OWASP

Update 25-January-2012

Seba Deleersnyder
Foundation Board, SAIT Zenitel Belgium
seba@owasp.org

Agenda

Introduction

Survey

OWASP Near You

Introduction

OWASP

The Open Web Application Security Project

http://www.owasp.org

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.

Thank you

Location sponsor

cisco

OWASP supporter

ascure

Sponsors Belgium 2011/2012

sait zenitel

ZION SECURITY
SECURING YOUR BUSINESS VALUE

BARRACUDA
NETWORKS

f5

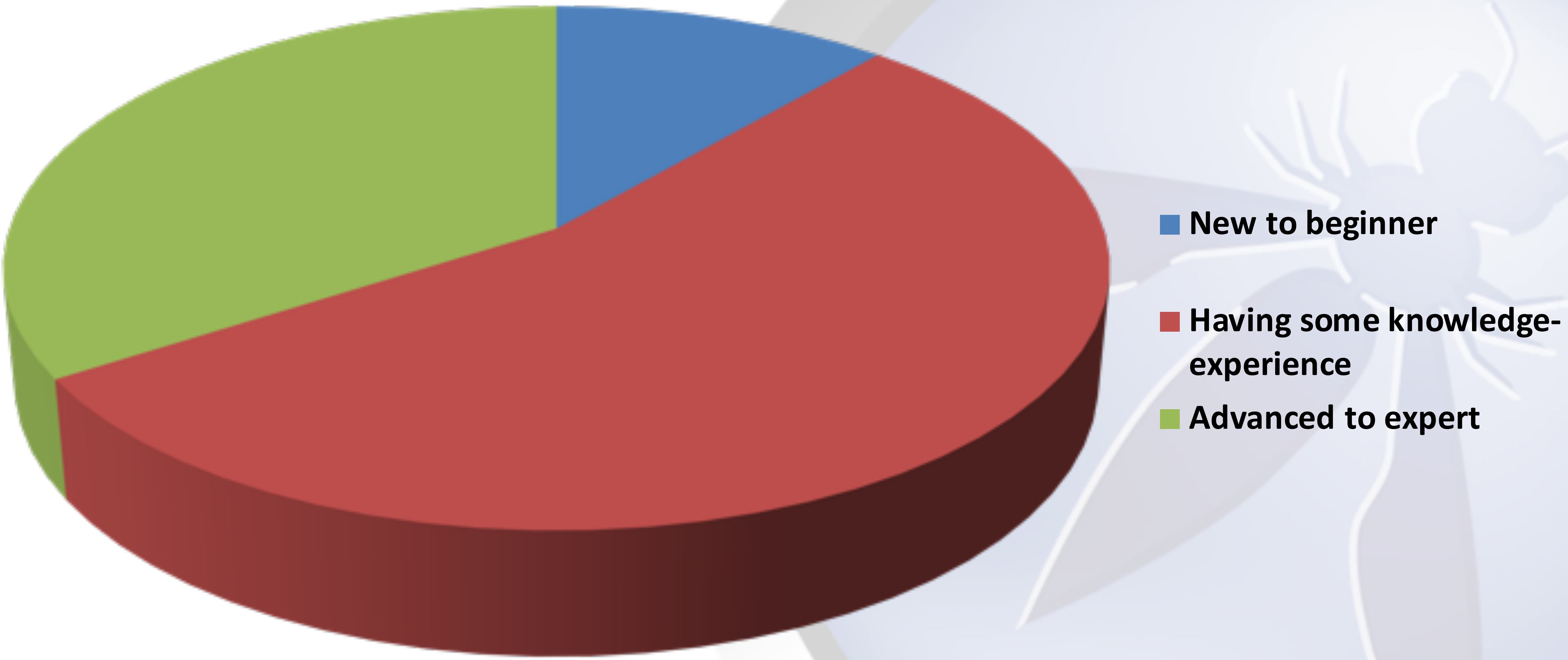
OWASP cannot recommend the use of products, services, or recommend specific companies

