OWASP, the Life,the Universe and the ElePHPhants

AFUP/MOZILLA/OWASP Meeting @Mozilla Paris
5th June 2014

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

OWASP
The Open Web Application Security Project

OWASP
The Open Web Application Security Project

OWASP
The Open Web Application Security Project

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

- Innovation and Technology @Advens && Application Security Expert
- OWASP France Leader & Founder & Evangelist
- 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 ?

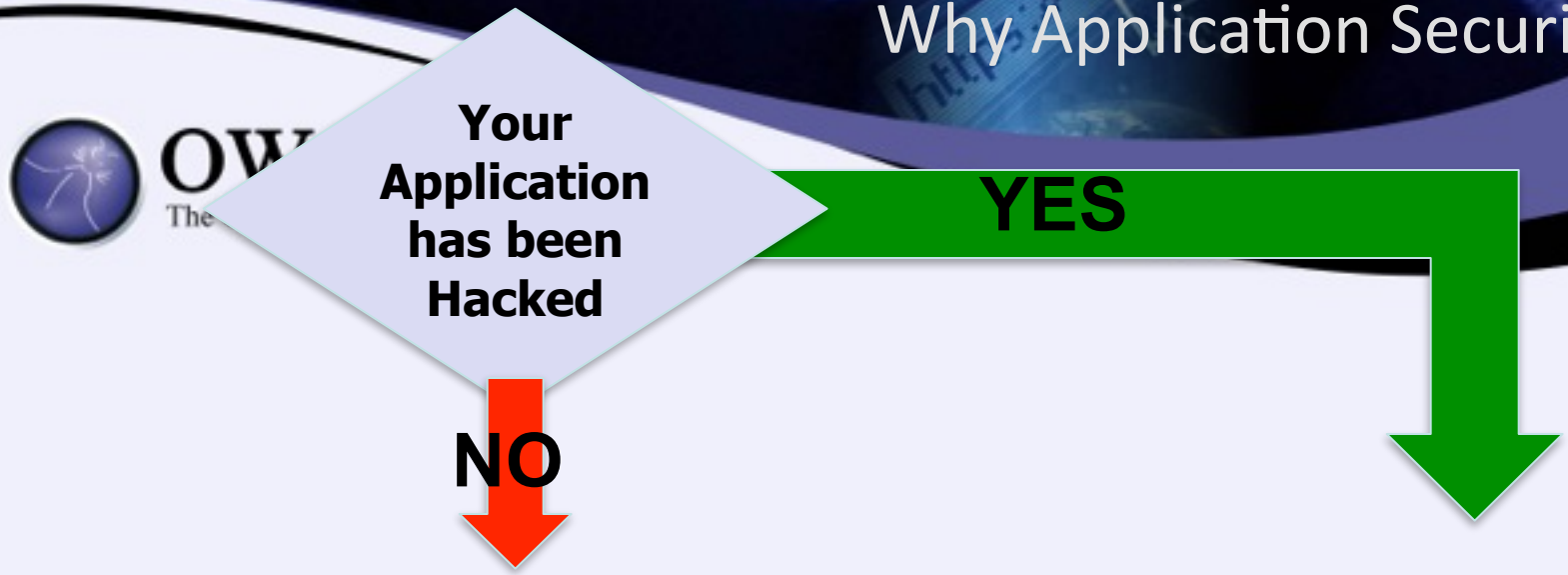
OWASP
The Open Web Application Security Project

Why Application Security ?

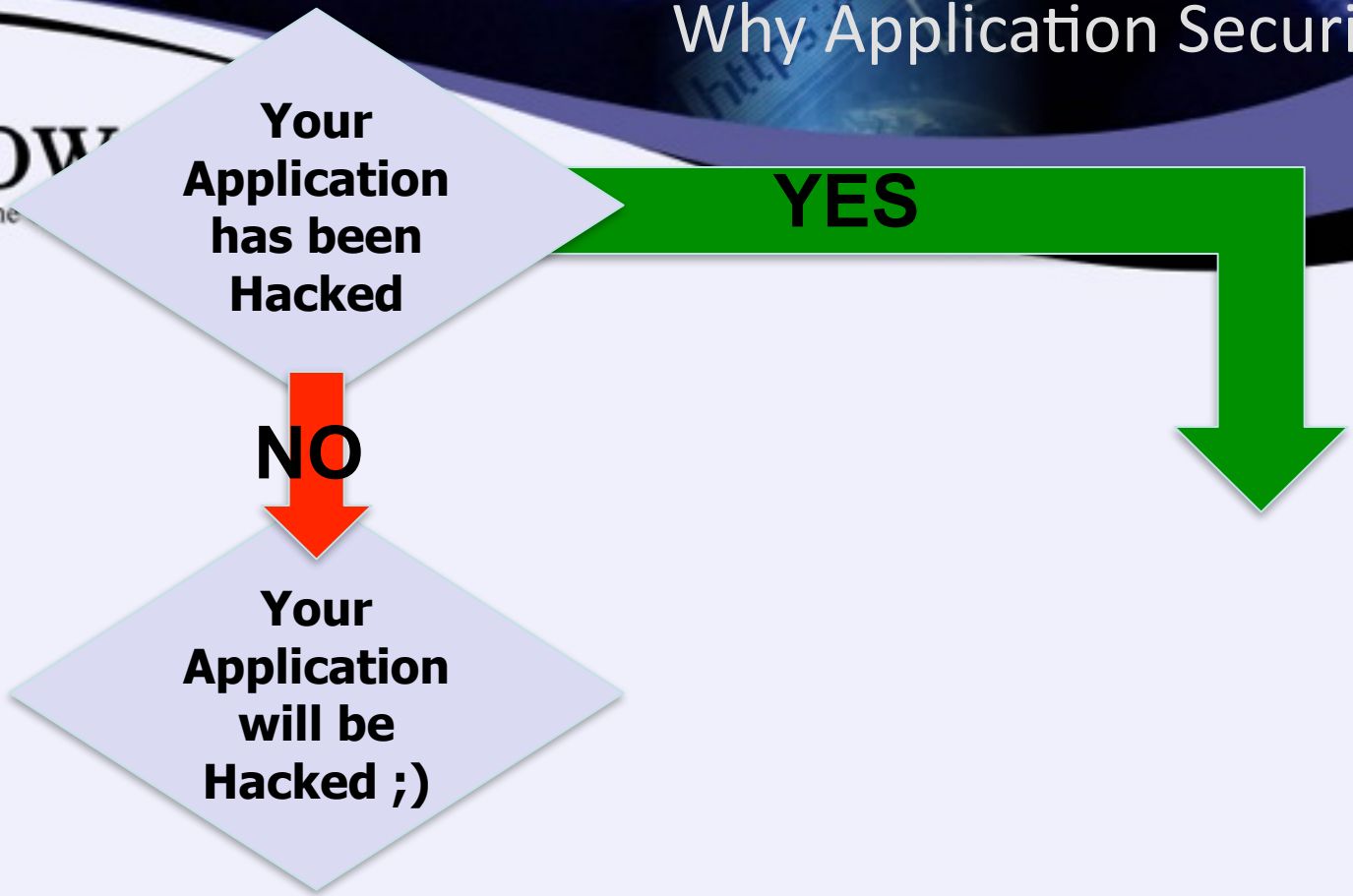
Your Application has been Hacked

Why Application Security ?

