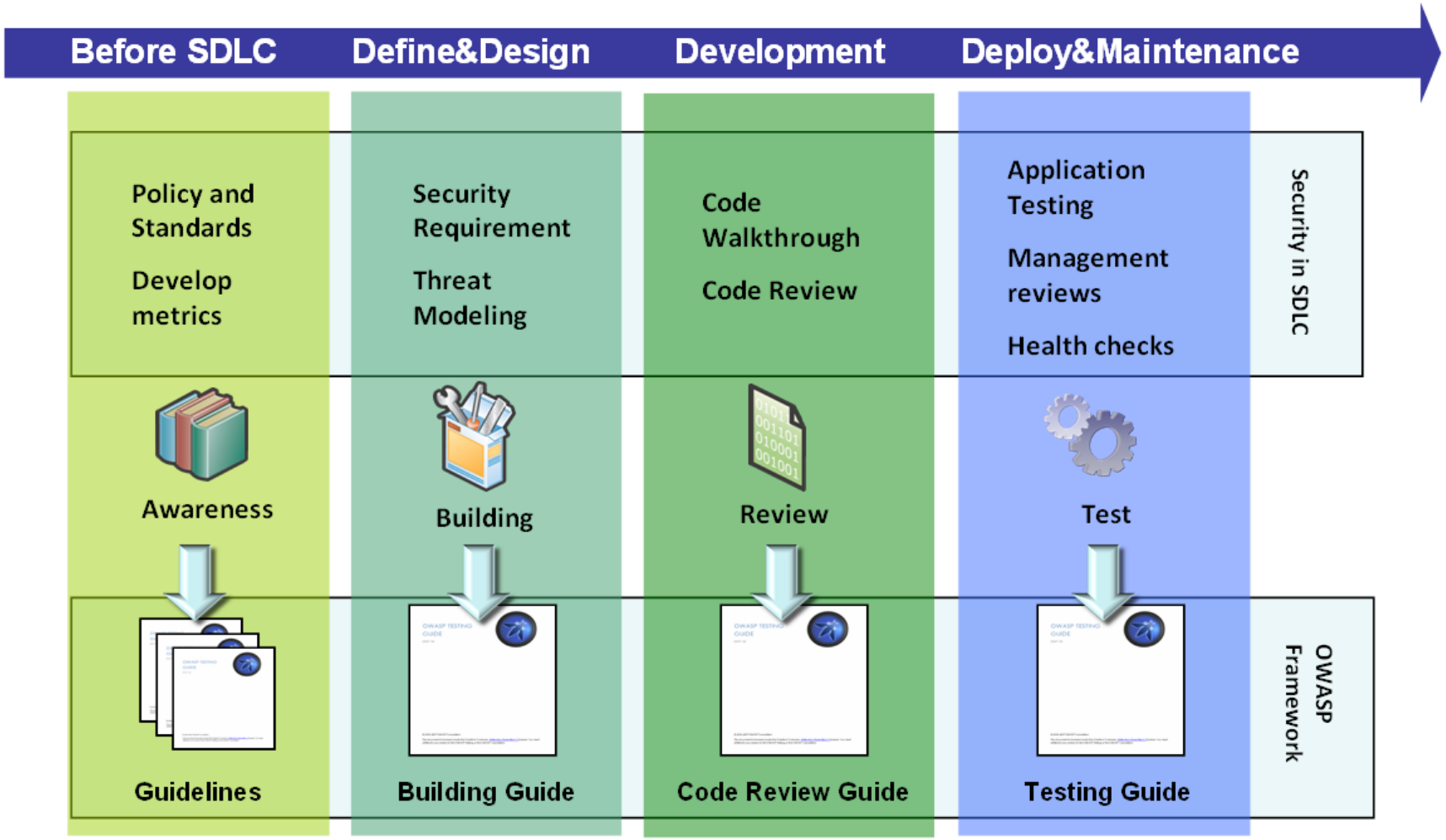
5. Establishing a baseline assessment of all OWASP Projects

OWASP Projects: Improve Quality and Suppo

- Define Criteria for Quality Levels
  - Alpha, Beta, Release

- **PROTECT** - These are tools and documents that can be used to guard against security-related design and implementation flaws.
- **DETECT** - These are tools and documents that can be used to find security-related design and implementation flaws.
- **LIFE CYCLE** - These are tools and documents that can be used to add security-related activities into the Software Development Life Cycle (SDLC).

