# OWASP, the Life,the Universe

## TechItDays 2014

Séminaire DT Solocal 2014

4th September 2014

**Sébastien Gioria**
Sebastien.Gioria@owasp.org
Chapter Leader & Evangelist OWASP France

OWASP
The Open Web Application Security Project

tech_it_d4ys_2014

# http://www.google.fr/#q=sebastien gioria

- Innovation and Technology @Advens && Application Security Expert
- OWASP France Leader & Founder & Evangelist,
- OWASP ISO Project & OWASP SonarQube Project Leader
- Application Security group leader for the CLUSIF
- Proud father of youngs kids trying to hack my digital life.

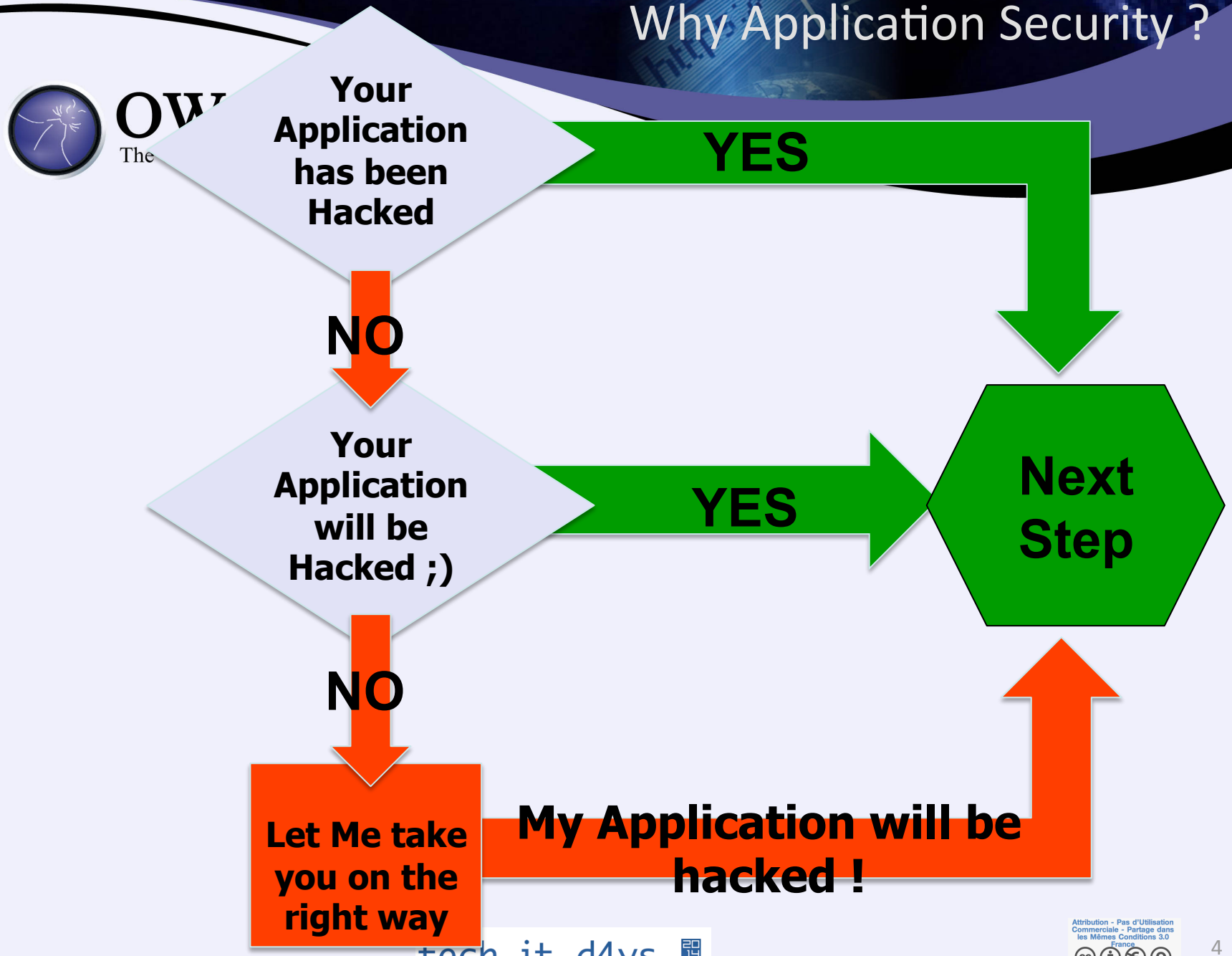
**Twitter :@SPoint/@OWASP_France**

# Agenda

OWASP
The Open Web Application Security Project

- Application Security :
  - where we are (no bullshit)
  - where we are (hopefully) going ?
- Open Web Application Security Project ?
- Major projects you can use

# Why Application Security ?



# SQL in Java

OWASP
The Open Web Application Security Project

http://stackoverflow.com/questions/9123084/how-to-execute-a-sql-statement-with-a-variable-as-where

Stack Overflow is a question and answer site for professional and enthusiast programmers. It's 100% free, no registration required.