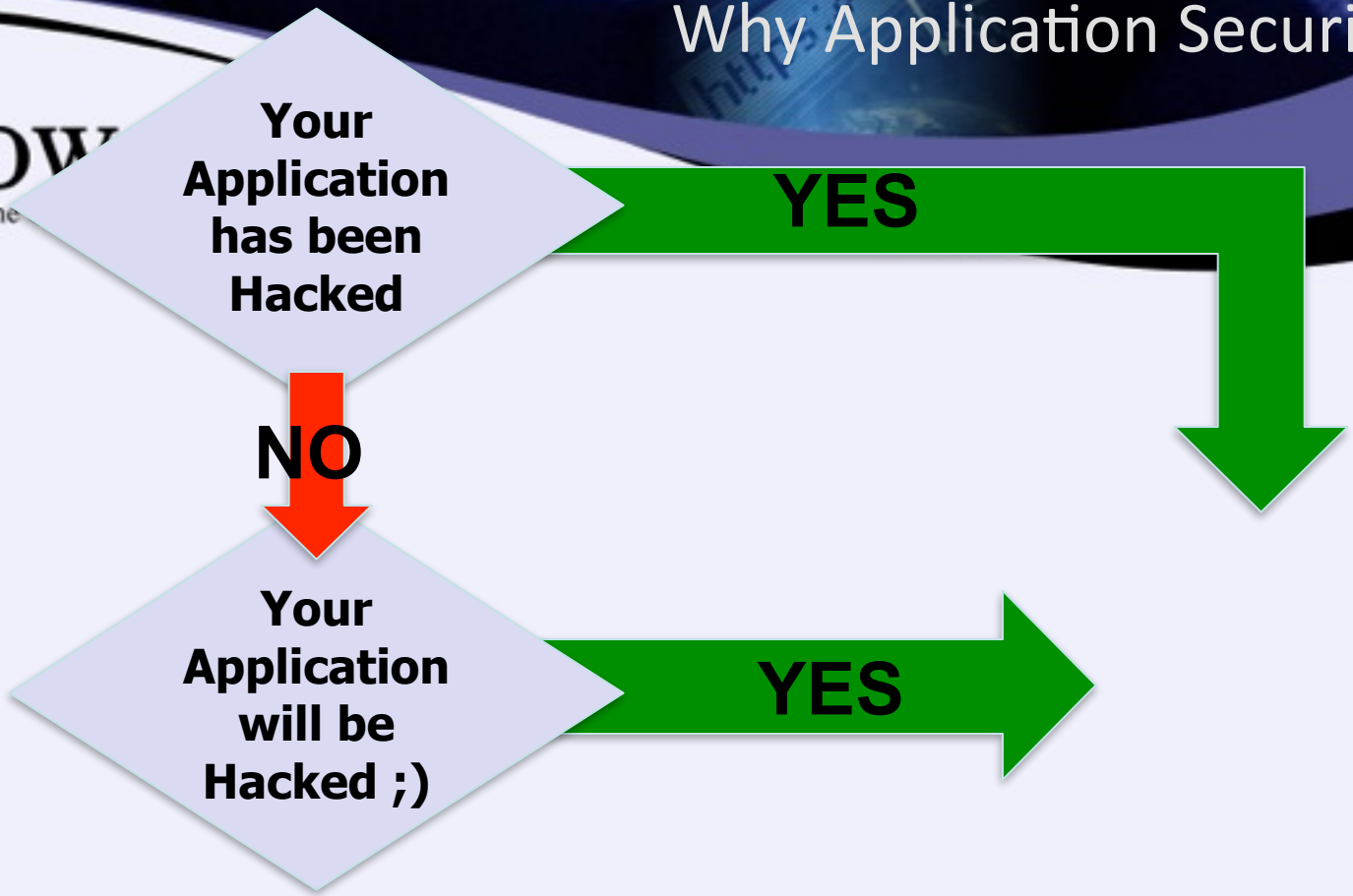
Why Application Security ?



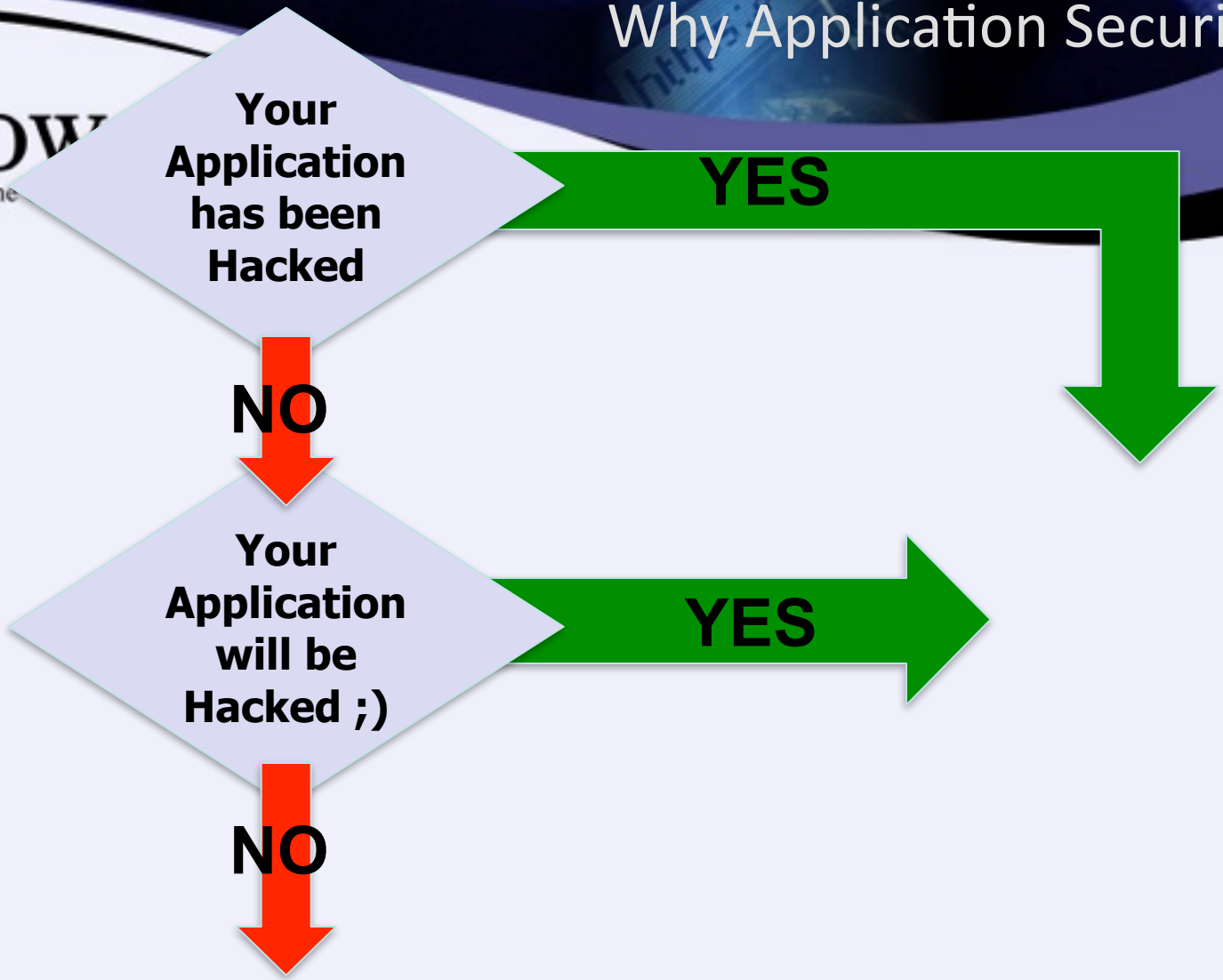
Why Application Security ?



