OWASP EUROPEAN TOUR

Eurecom, Nice 24/06/2013

OWASP
The Open Web Application Security Project

Ely de Travieso
ely.detravieso@owasp.org
OWASP France
Relations Partenaires

Introduction

OWASP
The Open Web Application Security Project

Ely de Travieso

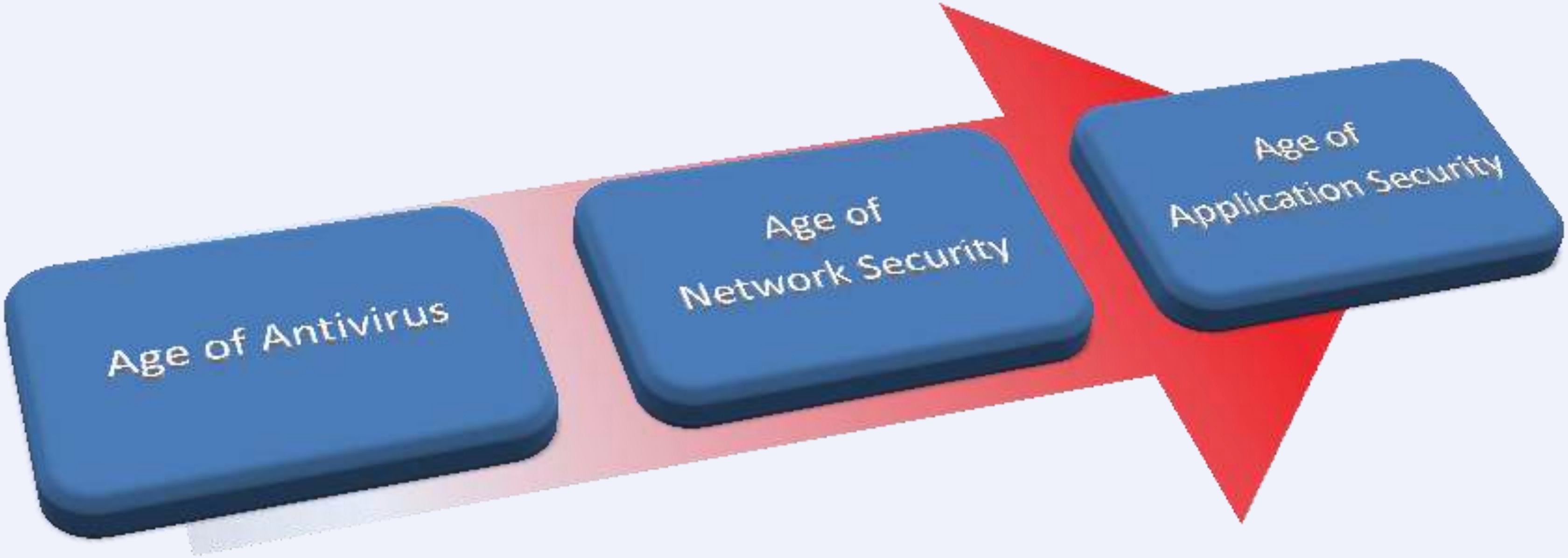
- *15 ans d'expérience dans la Sécurité des Systèmes d'Information et la Lutte contre la Cybercriminalité*
- *Directeur & Fondateur de la société Phonesec*

OWASP France : Responsable des Relations Partenaires depuis 2012

Pourquoi l'Owasp

OWASP
The Open Web Application Security Project

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



- La majorité des sites internet sont vulnérables aux attaques
- 75% des attaques visent les applications Web *(Source: Gartner)*