Program

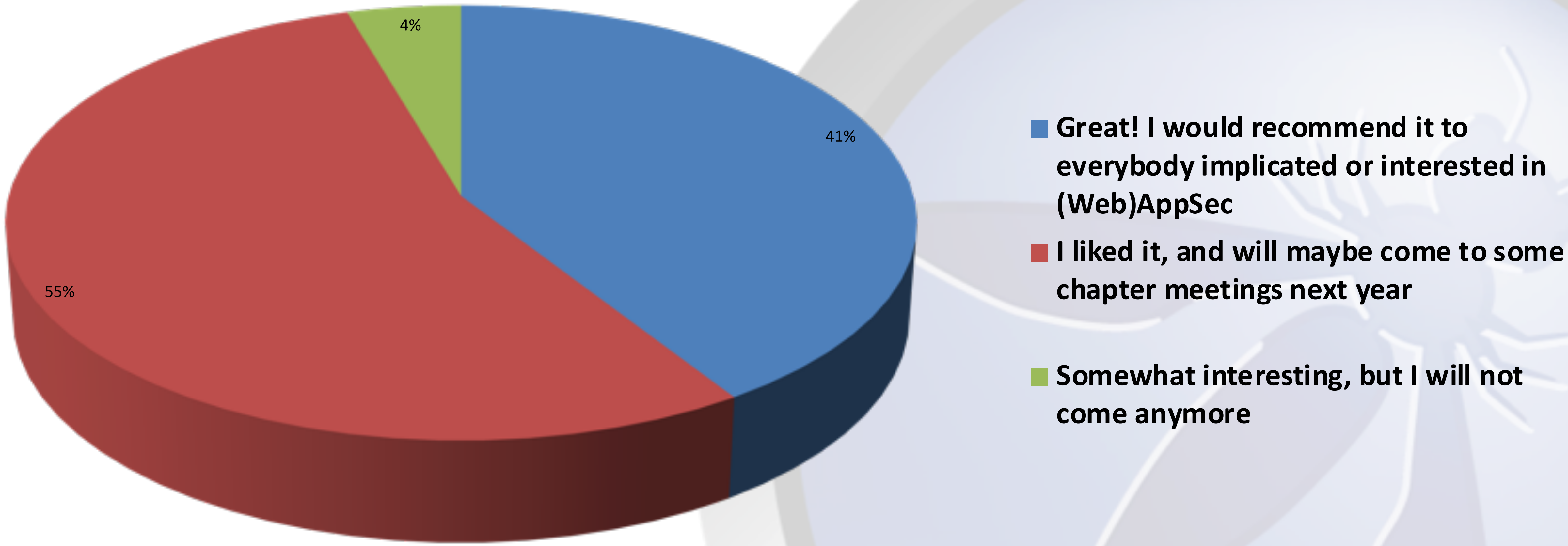
18h30 – 18h45	**OWASP update**	Seba Deleersnyder
18h45 - 19h45	**devops, secops, devsec or *ops?** **A gentle introduction to Devops** Kris Buytaert	
19h45 - 20h00	*Break*	
19h50 - 20h45	**Hardening web applications against malware attacks** Erwin Geirnaert	