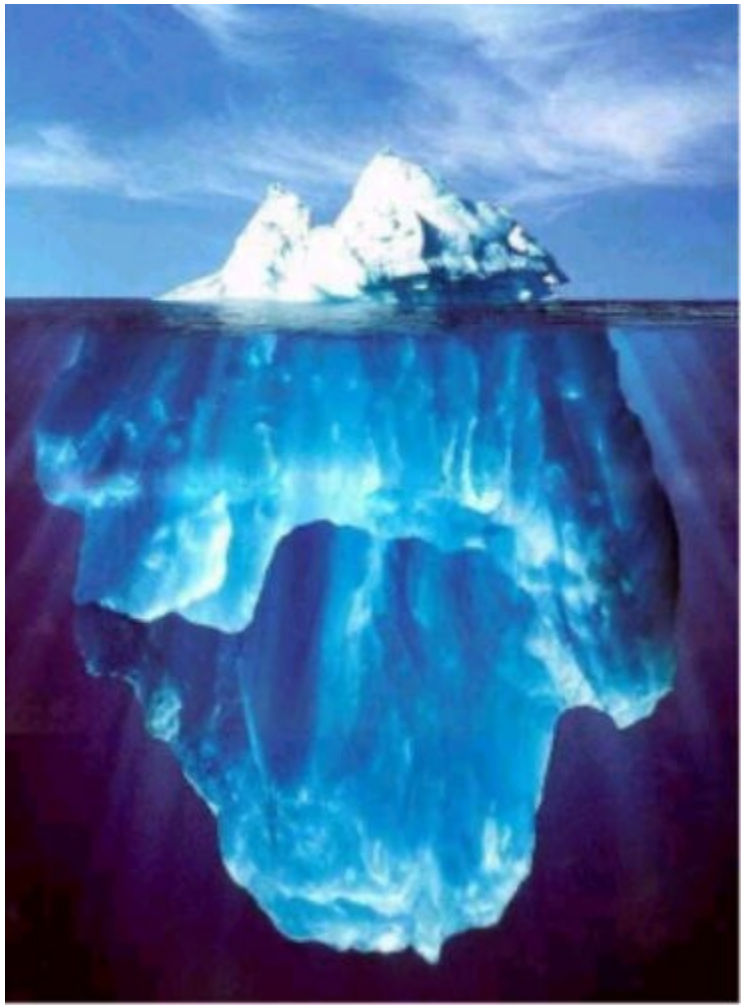
SDLC


Before SDLC
Define&Design
Development
Deploy&Maintenance
Policy and Standards
Develop metrics
Security Requirement
Threat Modeling
Code Walkthrough
Code Review
Application Testing
Management reviews
Health checks
Security in SDLC
Awareness
Building
Review
Test
Guidelines
Building Guide
Code Review Guide
Testing Guide
OWASP Framework

OWASP Top 10

- The Ten Most Critical Web Application Security Vulnerabilities
- 2007 Release
- A great start, but not a standard
- 4th version of the Top 10 200x coming soon

*Help Wanted

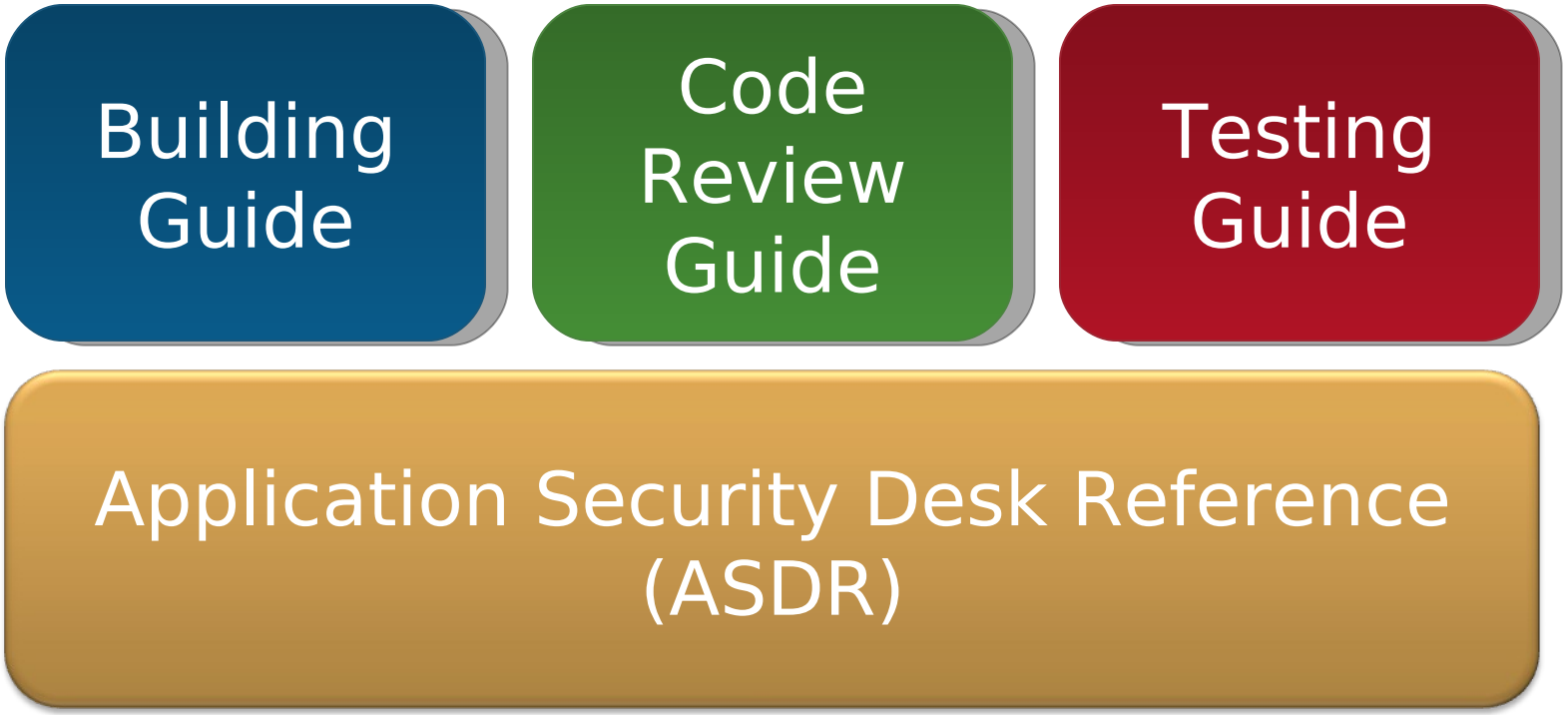


Key Application Security Vulnerabilities

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

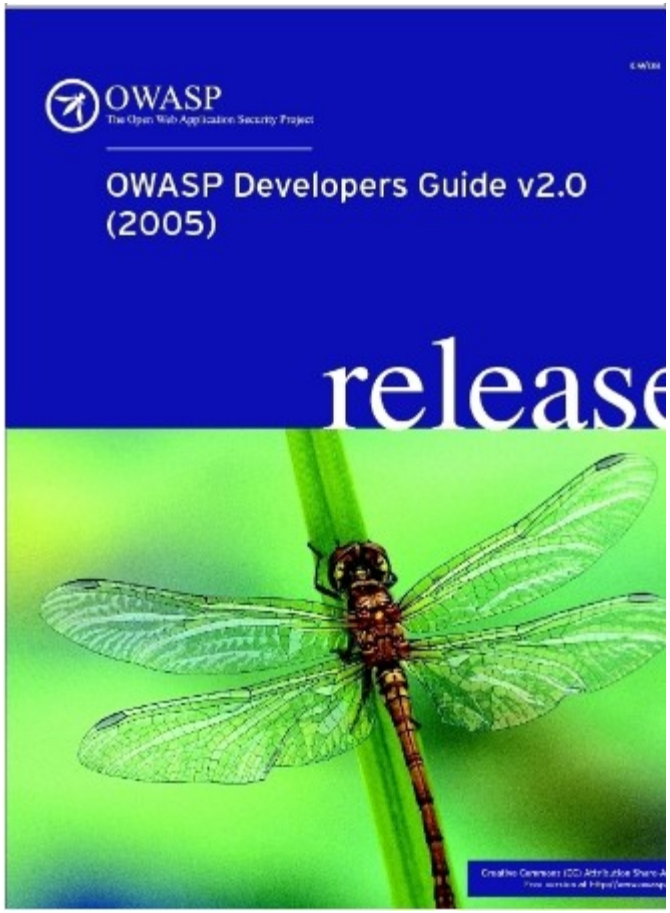
www.owasp.org/index.php?title=Top_10_2007

