Web hacks of 2007 and how to protect your web applications in 2008 with OWASP

Sebastien Deleersnyder, BeLux Chapter Board

Mar, 2008

OWASP
BeLux
Chapter

The OWASP Foundation
http://www.owasp.org

Seba?

- Developer + Security = AppSec Consultant
- Started OWASP Belgium Chapter
- OWASP Board Member
- Work @ Telindus

Agenda

- OWASP
- Web hacks 2007
- What to do?
- BeLux chapter

Agenda

- OWASP
- Web hacks 2007
- What to do?
- BeLux chapter

OWASP

- The Open Web Application Security Project (OWASP)
- International not-for-profit charitable Open Source organization funded primarily by volunteers time, OWASP Memberships, and OWASP Conference fees
- Participation in OWASP is free and open to all

OWASP Mission

- to make application security "visible," so that people and organizations can make informed decisions about application security risks

OWASP?

- Provide free resources to the community
  - Publications, Articles, Standards
  - Testing and Training Software
  - Local Chapters & Mailing Lists
- Dual license model:
  - Open Source Licenses
  - Commercial License for Members

www.owasp.org

Agenda

- OWASP
- Web hacks 2007
- What to do?
- BeLux chapter

Key Application Security Vulnerabilities

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

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

Top Ten Web Hacks 2007

1. XSS Vulnerabilities in Common Shockwave Flash Files
2. Universal XSS in Adobe's Acrobat Reader Plugin
3. Firefox's JAR: Protocol issues
4. Cross-Site Printing (Printer Spamming)
5. Hiding JS in Valid Images
6. Firefoxurl URI Handler Flaw
7. Anti-DNS Pinning (DNS Rebinding)
8. Google GMail E-mail Hijack Technique
9. PDF XSS Can Compromise Your Machine
10. Port Scan without JavaScript

Honorable Mention: Microsoft ASP.NET Request Validation Bypass Vulnerability (POC)

Blog poll Jeremiah Grossman (WhiteHatSec)

Public Health Warning

- XSS and CSRF have evolved
- Any website you visit could infect your browser
- An infected browser can do anything you can do
- An infected browser can scan, infect, spread
- 70-90% of web applications are 'carriers'

Examples

- Nov-07: IndiaTimes.com Visitors Risk High Exposure To Malware
  - "an entire cocktail of downloader Trojans and dropper Trojans"**434** malicious files (including scripts, binaries, cookies, and images)
- Of the sites hosing malware in 2007, 51% where legitimate sites that have been broken into (*)

(*) survey by WebSense

Recent Mass Web Attacks

- Mar-6: more than 101,000 Google search results that appeared to lead to pages of legitimate sites actually directed end users to sites that attempted to install malware (Dancho Danchev)

Search results for "photos a poil <IFRAME src=//72.232.39.252/a ...
What's new on ZDNet Asia. Search All, News, Insight, Reviews, Blogs, TechGuides, Photo Gallery, Videos, Jobs, IT Library, Downloads. Go. Create alert ...
www.zdnetasia.com/search/results.htm?query=photos+a+poil+%3CIFRAME%20src=//72.232.39.252/a/%3E.html - 43k - 17 hours ago - Cached - Similar pages

Search results for "pictures of a gorila <IFRAME src=//72.232 ...
Search All, News, Insight, Reviews, Blogs, TechGuides, Photo Gallery, Videos, Jobs, IT Library, Downloads. Go. Create alert ...
www.zdnetasia.com/search/results.htm?query=pictures+of+a+gorila+%3CIFRAME%20src=//72.232.39.252/a/%3E.html - 42k - 15 hours ago - Cached - Similar pages

Search results for "picture of a bintrong <IFRAME src=//72.232 ...
Featured Whitepapers. Search All, News, Insight, Reviews, Blogs, TechGuides, Photo Gallery, Videos, Jobs, IT Library, Downloads. Go. Create alert ...
www.zdnetasia.com/search/results.htm?query=picture+of+a+bintrong+%3CIFRAME%20src=//72.232.39.252/a/%3E.html - 42k - 15 hours ago - Cached - Similar pages

Search results for "peek a bo bikini <IFRAME src=//72.232.39.252/a ...
Featured Whitepapers. Search All, News, Insight, Reviews, Blogs, TechGuides, Photo Gallery, Videos, Jobs, IT Library, Downloads. Go. Create alert ...
www.zdnetasia.com/search/results.htm?query=peek+a+bo+bikini+%3CIFRAME%20src=//72.232.39.252/a/%3E.html - 43k - 16 hours ago - Cached - Similar pages