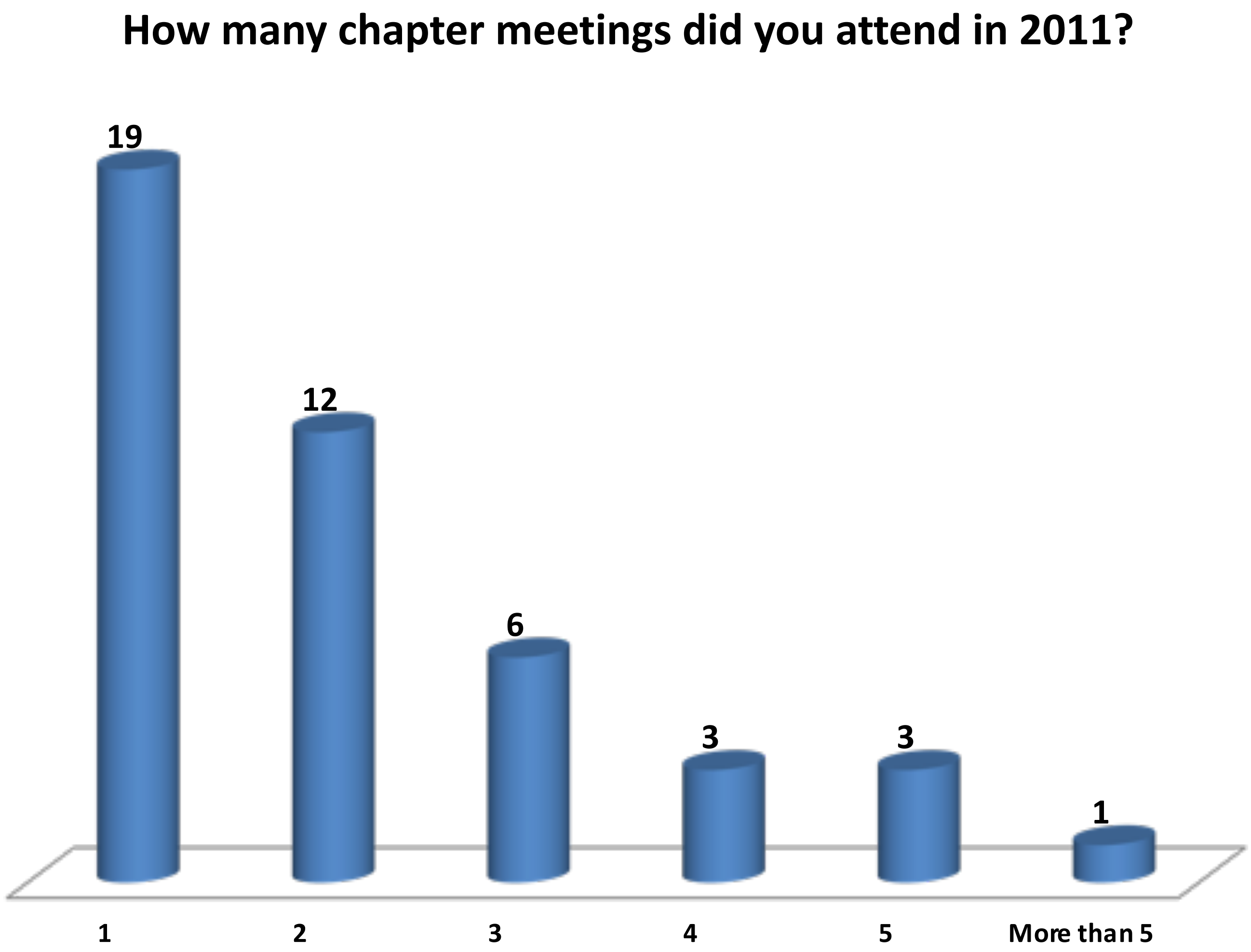
Survey

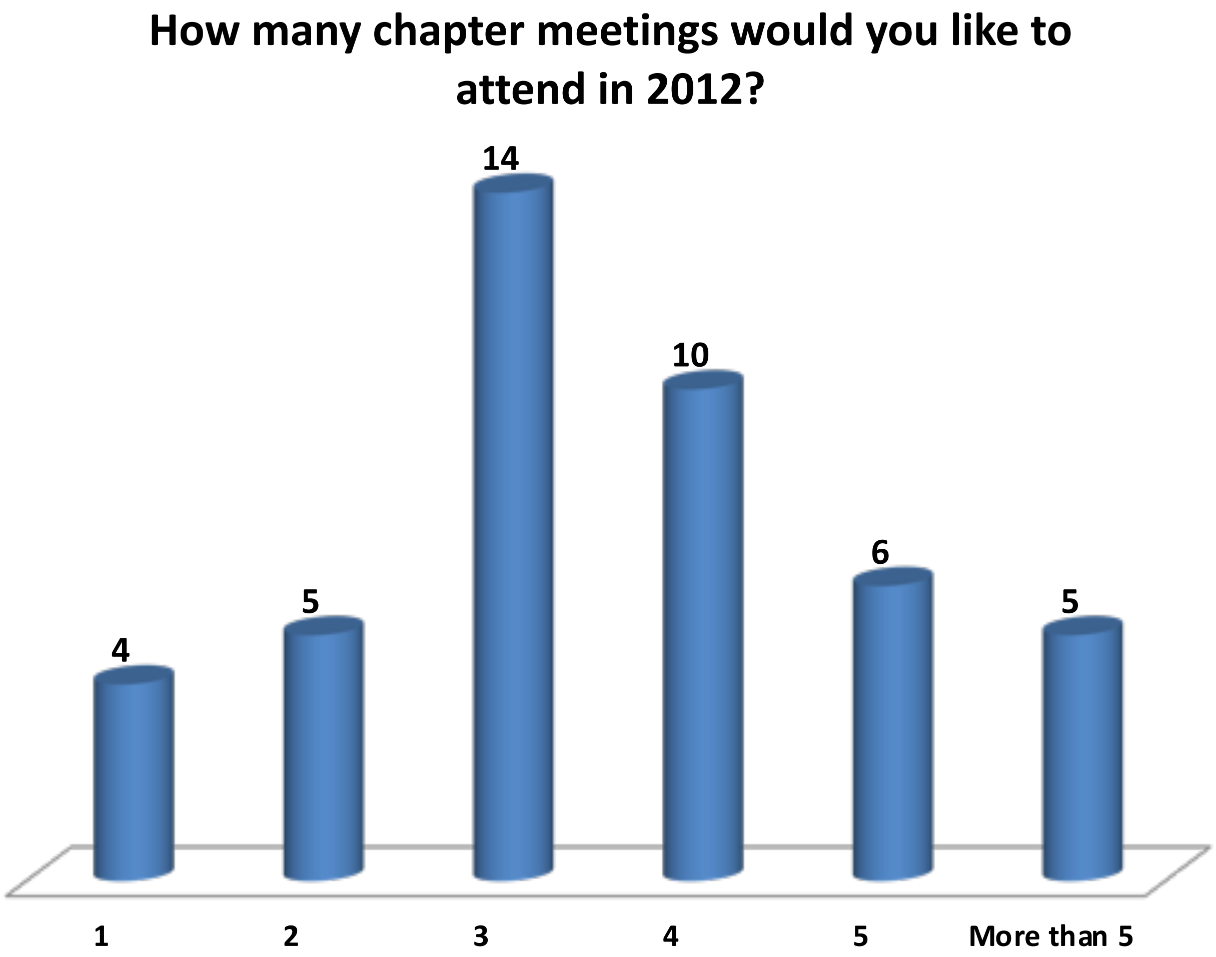
44 responses



Opinion 2011 Events




How many chapter meetings did you attend in 2011?
19
12
6
3
3
1
1
2
3
4
5
More than 5


How many chapter meetings would you like to attend in 2012?
4
5
14
10
6
5
1
2
3
4
5
More than 5

DIY

- If given some time to prepare a topic, would you consider preparing a session for a chapter meeting:
  - No: 24
  - Yes: 20 (7 blanks ☺)

Topic wish list 2012?