The ‘Big 4’ Documentation Projects



The Developer 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



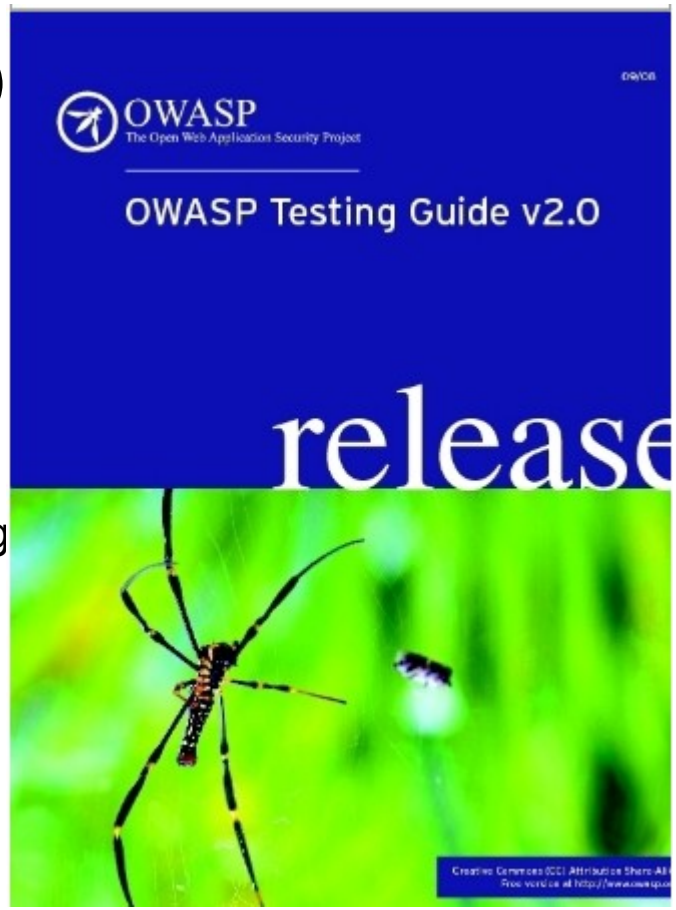
Uses of the Guide

- 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 (NOW AT VERSION 3.0)



OWASP Summer of Code 2008

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

Appendix D: Encoded Injection

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

What Is the OWASP Testing Guide?

- V2→ 8 sub-categories (for a total amount of 48 controls)
- V3 →10 sub-categories (for a total amount of 66 controls)
- 36 new articles!

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

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

Organization

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

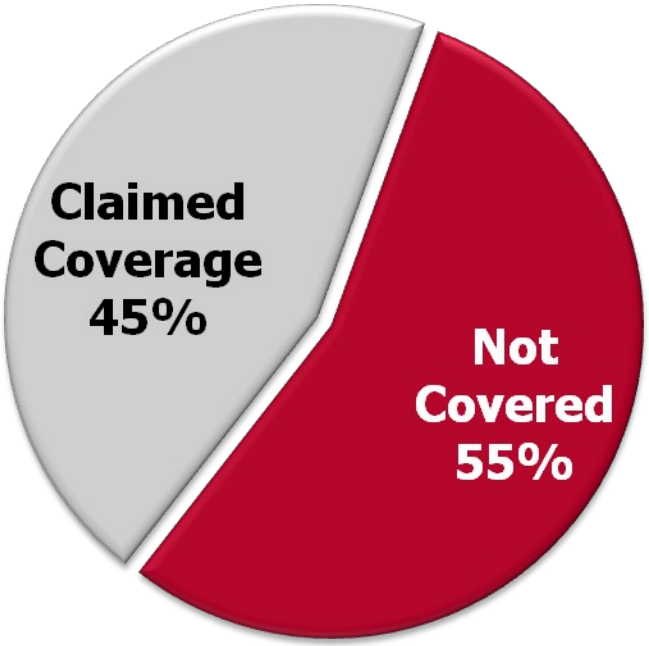
More generally, the Guide aims to provide a pen-testing standard that creates a 'common ground' between the testing groups and its ‘customers’.

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

Phoneix Project -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 – press this button and your secure ;)