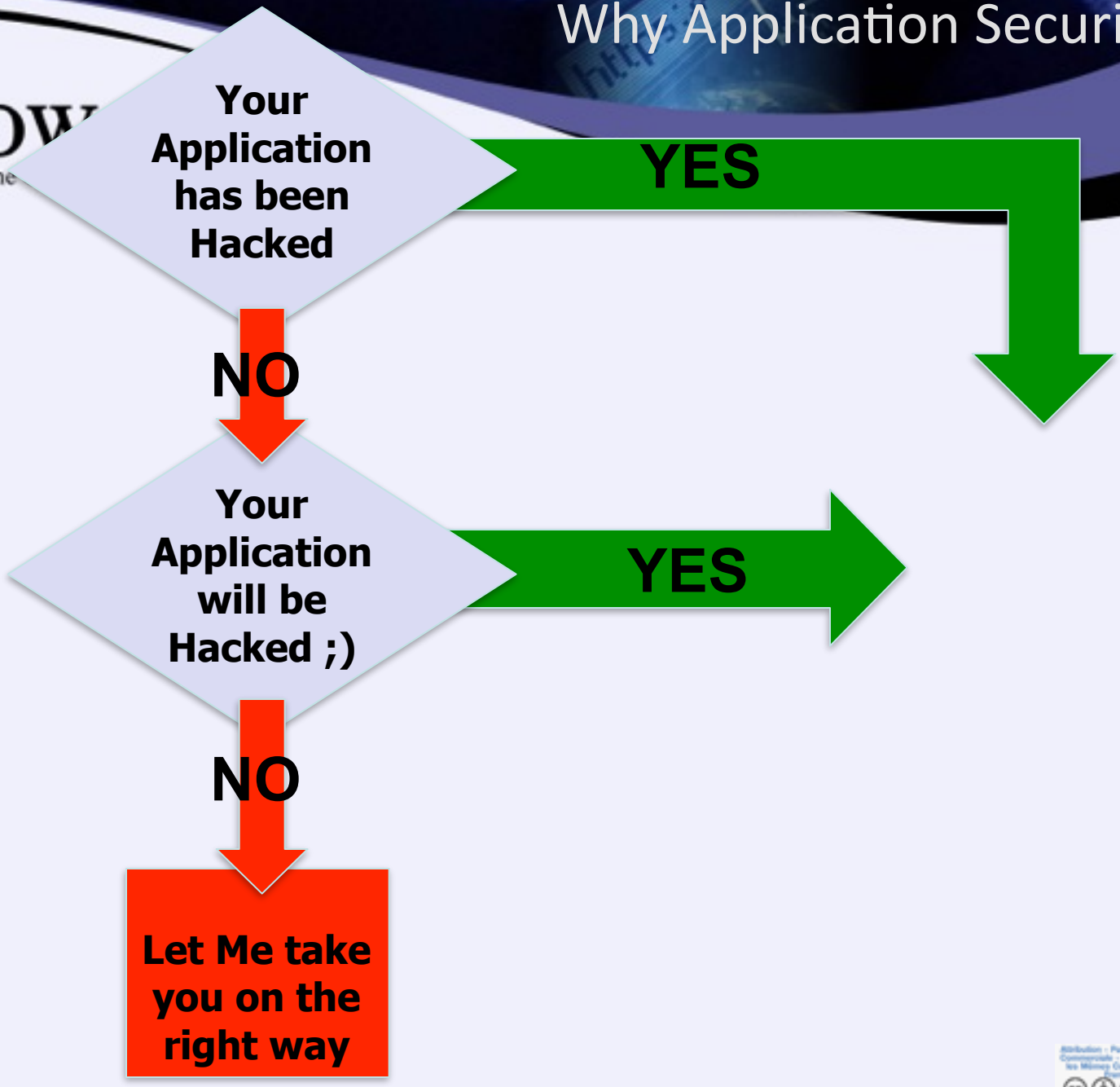
Why Application Security ?



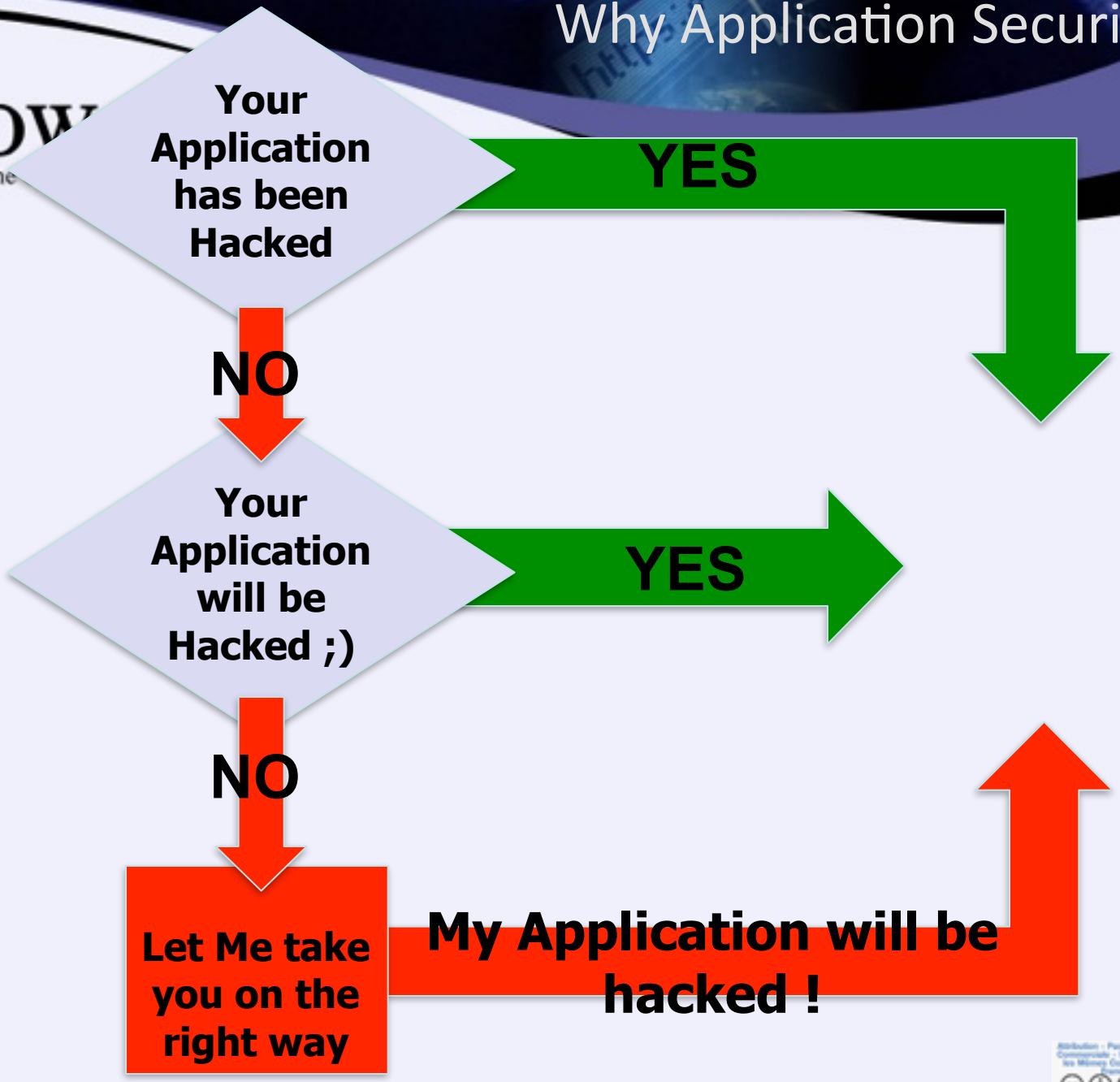
Why Application Security ?



