OWASP GERMAN DAY 2012

OWASP
The Open Web Application Security Project

Jim Manico
jim@owasp.org
Global Board Member

Jerry Hoff
jerry@owasp.org
OWASP Volunteer

SHOW OF HANDS

Demographics

Why this presentation

We are living in a Digital environment, in a Connected World

- Most of websites vulnerable to attacks
- 75% of Attacks at the Application Layer *(Source: Someone paid Gartner to say this)*
- Important % of web-based Business *(Services, Online Store, Self-care)*

The True Story

OWASP
The Open Web Application Security Project

The Open Web Application Security Project

OWASP:

Swarms of WASPS:
Local Chapters

What is OWASP

OWASP
The Open Web Application Security Project

Mission Driven

Nonprofit | World Wide | Unbiased

OWASP **does not endorse or recommend commercial products or services**

What is OWASP

OWASP
The Open Web Application Security Project

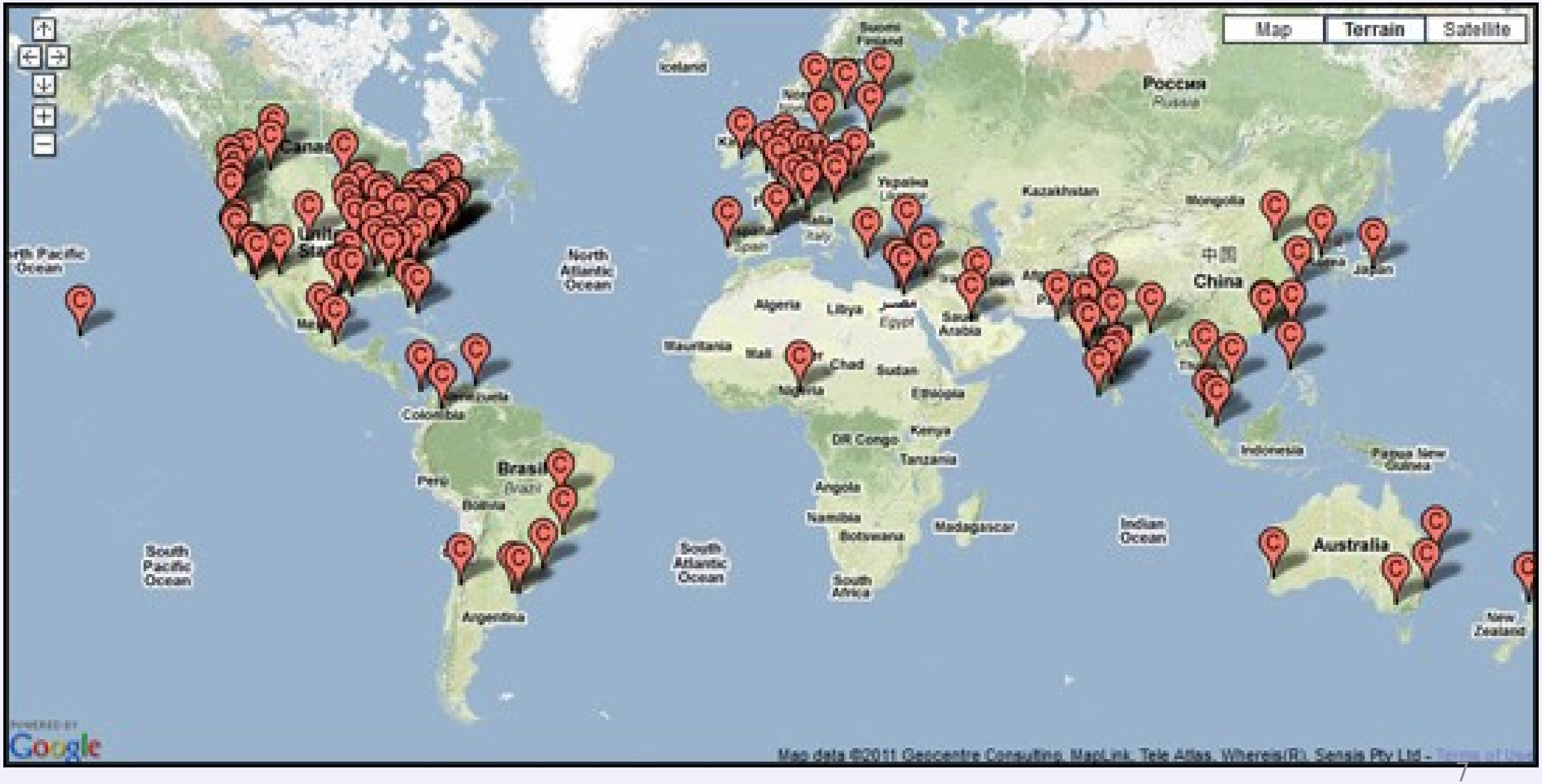
Community Driven

30,000 Mail List Participants
200 Active Chapters in 70 countries
1600+ Members, 56 Corporate Supporters
69 Academic Supporters

Around the World

OWASP
The Open Web Application Security Project

200 Chapters, ~1600 Members, 30000+ Builders, Breakers and Defenders



What is OWASP

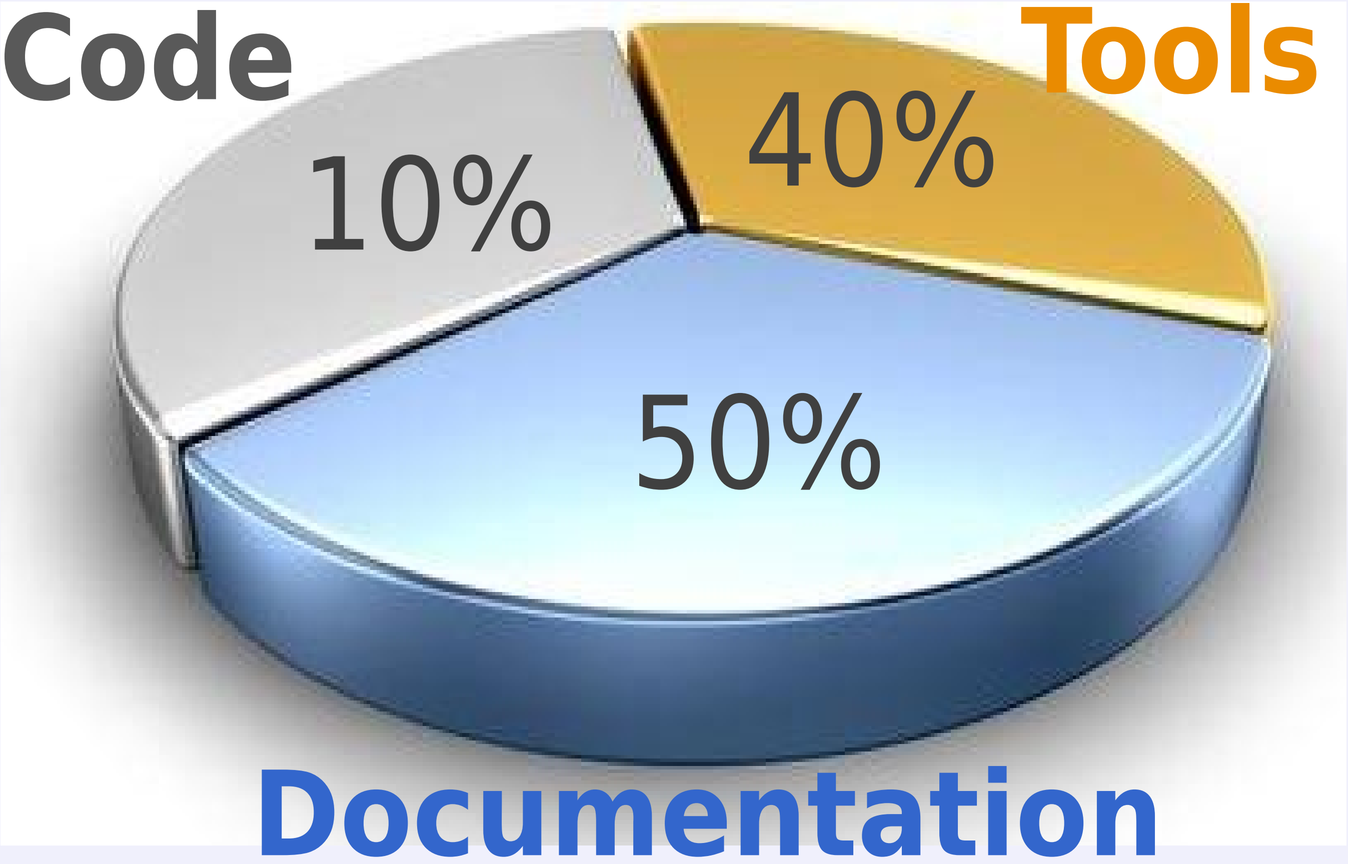
OWASP
The Open Web Application Security Project

Statistics!