Search results for "peek a boo bikini <IFRAME src=//72.232.39.252 ...
What's new on ZDNet Asia. Search All, News, Insight, Reviews, Blogs, TechGuides, Photo Gallery, Videos, Jobs, IT Library, Downloads. Go. Create alert ...
www.zdnetasia.com/search/results.htm?query=peek+a+boo+bikini+%3CIFRAME%20src=//72.232.39.252/a/%3E.html - 43k - 16 hours ago - Cached - Similar pages

Search results for "kari sweets rapidshare <IFRAME src=//72.232 ...
What's new on ZDNet Asia. Search All, News, Insight, Reviews, Blogs, TechGuides, Photo Gallery, Videos, Jobs, IT Library, Downloads. Go. Create alert ...
www.zdnetasia.com/search/results.htm?query=kari+sweets+rapidshare+%3CIFRAME%20src=//72.232.39.252/a/%3E.html - 41k - 19 hours ago - Cached - Similar pages

Search results for "pee-a-poo <IFRAME src=//72.232.39.252/a/> html ...
Featured Whitepapers. Search All, News, Insight, Reviews, Blogs, TechGuides, Photo Gallery, Videos, Jobs, IT Library, Downloads. Go. Create alert ...
www.zdnetasia.com/search/results.htm?query=pee-a-poo+%3CIFRAME%20src=//72.232.39.252/a/%3E.html - 34k - 17 hours ago - Cached - Similar pages

Search results for "peek-a-boo bikini <IFRAME src=//72.232.39.252 ...
Search All, News, Insight, Reviews, Blogs, TechGuides, Photo Gallery, Videos, Jobs, IT Library, Downloads. Go. Create alert ...
www.zdnetasia.com/search/results.htm?query=peek-a-boo+bikini+%3CIFRAME%20src=//72.232.39.252/a/%3E.html - 34k - 16 hours ago - Cached - Similar pages

Search results for "port grimaud beachwear <IFRAME src=//72.232 ...
Search All, News, Insight, Reviews, Blogs, TechGuides, Photo Gallery, Videos, Jobs, IT Library, Downloads. Go. Create alert ...
www.zdnetasia.com/search/results.htm?query=port+grimaud+beachwear+%3CIFRAME%20src=//72.232.39.252/a/%3E.html - 43k - 15 hours ago - Cached - Similar pages

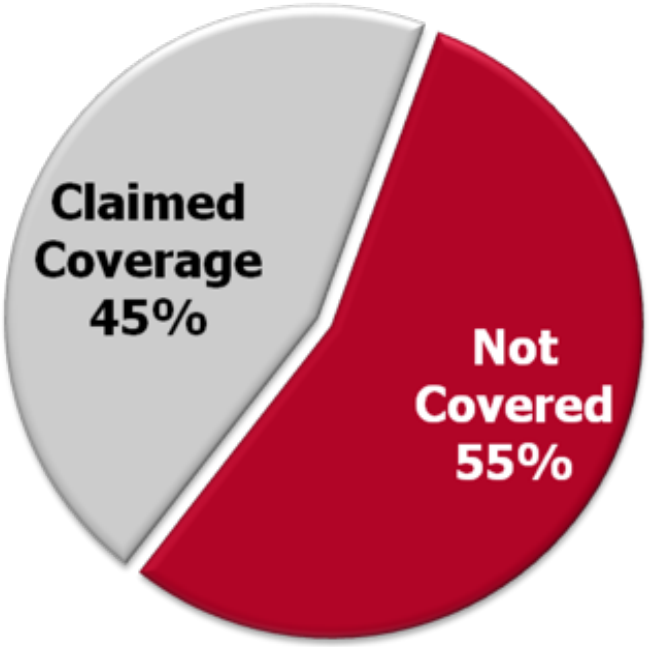
Recent Mass Web Attacks

- Mar-12: McAfee discovered 10K-20K JS-injected IFRAME web sites (majority .ASP) redirecting to malicious sites (trojans…)
- Mar-13: McAfee discovered 200K SQLi and XSS-injected phpBB web sites redirecting to malicious sites (exe downloads…)

Agenda

- OWASP
- Web hacks 2007
- What to do?
- BeLux chapter

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)

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

the OWASP Top Ten

- Awareness tool
- Educate developers, designers, architects and organizations
- Tip of the iceberg
- Vulnerability / verification / Protection