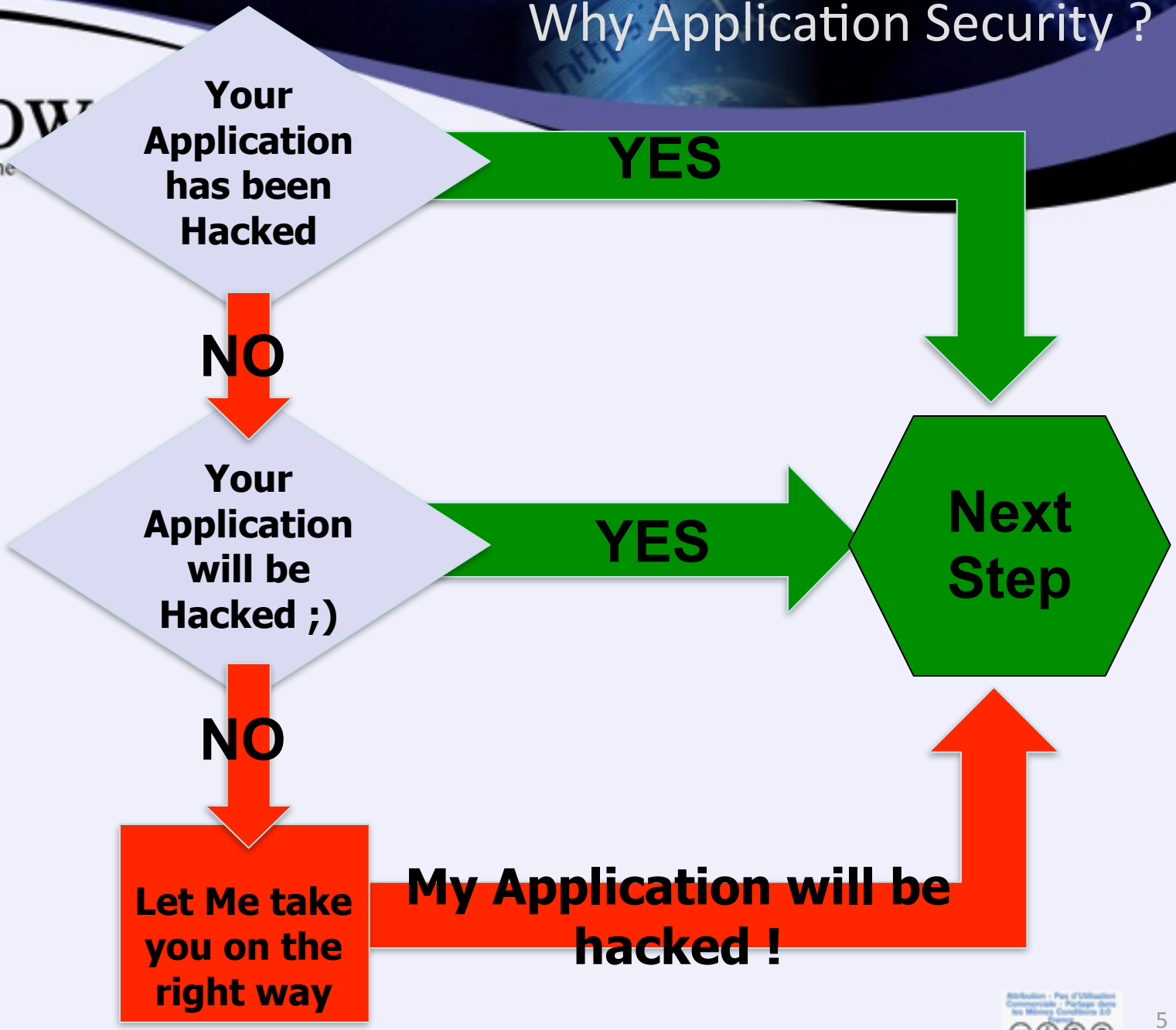
Why Application Security ?



Why Application Security ?



Why Application Security ?

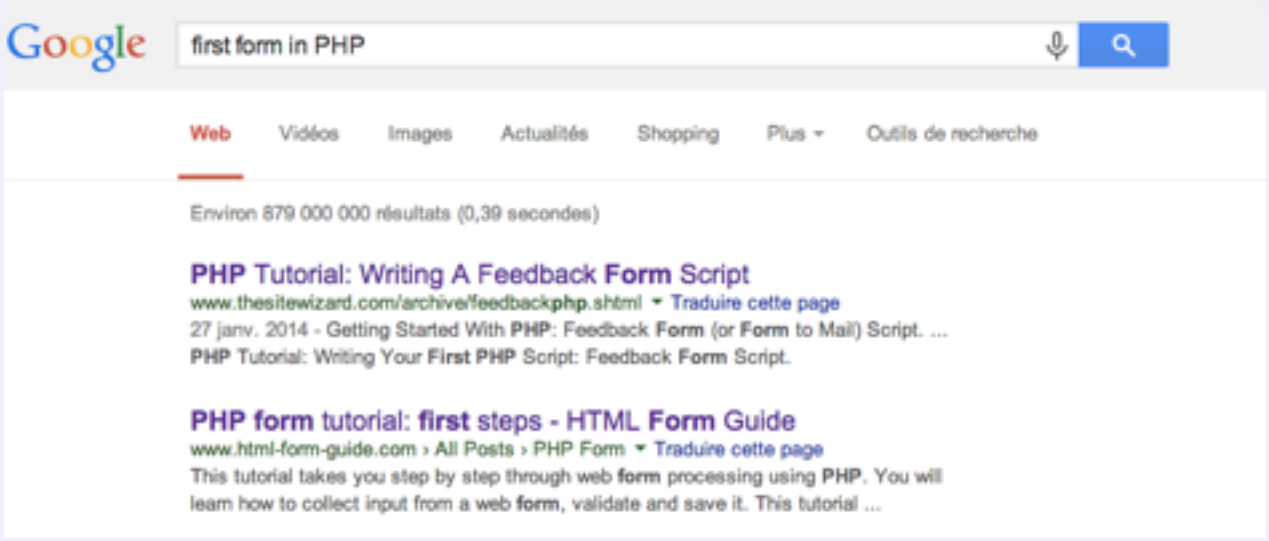


First form in PHP

OWASP
The Open Web Application Security Project

First form in PHP

OWASP
The Open Web Application Security Project



First form in PHP

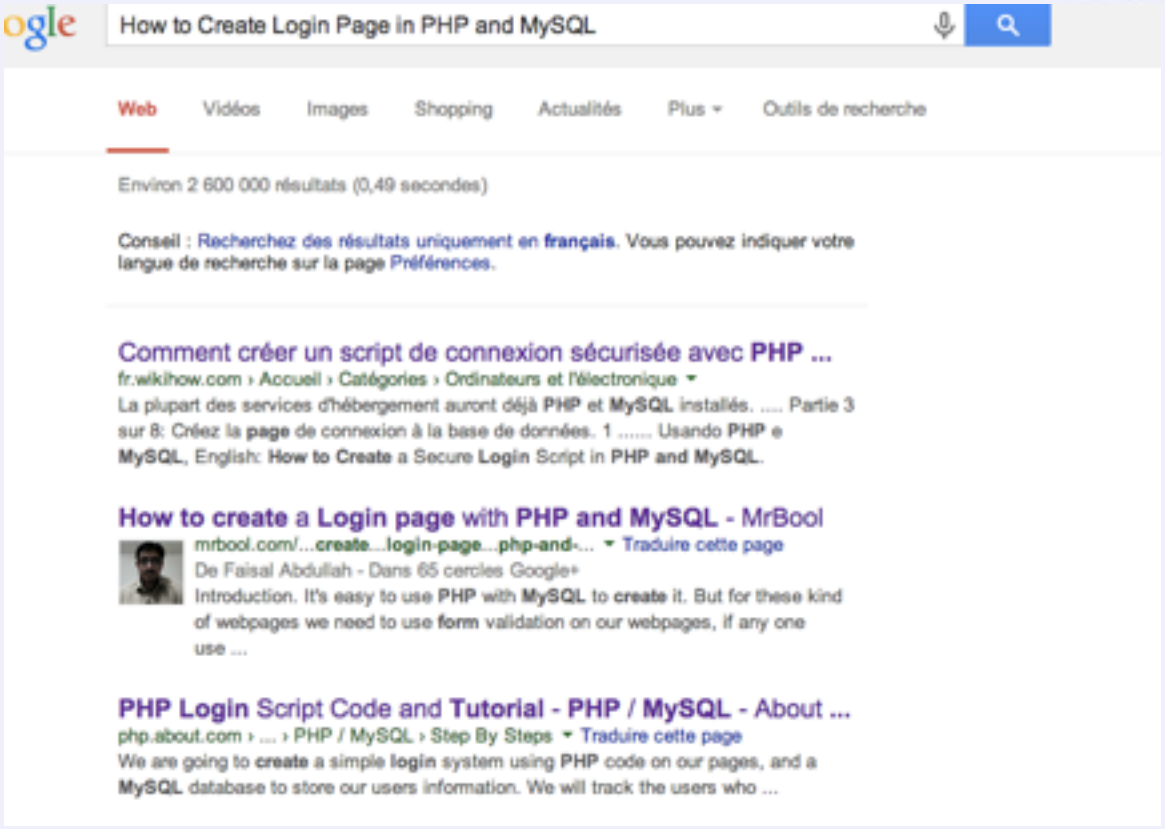

```
<?php
  $email = $_REQUEST['email'] ;
  $message = $_REQUEST['message'] ;

  mail( "yourname@example.com", "Feedback Form Results",
    $message, "From: $email" );
  header( "Location: http://www.example.com/thankyou.html" );
?>
```