**How to execute a SQL statement with a variable as WHERE?**



0

I have some Java code like

```
int userid = take user input;
```

And then execute following sql statement,

```
Class.forName(dbdriver);
conn = DriverManager.getConnection(url, username, password);
st = conn.createStatement();

st.executeUpdate("select * from person where uid = userid" );
```

Now, I don't know the returned result is `null`. I think `where uid = userid` is giving wrong result because it is searching for literal uid value "userid". Actually, I want to retrive information from person table about user provided uid values. Can anybody help me how to solve this?

```
ResultSet rs = stmd.executeQuery("select * from person where uid = "+ userid);
 while (rs.next()) {
                System.out.println("Name= " + rs.getString(1));
}
```


http://www.advens.fr/blog/les-injections-sql-dans-les-applications-web-pourquoi-navancons-nous-pas

# Game Over....

OWASP
The Open Web Application Security Project

- Did you develop Web Site?
- Did you develop embeded products ?
- Did you develop smartphone applications ?
- Did you have customers / partners over Internet ?

# Why Application Security ?

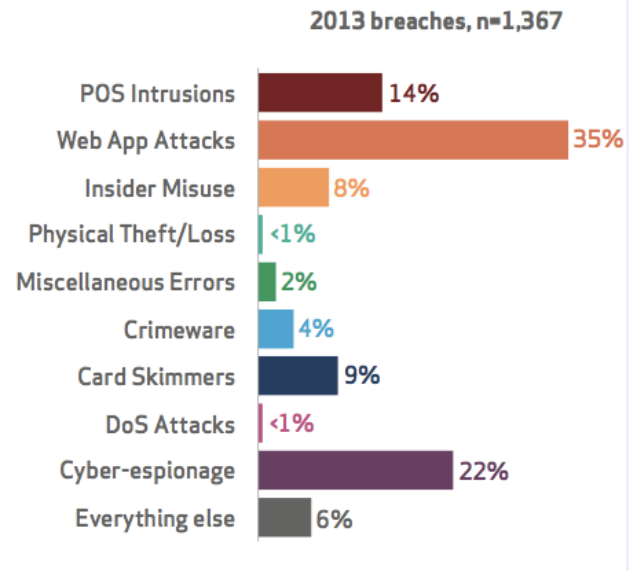
OWASP
The Open Web Application Security Project

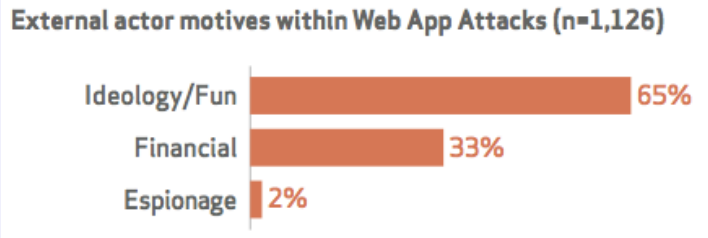
We are living in a Digital environment, in a Connected World


- Most of websites vulnerable to attacks
- Important % of web-based Business *(Services, Online Store, Self-care, Telcos, SCADA, ...)*

