



Where we are Where we are going

Seba Deleersnyder
seba@owasp.org
OWASP Foundation Board Member

Core Mission

The Open Web Application Security Project (OWASP) is a not-for-profit worldwide organization 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 true application security risks.

Everyone is free to participate in OWASP and all of our materials are available under a free and open software license.

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

Celebrating 10 years



<http://web.archive.org> Dec 2011

Owasp
OPEN WEB APPLICATION SECURITY PROJECT

Home: About OWASP

OWASP PROJECT COMMITTEE

The Project Committee is responsible for the organisation of OWASP including running this web site, funding, setting up the OWASP foundation. It also organizes speaking opportunities on behalf of the project and deals with press and publishing.

Mark Curphey Chair Charles Schwab	Dennis Groves Vice Chair	Kevin Jeong Site Manager
--	------------------------------------	------------------------------------

OWASP TECHNICAL STEERING COMMITTEE

The Technical Committee is made up of renowned application security experts who ensure that the work and ideas are technically sound. These people have a wealth of experience and knowledge and will be guiding much of the direction of the work in various areas. As well as participating on the mailing list the technical committee has a monthly conference call to discuss progress. They are the OWASP technical think tank!

Greg Hoglund ClickToSecure	Elias Levy SecurityFocus	John Viega Secure Software	Chris Wysopal @Stake
--------------------------------------	------------------------------------	--------------------------------------	--------------------------------

OWASP USER COMMITTEE

The User Committee was created to solicit feedback from the end users and developers of web applications and web systems. We have received lots of ideas on what work people feel is needed or where knowledge is lacking and the user committee gives us the ability to formally capture that feedback from the people that own and build these systems. This also ensures that the technical correct work is useful in the real world. The committee is run by **Robert Rodger** of the Bank of Bermuda.

Robert "Bob" Rodger Bank of Bermuda	John Blumenthal
---	------------------------

OWASP ACTIVE CONTRIBUTORS

Jeremiah Grossman White Hat Security	Izhar Bj-Gad Sanctum	David Endler iDefense	Martin Eizner
Bill Hau IBM	Sverre Huseby	Bill Pennington Guardent	Tim Smith Dimension Data
Nigel Tranter Finaplex	David Zimmer	David Wong Foundstone	

Home - Get Involved - Projects - Schedule - Tools - Tutorials - Contact

Copyright © 2011 The Open Web Application Security Project

Numbers

OWASP tools and documentation:

~15,000 downloads (per month)

~30,000 unique visitors (per month)

~2 million website hits (per month)