- **more on sdlc**, threat modeling and source code analysis.
- As a developer I am interested in **tools and frameworks** that help me tackle security issues, or threats, without the need to be an expert. Focusing on security is still considered far less important than added business value.
- Cloud security, **mobile security**, SDLC
- mod-security
- flash security
- Html5
- Increasing importance of security and continue the awareness pls!
- Up to date threats and responses.
- Security & reliability of software used in the critical infrastructures
- Security of mission-critical software applications
- Digital forensics analysis
- threat modeling, comparison SAST/DAST, **HTML5**, Cloud (security in RESTful environments)
- General questions as **how to implement** application security in your company.
- A Detail description about a current **malware**, how does it work, what is going on today on the internet. What are the trends.
- What do we have as solutions on the market ...
- Secure software development lifecycle
- Overview of web browser based authentication protocols.
- WS-* security architecture (tokens, proof-of-possessions, Bearer tokens and ActAs, STS, secure conversations, mixing WS-Federation passive profile with WS-Trust active profile).
- Reputation,
- Federated identities,
- Why SQL injections/XSS are still vulnerabilities?
- **Advanced SQL injection** (time based SQLi, practical session on different encodings), DNS tunneling as data ex-filtration example, attacks against 'safer' frameworks such as JAVA apps using spring/hibernate (e.g. is SQLi really not possible, how to do code injection), as many new attack types as possible, hands on explanations on topics such as JSON, AJAX (how to corrupt/change the data etc.),
- analysis of recent security incidents (what failed, which countermeasures would have helped)
- how to **defend/motivate security** related projects when IT budgets are under pressure

- Threat analysis
- Vulnerability mitigation for upcoming technologies (HTML5, GWT, ...)
- Open to anything but Privacy would be top of my list at the moment
- secure coding guidelines for J2EE/C/C++
- static code analysis tools review
- security aspects of **web frameworks**
- malware analysis
- Top 25 webapp **vulnerabities in DEPTH** ;-)
- Demos ! It is always awesome when you can see a live attack/feature from end-to-end.
- Something more practical, more related to the feasability.
- advanced pentesting techniques
- interesting frameworks and mitigation techniques
- **SAP security**
- - Advancement of **ESAPI** and other OWASP projects
- - latest attack techniques
- - state of the situation on **web app scanners**
- Instead of the focus on development techniques, also attention to **detection (post-factum)** of possible issues?
- - (Network) Detection techniques for Servers / Clients with rogue code / infections
- - Forensics for beginners: Quick-scan for OS/Application-compromise
- Hacking TCP/IP internet protocols.
- Security **trends**.
- New open source security initiatives.
- Security tooling.
- Security best practices and patterns.
- **Hackers in 'demo' action.**
- Hardening network or OS.
- Safest browser.
- Security related to social networks.
- Advanced Persistent Threat
- virtualisation/cloud computing and its effects on PCI compliance

