OWASP Geneva – Spring 09 meeting

April 23rd. 2009

Antonio FONTES (antonio.fontes@owasp.org)
Chapter Leader - Geneva

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

Who am I?

- 8 years developer experience
- 5 years infosec/appsec experience (CSSI 2004 ;)
- Lead Application Security Program,
  - New Access SA, Geneva – Switzerland

- OWASP Geneva chapter founder
- CWE Top 25 Programming Errors contributor
- Monblog.ch founder and architect
  - Free swiss community blogging platform
  - > 13mio. pageviews/monthly

monblog.ch

Agenda

- OWASP Foundation
- OWASP Projects
- Tonight’s meeting

The OWASP foundation

- Open Web Application Security Project
- International, non-profit organization
- Funding:
  - Volunteers time
  - OWASP memberships and sponsors
  - OWASP conference fees
- Participation and projects are free and open to everyone.

OWASP Mission

“Enabling organizations to develop, purchase, and maintain applications that can be trusted.”

OWASP Community

Documentation projects (wiki & books)

- Top 10, Code review, Testing, Building, Legal, …

Code projects

- Defensive, offensive (testing) tools, Education, processes, …

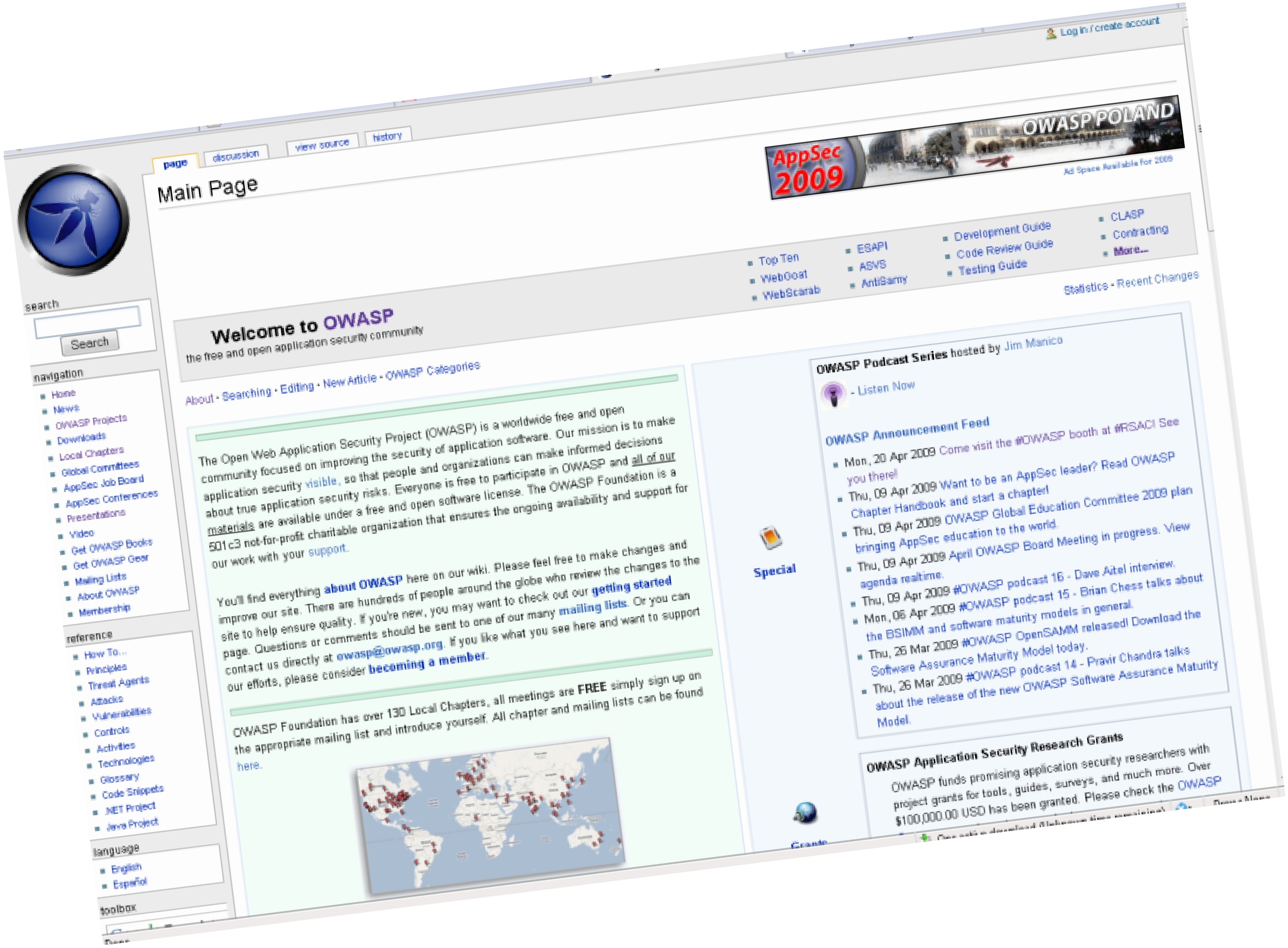
Chapters

- Over 130 chapters worldwide and growing

Conferences

- Major and minor events around the world

www.owasp.org



Main Page

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

Statistics - Recent Changes

- 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

- How To...
- Principles
- Threat Agents
- Attacks
- Vulnerabilities
- Controls
- Activities
- Technologies
- Glossary
- Code Snippets
- .NET Project
- Java Project

- English
- Español

Welcome to OWASP
the free and open application security community

About - Searching - Editing - New Article - OWASP Categories

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 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. The OWASP Foundation is a 501c3 not-for-profit charitable organization that ensures the ongoing availability and support for our work with your support.

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 changes to the site to help ensure quality. If you're new, you may want to check out our **getting started** page. Questions or comments should be sent to one of our many **mailing lists**. Or you can contact us directly at owasp@owasp.org. If you like what you see here and want to support our efforts, please consider **becoming a member**.

OWASP Foundation has over 130 Local Chapters, all meetings are **FREE** simply sign up on the appropriate mailing list and introduce yourself. All chapter and mailing lists can be found here.

