



Chapter Meeting OWASP France

Paris, 7 Feb 2013



OWASP

The Open Web Application Security Project

gemalto[★]
security to be free

Agenda



- Update - Projets OWASP
- Evolution du Cadre Légal
 - Developers, Software makers held liable for code?
- Données personnelles & WebApp Sec
 - Projet de Règlement Européen
- OWASP France Day
- Traduction OWASP Top Ten 2013
- Adhésions OWASP





Looking Forward... and Beyond

Distinctiveness Through Security Excellence

Chapter Meeting OWASP France
Paris, 7th Feb, 2013



OWASP

The Open Web Application Security Project

Ludovic Petit

Ludovic.Petit@owasp.org

Chapter Leader OWASP France
Global Connections Committee

About Me



OWASP

The Open Web Application Security Project

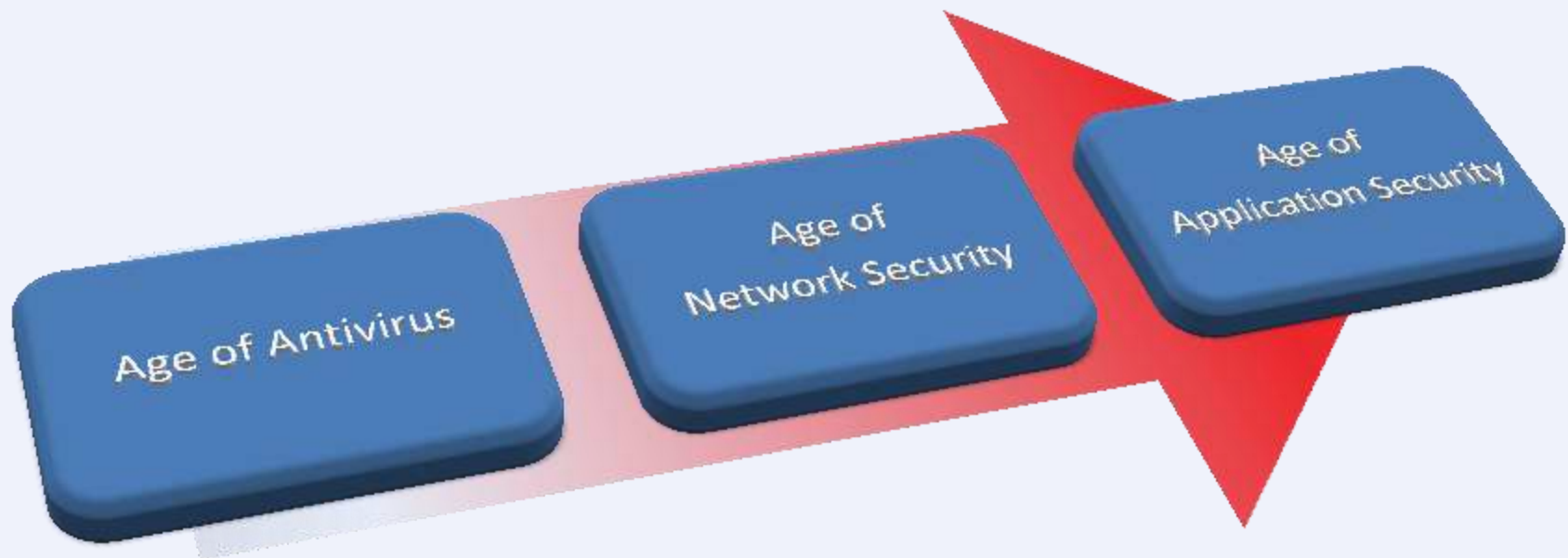
- Group Fraud & Information Security Advisor at , 2nd largest French Telecom Operator with subsidiaries in Brazil and Morocco
 - Working on Anti Fraud, Cybercrime, Technical Threat Intelligence, Law Enforcement and Security Futurology
 - 20 years' experience in Security Management within the Telecommunications industry, following 10 years in Information Technology
- Chapter Leader & Founder OWASP France
- Global Connections Committee Member
- 10 years in Application Security, OWASPer since 2003
- Contributor to various OWASP Projects
 - Translator of the OWASP Top Ten in French (*All versions*)
 - Application Security Guide For CISOs (*Marco Morana*)
 - OWASP Mobile Security Project (*Jack Mannino*)
 - OWASP Cloud Top10 Project (*Vinay Bensal*)
 - OWASP Secure Coding Practices - Quick Reference Guide (*Keith Turpin*)