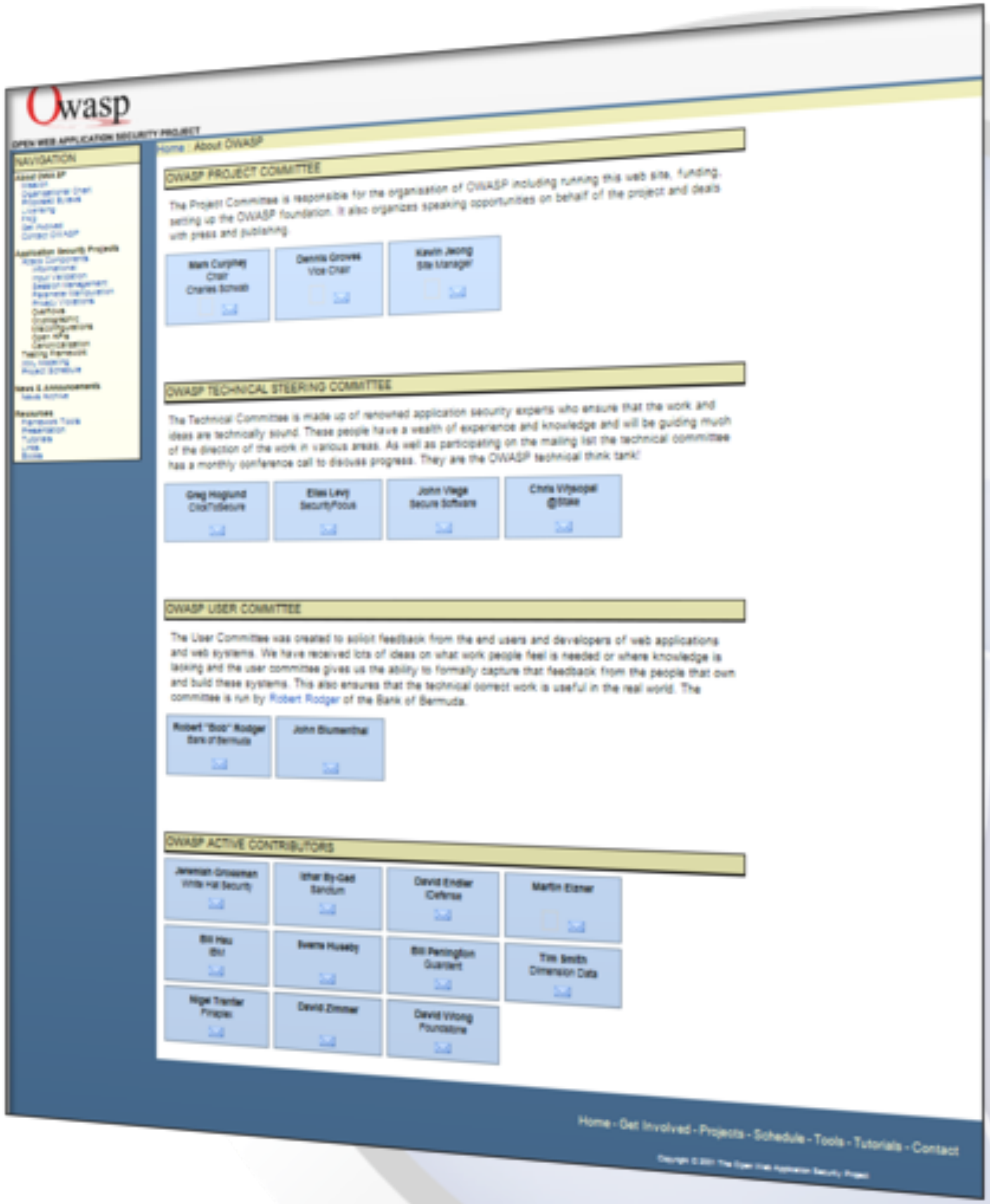
Recommendations 2012?

- Job postings, panel discussions, more beers :-)
- Discussion panel, walking diner
- The events are fine as they are. Their format and all.
- Some kind of 'more than formal' interactions with the peers - such as a **week-end camp** of security practitioners.
- I think you guys are doing a great job at the chapter meetings, I see them as an example of how chapter meetings need to be.
- 1 - A good speaker
- 2 - A good subject
- At the end of a presentation, have a **moderator** try to trigger an **open discussion**.
- Attending talks about infosec is great but I can do that on Youtube. We need to find a way to have something more, something where there is **interaction around a subject**. Maybe have a session on Youtube, everyone watches it, tries some things around the subject, submits some thoughts and we gather to discuss things. I don't really know how that would be but every time I attend a talk by someone who traveled a long distance to speak in front of 30 people and then leave, it makes me sad.
- some kind of **practice/hands on sessions** (should probably limited in number of attendants) to actually use the attack explained
- I like it the way it is ;-)
- As i'm a developer, I would be more interested in learning new attacks and countermeasures. In my opinion, I think there are not often technical oriented topics.
- The last session was too basic and do not cover all the topics announced.
- Keep it simple and convivial as you've done until now. Maintain the high level of your speakers, as you've done until now.
- randomize" locations, include Ghent etc…
- they are just right!
- **Involve people from the business side** as well: apart from developers / Security experts, let also business managers express their concerns / solutions for given issues ?
- Not only creating awareness, but more **live demo's** in a lab-like environment. More practical approach instead of academic approach.
- Being organized in Brussels.