OWASP community is blossoming worldwide

1500+ OWASP Members in active chapters worldwide

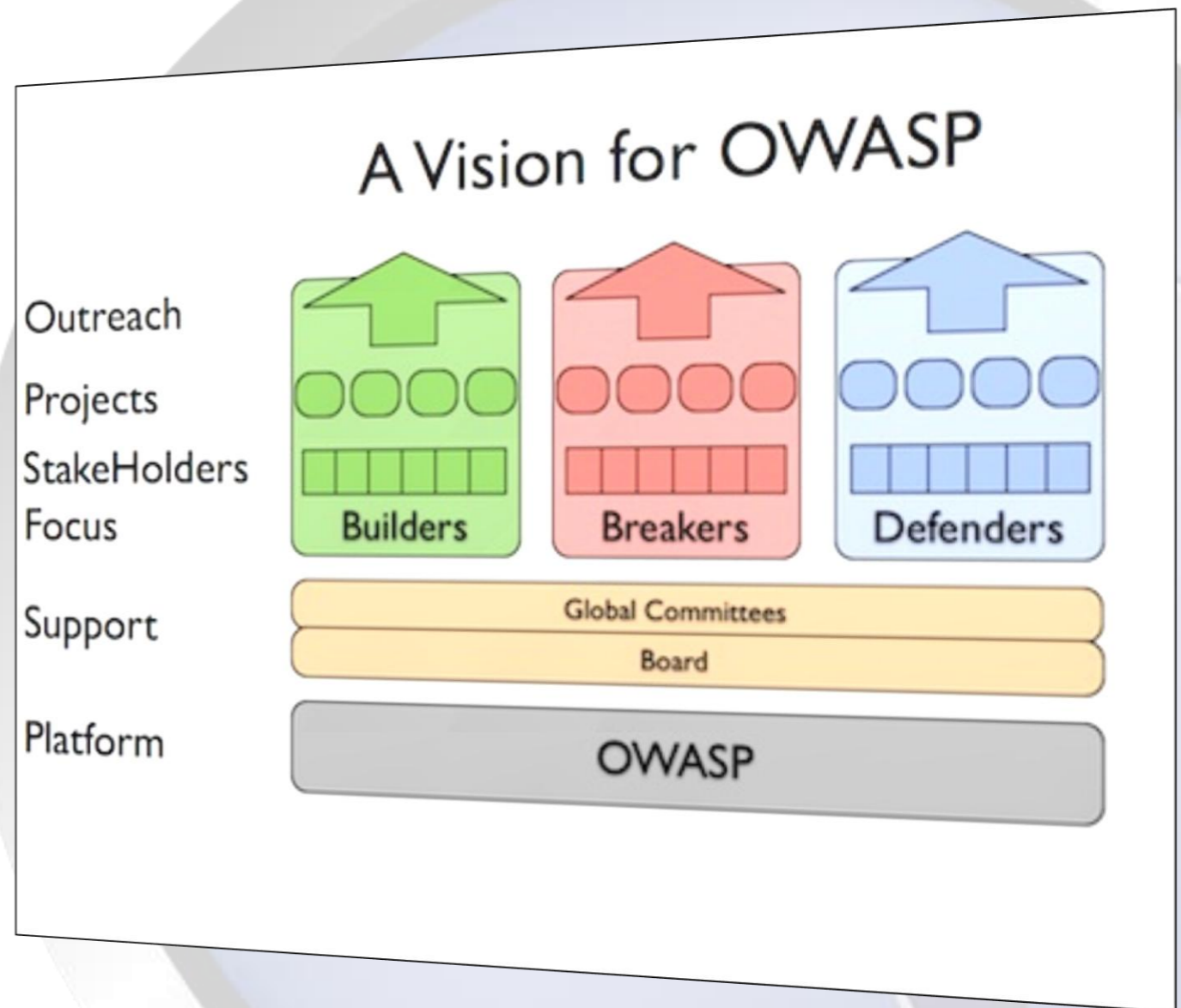
20,000+ participants

~140 Projects

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).



New projects – last months

Common Numbering Project
HTTP Post Tool
Forward Exploit Tool Project
Java XML Templates Project
ASIDE Project
Secure Password Project
Secure the Flag Competition Project
Security Baseline Project
ESAPI Objective – C Project
Academy Portal Project
Exams Project
Portuguese Language Project
Browser Security ACID Tests Project
Web Browser Testing System Project
Java Project
Myth Breakers Project
LAPSE Project
Software Security Assurance Process
Enhancing Security Options Framework

German Language Project
Mantra – Security Framework
Java HTML Sanitizer
Java Encoder Project
WebScarab NG Project
Threat Modelling Project
Application Security Assessment Standards Project
Hackademic Challenges Project
Hatkit Proxy Project
Hatkit Datafiddler Project
ESAPI Swingset Interactive Project
ESAPI Swingset Demo Project
Web Application Security Accessibility Project
Cloud - 10 Project
Web Testing Environment Project
iGoat Project
Opa
Mobile Security Project – Mobile Threat Model
Codes of Conduct

Spotlight

Zed Attack Proxy (ZAP):

- Intercepting Proxy
- Automated scanner
- Passive scanner
- Brute Force scanner
- Spider
- Fuzzer
- Port scanner
- Dynamic SSL certificates
- API
- Beanshell integration

- 5 main coders, 15 contributors
- Fully internationalized
- Translated into 9 languages: Brazilian Portuguese, Chinese, French, German, Greek, Indonesian, Japanese, Polish, Spanish

Untitled Session - OWASP ZAP

File Edit View Analyse Report Tools Help

Sites

- http://localhost:8080
 - GET:RELEASE-NOTES.txt
 - GET:bodgeit
 - bodgeit
 - GET:about.jsp
 - GET:admin.jsp
 - GET:basket.jsp
 - GET:contact.jsp
 - GET:home.jsp
 - GET:login.jsp
 - GET:logout.jsp
 - GET:password.jsp
 - GET:product.jsp(prodid)
 - GET:product.jsp(typeid)
 - GET:register.jsp
 - GET:score.jsp
 - POST:basket.jsp(price,productid,qu
 - POST:basket.jsp(quantity_31,quant
 - POST:basket.jsp(update)
 - POST:contact.jsp(comments,null)
 - POST:contact.jsp(comments,test2c

POST:login.jsp(password,username)

Filter history

Select the required filters below. You can select in each element. An element is not used for filter of the rows in it are selected.