**92%**

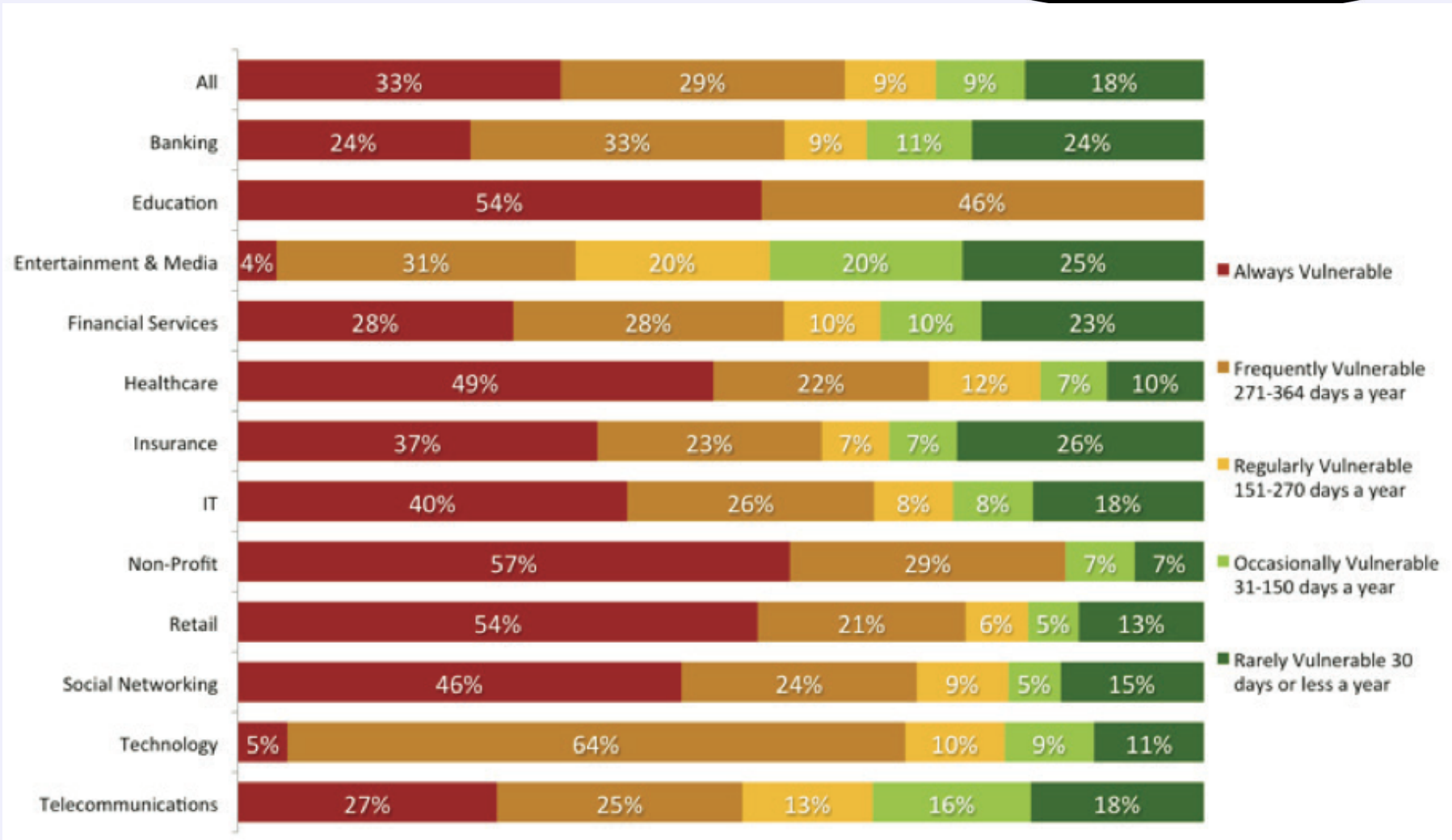
THE UNIVERSE OF THREATS MAY SEEM LIMITLESS, BUT 92% OF THE 100,000 INCIDENTS WE'VE ANALYZED FROM THE LAST 10 YEARS CAN BE DESCRIBED BY JUST NINE BASIC PATTERNS.



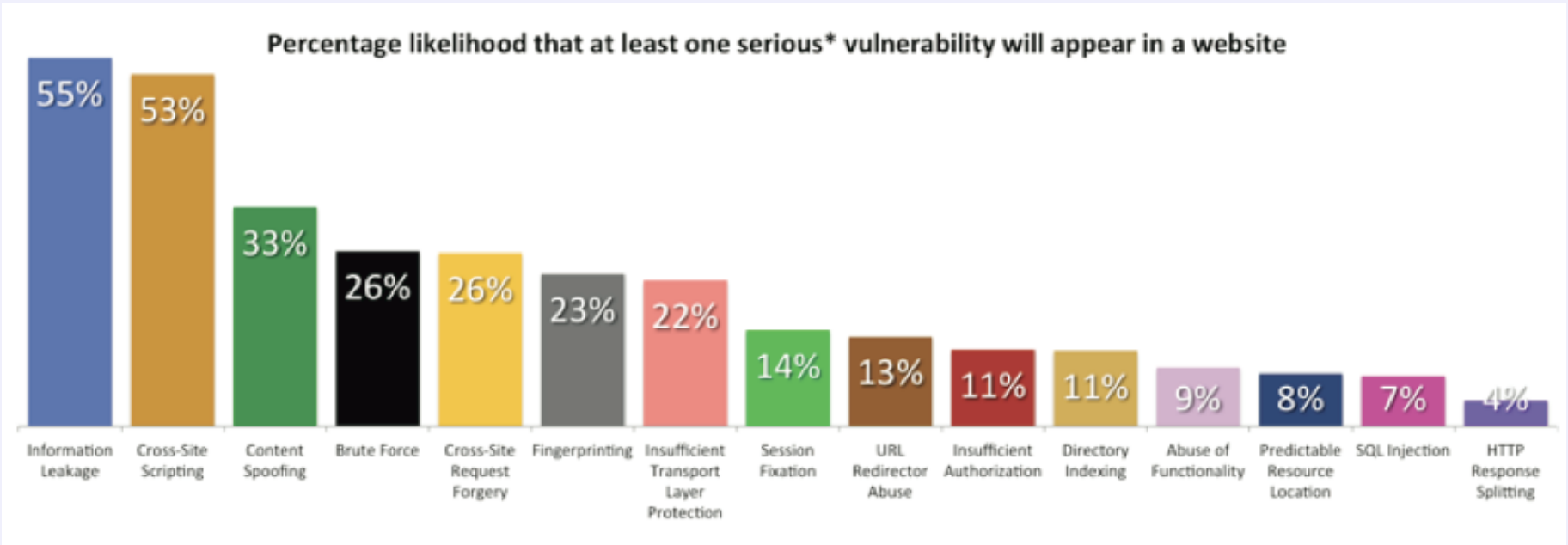
# Who win ?