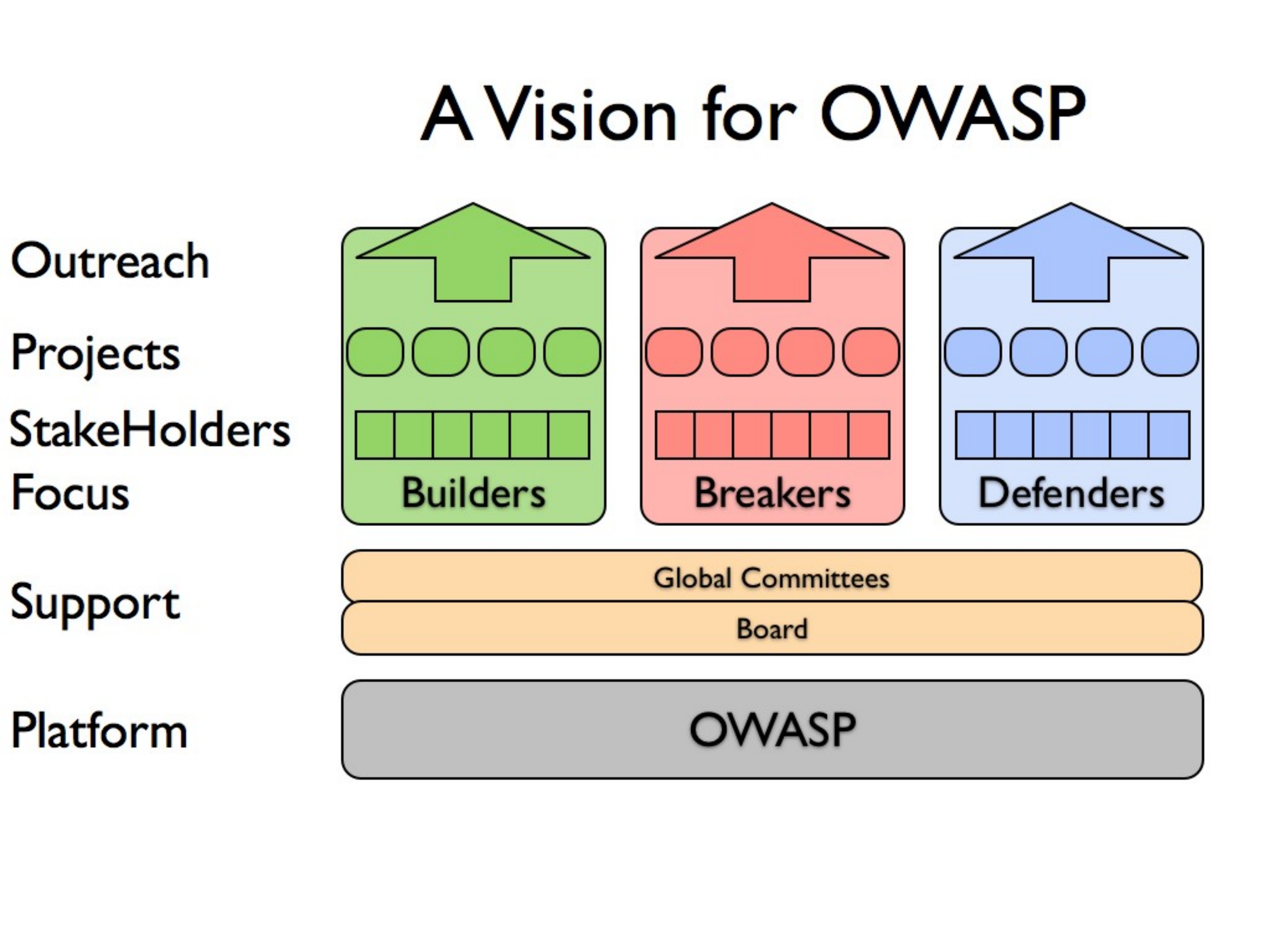
200+ Projects
15,000+ downloads of tools, documentation
250,000+ unique visitors
2,000,000+ page views