Why this presentation



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



- ❖ Most websites vulnerable to attacks
- ❖ 75% of Attacks at the Application Layer *(Source: Gartner)*
- ❖ Important % of web-based Business *(Services, Online Store, Self-care)*

But also because...



The legal framework rules the technical means required to be compliant!



Agenda



- What is OWASP, what we could bring

- OWASP Projects

- Talking Legal

- Evolutions of the legal framework
- Developers, Software makers held liable for code?



The True Story



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



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



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

Outreach

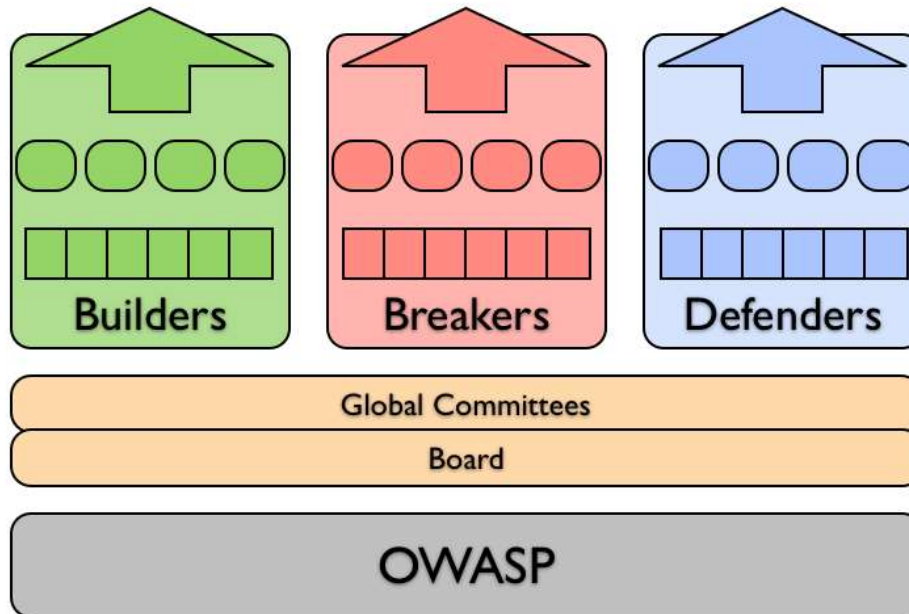
Projects

StakeHolders

Focus

Support

Platform



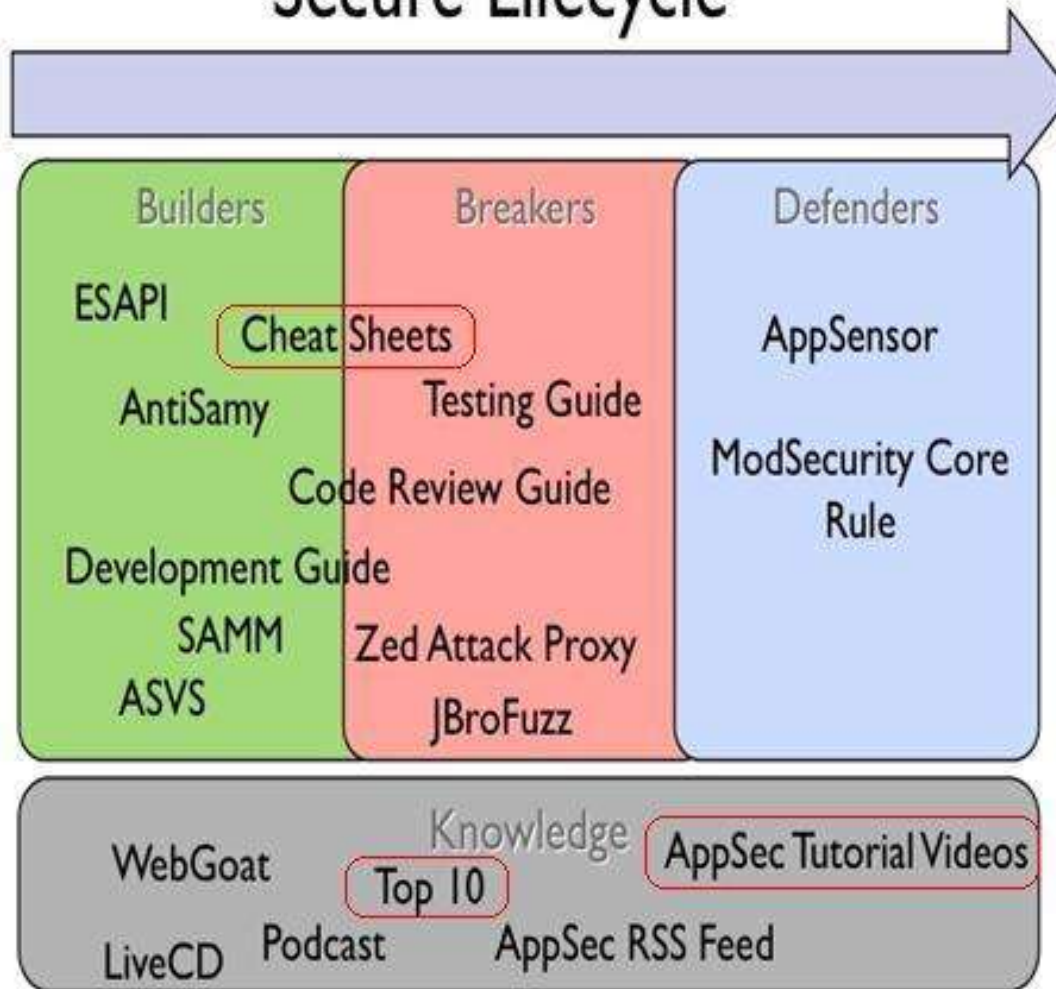
Security Resources



OWASP

The Open Web Application Security Project

Secure Lifecycle



The OWASP Top Ten

TOP 10 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](#))



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



7 Global Committees



OWASP

The Open Web Application Security Project

OWASP GLOBAL COMMITTEES

OWASP GLOBAL COMMITTEE	Projects	Membership	Education	Conferences	Industry	Chapters	Connections