Agenda

OWASP
The Open Web Application Security Project

- *La fondation OWASP*
- *Les Projets OWASP*
- *Devenir Membre*

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

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

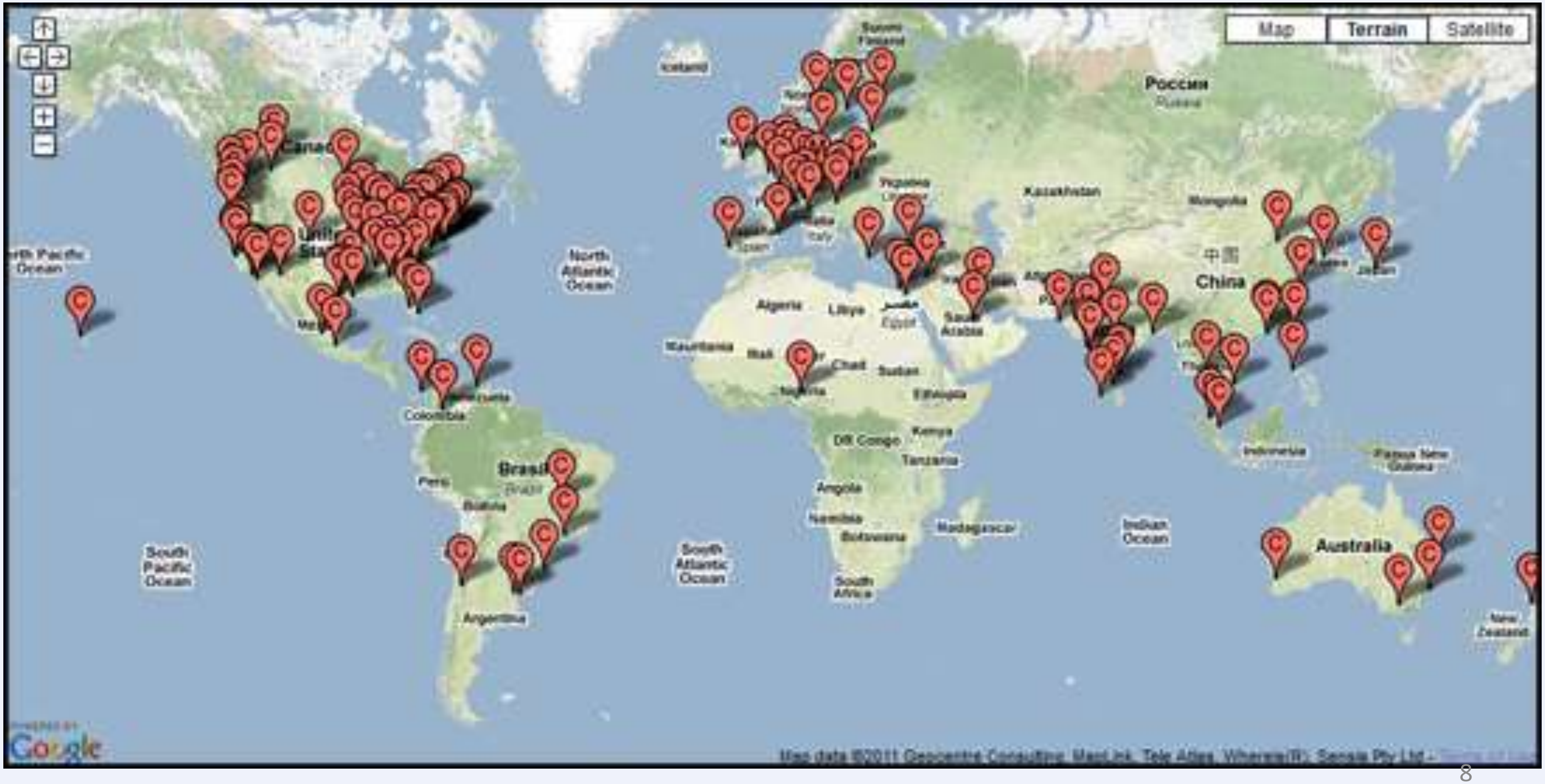
1600+ Members, 56 Corporate Supporters

69 Academic Supporters

What is OWASP

OWASP