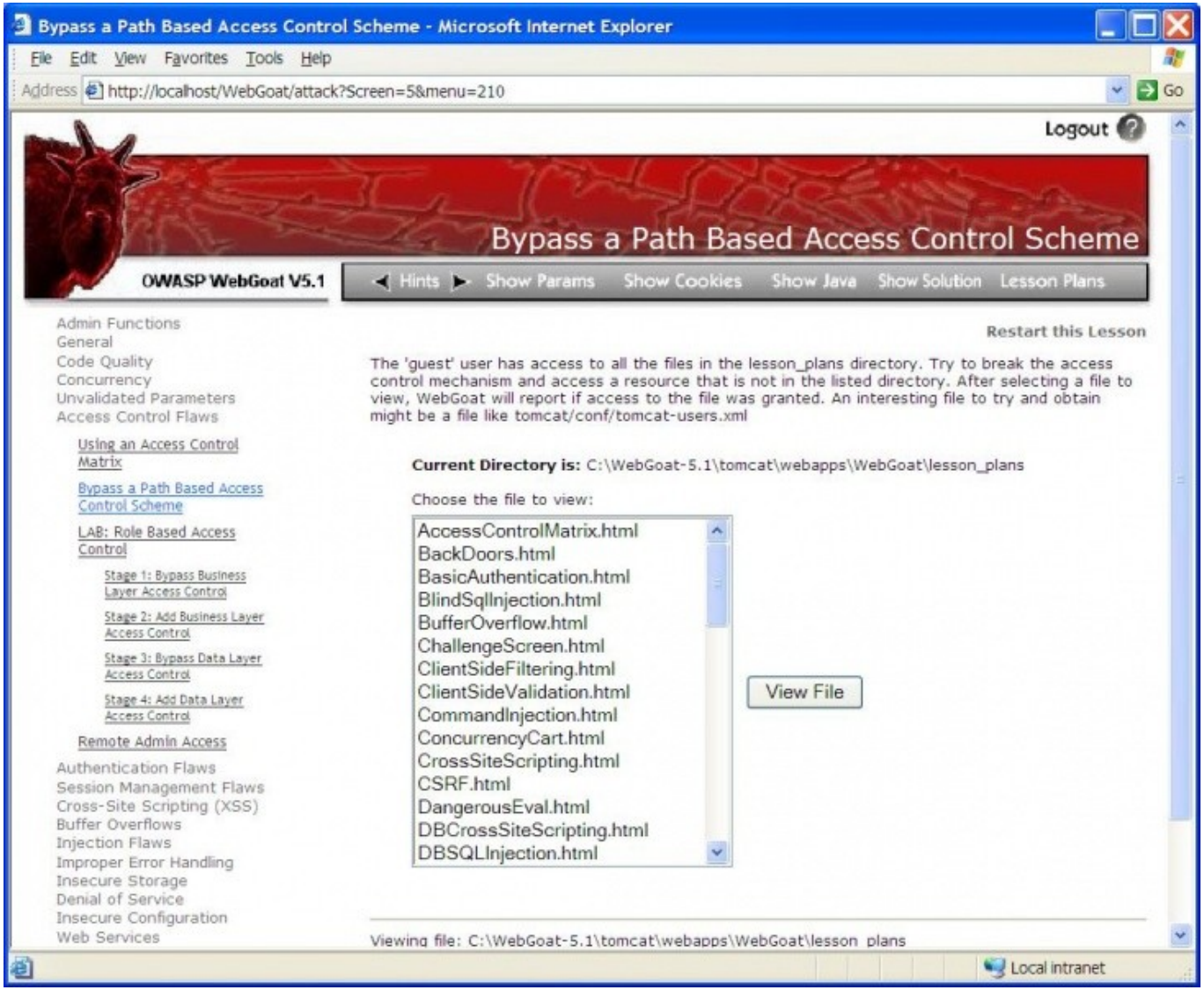
Tools – At Best 45%



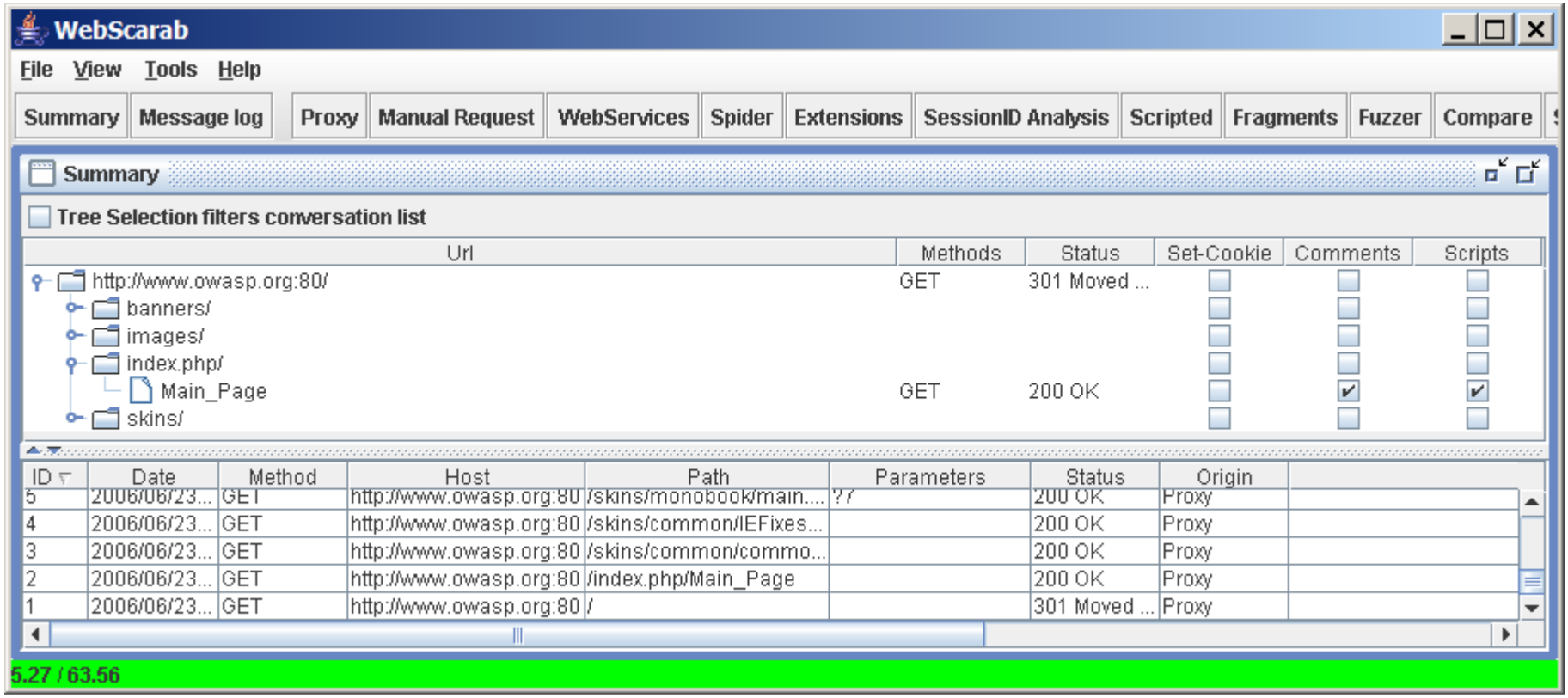
- MITRE found that all application security tool vendors' claims put together cover only 45% of the known vulnerability types (over 600 in CWE)
- They found very little overlap between tools, so to get 45% you need them all (assuming their claims are true)
- NIST and SAMATE Static Analysis