Special

OWASP Podcast Series hosted by Jim Manico

- Listen Now

OWASP Announcement Feed

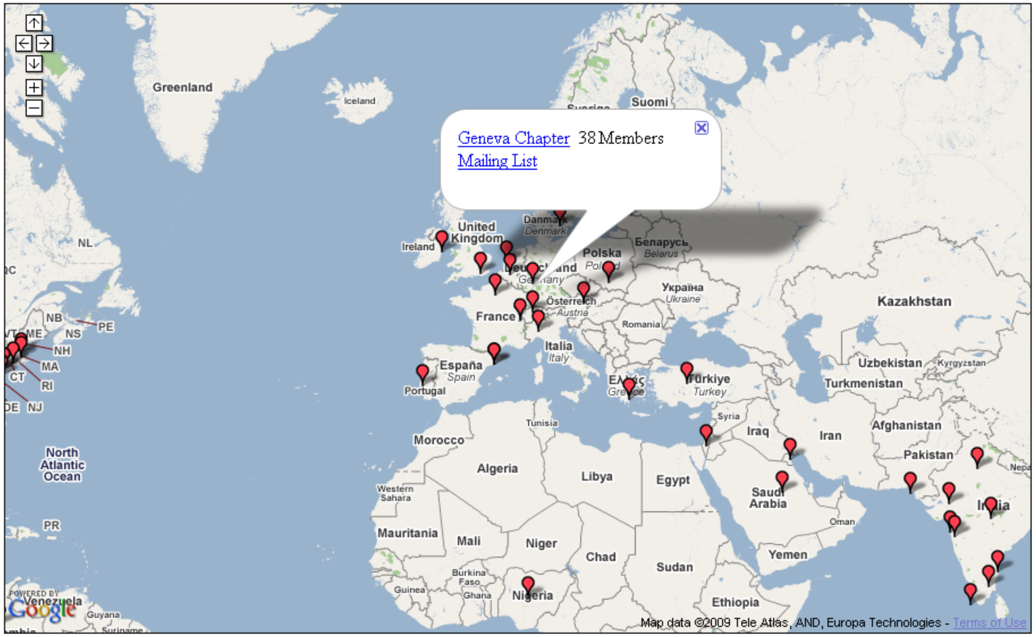
- Mon, 20 Apr 2009 Come visit the #OWASP booth at #RSAC! See you there!
- Thu, 09 Apr 2009 Want to be an AppSec leader? Read OWASP Chapter Handbook and start a chapter!
- Thu, 09 Apr 2009 OWASP Global Education Committee 2009 plan bringing AppSec education to the world.
- Thu, 09 Apr 2009 April OWASP Board Meeting in progress. View agenda realtime.
- Thu, 09 Apr 2009 #OWASP podcast 16 - Dave Aitel interview.
- Mon, 06 Apr 2009 #OWASP podcast 15 - Brian Chess talks about the BSIMM and software maturity models in general.
- Thu, 26 Mar 2009 #OWASP OpenSAMM released! Download the Software Assurance Maturity Model today.
- Thu, 26 Mar 2009 #OWASP podcast 14 - Pravir Chandra talks about the release of the new OWASP Software Assurance Maturity Model.

OWASP Application Security Research Grants

OWASP funds promising application security researchers with project grants for tools, guides, surveys, and much more. Over $100,000.00 USD has been granted. Please check the OWASP