Quality Resources

OWASP
The Open Web Application Security Project



Security Lifecycle



A Vision for OWASP

Outreach

Projects

StakeHolders

Focus

Builders

Breakers

Defenders

Support

Global Committees

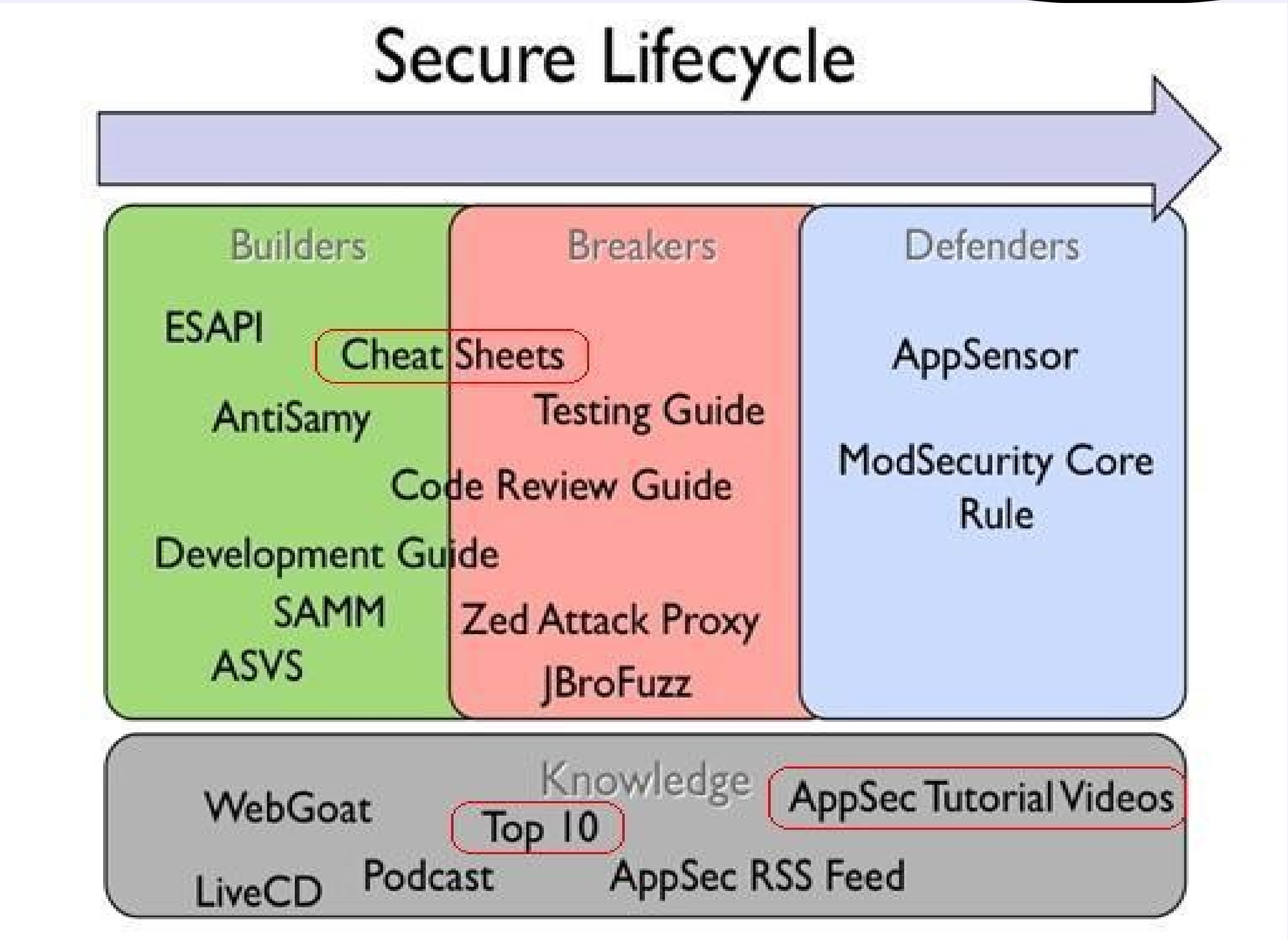
Board

Platform

OWASP

Security Resources

OWASP
The Open Web Application Security Project



Secure Lifecycle

The OWASP Top Ten

TOP 10 WEB APPLICATION SECURITY RISKS

News

a Blog

A Podcast

Membership

Mailing Lists

A Newsletter

Apple App Store

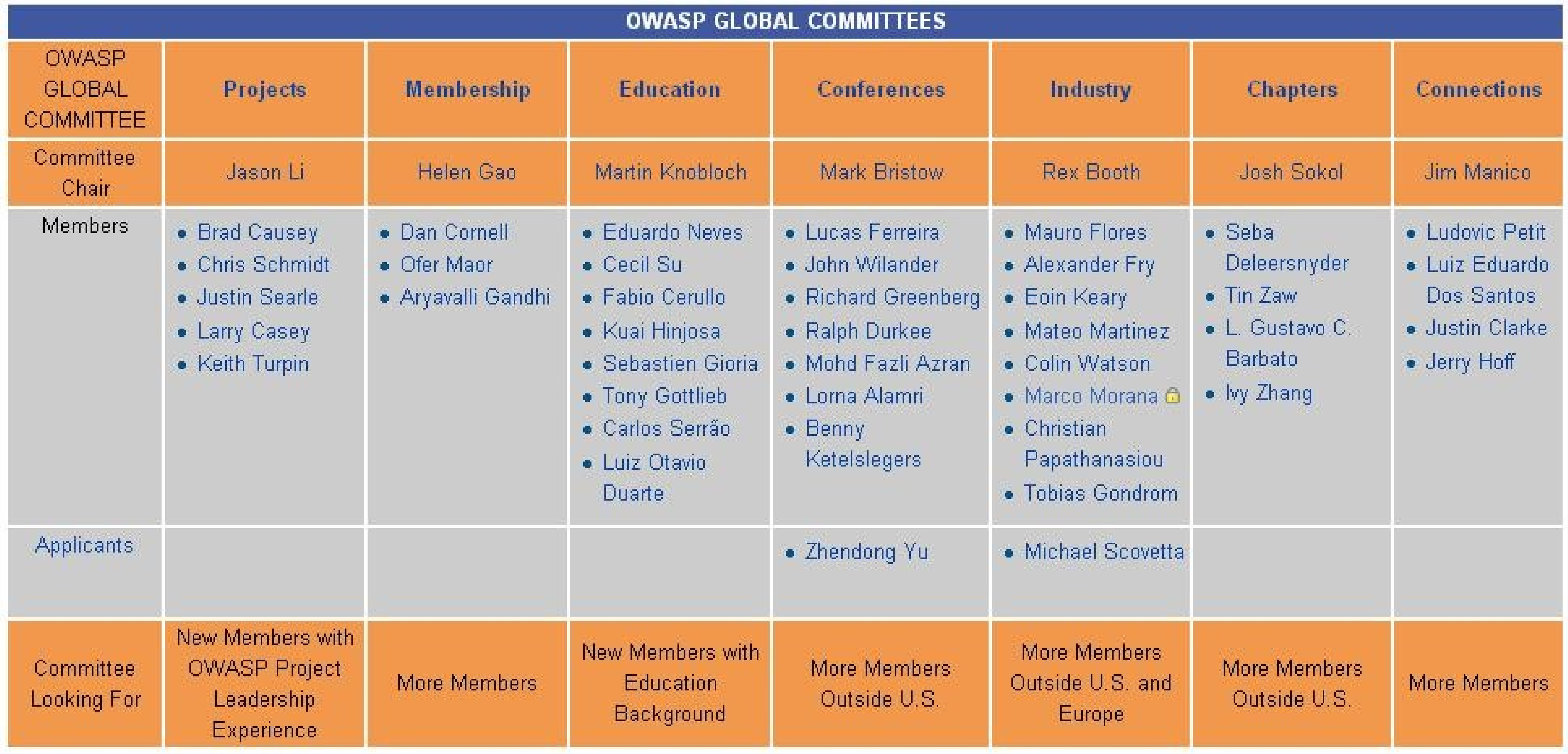
Video Tutorials

Training Sessions

Social Networking

/ Global Committees

OWASP
The Open Web Application Security Project



OWASP GLOBAL COMMITTEES

OWASP GLOBAL COMMITTEE	Projects	Membership	Education	Conferences	Industry	Chapters	Connections
Committee Chair	Jason Li	Helen Gao	Martin Knobloch	Mark Bristow	Rex Booth	Josh Sokol	Jim Manico