Committee Chair	Jason Li	Helen Gao	Martin Knobloch	Mark Bristow	Rex Booth	Josh Sokol	Jim Manico
Members	<ul style="list-style-type: none"> • Brad Causey • Chris Schmidt • Justin Searle • Larry Casey • Keith Turpin 	<ul style="list-style-type: none"> • Dan Cornell • Ofer Maor • Aryavalli Gandhi 	<ul style="list-style-type: none"> • Eduardo Neves • Cecil Su • Fabio Cerullo • Kuai Hinjosa • Sebastien Gioria • Tony Gottlieb • Carlos Serrão • Luiz Otavio Duarte 	<ul style="list-style-type: none"> • Lucas Ferreira • John Wilander • Richard Greenberg • Ralph Durkee • Mohd Fazli Azran • Lorna Alamri • Benny Ketelslegers 	<ul style="list-style-type: none"> • Mauro Flores • Alexander Fry • Eoin Keary • Mateo Martinez • Colin Watson • Marco Morana 🗝 • Christian Papathanasiou • Tobias Gondrom 	<ul style="list-style-type: none"> • Seba Deleersnyder • Tin Zaw • L. Gustavo C. Barbato • Ivy Zhang 	<ul style="list-style-type: none"> • Ludovic Petit • Luiz Eduardo Dos Santos • Justin Clarke • Jerry Hoff
Applicants				<ul style="list-style-type: none"> • Zhendong Yu 	<ul style="list-style-type: none"> • Michael Scovetta 		
Committee Looking For	New Members with OWASP Project Leadership Experience	More Members	New Members with Education Background	More Members Outside U.S.	More Members Outside U.S. and Europe	More Members Outside U.S.	More Members