OWASP
The Open Web Application Security Project



# Vulnerabilities ?

OWASP
The Open Web Application Security Project



OWASP
The Open Web Application Security Project

# Anything else ?

# What is OWASP

OWASP
The Open Web Application Security Project

## 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

# Around the World

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

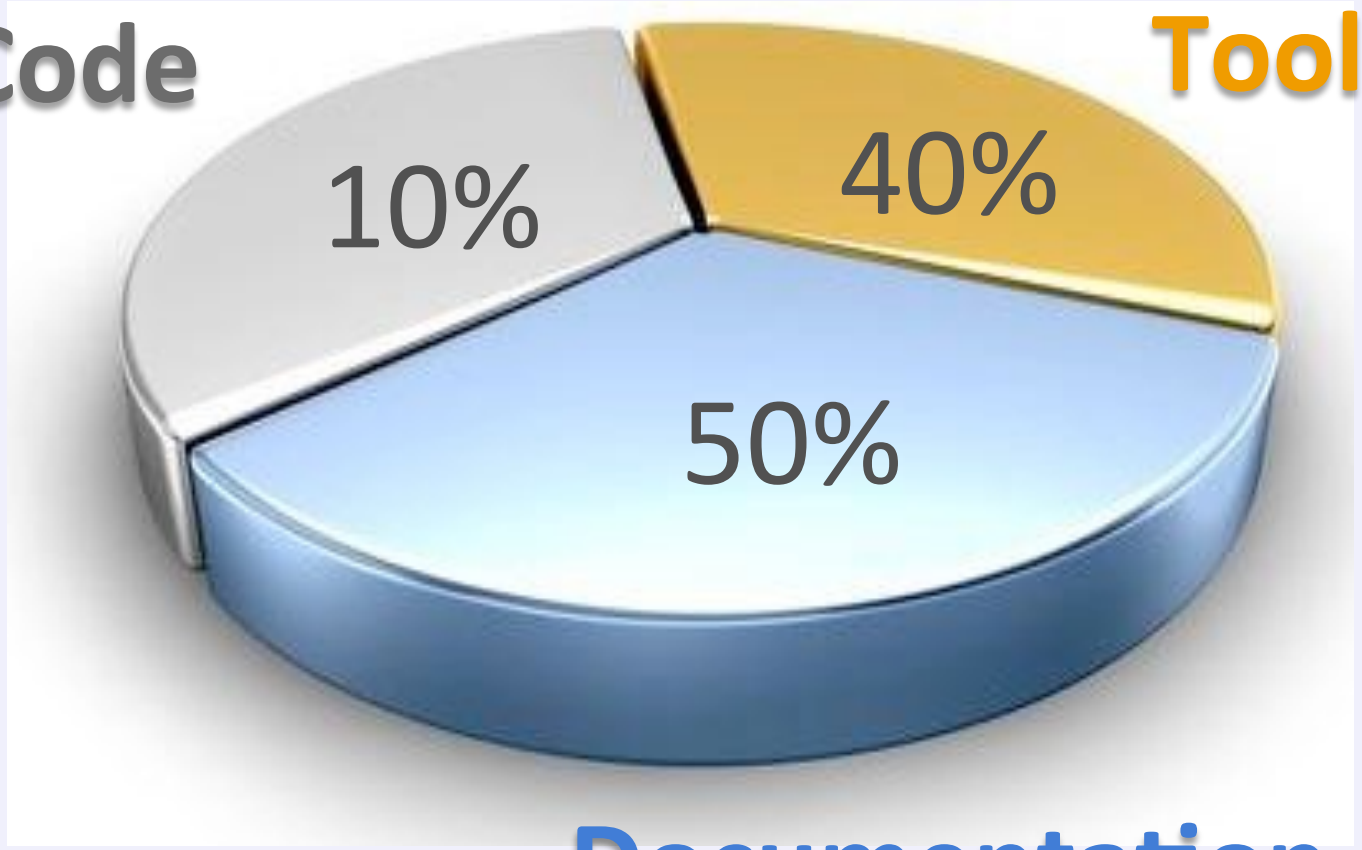
15,000+ downloads of tools, documentation