The Open Web Application Security Project

200 Chapters, 1 600+ Members, 20 000+ Builders, Breakers and Defenders



What is OWASP

OWASP
The Open Web Application Security Project

Quality Resources

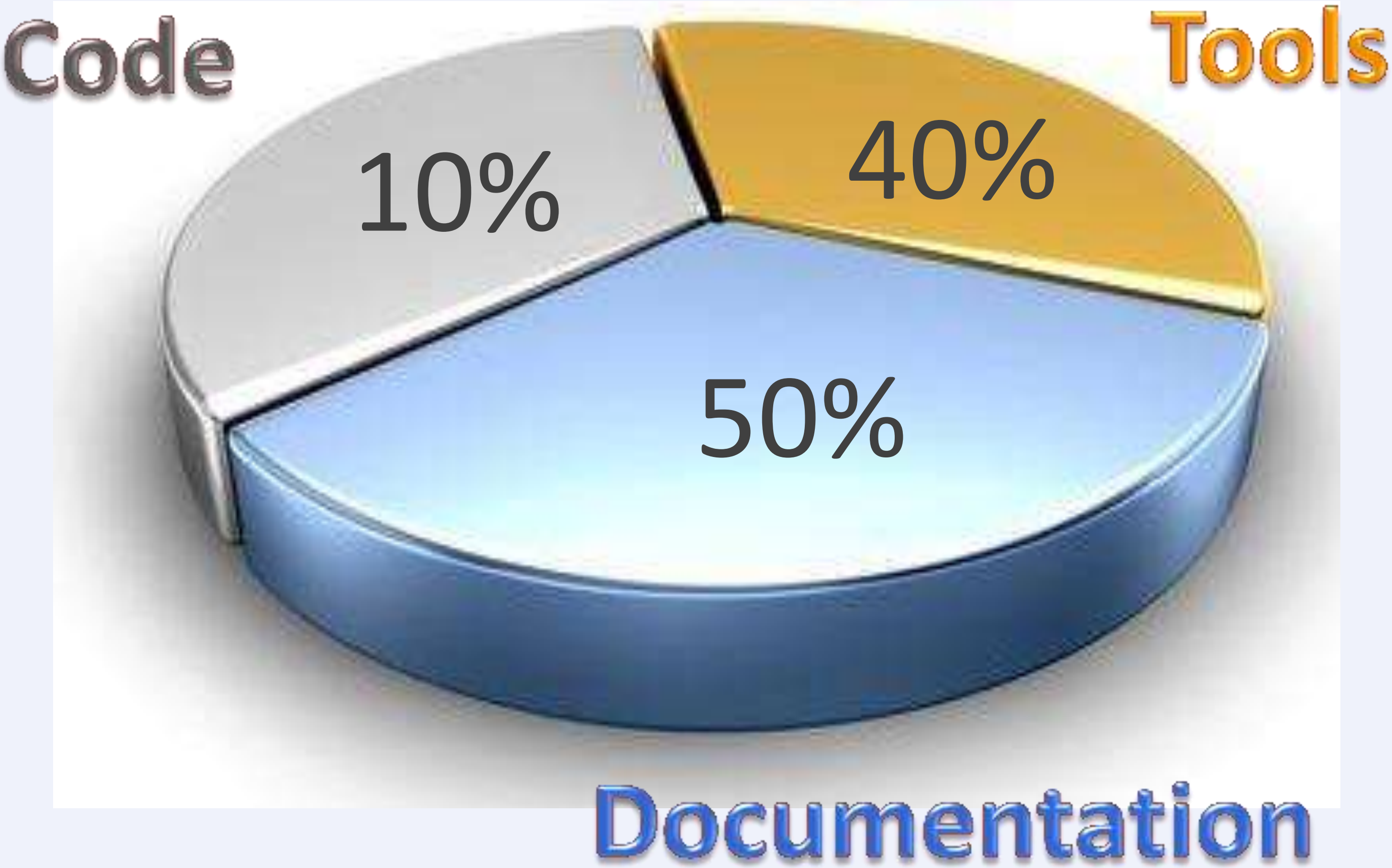
200+ Projects

15,000+ downloads of tools, documentation

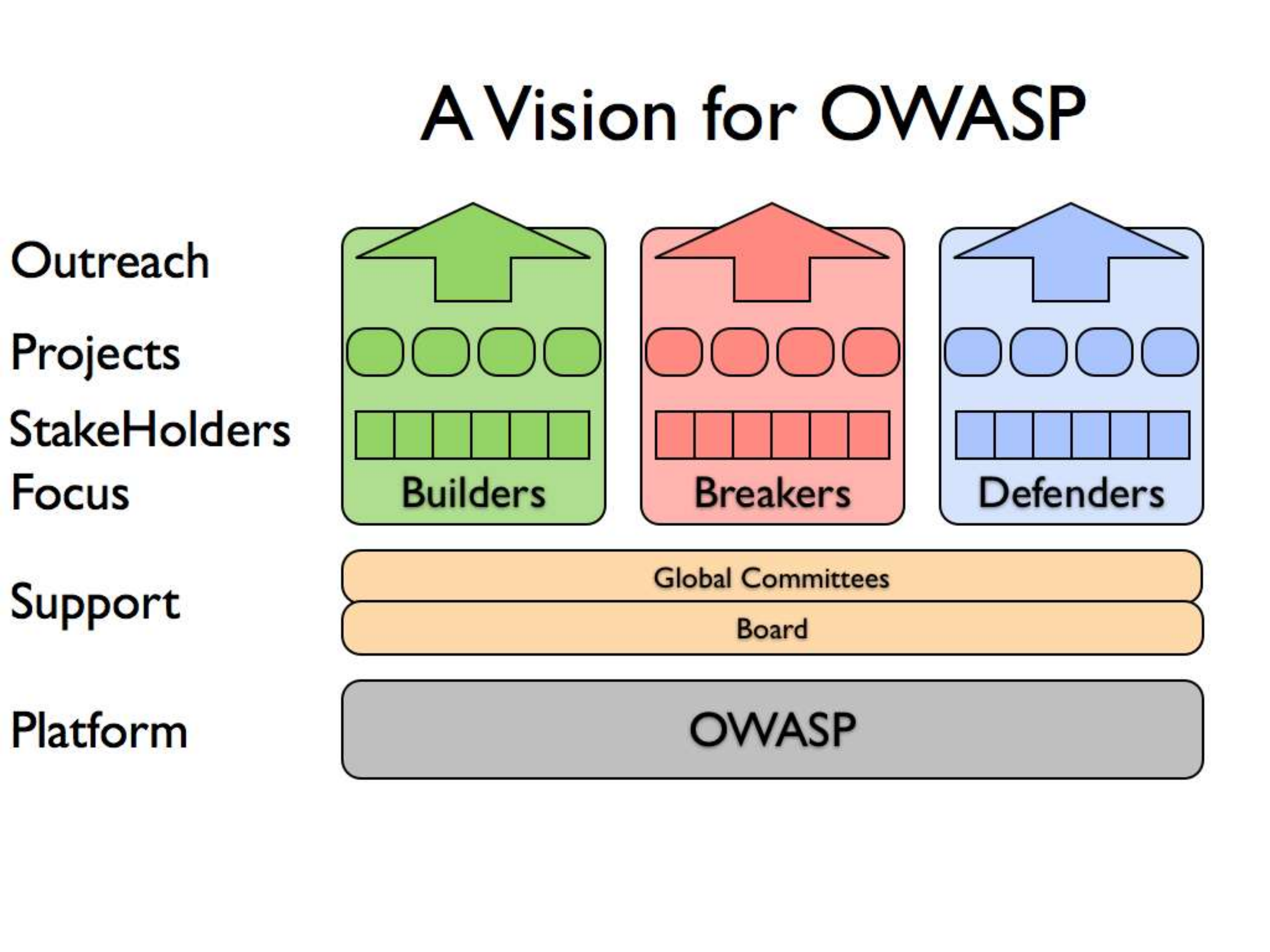
250,000+ unique visitors

800,000+ page views (monthly)