OWASP near you

Celebrating 10 years

http://web.archive.org Dec 2011



Owasp
OPEN WEB APPLICATION SECURITY PROJECT
NAVIGATION
Application Security Projects
Testing Framework
News & Announcements
Resources

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 commitee 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 By-Gad
Sanctum | David Endler
iDefense | Martin Eizner

Bill Hau
IBM | Sverre Huseby | Bill Pennington
Guardent | Tim Smith
Dimension Data

Nigel Tranter
Pinapes | David Zimmer | David Wong
Foundstone

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

Copyright © 2001 The Open Web Application Security Project

2012 Strategic Goals

Build the OWASP platform

Expand communication channels

Grow the OWASP community

Financial stability

Next chapter meeting

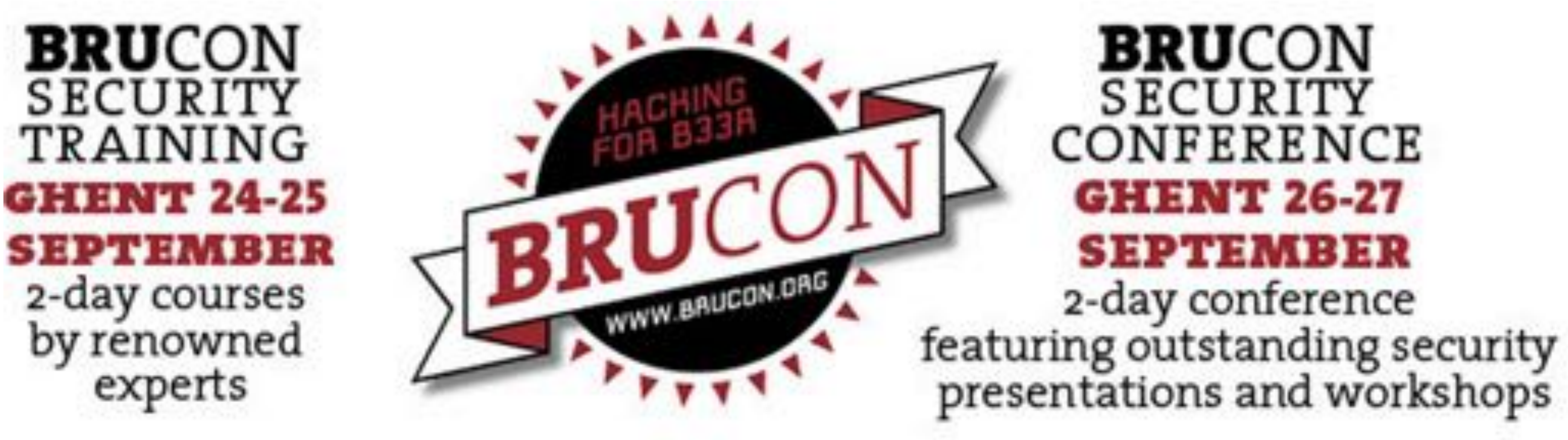
SecureApplication Development
secappdev.org

- Co-organized with SecAppDev
- 6-Mar, Leuven (Pizza's ☺)
- Mobile Security by Ken van Wyck
- Access Control Design Best Practices by Jim Manico

AppSecEU

OWASP
AppSec Research 2012
10-13 July Athens Greece

BruCON 2012



BRUCON
SECURITY
TRAINING
GHENT 24-25
SEPTEMBER
2-day courses
by renowned
experts

BRUCON
SECURITY
CONFERENCE
GHENT 26-27
SEPTEMBER
2-day conference
featuring outstanding security
presentations and workshops