250,000+ unique visitors

800,000+ page views (monthly)

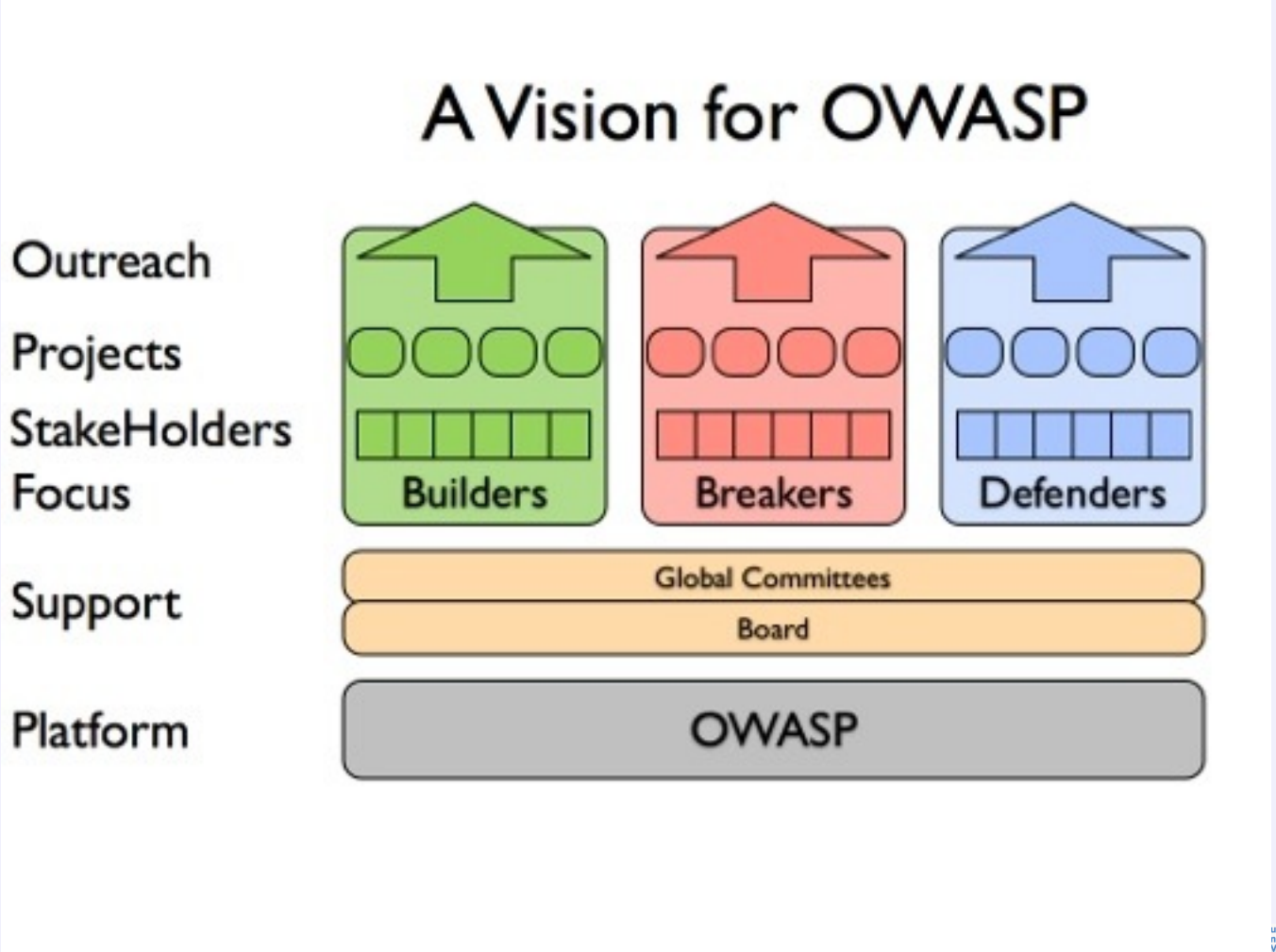
# Quality Resources

OWASP
The Open Web Application Security Project



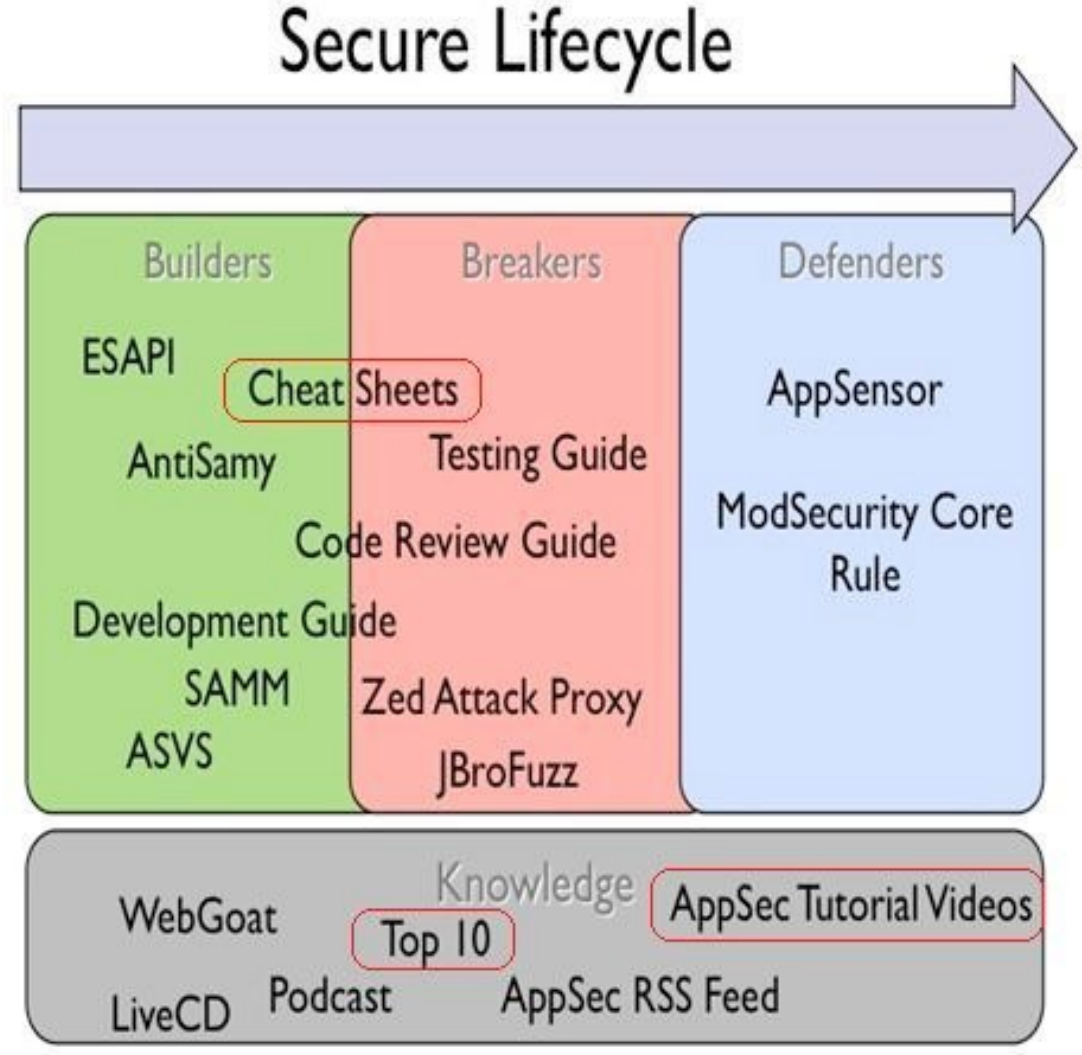
# Security Lifecycle

OWASP
The Open Web Application Security Project



# Security Resources

OWASP
The Open Web Application Security Project



# OWASP

The Open Web Application Security Project

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









# OWASP Projects


Welcome | Project Inventory | Project Task Force | Online Resources | Starting a New Project | Project Assessments | Brand Resources | Terminology | Sponsorships and Donations | PM Information | Contact US

## OWASP Project Inventory

All OWASP tools, document, and code library projects are organized into the following categories:

- **Flagship Projects:** The OWASP Flagship designation is given to projects that have demonstrated strategic value to OWASP and application security as a whole.
- **Lab Projects:** OWASP Labs projects represent projects that have produced an OWASP reviewed deliverable of value.
- **Incubator Projects:** OWASP Incubator projects represent the experimental playground where projects are still being fleshed out, ideas are still being proven, and development is still underway.