Members	• Brad Causey • Chris Schmidt • Justin Searle • Larry Casey • Keith Turpin	• Dan Cornell • Ofer Maor • Aryavalli Gandhi	• Eduardo Neves • Cecil Su • Fabio Cerullo • Kuai Hinjosa • Sebastien Gioria • Tony Gottlieb • Carlos Serrão • Luiz Otavio Duarte	• Lucas Ferreira • John Wilander • Richard Greenberg • Ralph Durkee • Mohd Fazli Azran • Lorna Alamri • Benny Ketelslegers	• Mauro Flores • Alexander Fry • Eoin Keary • Mateo Martinez • Colin Watson • Marco Morana • Christian Papathanasiou • Tobias Gondrom	• Seba Deleersnyder • Tin Zaw • L. Gustavo C. Barbato • Ivy Zhang	• Ludovic Petit • Luiz Eduardo Dos Santos • Justin Clarke • Jerry Hoff
Applicants				• Zhendong Yu	• Michael Scovetta		
Committee Looking For	New Members with OWASP Project Leadership Experience	More Members	New Members with Education Background	More Members Outside U.S.	More Members Outside U.S. and Europe	More Members Outside U.S.	More Members

Cheat Sheets

OWASP
The Open Web Application Security Project

Developer Cheat Sheets

- OWASP Top Ten Cheat Sheet
- Authentication Cheat Sheet
- Cross-Site Request Forgery (CSRF) Prevention Cheat Sheet
- Cryptographic Storage Cheat Sheet