SECURITY INNOVATION · FORTIFY SOFTWARE · PALAMIDA · watchfire · Klocwork · Secure Software · AppSIC · CENZIC · CORE SECURITY TECHNOLOGIES · PARASOFT · Coverity · proServices · SofCheck · SPI DYNAMICS · VERACODE · OUNCE LABS

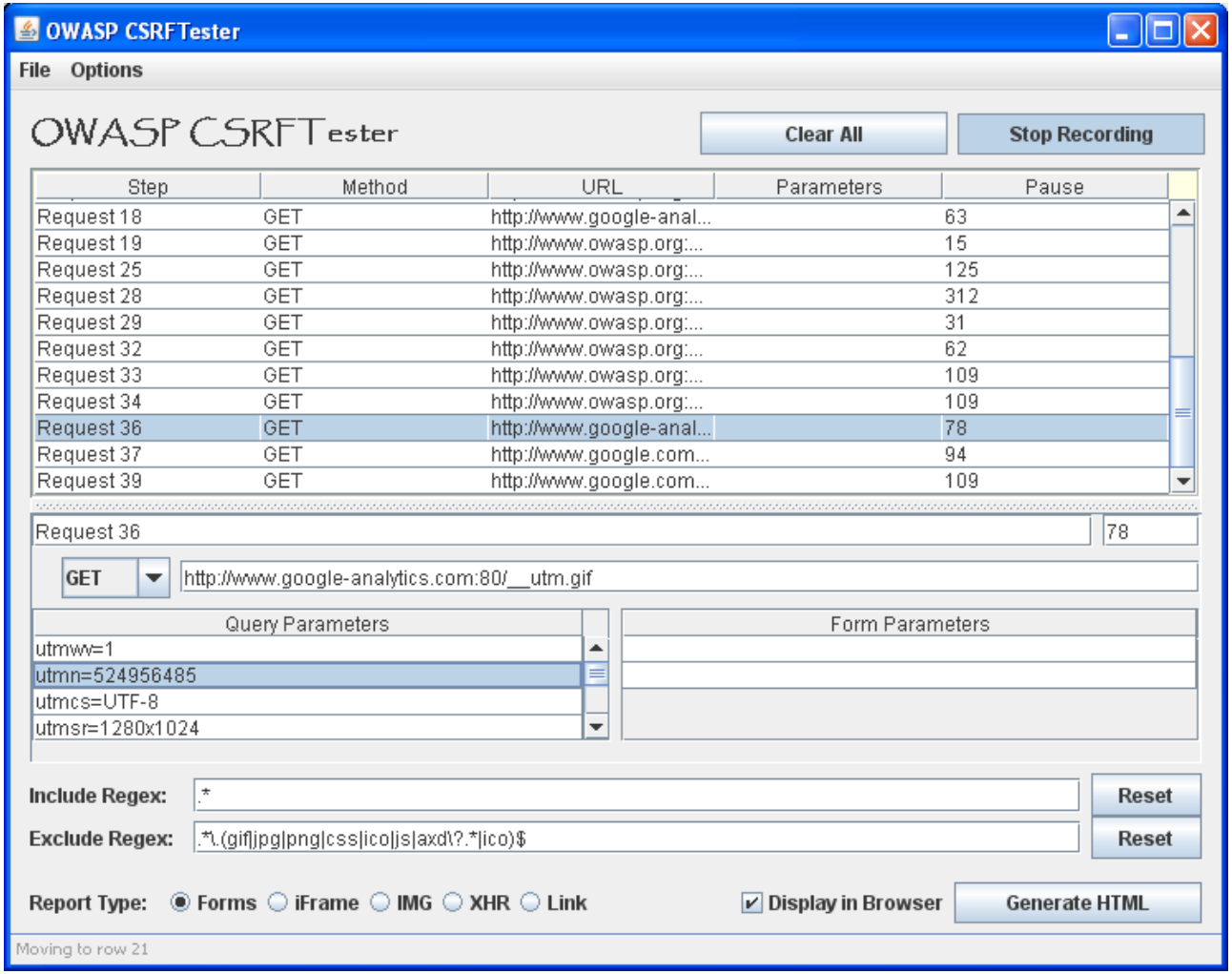
OWASP WebGoat



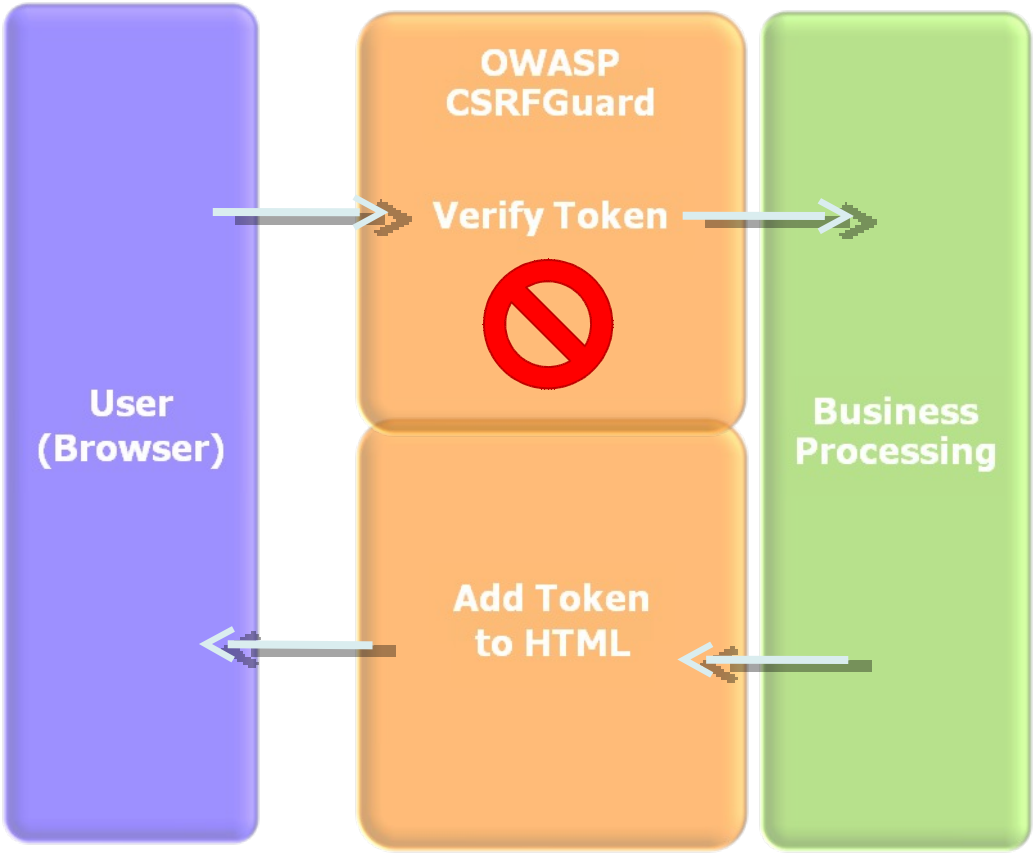
OWASP WebScarab



OWASP CSRFTester



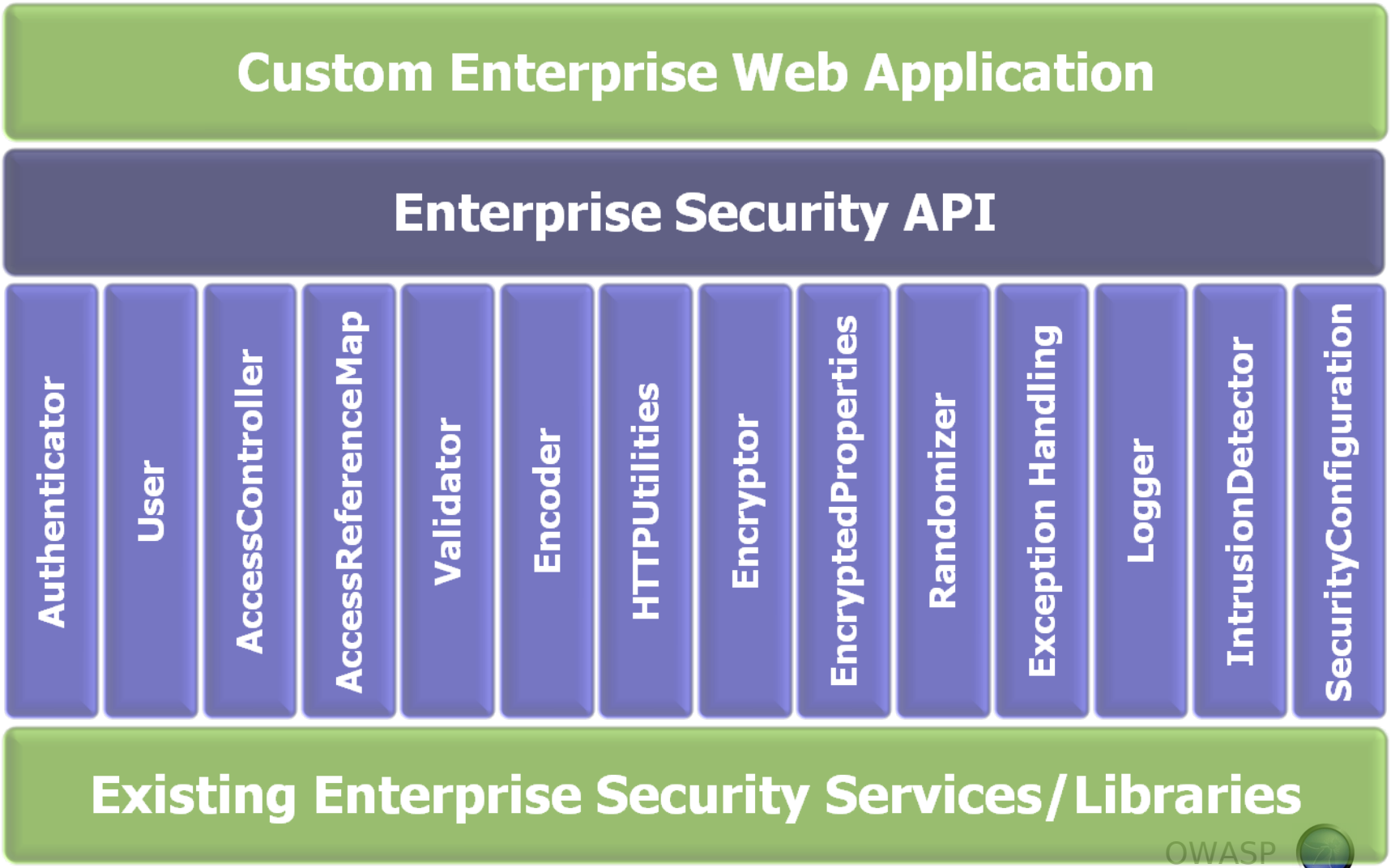
OWASP CSRFGuard 2.0



- 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



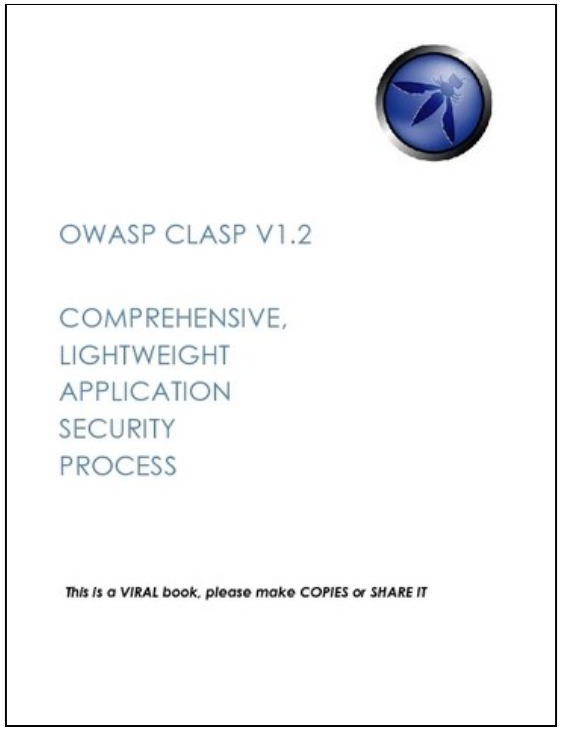
Coverage

OWASP Top Ten	OWASP ESAPI
A1. Cross Site Scripting (XSS)	Validator, Encoder
A2. Injection Flaws	Encoder
A3. Malicious File Execution	HTTPUtilities (upload)
A4. Insecure Direct Object Reference	AccessReferenceMap
A5. Cross Site Request Forgery (CSRF)	User (csrftoken)
A6. Leakage and Improper Error Handling	EnterpriseSecurityException, HTTPUtils
A7. Broken Authentication and Sessions	Authenticator, User, HTTPUtils
A8. Insecure Cryptographic Storage	Encryptor
A9. Insecure Communications	HTTPUtilities (secure cookie, channel)
A10. Failure to Restrict URL Access	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