## Welcome to the OWASP Global Projects Page

An OWASP project is a collection of related tasks that have a defined roadmap and team members. OWASP project leaders are responsible for defining the vision, roadmap, and tasks for the project. The project leader also promotes the project and builds the team. OWASP currently has over 142 active projects, and new project applications are submitted every week.

This is one of the most popular divisions of OWASP as it gives members an opportunity to freely test theories and ideas with the professional advice and support of the OWASP community. Every project has an associated mail list. You can view all the lists, examine their archives, and subscribe to any project by visiting the OWASP Project Mailing Lists page. A summary of recent project announcements is available on the OWASP Updates page.

**Download the OWASP Project Handbook 2014**

# OWASP Top10 2013

OWASP
The Open Web Application Security Project

| | | | |
|---|---|---|---|
| A1: Injection | A2: Violation de Gestion d'authentification et de session | A3: Cross Site Scripting (XSS) | A4:Référence directe non sécurisée à un objet |
| A5: Mauvaise configuration sécurité | A6 : Exposition de données sensibles | A7: Manque de contrôle d'accès fonctionnel | A8: Cross Site Request Forgery (CSRF) |
| | A9: Utilisation de composants avec des vulnérabilités connues | A10: Redirections et transferts non validés | |

ex-A9(transport non sécurisé) + A7(Stockage crypto)

# Cheat Sheets

OWASP
The Open Web Application Security Project

## Developer Cheat Sheets

- PHP Security Cheat Sheet
- OWASP Top Ten Cheat Sheet
- Authentication Cheat Sheet
- **Cross-Site Request Forgery (CSRF) Prevention Cheat Sheet**
- Cryptographic Storage Cheat Sheet
- Input Validation Cheat Sheet
- **XSS (Cross Site Scripting) Prevention Cheat Sheet**
- DOM based XSS Prevention Cheat Sheet
- Forgot Password Cheat Sheet
- **Query Parameterization Cheat Sheet**
- **SQL Injection Prevention Cheat Sheet**
- Session Management Cheat Sheet
- **HTML5 Security Cheat Sheet**
- Transport Layer Protection Cheat Sheet
- Web Service Security Cheat Sheet
- Logging Cheat Sheet
- JAAS Cheat Sheet

## Mobile Cheat Sheets

- IOS Developer Cheat Sheet
- Mobile Jailbreaking Cheat Sheet

## Draft Cheat Sheets

- Access Control Cheat Sheet
- REST Security Cheat Sheet
- Abridged XSS Prevention Cheat Sheet
- Password Storage Cheat Sheet
- Secure Coding Cheat Sheet
- Threat Modeling Cheat Sheet
- Clickjacking Cheat Sheet
- Virtual Patching Cheat Sheet
- Secure SDLC Cheat Sheet
- Web Application Security Testing Cheat Sheet
- Application Security Architecture 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

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

# Java HTML Sanitizer, Java Encoder

OWASP
The Open Web Application Security Project

**Project Leader:** Mike Samuel Mike.samuel@owasp.org

**Purpose**: The OWASP HTML Sanitizer is a fast and easy to configure HTML Sanitizer written in Java which **lets you include HTML authored by third-parties in your web application** while protecting against **XSS**.

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

**Project Leader:** Jeff Ichnowski

**Purpose**: The OWASP Java Encoder is a Java 1.5+ simple-to-use drop-in high-performance encoder class with no dependencies and little baggage. This project will help Java web developers defend against Cross Site Scripting!

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

# Java Encoder Project

OWASP
The Open Web Application Security Project

**Project Leader:** Mike Samuel Mike.samuel@owasp.org

**Purpose**: The OWASP Java Encoder is a Java 1.5+ simple-to-use drop-in high-performance encoder class with no dependencies and little baggage. This project will help Java web developers defend against Cross Site Scripting!

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

# OWASP Top10 Mobile project

OWASP
The Open Web Application Security Project

# OWASP IoT Project

OWASP
The Open Web Application Security Project

- The OWASP Internet of Things Top 10 - 2014 is as follows:

- I1 Insecure Web Interface
- I2 Insufficient Authentication/Authorization
- I3 Insecure Network Services
- I4 Lack of Transport Encryption
- I5 Privacy Concerns
- I6 Insecure Cloud Interface
- I7 Insecure Mobile Interface
- I8 Insufficient Security Configurability
- I9 Insecure Software/Firmware
- I10 Poor Physical Security

# Guides

OWASP
The Open Web Application Security Project

**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

**Application Security Verification Standard (ASVS):** comprehensive manual for designing, verify the security of an application