- Input Validation Cheat Sheet
- XSS (Cross Site Scripting) Prevention Cheat Sheet
- DOM based XSS Prevention Cheat Sheet
- Forgot Password Cheat Sheet
- Query Parameterization Cheat Sheet
- SQL Injection Prevention Cheat Sheet
- Session Management Cheat Sheet
- HTML5 Security Cheat Sheet
- Transport Layer Protection Cheat Sheet
- Web Service Security Cheat Sheet
- Logging Cheat Sheet
- JAAS Cheat Sheet

Mobile Cheat Sheets

- IOS Developer Cheat Sheet
- Mobile Jailbreaking Cheat Sheet

Draft Cheat Sheets

- Access Control Cheat Sheet
- REST Security Cheat Sheet
- Abridged XSS Prevention Cheat Sheet
- PHP Security Cheat Sheet
- Password Storage Cheat Sheet
- Secure Coding Cheat Sheet
- Threat Modeling Cheat Sheet
- Clickjacking Cheat Sheet
- Virtual Patching Cheat Sheet
- Secure SDLC Cheat Sheet
- Web Application Security Testing Cheat Sheet
- Application Security Architecture Cheat Sheet

Zed Attack Proxy

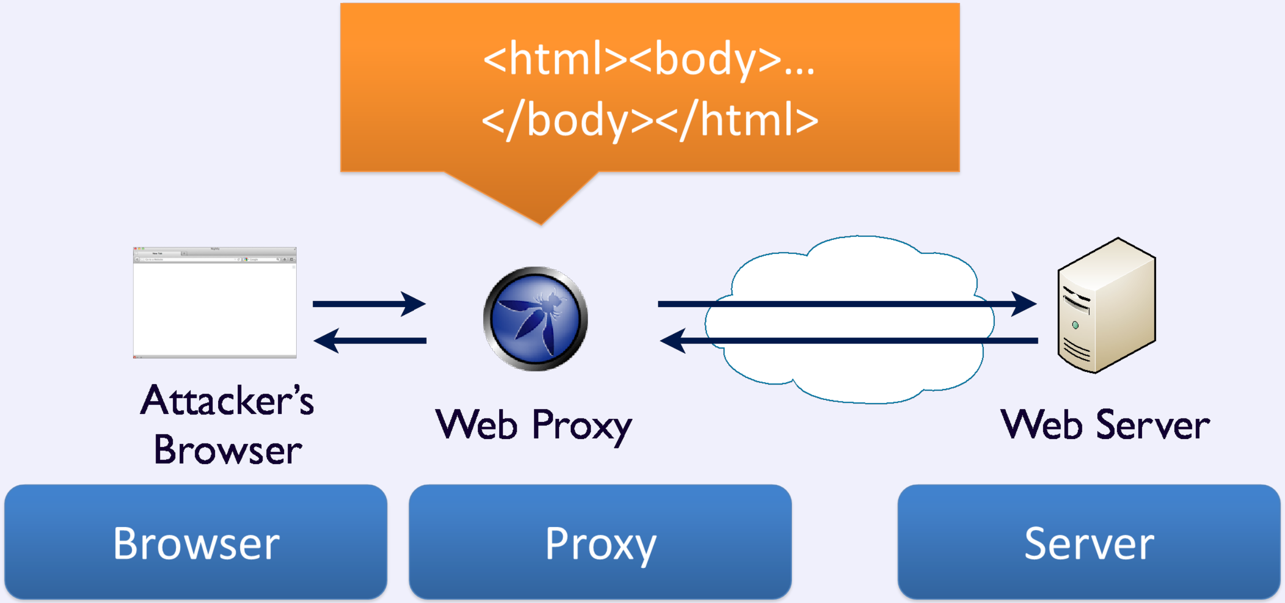
OWASP
The Open Web Application Security Project