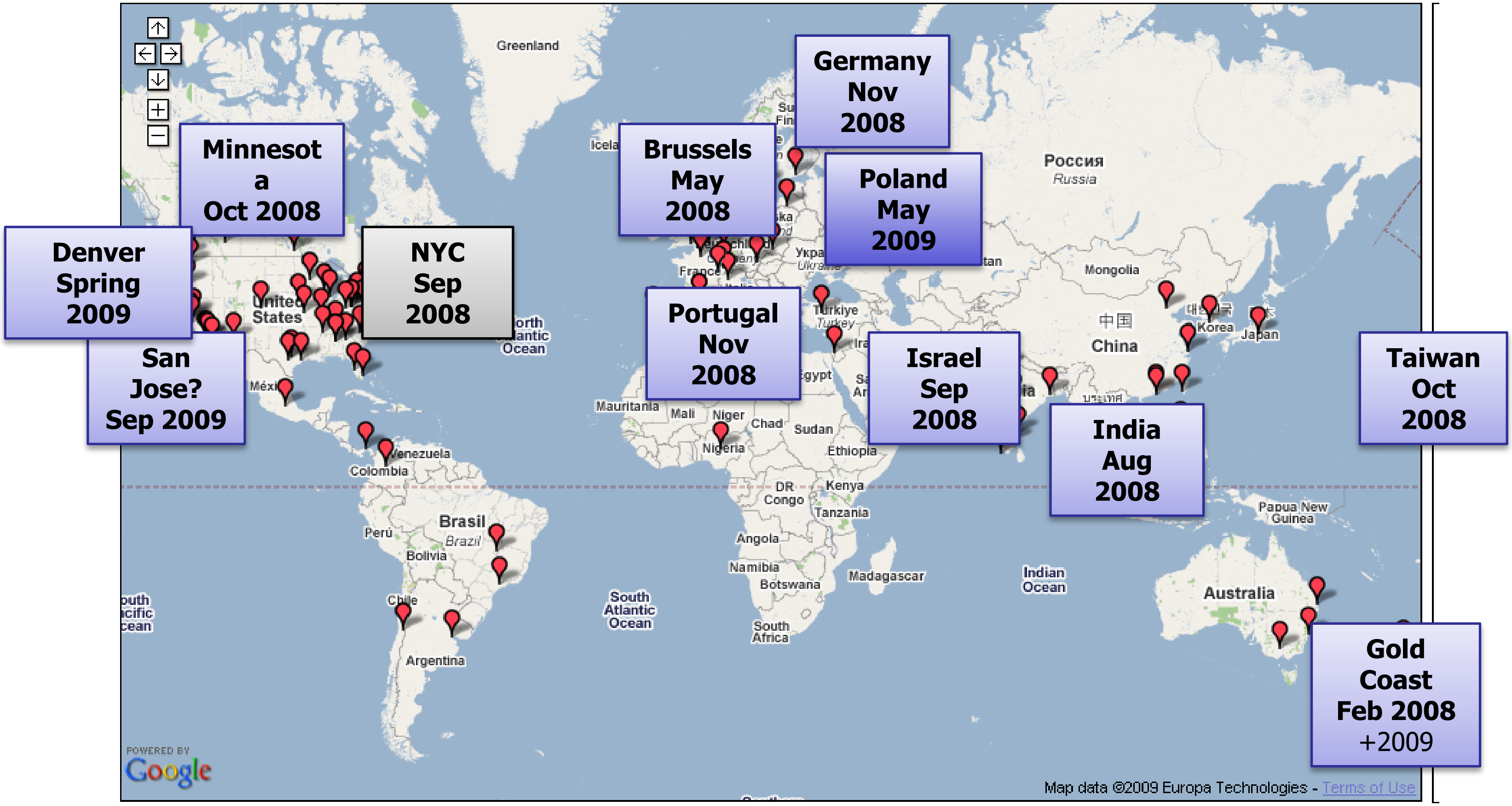
Grants

130+ Chapters worldwide



11412 chapter members worldwide
5340 project members worldwide

OWASP Conferences



Minnesota
Oct 2008

Denver
Spring
2009

San
Jose?
Sep 2009

NYC
Sep
2008

Brussels
May
2008

Germany
Nov
2008

Poland
May
2009

Portugal
Nov
2008

Israel
Sep
2008

India
Aug
2008

Taiwan
Oct
2008

Gold
Coast
Feb 2008
+2009

OWASP Conferences

- Next:
  - 11th-14th May 09: **Krakow, Poland (Appsec Europe)**
  - June 09: Dublin (Appsec)
  - Oct. 09: Washington D.C. (Appsec USA)

OWASP EU Summit

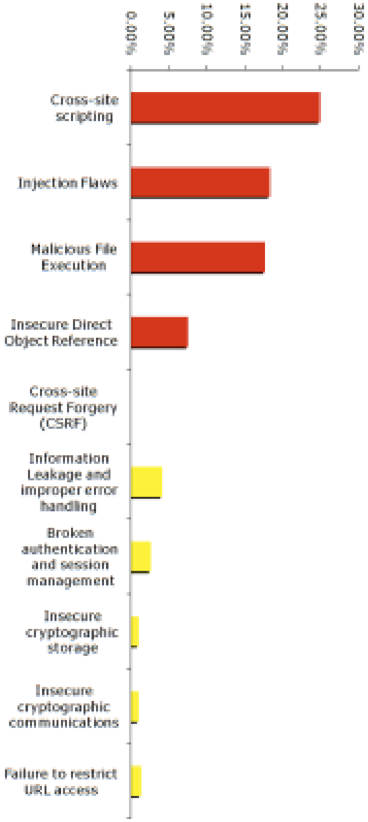
- 2009 Focus
  - 80+ application security experts from 20+ countries during one week
- A fantastic and high standing SPA right at the beach!
- New projects:
  - outreach program: technology vendors, framework providers, and standards bodies
  - educational program: new program to provide free one- day seminars at universities and developer conferences worldwide
  - new global committee structure: education, chapters, conferences, industry, projects and tools, membership
- Actually, we didn't have time to go the beach...once in the week!
- *And...a new local chapter was created.*

Agenda

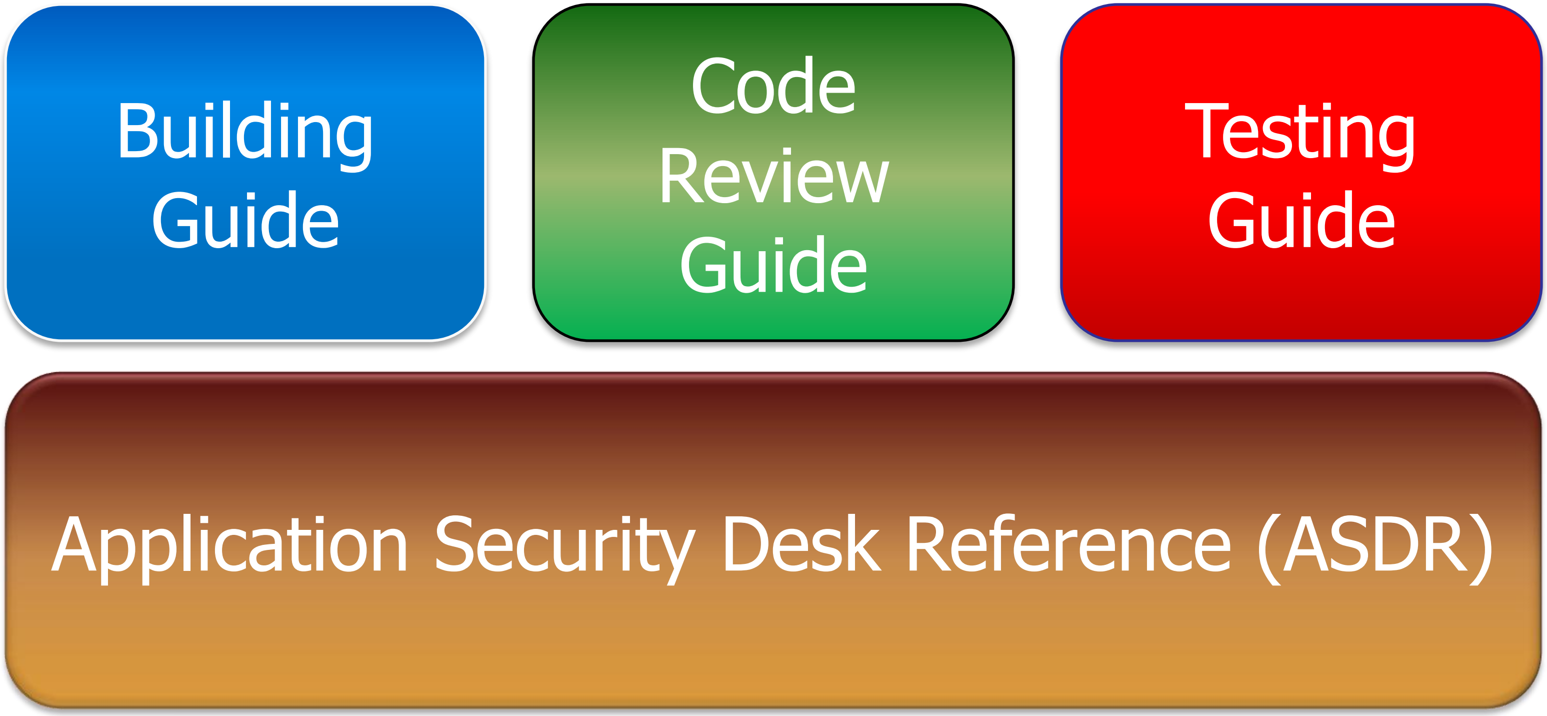
- OWASP Foundation
- OWASP Projects
- Tonight’s meeting

OWASP Top 10

- The Ten Most Critical Web Application Security Vulnerabilities
- Current: 2007 Release
- 2009 release in progress
- A reference, but not a standard (yet?)