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

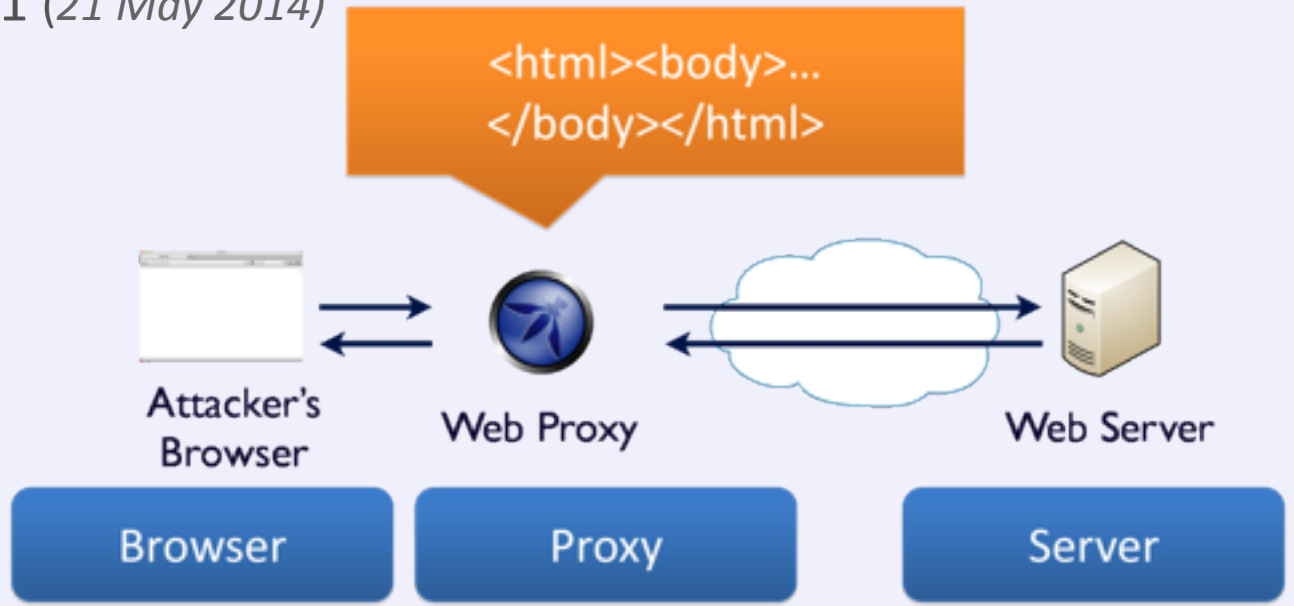
# Zed Attack Proxy

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 2.3.1 (*21 May 2014*)




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

# The OWASP Secure Software Contract Annex

OWASP
The Open Web Application Security Project

Intended to help software developers and their clients negotiate important contractual terms and conditions related to the security of the software to be developed or delivered.

**CONTEXT**: Most contracts are silent on these issues, and the parties frequently have dramatically different views on what has actually been agreed to.

**OBJECTIVE**: Clearly define these terms is the best way to ensure that both parties can make informed decisions about how to proceed.

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

# Dates

OWASP
The Open Web Application Security Project

- 11 Septembre 2014 – OWASP France Meeting Paris @Mozilla Office
  - **Programme :**
  - 18h30 : Ouverture des portes
  - 19h : Welcome by OWASP France et Mozilla
  - 19h15 : SonarQube pour la sécurité par Sébastien Gioria (OWASP France)
  - 19h45 : Warning Ahead: Security Storms are Brewing in Your JavaScript - Par Laurent Levi (Checkmarx) - En Francais
  - 20h15 : OWASP News && Closing par Sébastien Gioria (OWASP France)
  - 20h30 : Networking

  **http://www.eventbrite.fr/e/billets-owasp-france-meeting-septembre-2014-12738480137**

- Application Security Forum Western Switzerland – Yverdon les Bains – 4/6 Novembre 2014
  - http://www.appsec-forum.ch/

- Club 27001 /Paris - 25 Septembre 2014
  - Présentation de la norme ISO 27034

# Soutenir l'OWASP

OWASP
The Open Web Application Security Project

- Différentes solutions :
  - Membre Individuel : 50 $
  - Membre Entreprise : 5000 $
  - Donation Libre
- Soutenir uniquement  le chapitre France :
  - Single Meeting supporter
    - Nous offrir une salle de meeting !
    - Participer par un talk ou autre !
    - Donation simple
  - Local Chapter supporter :
    - 500 $ à 2000 $

# License

OWASP
The Open Web Application Security Project




@SPoint

sebastien.gioria@owasp.org