Project Leader: Simon Bennetts (aka Psiinon), psiinon@gmail.com

Purpose: The Zed Attack Proxy (ZAP) provides automated scanners as well as a set of tools that allow you to find security vulnerabilities manually in web applications.

Last Release: ZAP 1.4.1 – *August 2012*

for Reboot


<html><body>…
</body></html>

Attacker's Browser

Web Proxy

Web Server

Browser

Proxy

Server

https://www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project

Mobile Security Project

OWASP
The Open Web Application Security Project

Project Leader: Jack Mannino, Jack@nvisiumsecurity.com

Purpose: Establish an OWASP Top 10 Mobile Risks. Intended to be platform-agnostic. Focused on areas of risk rather than individual vulnerabilities.

Deliverables

- Top 10 Mobile Risks *(currently Release Candidate v1.0)*
- Top 10 Mobile Controls *(OWASP/ENISA Collaboration)*
    - Wiki OWASP, ‘Smartphone Secure Development Guidelines’ (ENISA)
- Mobile Cheat Sheet Series
- OWASP GoatDroid Project
- OWASP Mobile Threat Model Project

SELECTED QUALITY ★ SELECTED QUALITY ★ SELECTED QUALITY ★
SELECTED

for Reboot

https://www.owasp.org/index.php/OWASP_Mobile_Security_Project

Top 10 Mobile Risks

OWASP
The Open Web Application Security Project

- M1. Insecure Data Storage
- M2. Weak Server Side Controls
- M3. Insufficient Transport Layer Protection
- M4. Client Side Injection
- M5. Poor Authorization and Authentication
- M6. Improper Session Handling
- M7. Security Decisions via Untrusted Inputs
- M8. Side Channel Data Leakage
- M9. Broken Cryptography
- M10. Sensitive Information Disclosure

“If you think education is expensive, you should try ignorance!”

APT

' ;

- You can’t improve what you can’t measure
- **We need to…**
  - Experiment
  - Share what works and what does not
  - Collaborate our efforts
- Expect another 10 years!

CORE MISSION

The Open Web Application Security Project (OWASP) is a 501c3 not-for-profit also registered in Europe as a worldwide charitable organization focused on **improving the security of software.**

Our mission is to **make application security visible**, so that people and organizations can **make informed decisions** about true application security risks.

Everyone is welcomed to participate in OWASP and all of our materials are available **under free and open software licenses.**

Core Values

OPEN Everything at OWASP is radically transparent from our finances to our code.

INNOVATION OWASP encourages and supports innovation/experiments for solutions to software security challenges.

GLOBAL Anyone around the world is encouraged to participate in the OWASP community.

INTEGRITY OWASP is an honest and truthful, vendor agnostic, global community.

Approach = "Open"

OWASP
The Open Web Application Security Project

- Open means rough consensus and running code
- Open means free to use and modify
- Open means independent
- Open means open information sharing
- Open means wider audience and participation
- Open means everyone is a peer in this global community

WHY OWASP WILL WIN?

BECAUSE OF YOU!

Jim Manico and Jerry Hoff

jim@owasp.org jerry@owasp.org