BeNeLux 2012

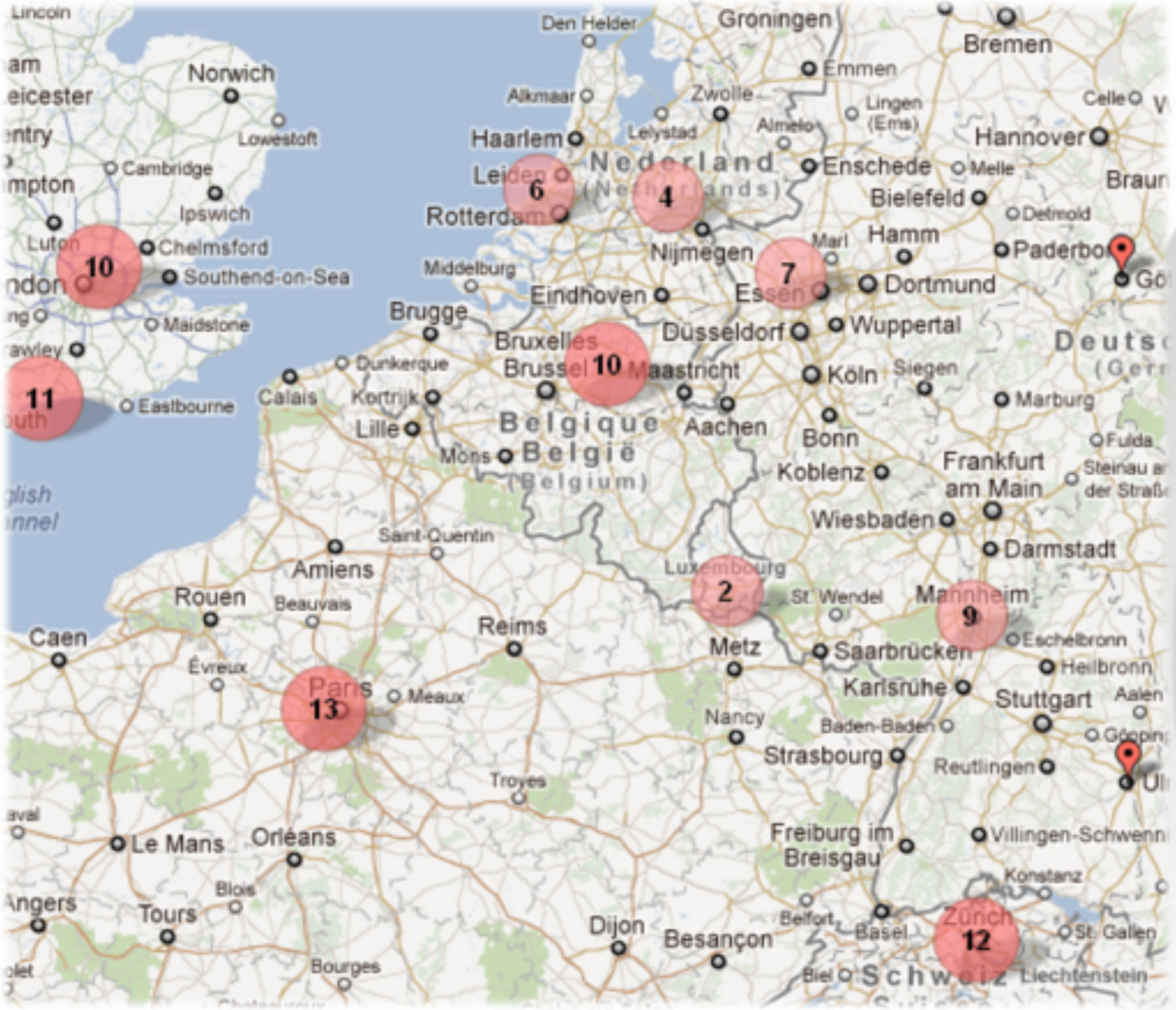
- ~ Dec 2012
  - One day OWASP Training
  - One day conference
- University of Leuven
- Details to follow...

Subscribe mailing list

www.owasp.be

Keep up to date!

Want to support OWASP?



http://batchgeo.com/map/4f35033fd964eb692a5268d81d15e18c

Become member, annual donation of:

- $50 Individual
- $5000 Corporate

Enables the support of OWASP projects, mailing lists, conferences, podcasts, grants and global steering activities…