Big 4 (not to be confused with...)



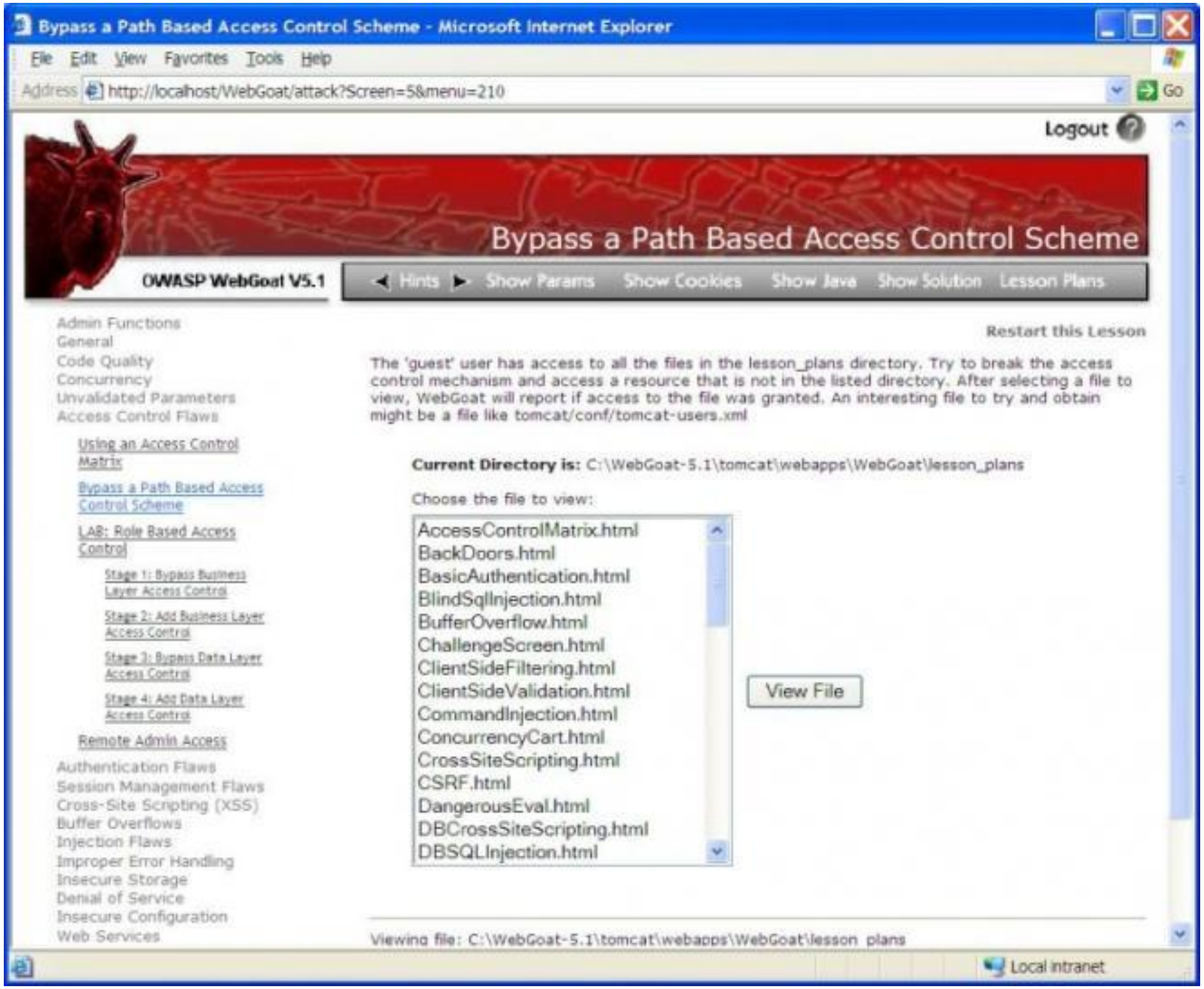
Building Guide

Code Review Guide

Testing Guide

Application Security Desk Reference (ASDR)

Education: Webgoat


Bypass a Path Based Access Control Scheme - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Address http://localhost/WebGoat/attack?Screen=5&menu=210
Go
Logout
Bypass a Path Based Access Control Scheme
OWASP WebGoat V5.1
Hints
Show Params
Show Cookies
Show Java
Show Solution
Lesson Plans
Admin Functions
General
Code Quality
Concurrency
Unvalidated Parameters
Access Control Flaws
Using an Access Control Matrix
Bypass a Path Based Access Control Scheme
LAB: Role Based Access Control
Stage 1: Bypass Business Layer Access Control
Stage 2: Add Business Layer Access Control
Stage 3: Bypass Data Layer Access Control
Stage 4: Add Data Layer Access Control
Remote Admin Access
Authentication Flaws
Session Management Flaws
Cross-Site Scripting (XSS)
Buffer Overflows
Injection Flaws
Improper Error Handling
Insecure Storage
Denial of Service
Insecure Configuration
Web Services
Restart this Lesson
View File
Local intranet

The 'guest' user has access to all the files in the lesson_plans directory. Try to break the access control mechanism and access a resource that is not in the listed directory. After selecting a file to view, WebGoat will report if access to the file was granted. An interesting file to try and obtain might be a file like tomcat/conf/tomcat-users.xml