OWASP
The Open Web Application Security Project

How to create a login page in PHP and Mysql

OWASP
The Open Web Application Security Project



OWASP
The Open Web Application Security Project

```php
<?php
define('DB_HOST', 'localhost');
define('DB_NAME', 'practice');
define('DB_USER','root');
define('DB_PASSWORD','');

$con=mysql_connect(DB_HOST,DB_USER,DB_PASSWORD) or die("Failed to connect to MySQL: " . mysql_error());
$db=mysql_select_db(DB_NAME,$con) or die("Failed to connect to MySQL: " . mysql_error());
/* $ID = $_POST['user']; $Password = $_POST['pass']; */

function SignIn() {
        session_start(); //starting the session for user profile page
        if(!empty($_POST['user'])) //checking the 'user' name which is from Sign-In.html, is it empty or have some text
        {
         $query = mysql_query("SELECT * FROM UserName where userName = '$_POST[user]' AND pass = '$_POST[pass]'")
or die(mysql_error());
         $row = mysql_fetch_array($query) or die(mysql_error());

                if(!empty($row['userName']) AND !empty($row['pass']))
                {
                $_SESSION['userName'] = $row['pass'];
                        echo "SUCCESSFULLY LOGIN TO USER PROFILE PAGE...";
                } else {
                echo "SORRY... YOU ENTERD WRONG ID AND PASSWORD... PLEASE RETRY...";
                 }
        }
 }

if(isset($_POST['submit']))
{
 SignIn();
} ?>
```

OWASP
The Open Web Application Security Project

Game Over....

OWASP
The Open Web Application Security Project

- Did you have VoIP Phone ?
- Did you have IP Router / Broadband box ?
- Did you have smartphone ?
- Did you have customers / partners over Internet ?

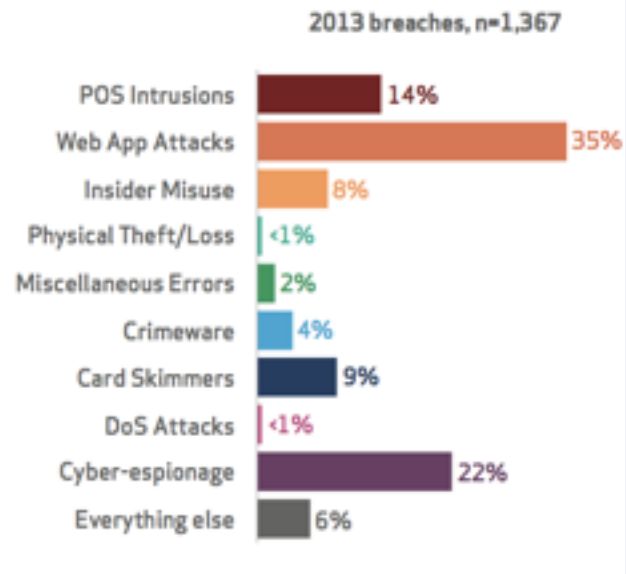
Anything else ?

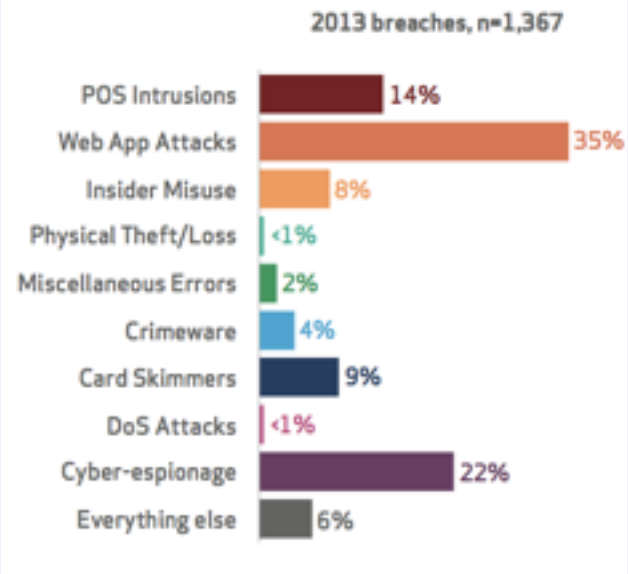
Why Application Security ?

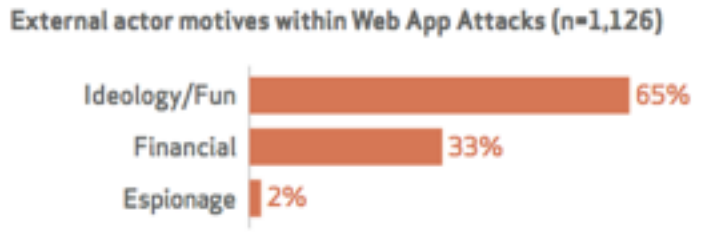
OWASP
The Open Web Application Security Project