Quality Resources

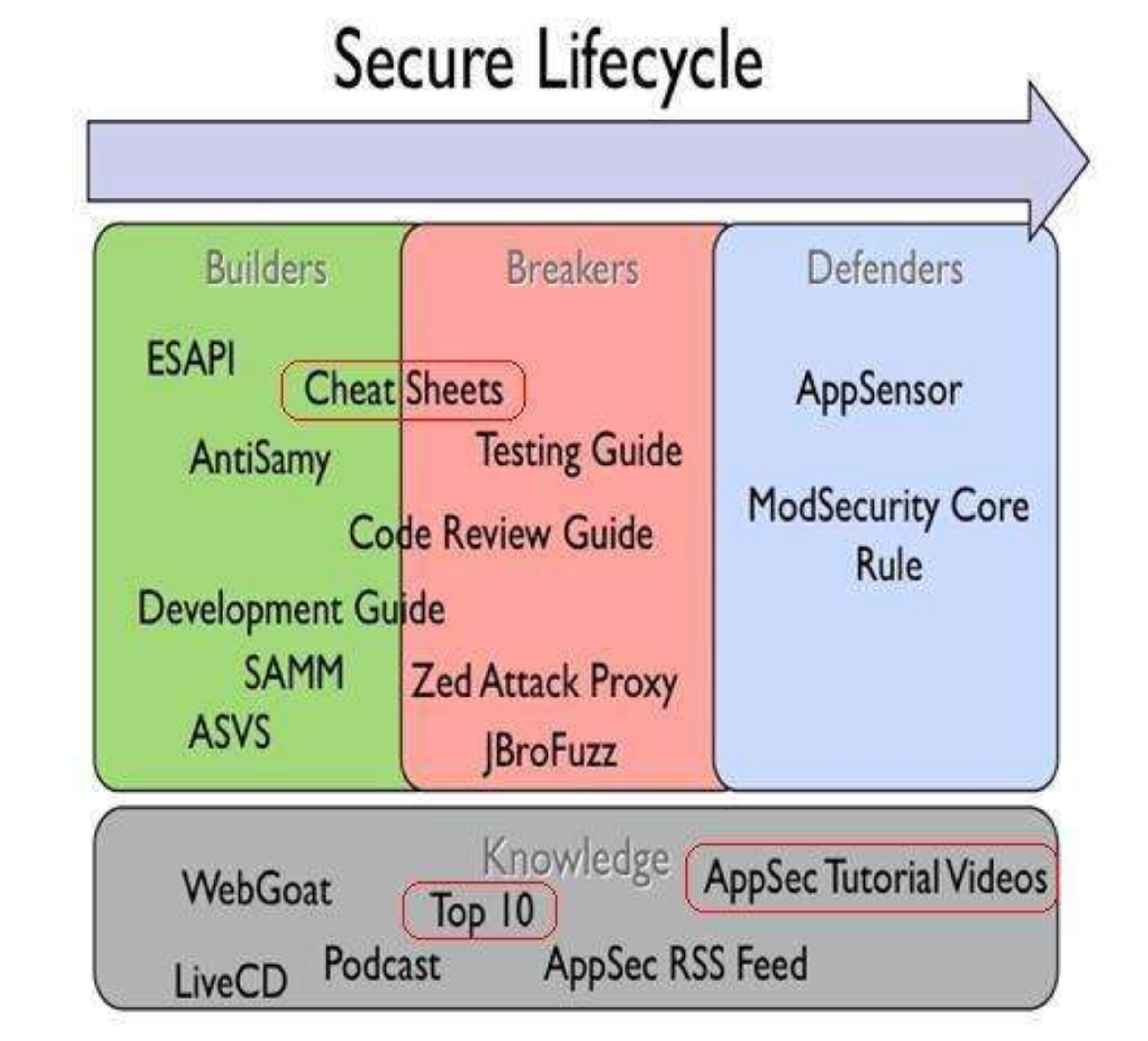


Security Lifecycle



A Vision for OWASP

Security Resources



Secure Lifecycle

Builders

ESAPI

Cheat Sheets

AntiSamy

Code Review Guide

Development Guide

SAMM

ASVS

Breakers

Testing Guide

Zed Attack Proxy

JBroFuzz

Defenders

AppSensor

ModSecurity Core Rule

Knowledge

WebGoat

Top 10

AppSec Tutorial Videos

LiveCD

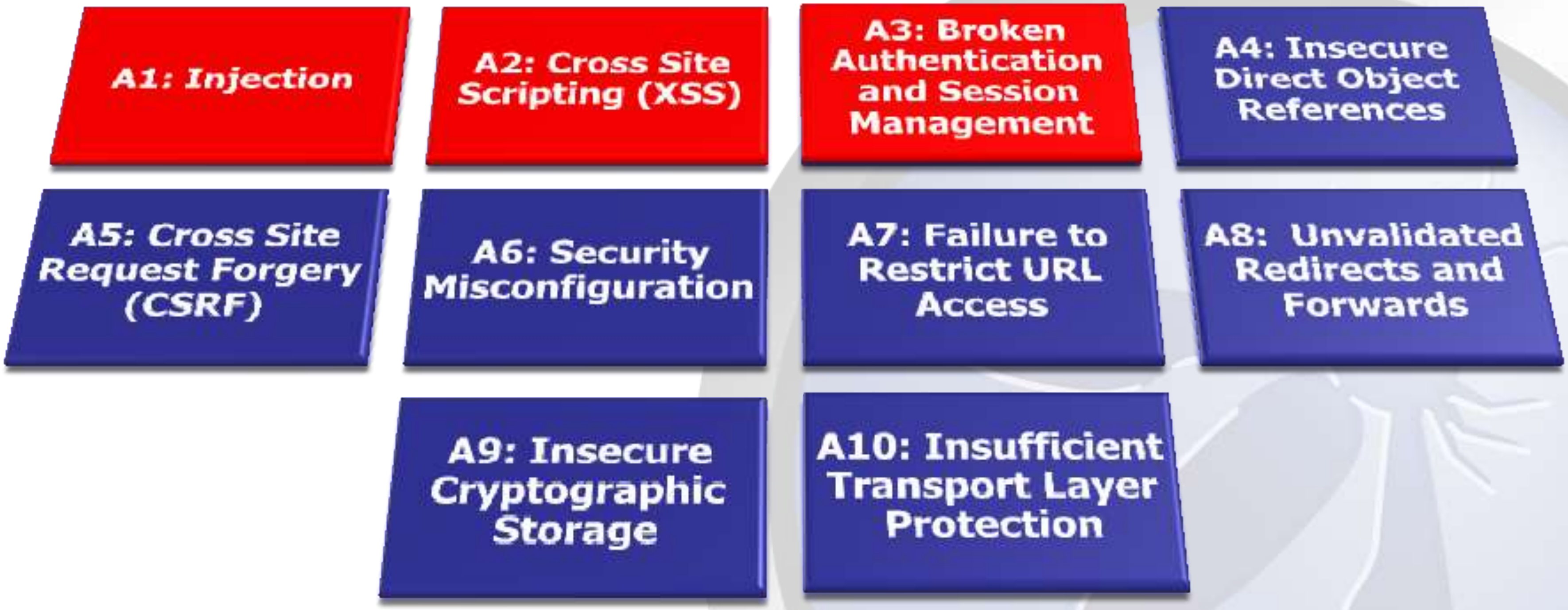
Podcast

AppSec RSS Feed

The OWASP Top Ten

TOP 10 WEB APPLICATION SECURITY RISKS

TOP 3 WEB APPLICATION SECURITY RISKS



- A1: Injection
- A2: Cross Site Scripting (XSS)
- A3: Broken Authentication and Session Management
- A4: Insecure Direct Object References
- A5: Cross Site Request Forgery (CSRF)
- A6: Security Misconfiguration
- A7: Failure to Restrict URL Access
- A8: Unvalidated Redirects and Forwards
- A9: Insecure Cryptographic Storage
- A10: Insufficient Transport Layer Protection

The OWASP Appsec Tutorial Series (Videos)

- News
- A Blog
- A Podcast
- Memberships
- Mailing Lists
- A Newsletter
- Apple App Store
- Video Tutorials
- Training Sessions
- Social Networking

OWASP Projects

OWASP
The Open Web Application Security Project

Cheat Sheets