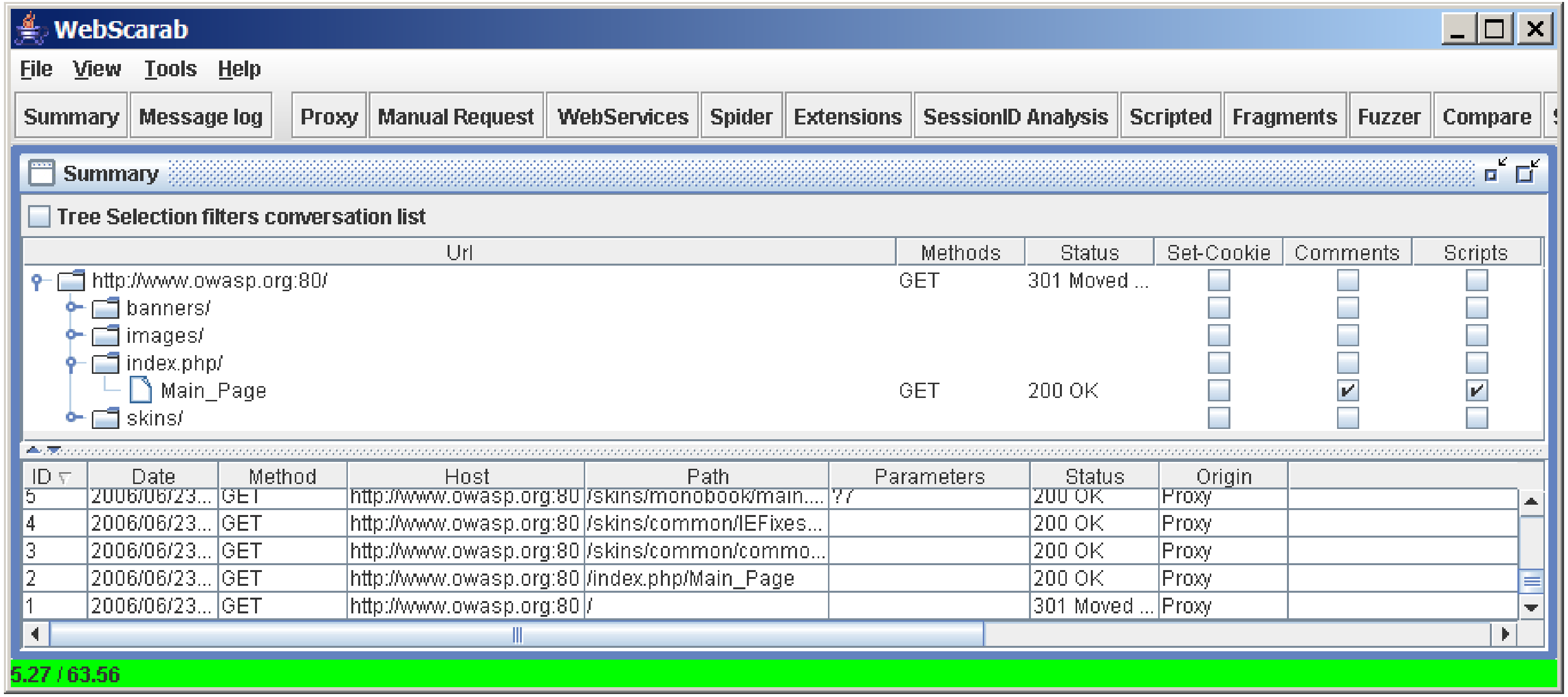
Current Directory is: C:\WebGoat-5.1\tomcat\webapps\WebGoat\lesson_plans

Choose the file to view:

AccessControlMatrix.html
BackDoors.html
BasicAuthentication.html
BlindSqlInjection.html
BufferOverflow.html
ChallengeScreen.html
ClientSideFiltering.html
ClientSideValidation.html
CommandInjection.html
ConcurrencyCart.html
CrossSiteScripting.html
CSRF.html
DangerousEval.html
DBCrossSiteScripting.html
DBSQLInjection.html

Viewing file: C:\WebGoat-5.1\tomcat\webapps\WebGoat\lesson_plans

Testing: Webscarab



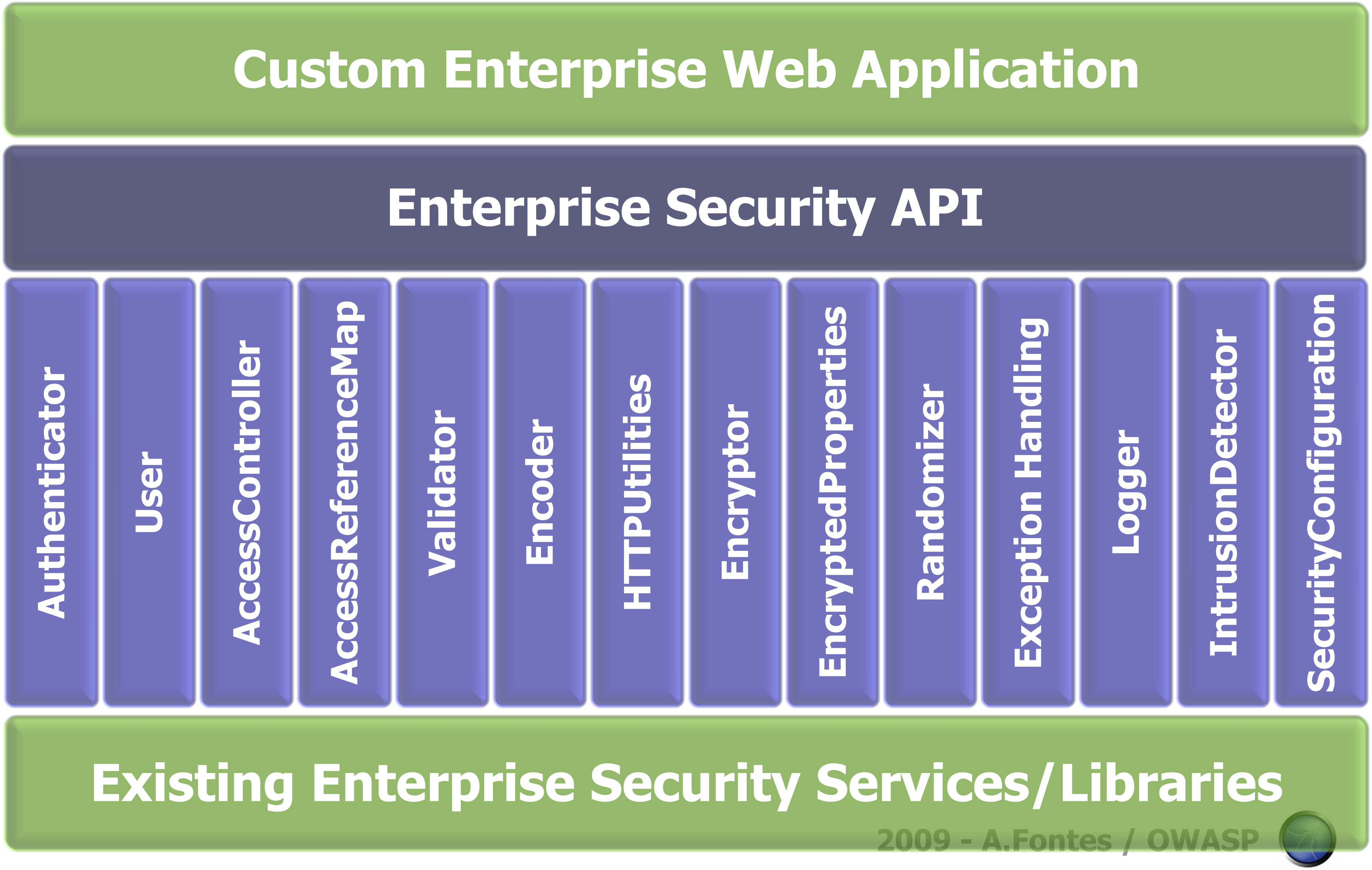
□ Tree Selection filters conversation list