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, ...)*

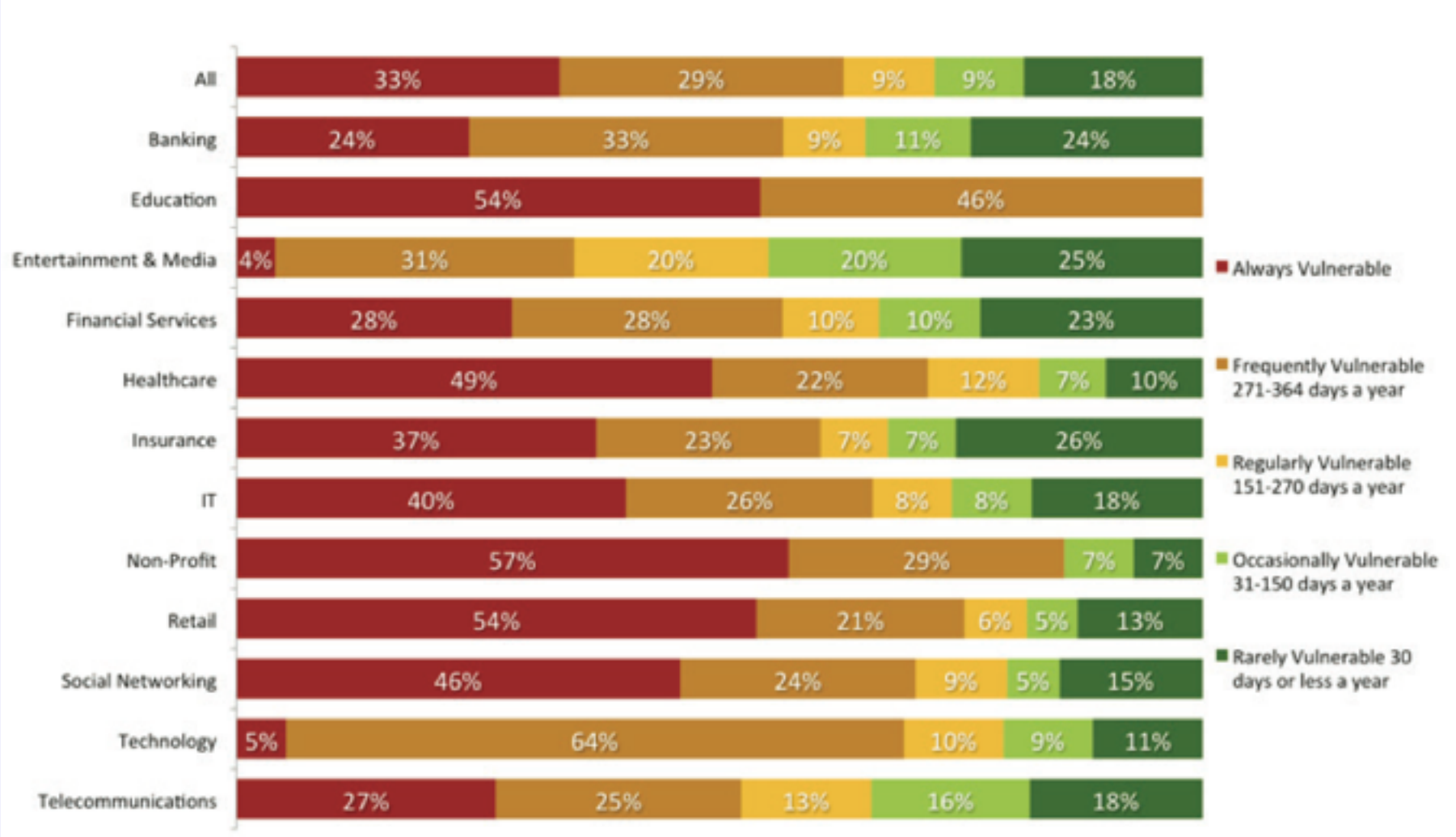






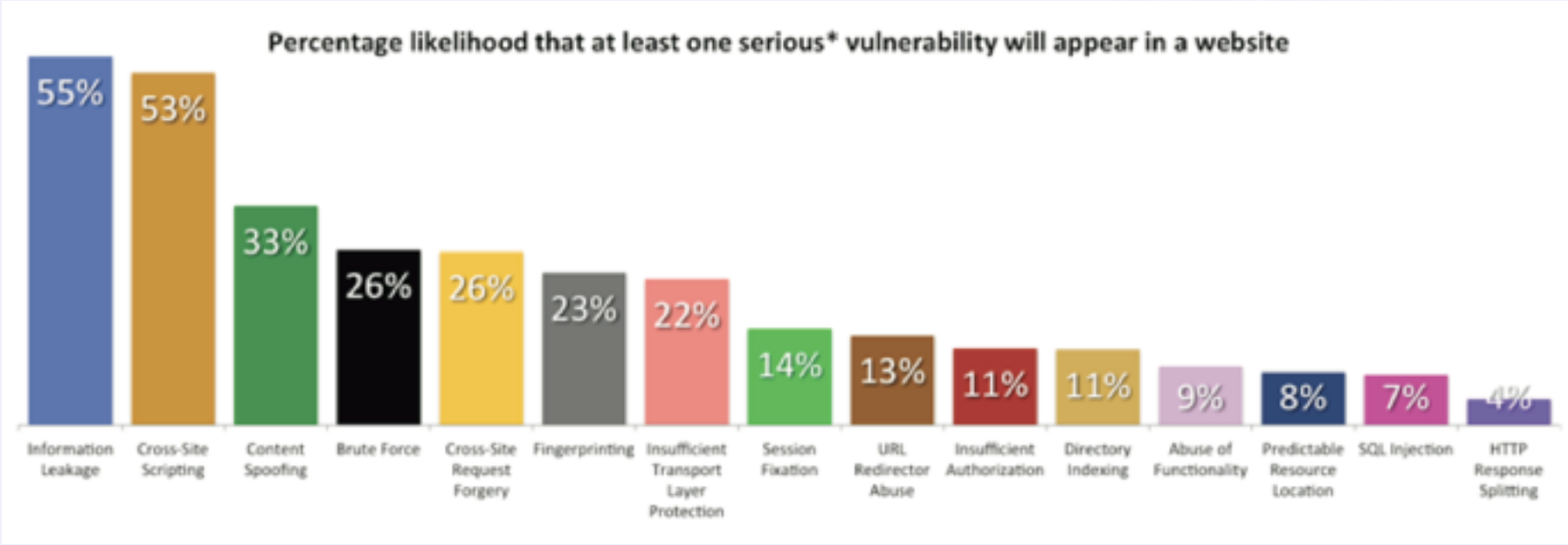
Who win ?

OWASP
The Open Web Application Security Project



Vulnerabilities ?