Methods:	Codes:	Tags:
<input type="checkbox"/> OPTIONS	100	<input type="checkbox"/> Form
<input type="checkbox"/> GET	101	<input type="checkbox"/> Hidden
<input type="checkbox"/> HEAD	200	<input type="checkbox"/> Password
<input type="checkbox"/> POST	201	<input type="checkbox"/> Script
<input type="checkbox"/> PUT	202	
<input type="checkbox"/> DELETE	203	
<input type="checkbox"/> TRACE	204	
<input type="checkbox"/> CONNECT	205	

Notes: Ignore

Cancel Clear Apply

History Search Break Points Alerts Active Scan Spider Brute Fo

Filter: OFF

1	GET	http://localhost:8080/bodgeit/
3	GET	http://localhost:8080/bodgeit/product.jsp?typeid=6
5	GET	http://localhost:8080/bodgeit/product.jsp?typeid=2
6	GET	http://localhost:8080/bodgeit/product.jsp?prodid=6
7	GET	http://localhost:8080/bodgeit/images/130.png
8	GET	http://localhost:8080/bodgeit/images/129.png
10	POST	http://localhost:8080/bodgeit/basket.jsp
11	GET	http://localhost:8080/bodgeit/product.jsp?typeid=7
12	GET	http://localhost:8080/bodgeit/product.jsp?prodid=31
13	POST	http://localhost:8080/bodgeit/basket.jsp

Alerts 2 1 2 0

Spotlight

OWASP Mobile Security:

- Security testing
- Development guidance
- Top 10 controls
- Mobile threat model
- GoatDroid
- Top 10 risks

Top 10 Mobile Risks:

1. Insecure Data Storage
2. Weak Server Side Controls
3. Insufficient Transport Layer Protection
4. Client Side Injection
5. Poor Authorization and Authentication
6. Improper Session Handling
7. Security Decisions Via Untrusted Inputs
8. Side Channel Data Leakage
9. Broken Cryptography
10. Sensitive Information Disclosure



220 Chapters ~ 100 active



Conferences

Global AppSec Events

Global AppSec Events	Date	Location	GCC Rep	OWASP Introduction/Keynote
Global AppSec North America 2011	Sept. 20, 2011 - Sept. 23, 2011	Minneapolis, MN, USA	Mark Bristow	Entire Board
Global AppSec Latin America 2011	Oct. 4, 2011 - Oct. 7, 2011	Porto Alegre, Brazil	Lucas Ferreira	Tom Brennan
Global AppSec Asia 2011	Nov. 8, 2011 - Nov. 11, 2011	Beijing, China	Lucas Ferreira	Seba
Global AppSec AsiaPac 2012	March 12, 2012 - March 16, 2012	Sydney, Australia	Mohd Fazli Azran	TBD
Global AppSec Research 2012 (Wiki)	July 10, 2012 - July 13, 2012	Athens, Greece	John Wilander	TBD
Global AppSec North America 2012	Oct. 22, 2012 - Oct. 26, 2012	Austin, TX	TBD	Entire Board
Global AppSec Latin America 2012	Nov. 14, 2012 - Nov. 16, 2012	Buenos Aires, Argentina	TBD	TBD

Regional and Local Events

Event	Type	Date	Location	OWASP Introduction/Keynote
OWAND'11	Local Event	Sept. 13, 2011 - Sept. 13, 2011	Cádiz	TBD
OWASP Israel 2011	Regional Event	Sept. 15, 2011 - Sept. 15, 2011	Herzliya, Israel	TBD
[OWASP DAY KL 2011]	Local Event	Sept. 20, 2011 - Sept. 21, 2011	Kuala Lumpur, Malaysia	TBD
OWASP BASC 2011	Local Event	Oct. 8, 2011 - Oct. 8, 2011	Cambridge, MA	TBD
OWASP Day Mexico 2011	Local Event	Nov. 10, 2011 - Nov. 11, 2011	Aguascalientes, MX	TBD
Germany OWASP Day 2011 #4	Local Event	Nov. 17, 2011 - Nov. 17, 2011	München	TBD
OWASP BeNeLux 2011	Regional Event	Nov. 30, 2011 - Dec. 1, 2011	Luxembourg	TBD
AppSec DC 2012	Regional Event	April 2, 2012 - April 5, 2012	Washington, DC	TBD



**OWASP
SUMMIT
2011**

**LISBON
PORTUGAL
FEB 8-11**

“I saw the ‘blossoming’ of OWASP in Portugal’s Spring. From an external viewpoint, OWASP has moved from niche to widely relevant, from localized to global, from pen testing to SDLC, from server to every component of the application’s delivery and use, from InfoSec to business process relevance.”
– Colin Watson



Massive Outreach

- OWASP-Portugal Partnership
- OWASP Outreach to Educational Institutions
- OWASP Industry Outreach
- OWASP Browser Security Project
- OWASP-Apache Partnership
- OWASP Mobile Security Initiative
- OWASP Governance Expansion
- International Focus
- Application Security Programs
- Application Security Certification



Board Election

- OWASP Governance maturing – OWASP updated its Bylaws and worked out procedures for the Board elections. These governance updates support the dynamic and growing OWASP community.
- Currently (5) board members are elected.