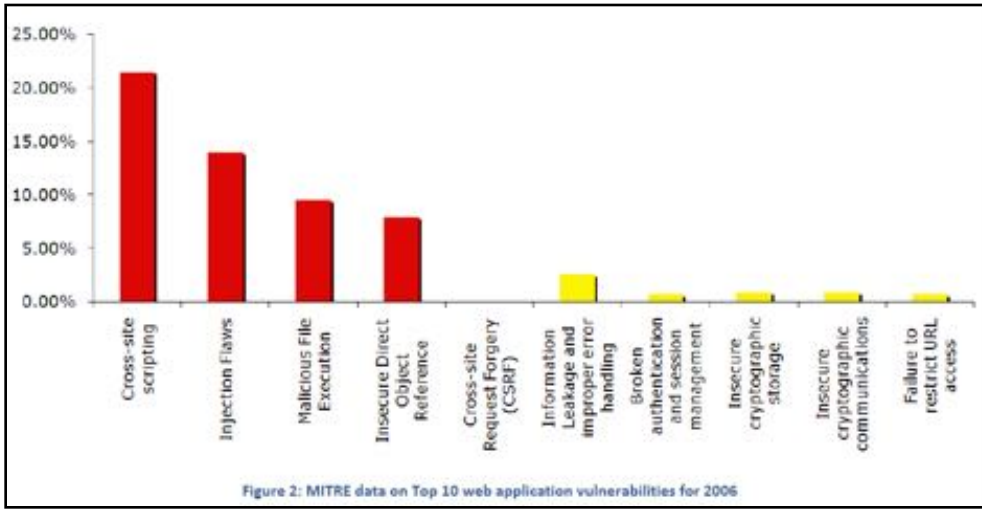
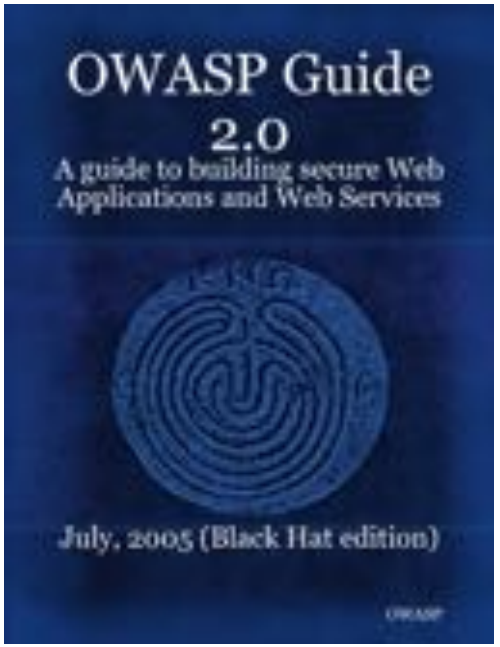