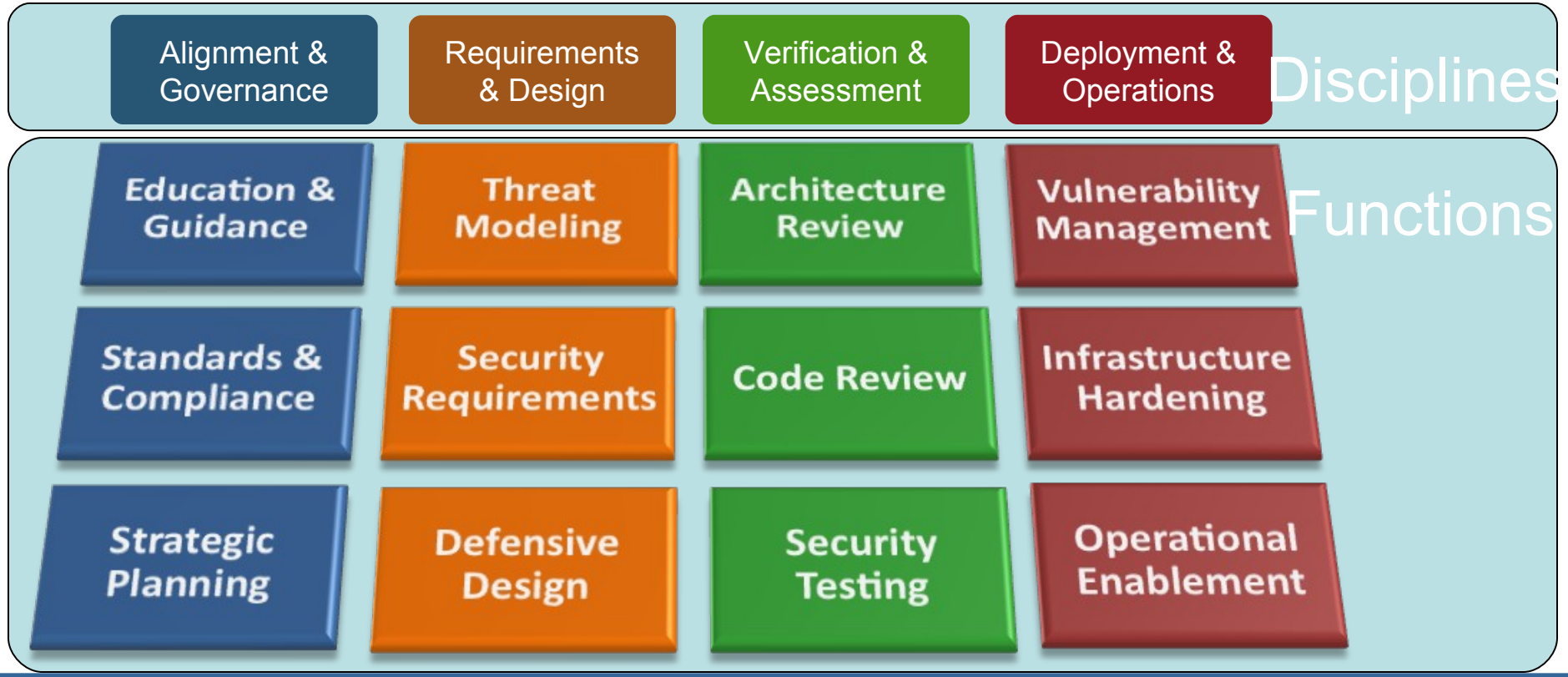
- Comprehensive, Lightweight Application Security Process
  - Prescriptive and Proactive
  - Centered around 7 AppSec Best Practices
  - Cover the entire software lifecycle (not just development)
- Adaptable to any development process
  - CLASP defines roles across the SDLC
  - 24 role-based process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

The CLASP Best Practices

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

OWASP Software Assurance Maturity Model (SAMM)

- The 4 Disciplines are high-level categories for activities
  - Three security Functions under each Discipline are the specific silos for improvement within an organization



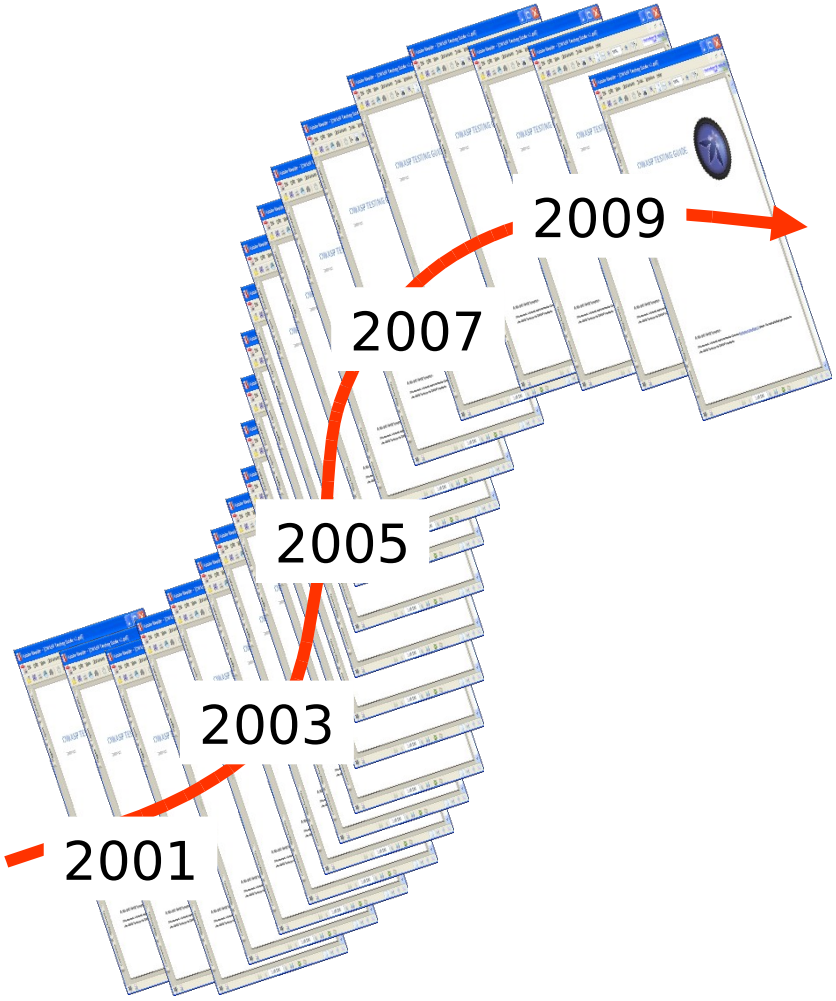
Want More ?