Url	Methods	Status	Set-Cookie	Comments	Scripts
http://www.owasp.org:80/	GET	301 Moved ...	□	□	□
banners/			□	□	□
images/			□	□	□
index.php/			□	□	□
Main_Page	GET	200 OK	□	☑	☑
skins/			□	□	□

ID	Date	Method	Host	Path	Parameters	Status	Origin
5	2006/06/23...	GET	http://www.owasp.org:80	/skins/monobook/main....	??	200 OK	Proxy
4	2006/06/23...	GET	http://www.owasp.org:80	/skins/common/IEFixes...		200 OK	Proxy
3	2006/06/23...	GET	http://www.owasp.org:80	/skins/common/commo...		200 OK	Proxy
2	2006/06/23...	GET	http://www.owasp.org:80	/index.php/Main_Page		200 OK	Proxy
1	2006/06/23...	GET	http://www.owasp.org:80	/		301 Moved ...	Proxy

5.27 / 63.56

Reference libraries: OWASP ESAPI



Custom Enterprise Web Application

Enterprise Security API

Authenticator

User

AccessController

AccessReferenceMap

Validator

Encoder

HTTPUtilities

Encryptor

EncryptedProperties

Randomizer

Exception Handling

Logger

IntrusionDetector

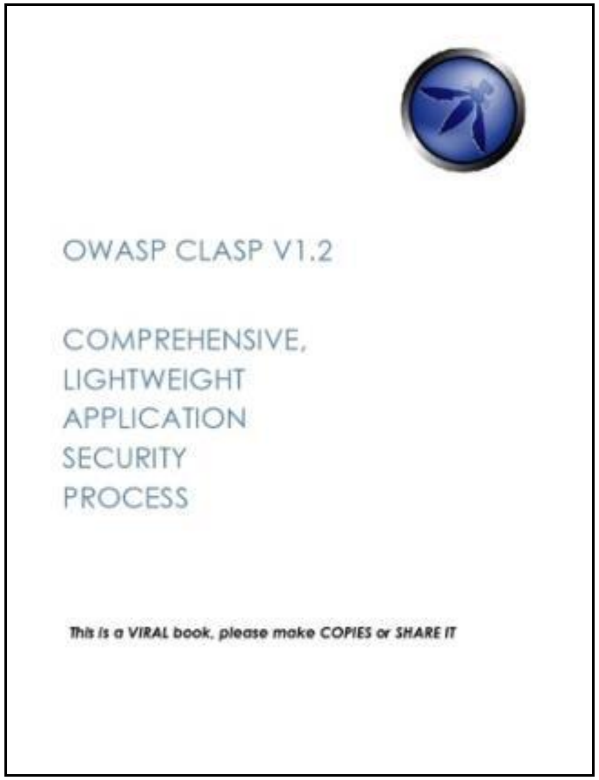
SecurityConfiguration

Existing Enterprise Security Services/Libraries

Methods and processes: CLASP

- Comprehensive, Lightweight Application Security Process
  - Centered around 7 AppSec Best Practices
  - Prescriptive and Proactive
  - Covers the entire software lifecycle (not just for developers)

- Adaptable to any development process
  - CLASP defines roles across the SDLC
  - 24 role-based process components
  - **You can start small**