OWASP
The Open Web Application Security Project

Developer Cheat Sheets (Builder)

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

Assessment Cheat Sheets (Breaker)

- Attack Surface Analysis Cheat Sheet
- XSS Filter Evasion Cheat Sheet

Mobile Cheat Sheets

- IOS Developer Cheat Sheet
- Mobile Jailbreaking Cheat Sheet

Draft Cheat Sheets

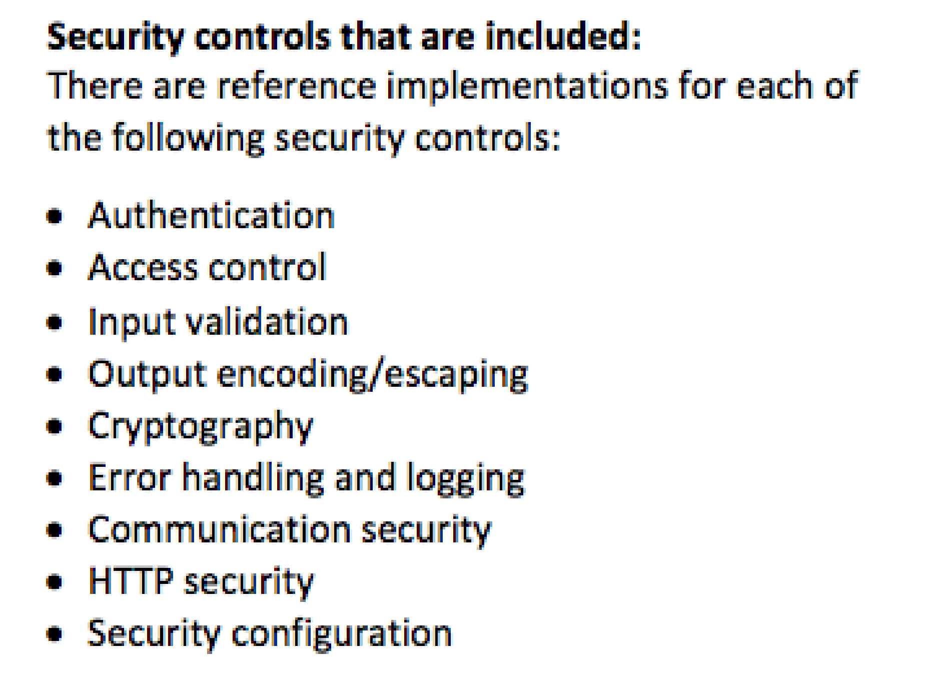
- Access Control Cheat Sheet
- Application Security Architecture Cheat Sheet
- Password Storage Cheat Sheet
- PHP Security Cheat Sheet
- .NET Security Cheat Sheet
- Secure Coding Cheat Sheet
- Secure SDLC Cheat Sheet
- Threat Modeling Cheat Sheet
- Virtual Patching Cheat Sheet
- Web Application Security Testing Cheat Sheet
- Grails Secure Code Review Cheat Sheet
- IOS Application Security Testing Cheat Sheet

Enterprise Security API

OWASP
The Open Web Application Security Project

Project Leader: Chris Schmidt, Chris.Schmidt@owasp.org

Purpose: A free, open source, web application security control library that makes it easier for programmers to write lower-risk applications



Security controls that are included:
There are reference implementations for each of the following security controls:

- Authentication
- Access control
- Input validation
- Output encoding/escaping
- Cryptography
- Error handling and logging
- Communication security
- HTTP security
- Security configuration

SELECTED

for Reboot

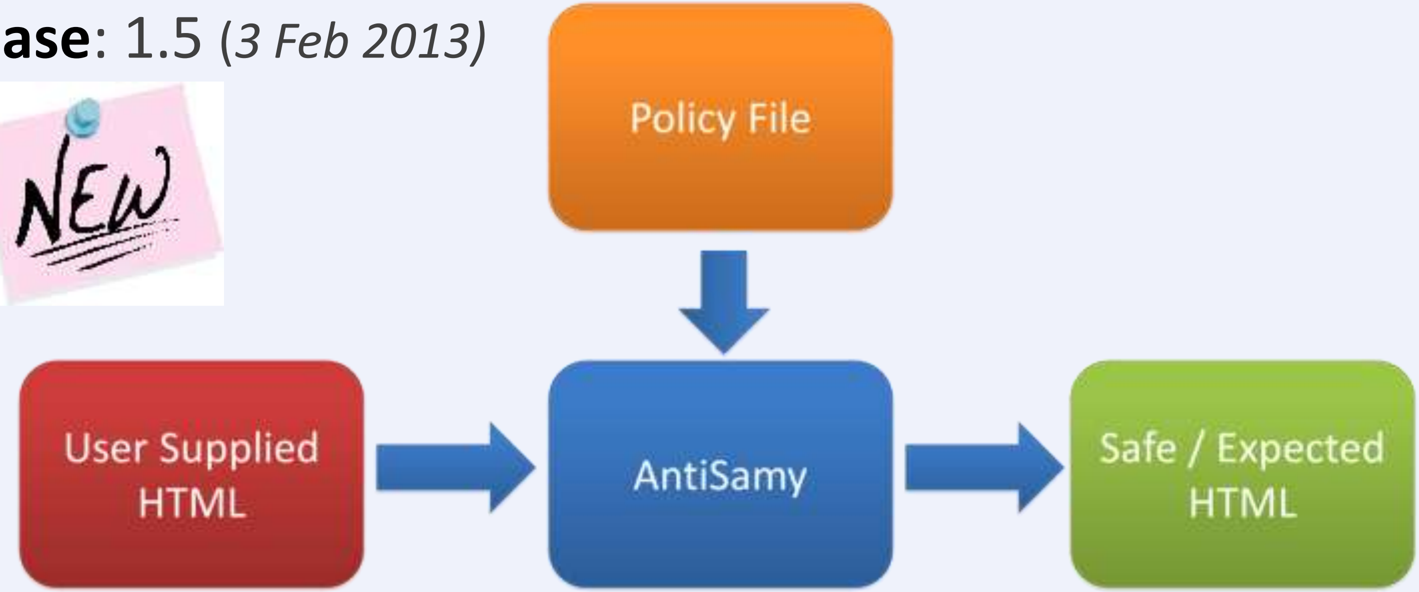
https://www.owasp.org/index.php/Category:OWASP_Enterprise_Security_API

AntiSamy

Project Leader: Jason Li, jason.li@owasp.org

Purpose: An API for ensuring user-supplied HTML/CSS is in compliance within an application's rules, that helps you make sure that clients don't supply malicious code in the HTML they supply for their profile, comments, etc., that get persisted on the server.

Last Release: 1.5 *(3 Feb 2013)*



Policy File

User Supplied HTML

AntiSamy

Safe / Expected HTML

https://www.owasp.org/index.php/Category:OWASP_AntiSamy_Project

Guides

Development Guide: comprehensive manual for designing, developing and deploying secure Web Applications and Web Services

Code Review Guide: mechanics of reviewing code for certain vulnerabilities & validation of proper security controls

Testing Guide: understand the what, why, when, where, and how of testing web applications

SELECTED QUALITY • SELECTED QUALITY • SELECTED

for Reboot

https://www.owasp.org/index.php/Category:OWASP_Guide_Project
https://www.owasp.org/index.php/Category:OWASP_Code_Review_Project
https://www.owasp.org/index.php/Category:OWASP_Testing_Project

Zed Attack Proxy

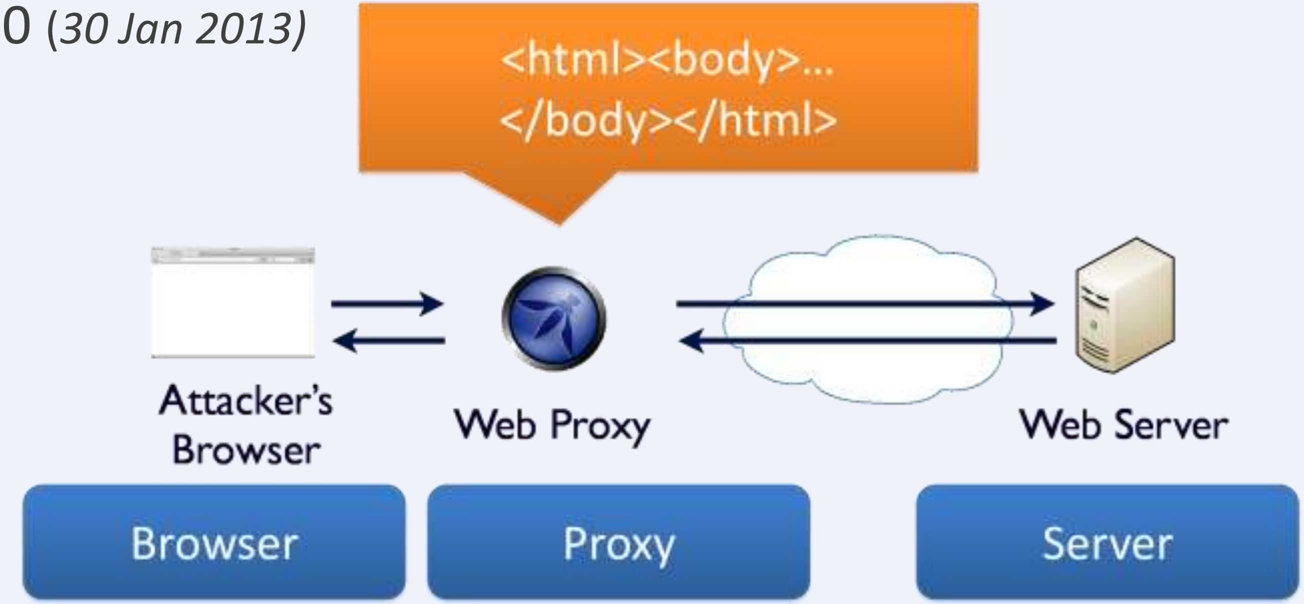
OWASP
The Open Web Application Security Project