2011 Election Results

OWASP is a non-profit governed according to its [mission](#), [ethics](#), [core purpose](#), and [bylaws](#).

Turnout: 771 (46.2%) of 1670 electors voted in this ballot.

Top (3) have been elected.

Michael Coates - 524 (31.0%)

Dave Wichers - 460 (27.2%)


Sebastien Deleersnyder - 423 (25.0%)

Christian Heinrich - 286 (16.9%)

6 June 2011

- OWASP Europe non-profit established
- Global extension of organisation
- Legal & financial support

Mod 2.2


Federale Overheidsdienst
Justitie

Luik A : In alle gevallen in te vullen
Luik B : Bekend te maken tekst in de bijlagen bij het Belgisch Staatsblad
Luik C : Enkel in te vullen bij oprichting

In te vullen door de griffie

Aantal Bladzijden Blz(n)

Tarief Oprichting
 Tarief Wijziging
 Gratis bekendmaking

Verenigingen, Stichtingen en Organismen

In hoofdletters invullen en bij de eerste neerlegging ter griffie voegen

Aanvraagformulier I tot inschrijving (KBO) en/of tot bekendmaking in de bijlagen bij het Belgisch Staatsblad

Niet invullen bij oprichting

Luik A Identificatie

1° Ondernemingsnummer :

2° Benaming
(voluit) : **OWASP Europe**
(verkort) :

Evt. letterwoord :

3° Rechtsvorm : Vereniging zonder winstoogmerk
Andere :

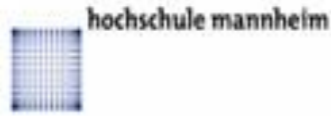
Global Committees

OWASP GLOBAL COMMITTEES							
OWASP GLOBAL COMMITTEE	Projects	Membership	Education	Conferences	Industry	Chapters	Connections
Committee Chair	Jason Li	Dan Cornell	Martin Knobloch	Mark Bristow	Rex Booth	Tin Zaw	Jim Manico
Members	<ul style="list-style-type: none"> ■ Brad Causey ■ Chris Schmidt ■ Justin Searle ■ Larry Casey ■ Keith Turpin 	<ul style="list-style-type: none"> ■ Michael Coates ■ Ofer Maor ■ Helen Gao 	<ul style="list-style-type: none"> ■ Eduardo Neves ■ Cecil Su ■ Fabio Cerullo ■ Kuai Hinjosa ■ Sebastien Gioria ■ Tony Gottlieb ■ Carlos Serrão 	<ul style="list-style-type: none"> ■ Lucas Ferreira ■ John Wilander ■ Richard Greenberg ■ Ralph Durkee ■ Cassio Goldschmidt ■ Mohd Fazli Azran 	<ul style="list-style-type: none"> ■ Joe Bernik ■ Lorna Alamri ■ David Campbell ■ Mauro Flores ■ Alexander Fry ■ Eoin Keary ■ Nishi Kumar ■ Mateo Martinez ■ Colin Watson ■ Marco Morana ■ Sherif Koussa ■ Christian Papathanasiou 	<ul style="list-style-type: none"> ■ Andrew van der Stock ■ Seba Deleersnyder ■ Puneet Mehta ■ Josh Sokol ■ Mandeep Khara ■ L. Gustavo C. Barbato 	<ul style="list-style-type: none"> ■ Justin Clarke ■ Doug Wilson ■ Ludovic Petit
Applicants		<ul style="list-style-type: none"> ■ Aryavalli Gandhi 		<ul style="list-style-type: none"> ■ Zhendong Yu 	<ul style="list-style-type: none"> ■ Michael Scovetta 		<ul style="list-style-type: none"> ■ Jerry Hoff
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

OWASP Members



Academic Supporters



Organization Supporters





Strategic Goals



2012 Strategic Goals

Build the OWASP platform

Expand communication channels

Grow the OWASP community

Financial stability



OWASP Platform

Define the processes, resources, and tools to enable volunteers to quickly join and contribute to OWASP in the areas of projects, chapters, education, conferences and connections

Communication Channels

Establish effective communication channels into developer groups, universities, and industry groups

OWASP Community

Build and grow the OWASP community throughout the world by focusing on the quality of chapters, conferences, and social technologies

Financial Stability

Further build out a stable financial foundation and create new sources of income for the organisation to achieve the goals of 2012 and future years.



Our Challenge



Application Security Is Just Getting Started

- You can't improve what you can't measure
- We need to...
 - Experiment
 - Share what works
 - Combine our efforts
- Expect another 10 years!

Call for action

- Start or join your OWASP chapter
- Start or join OWASP projects
- Translate material (documents, tool interfaces)
- Join as member
- Become active in OWASP organisation (committees, board election 2013)
- Together we will achieve our mission!



Enjoy German OWASP Day 2011