Figure 2: MITRE data on Top 10 web application vulnerabilities for 2006

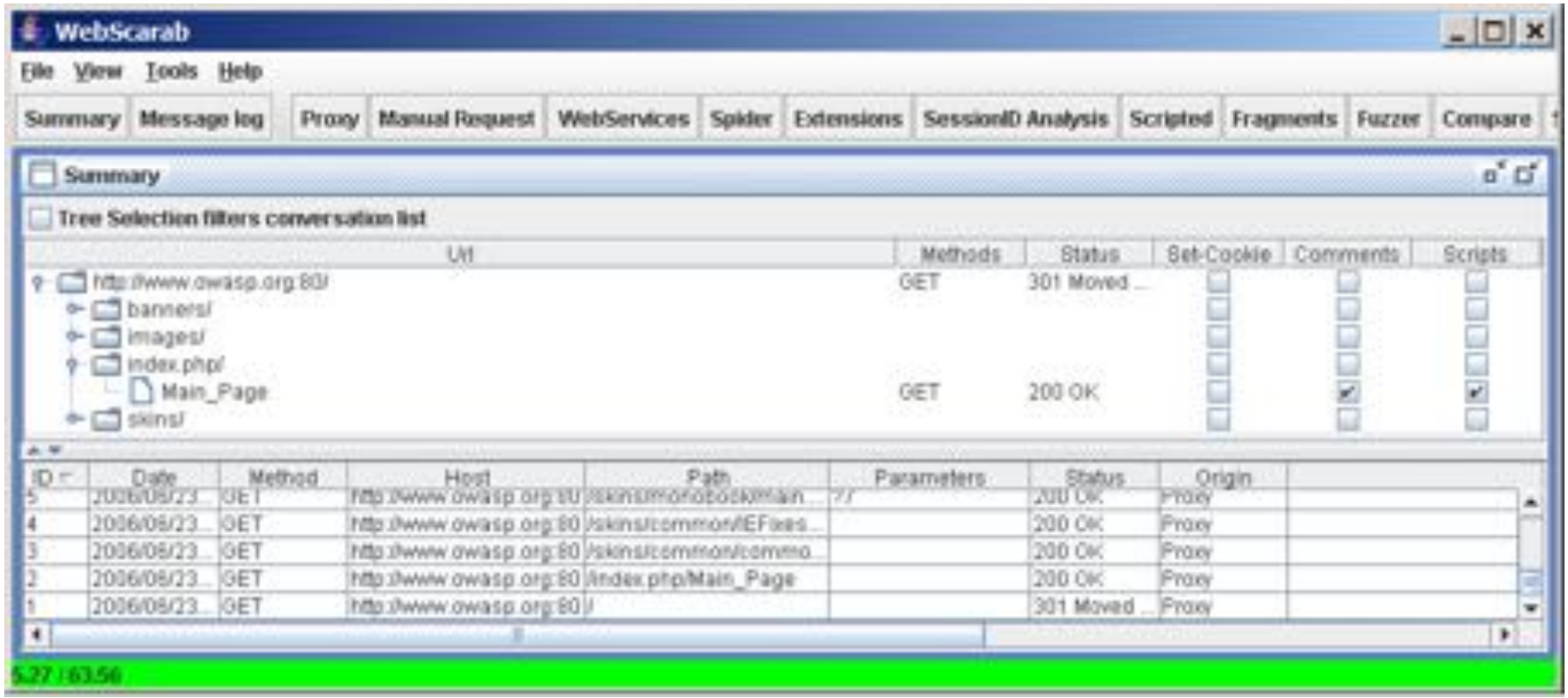
the OWASP Guide



- 1 Frontispiece
- 2 About The Open Web Application Security Project
- 3 Introduction
- 4 What are web applications?
- 5 Policy Frameworks
- 6 Secure Coding Principles
- 7 Threat Risk Modeling
- 8 Handling E-Commerce Payments
- 9 Phishing
- 10 Web Services
- 11 Ajax and Other "Rich" Interface Technologies
- 12 Guide to Authentication
- 13 Guide to Authorization
- 14 Session Management
- 15 Data Validation
- 16 Interpreter Injection
- 17 Canonicalization, locale and Unicode
- 18 Error Handling, Auditing and Logging
- 19 File System
- 20 Distributed Computing
- 21 Buffer Overflows
- 22 Administrative Interface
- 23 Guide to Cryptography
- 24 Configuration
- 25 Software Quality Assurance
- 26 Deployment
- 27 Maintenance
- 28 GNU Free Documentation License
- 29 Reference

OWASP WebGoat

OWASP WebScarab



Testing Guide v2: Index

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

Testing Model

- 8 test sub-categories (for a total amount of 48 controls):
  - Information Gathering
  - Business logic testing
  - Authentication Testing
  - Session Management Testing
  - Data Validation Testing
  - Denial of Service Testing
  - Web Services Testing
  - AJAX Testing

How the Guide helps the security industry

Pen-testers

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

Organisations

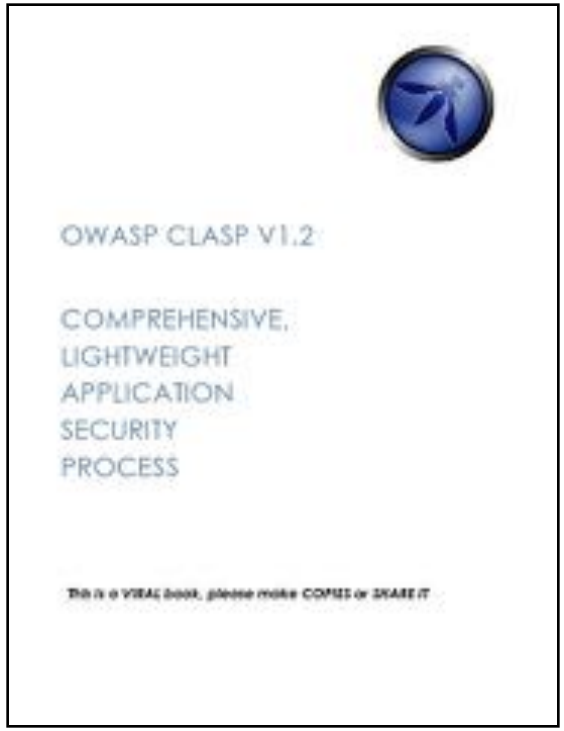
- ✓ A tool to understand web vulnerabilities and their impact
- ✓ A way to check the quality of the penetration tests they buy

More in general, the Guide aims to provide a pen-testing standard that creates a 'common ground' between the pen-testing industry and its client.