OWASP CLASP V1.2

COMPREHENSIVE,
LIGHTWEIGHT
APPLICATION
SECURITY
PROCESS

This is a VIRAL book, please make COPIES or SHARE IT

Quality and coaching: Seasons of Code

Deliverables

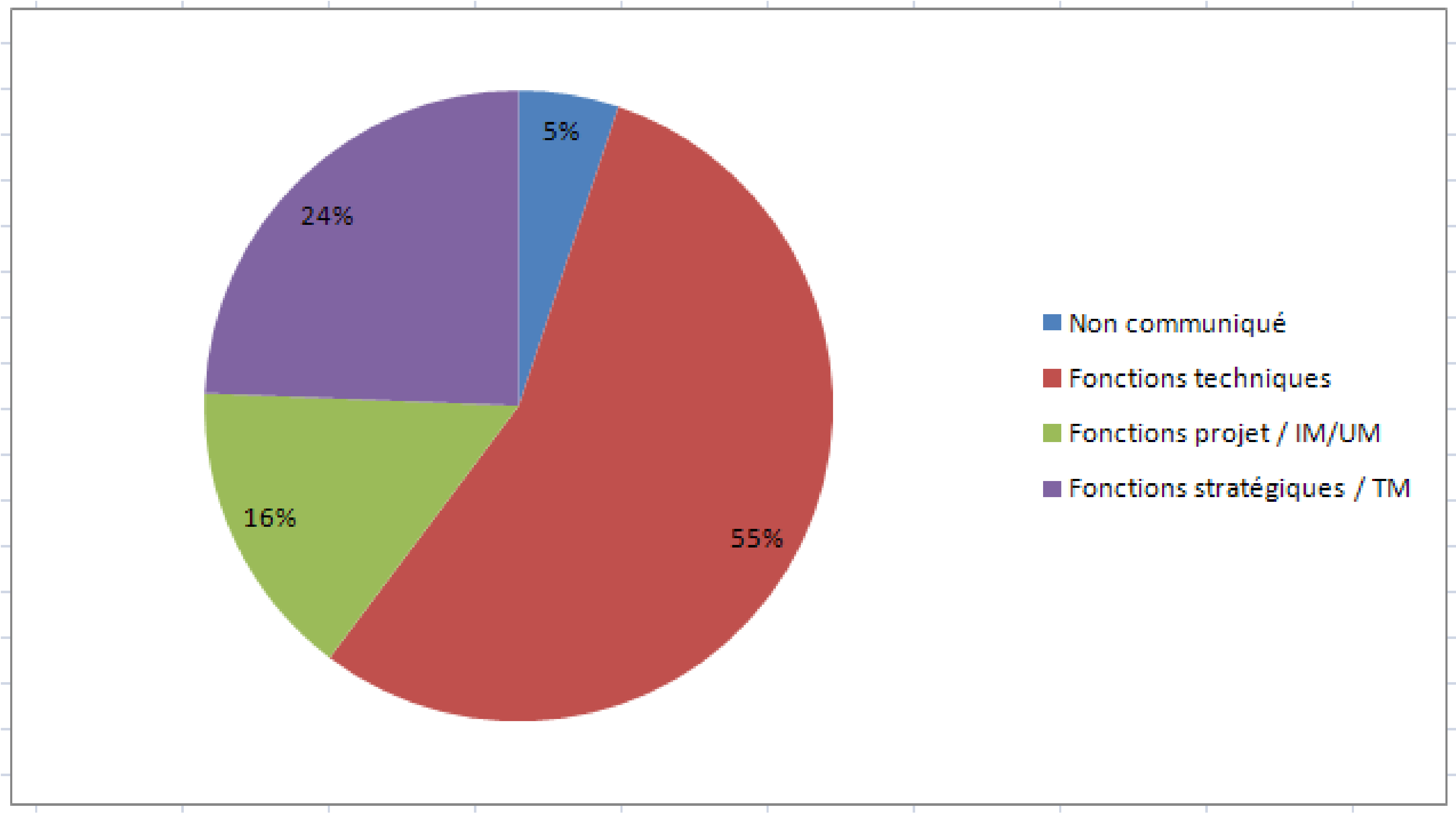
- OWASP .NET Project
- OWASP ASDR Project
- OWASP AntiSamy Project
- OWASP AppSec FAQ Project
- OWASP Application Security Assessment Standards Project
- OWASP Application Security Metrics Project
- OWASP Application Security Requirements Project
- OWASP CAL9000 Project
- OWASP CLASP Project
- OWASP 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

Agenda

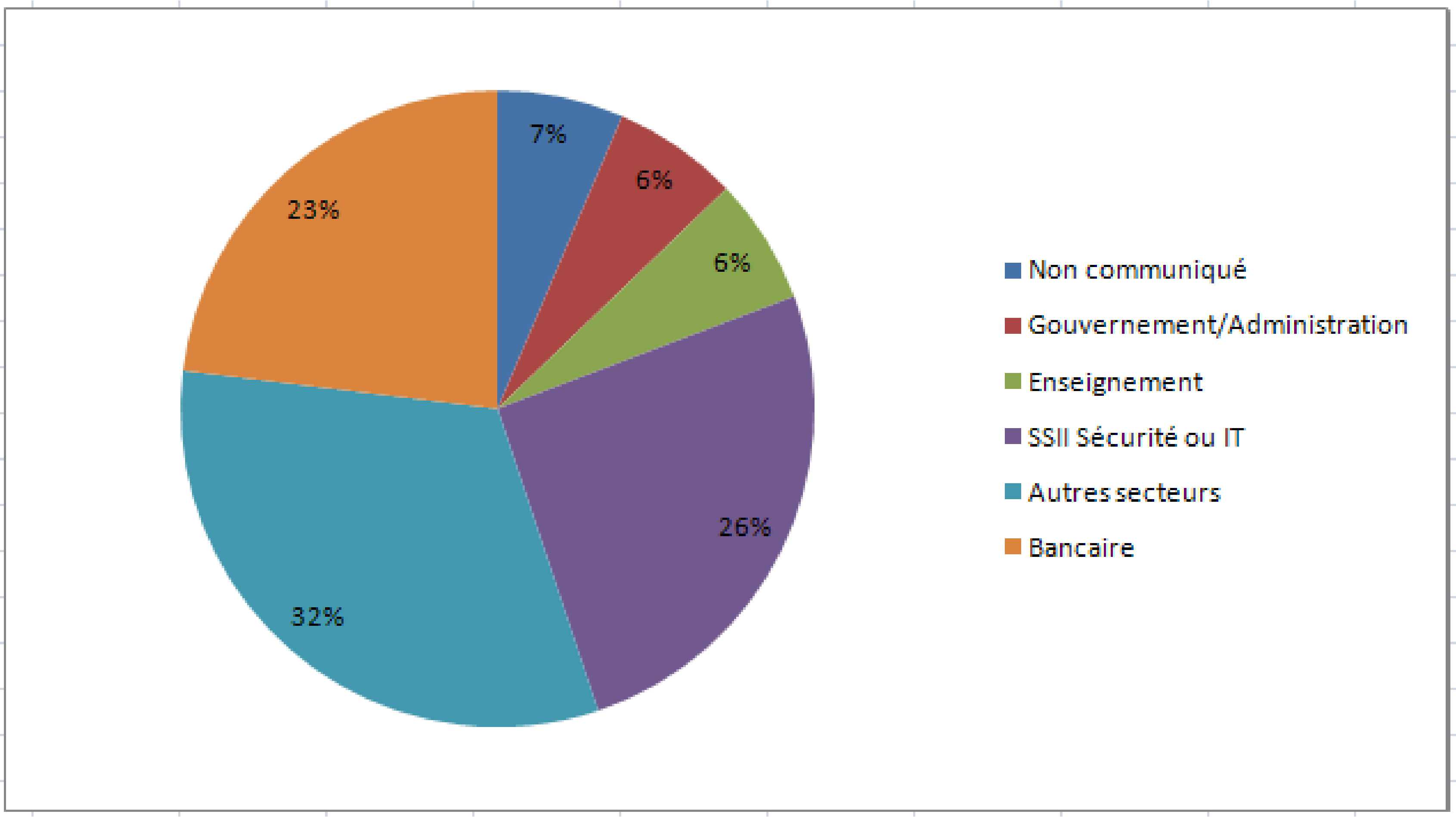
- OWASP Foundation
- OWASP Projects
- Tonight's meeting

Who is sitting (or standing) in this room?