OWASP
The Open Web Application Security Project



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

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

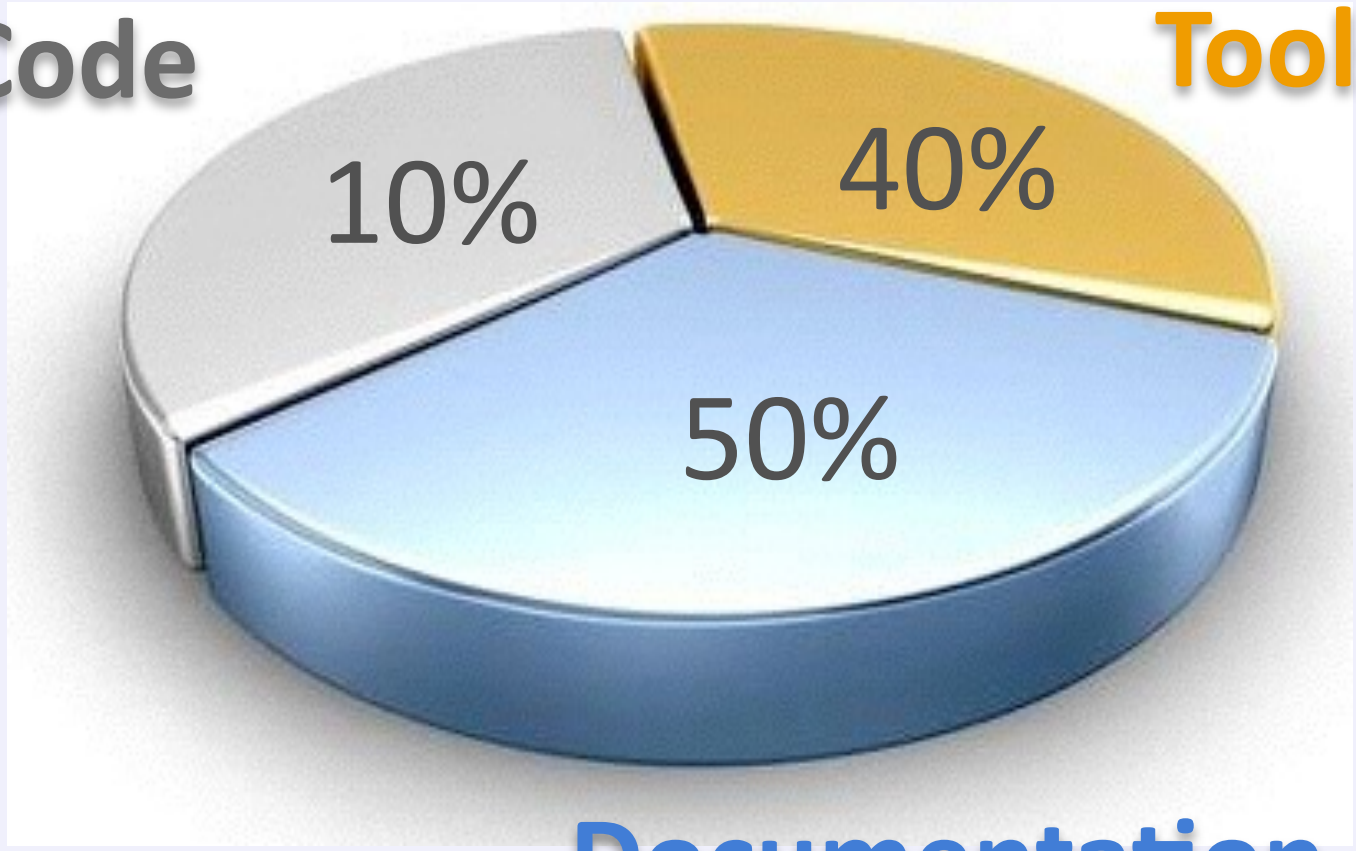
Quality Resources

200+ Projects

15,000+ downloads of tools, documentation

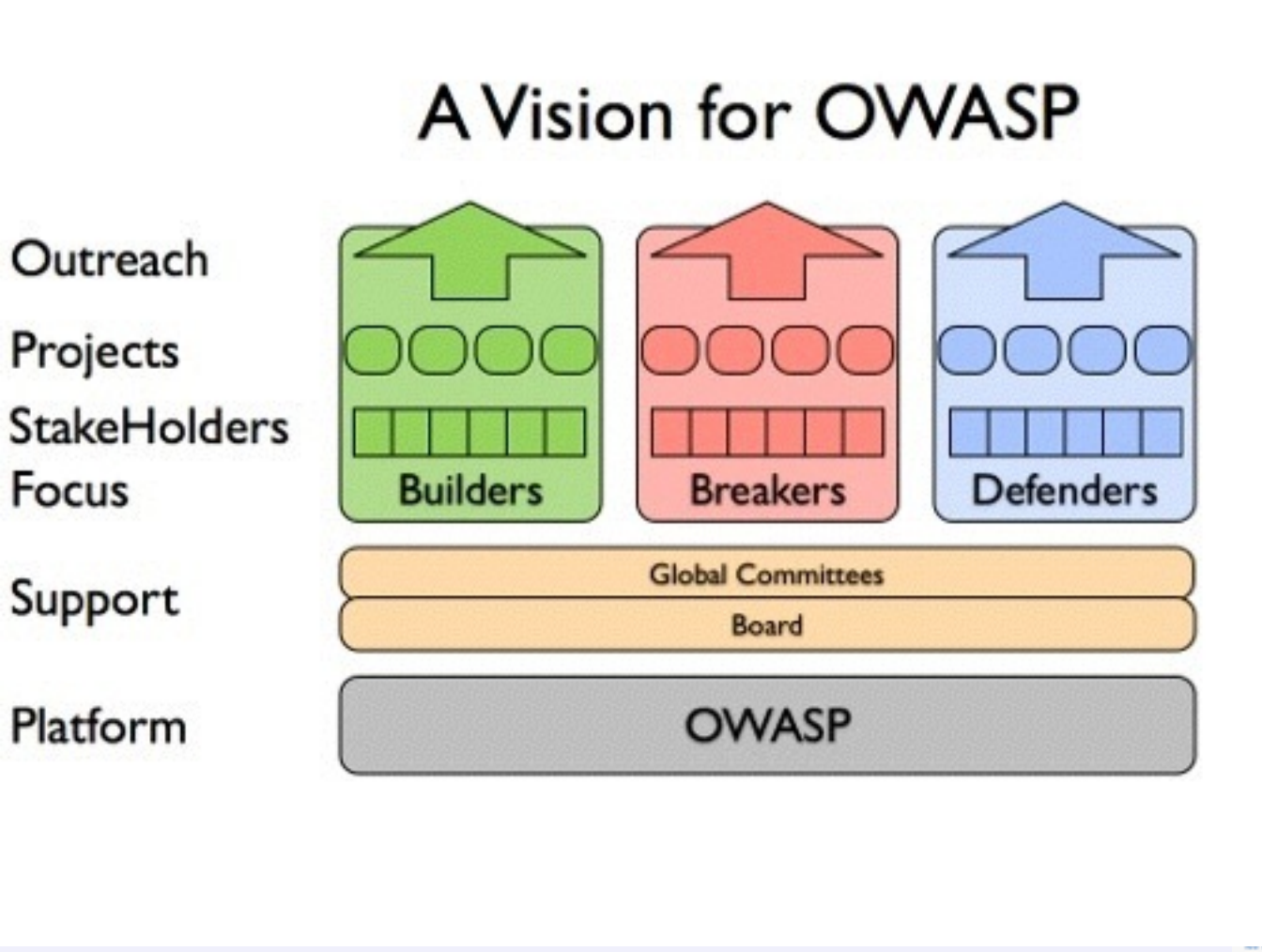
Quality Resources

OWASP
The Open Web Application Security Project



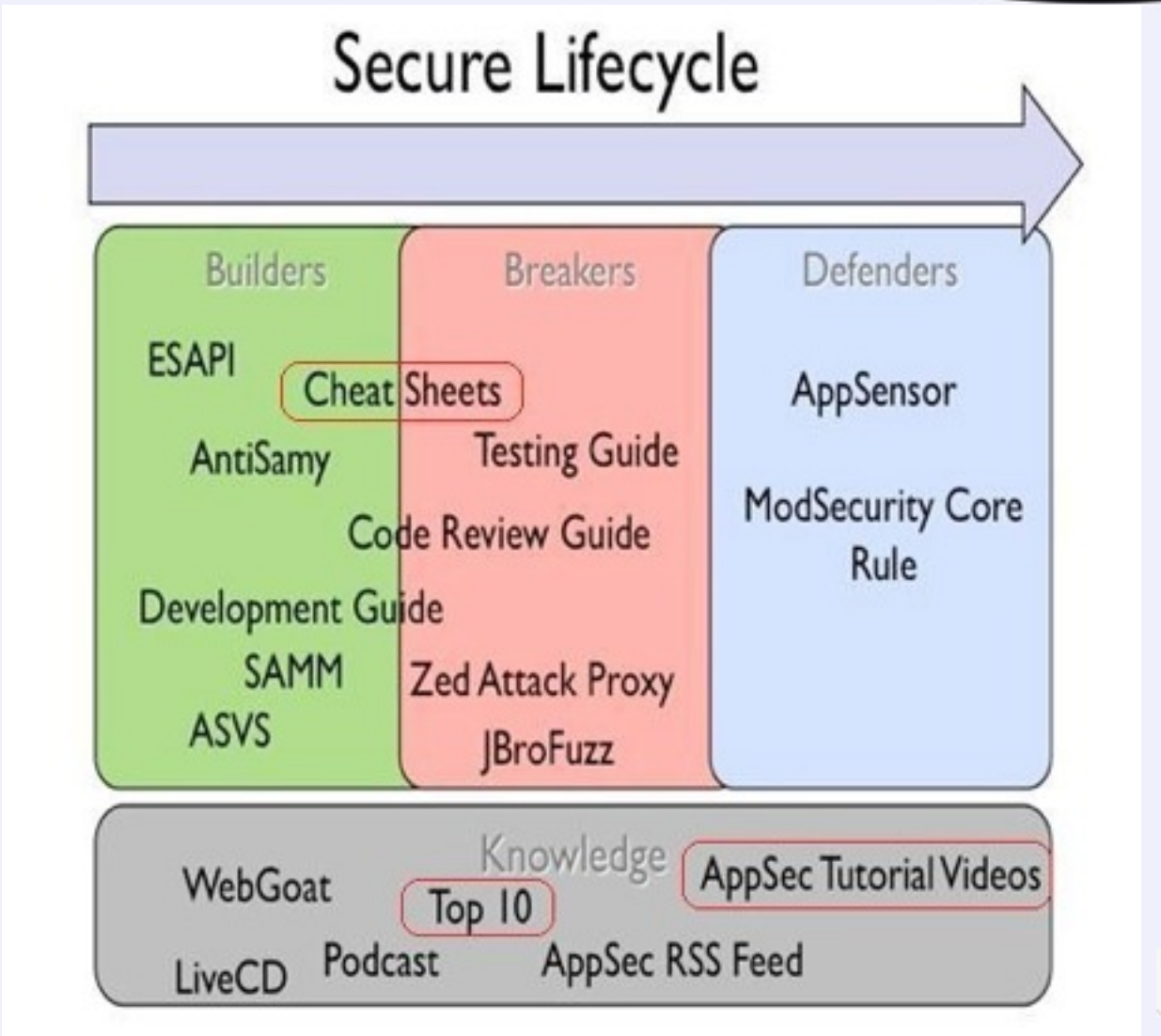
Security Lifecycle

OWASP
The Open Web Application Security Project



Security Resources

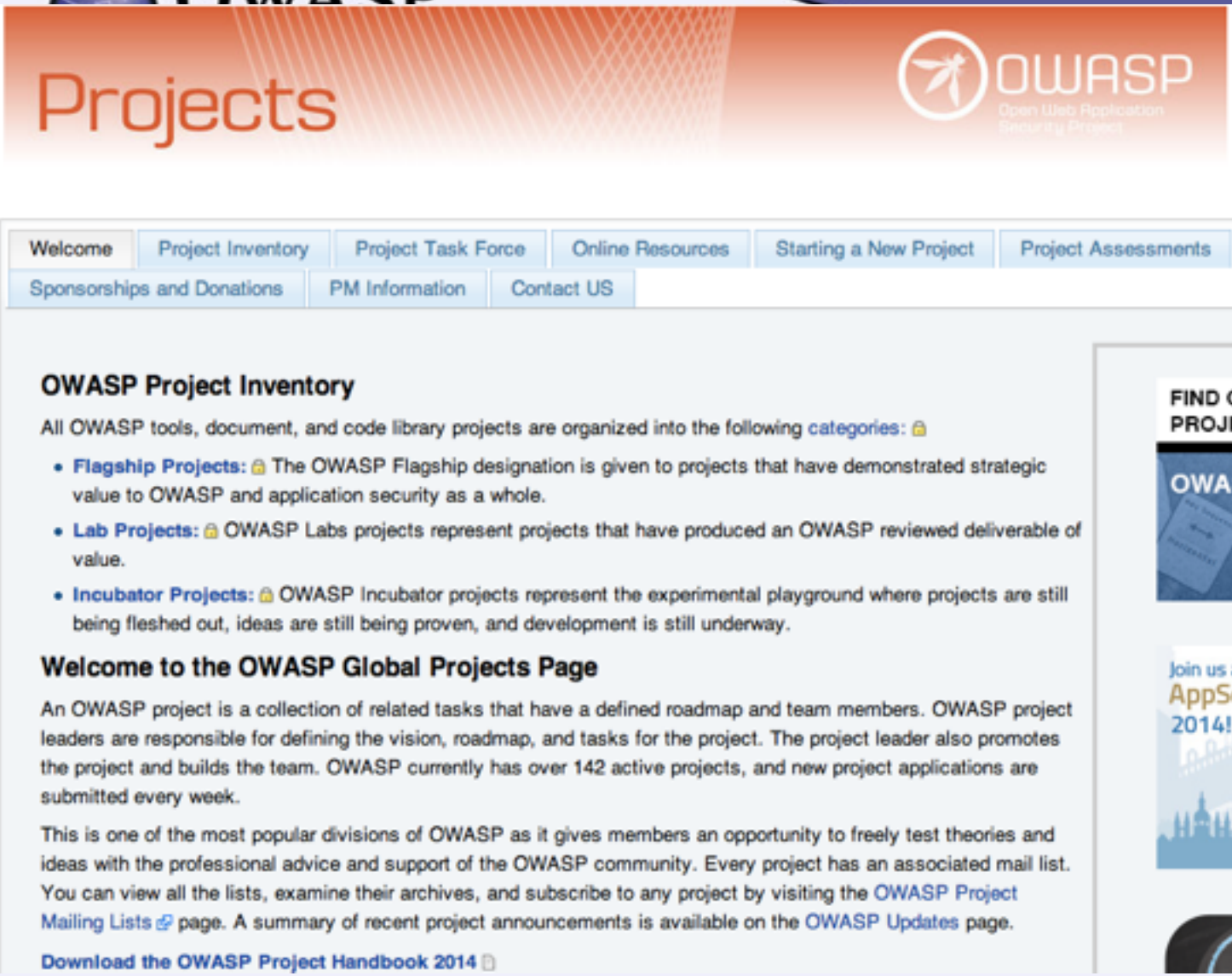
OWASP
The Open Web Application Security Project



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



OWASP Top10 2013

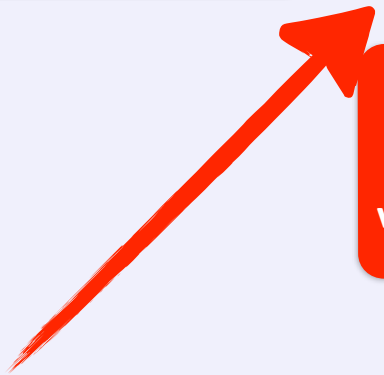
OWASP
The Open Web Application Security Project

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	

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)

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

PHP Version : https://code.google.com/p/owasp-esapi-php/

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

OWASP PHP Security Project

OWASP
The Open Web Application Security Project

Project Leader: Abbas Naderi,
Abbas.Naderi@owasp.org

Purpose: OWASP PHP Security Project is an effort by a group of PHP developers in securing PHP web applications, using a **collection of decoupled flexible secure PHP libraries, as well as a collection of PHP tools.**