- 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?

Got OWASP?


Россия
Russia
Kazakhstan
Mongolia
China
Brazil
Australia

Upcoming “Big”Conferences

- **OWASP AppSec Europe 2009 - Poland May 11th-14th - 3 track conference and 8 tutorials, Krakow, Poland**
- **OWASP AppSec Ireland 2009 September 10th Conference at Trinity College in Dublin November 2009**
- **OWASP AppSec US 2009 – November Washington, D.C.**

www.owasp.tv

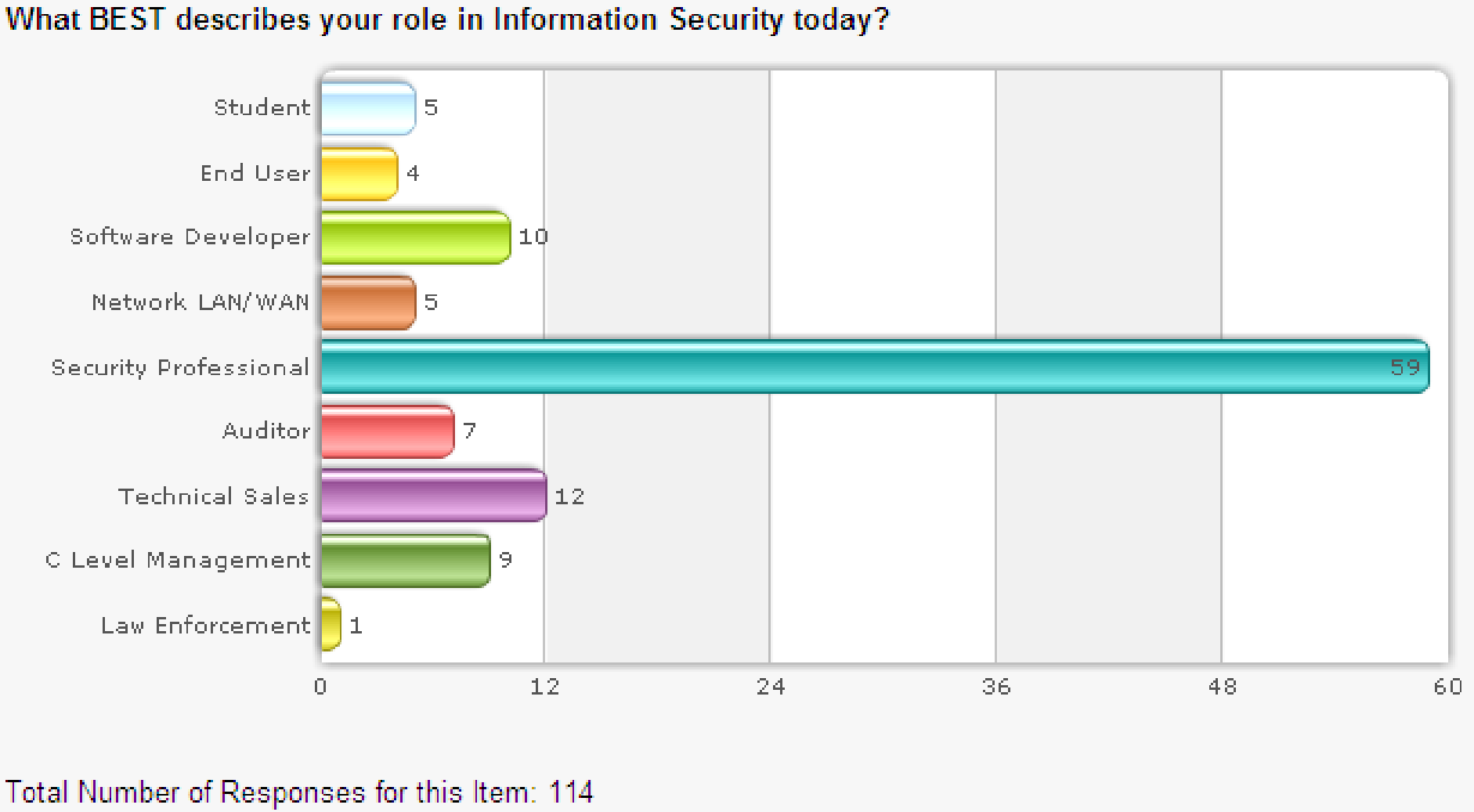
56 videos

40+ hrs

Local Chapter Resources

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

Who comes to a OWASP meeting?



TTD

- Visit www.owasp.org
- Find your local chapter / conferences
- Listen to PodCasts
- Watch Videos
- Read Materials
- Post your (Web)AppSec questions
- Spread the word invite peers
  - Pentagon City Mall / 6pm Phones @ Panda Express
- Contribute to discussions

Get Involved
WWW.OWASP.ORG

Tom Brennan
OWASP Foundation, Board Member
tomb@owasp.org / 973-202-0122