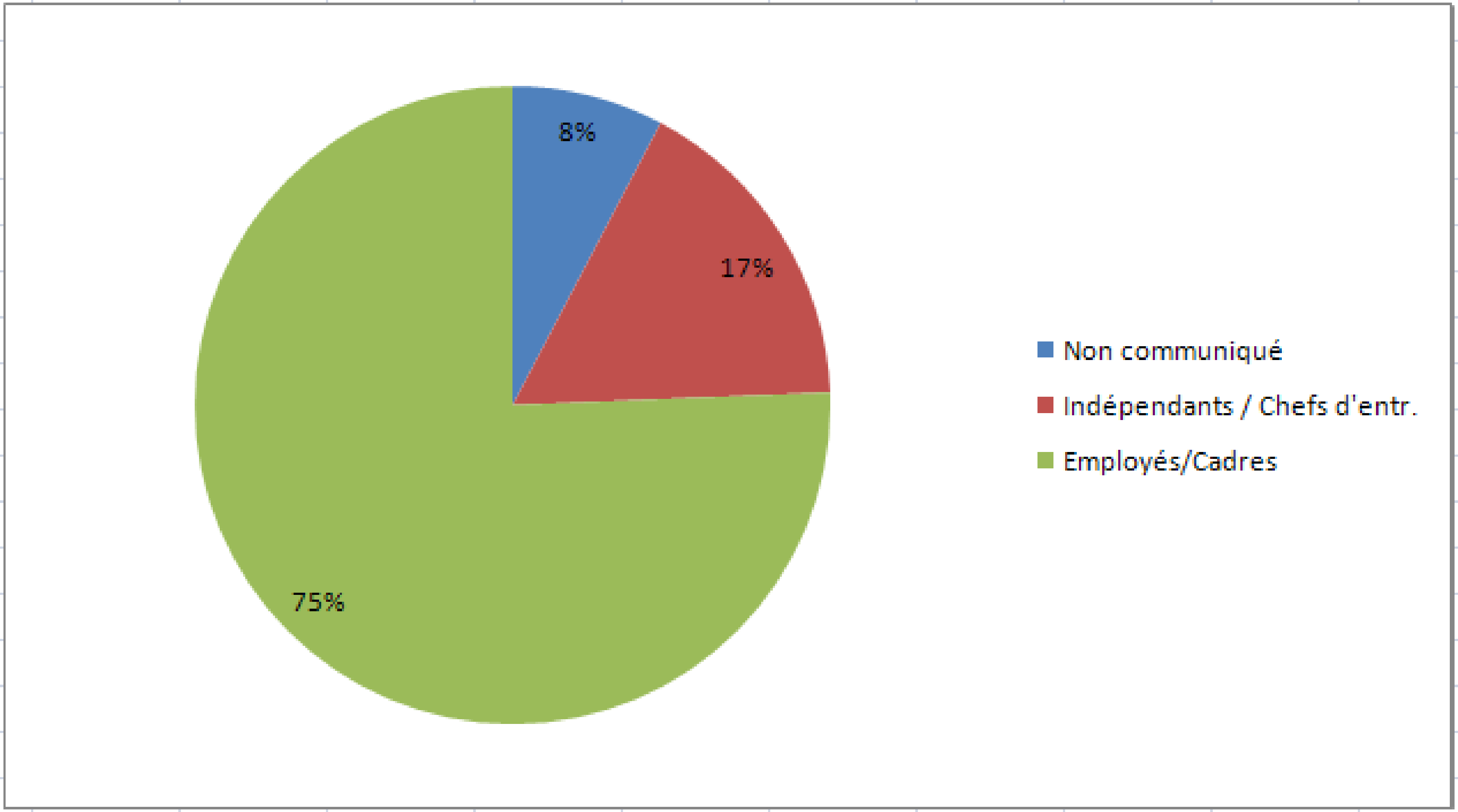
Audience (1/3)


5%
24%
16%
55%
🟦 Non communiqué
🟥 Fonctions techniques
🟩 Fonctions projet / IM/UM
🟪 Fonctions stratégiques / TM

Audience (2/3)


7%
6%
6%
26%
32%
23%
Non communiqué
Gouvernement/Administration
Enseignement
SSII Sécurité ou IT
Autres secteurs
Bancaire

Audience 3/3


8%
17%
75%
Non communiqué
Indépendants / Chefs d'entr.
Employés/Cadres

Agenda

- 18h00: Accueil

- 18h15: OWASP Top 10
  Sebastien Gioria, Chapter Leader - OWASP France
- 19h05: Pause (5 minutes)
- 19h10: La sécurité dans le cycle de vie développement d'une application web: de la théorie à la pratique
  Gilbert K. Agopome (CISSP, CSSI 2004, CISA)
- 20h00: Cocktail offert par HEC Genève

- 21h00: Fin de la manifestation

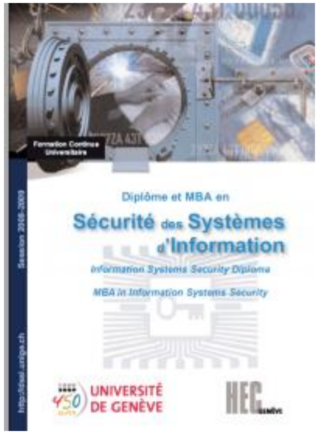
Geneva's Chapter and you

- Next meeting: June 2009 (well, will try…)
- Join the list!
  - Post your (Web)AppSec questions
  - Keep up to date
  - Contribute to discussions
- Become an OWASP member!
  - *Or even a sponsor (told you!)*

THANK YOU!

- http://www.owasp.org
- http://www.owasp.org/index.php/Geneva
  antonio.fontes@owasp.org

Tonight's sponsors:



Formation Continue Universitaire

Session 2008-2009

Diplôme et MBA en

Sécurité des Systèmes d'Information

Information Systems Security Diploma

MBA in Information Systems Security

http://dsi.unige.ch