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

Libraries Offered

- Basic Password Library
- Advance Password Library
- User Library and Management
- Crypto Library
- Password Library
- Database Library
- Download Manager Library
- HTTP Library
- Tainted Library
- Logs Library
- Session Library
- Core Library
- Scanner Tool

Tools Offered

- XSS Resolver
- SQL Injection Detector
- Taint Tracker

Damages Mitigated

- Brute Force Attacks
- Cross-site Scripting(XSS) Attacks
- SQL Injection Attacks
- Session Fixation, Session Hijacking, Session Guessing
- Encrypting sensitive information in configuration files
- Replacement of native PHP's faulty functions
- A secure PRNG (Pseudorandom number generator)
- Secure implementation of "remember-me" and "temporary password" features
- Capability to mark/disallow suspicious

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

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

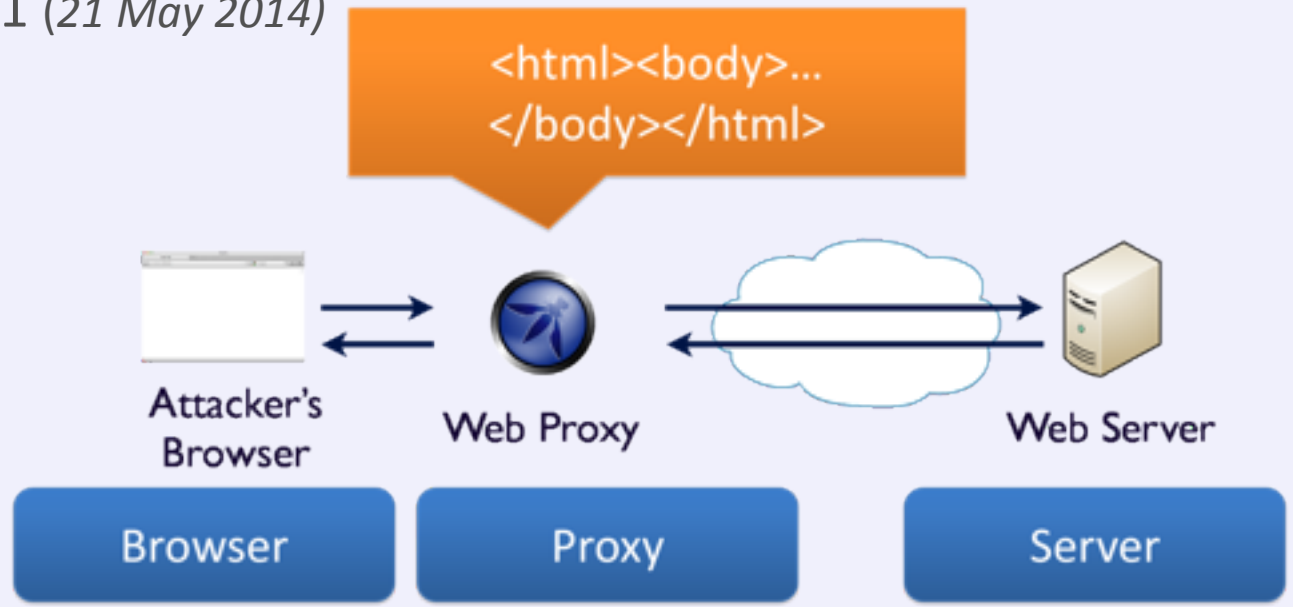
Zed Attack Proxy

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 2.3.1 (*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

- RSSIA Bordeaux : 20 Juin
  - HeartBleed revisited
- AppSec Europe 2014 - Cambridge :

- Java User Groupe Lille & Paris
  - Secure Coding for Java a la rentrée 2014
- 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