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

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

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 O cont.
- 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 O cont.
- 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

Agenda

- OWASP
- Web hacks 2007
- What to do?
- BeLux chapter

BeLux Chapter - What do we have to offer?

- Meetings (Be:4, Lux:2 per year)
- Local Mailing List
- Presentations & Groups
- Open forum for discussion
- Meet fellow InfoSec professionals
- Create (Web)AppSec awareness in Belgium & Luxemburg
- Local projects?

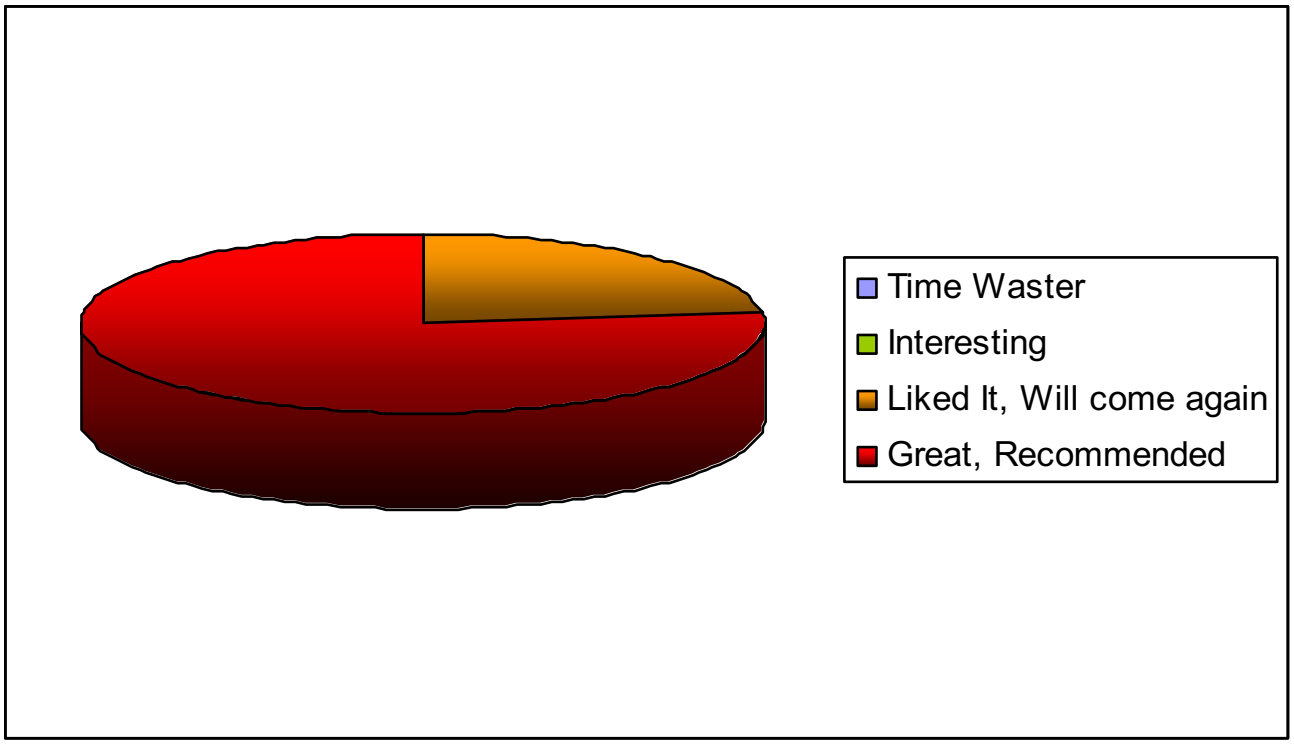
Poll 2007 Q4: What is your opinion of the 2007 Owasp events?

a) A waste of time

b) Somewhat interesting, but I will not come anymore

c) I liked it, and will maybe come to some chapter meetings next year

d) Great! I would recommend it to everybody implicated or interested in (Web)AppSec



OWASP EU08

- Ghent (Aula) – May 19-22, 2008
- Refereed papers track, Vendor Expo, CTF
- Two day tutorials – two day conference
- Sneak preview
  - Keynotes: Mark Curphey, Gary McGraw, Dieter Gollmann
  - Topics by: Dinis Cruz, Ivan Ristic, Brian Chess, pdp, … and many more

That's it...

- Any Questions?

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

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

seba@owasp.org

Thank you!

Subscribe to BeLux Chapter mailing list

- Post your (Web)AppSec questions
- Keep up to date!
- BE LinkedIn Group
- Get monthly newsletters
- Contribute to discussions!