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 2.0.0 *(30 Jan 2013)*

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

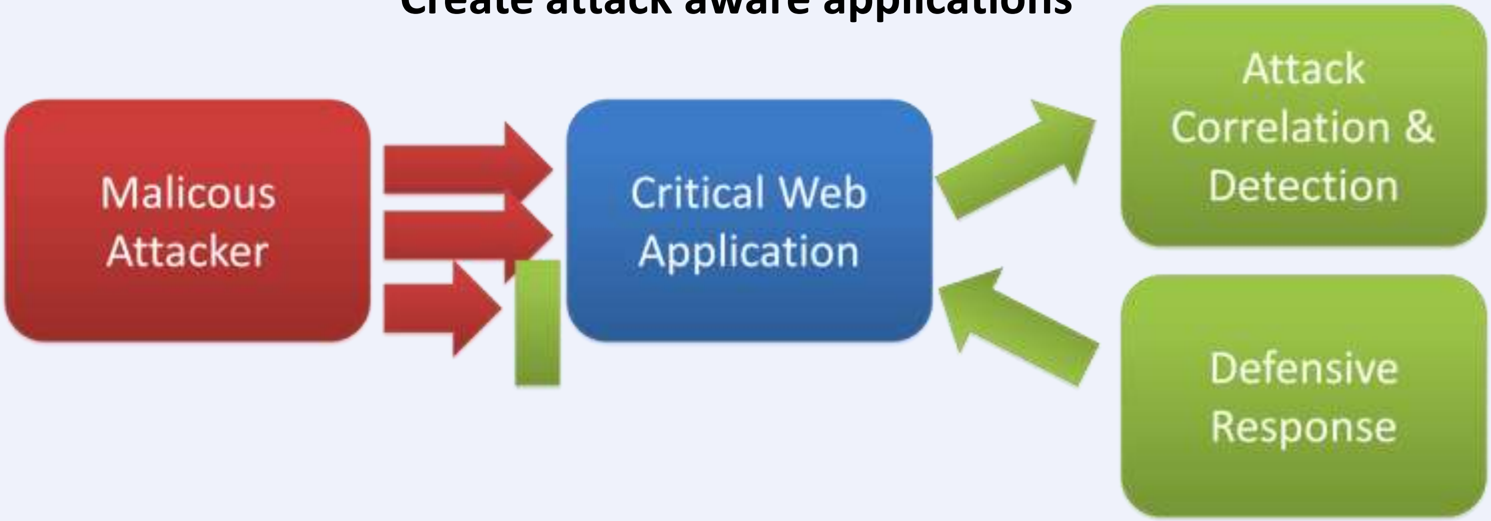
AppSensor

Project Leader(s): Michael Coates, John Melton, Colin Watson

Purpose: Defines a conceptual framework and methodology that offers prescriptive guidance to implement intrusion detection and automated response into an existing application.

Release: AppSensor 0.1.3 - *Nov 2010 (Tool) & September 2008 (doc)*

Create attack aware applications



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

Cloud Top10 Project

OWASP
The Open Web Application Security Project

Project Leader: Vinay Bansal, Vinaykbansal@gmail.com

Purpose: Develop and maintain a list of Top 10 Security Risks faced with the Cloud Computing and SaaS Models. Serve as a Quick List of Top Risks with Cloud adoption, and Provide Guidelines on Mitigating the Risks.

Deliverables

- Cloud Top 10 Security Risks *(Draft expected for early 2013)*

https://www.owasp.org/index.php/Category:OWASP_Cloud_%E2%80%90_10_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)*
    - OWASP Wiki, 'Smartphone Secure Development Guidelines' (ENISA)
- Mobile Cheat Sheet Series
- OWASP GoatDroid Project
- OWASP Mobile Threat Model Project

SELECTED QUALITY
SELECTED
for Reboot

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

Threat Modeling Project

OWASP
The Open Web Application Security Project

Project Leader: Anurag "Archie" Agarwal, anurag.agarwal@owasp.org

Purpose: Establish a single and inclusive software-centric OWASP Threat modeling Methodology, addressing vulnerability in client and web application-level services over the Internet.

Deliverables *(1st Draft expected for end of 2012 / early 2013)*

- An OWASP Threat Modeling methodology
- A glossary of threat modeling terms

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

Projects Reboot 2012

OWASP
The Open Web Application Security Project

Refresh, revitalize & update Projects, rewrite & complete Guides or Tools.