All over the world



OWASP

The Open Web Application Security Project



OWASP Projects



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



for Reboot

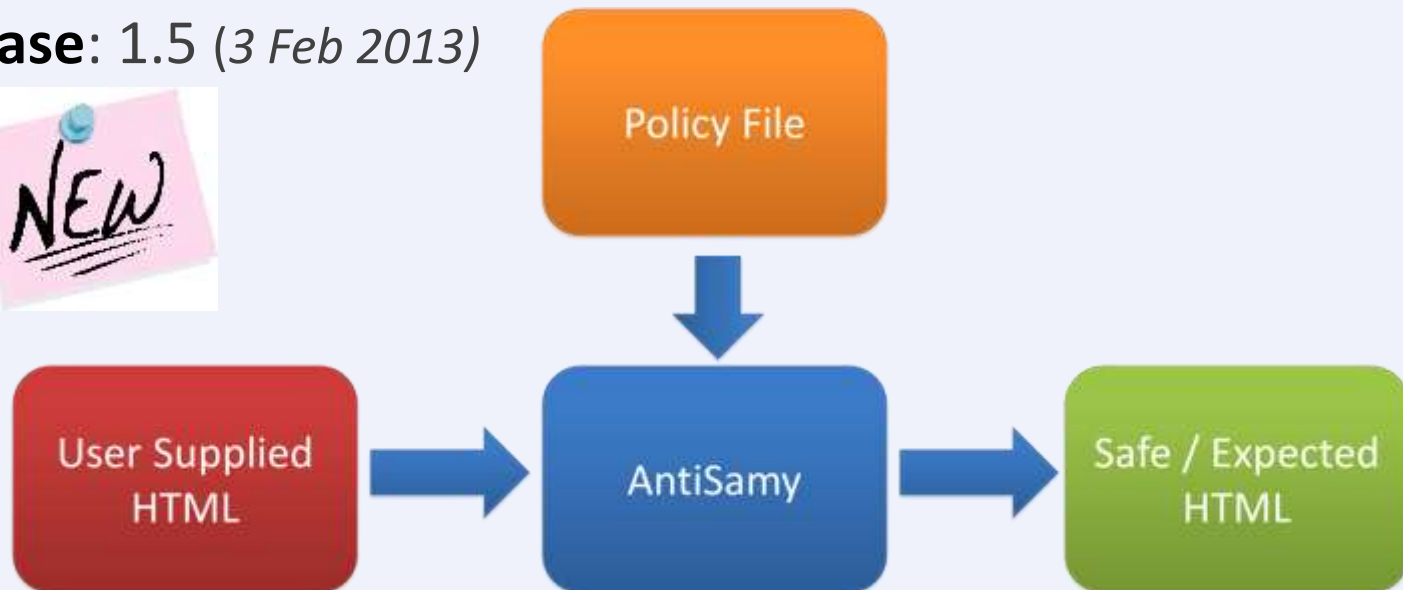
AntiSamy



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)