Initial Submissions

- OWASP Application Security Guide For CISOs - *Selected for Reboot*
- OWASP Development Guide - *Selected for Reboot*
- Zed Attack Proxy - *Selected for Reboot*
- OWASP WebGoat
- OWASP AppSensor
- OWASP Mobile Project - *Selected for Reboot*
- OWASP Portuguese Language Project
- OWASP_Application_Testing_guide_v4
- OWASP ESAPI
- OWASP Eliminate Vulnerable Code Project
- OWASP_Code_Review_Guide_Reboot

Projects selected via first round of review

1. **OWASP Development Guide**: Funding Amount: $5000 initial funding
2. **OWASP CISO Guide**: Funding Amount: $5000 initial funding
3. **OWASP Zed Attack Proxy**: Funding Amount: $5000 initial funding
4. **OWASP Mobile Project**: Funding Amount: $5000 initial funding

*Ongoing discussions about the **Code Review** and the **Testing Guides***

https://www.owasp.org/index.php/Projects_Reboot_2012

MEMBERSHIP ?

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

Abraham Lincoln

Teamwork

TEAM stands for… Together Each Achieves More

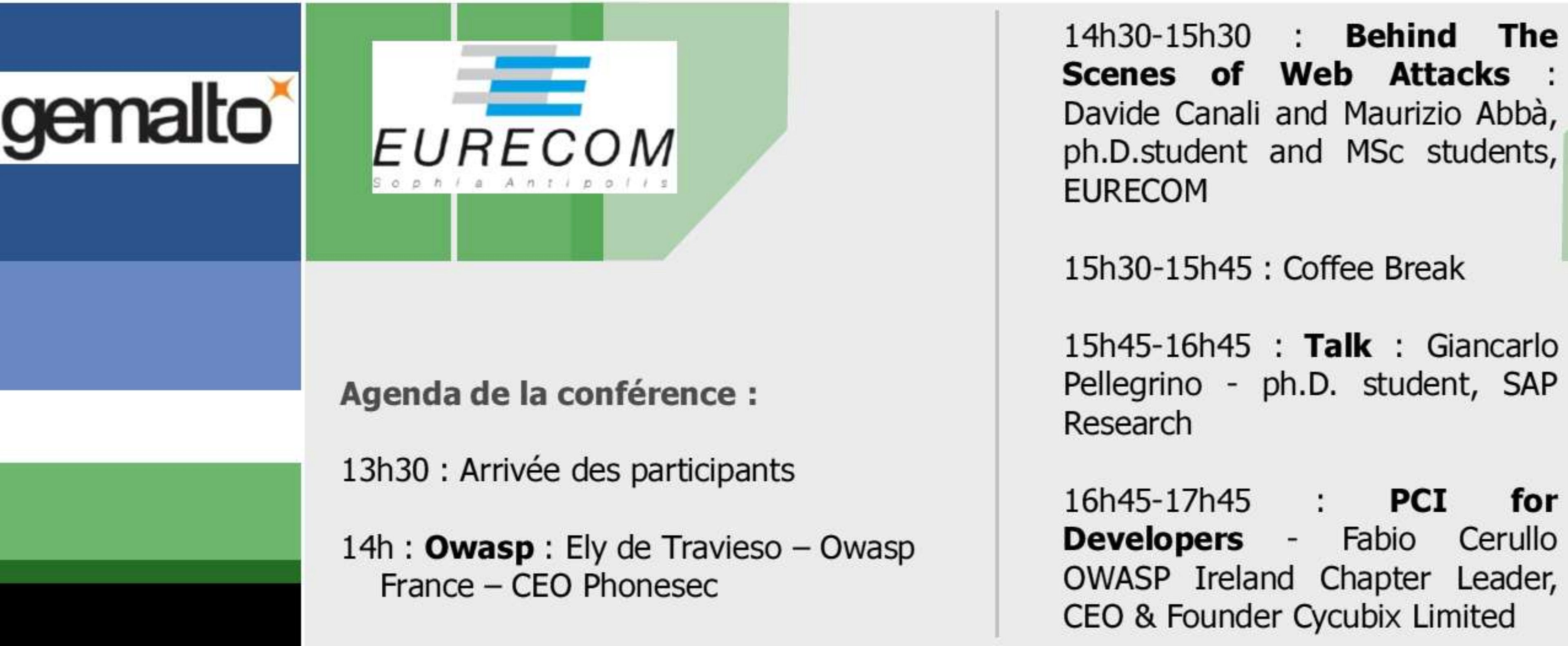
You guys are welcome to attend our meetings and have talks at OWASP.

The OWASP French Chapter welcomes you!

Q&A

OWASP
The Open Web Application Security Project

Ely de Travieso
ely.detravieso@owasp.org
+33 (0) 629 424 286


gemalto
EURECOM
Sophia Antipolis

Agenda de la conférence :

13h30 : Arrivée des participants

14h : **Owasp** : Ely de Travieso – Owasp France – CEO Phonesec

14h30-15h30 : **Behind The Scenes of Web Attacks** : Davide Canali and Maurizio Abbà, ph.D.student and MSc students, EURECOM

15h30-15h45 : Coffee Break

15h45-16h45 : **Talk** : Giancarlo Pellegrino - ph.D. student, SAP Research

16h45-17h45 : **PCI for Developers** - Fabio Cerullo OWASP Ireland Chapter Leader, CEO & Founder Cycubix Limited