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



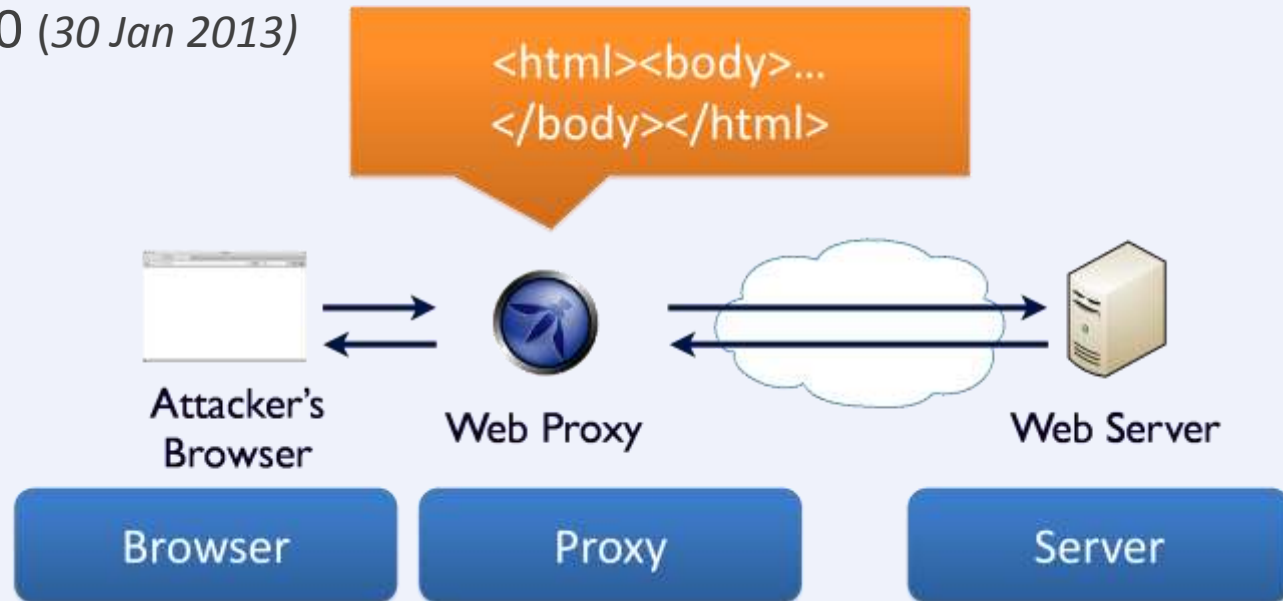
Project Leader: Simon Bennetts (aka Psiinon), psiinon@gmail.com

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



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



Cloud Top10 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

Cloud Top10 Security Risks



OWASP

The Open Web Application Security Project

- **R1.** Accountability & Data Risk
- **R2.** User Identity Federation
- **R3.** Legal & Regulatory Compliance
- **R4.** Business Continuity & Resiliency
- **R5.** User Privacy & Secondary Usage of Data
- **R6.** Service & Data Integration
- **R7.** Multi-tenancy & Physical Security
- **R8.** Incidence Analysis & Forensics
- **R9.** Infrastructure Security
- **R10.** Non-production Environment Exposure

Mobile 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



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

Top 10 Mobile Risks



OWASP

The Open Web Application Security Project

- **M1.** Insecure Data Storage
- **M2.** Weak Server Side Controls
- **M3.** Insufficient Transport Layer Protection
- **M4.** Client Side Injection
- **M5.** Poor Authorization and Authentication
- **M6.** Improper Session Handling
- **M7.** Security Decisions via Untrusted Inputs
- **M8.** Side Channel Data Leakage
- **M9.** Broken Cryptography
- **M10.** Sensitive Information Disclosure

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***

Agenda



- What is OWASP, what we could bring
- Update - OWASP Projects
- Talking Legal
 - Evolution of Legal framework
 - Developers, Software makers held liable for code?



Remember this?



OWASP

The Open Web Application Security Project

**THE
USUAL SUSPECTS**





In case of security breach, **what's going on from a Legal perspective?**

- ❖ Who *could be* accountable for what?
- ❖ Who *should be* accountable for what?
- ❖ Who *would be* accountable for what?



In fact, **who is accountable for what?**...

Do you...Legal? 2/2

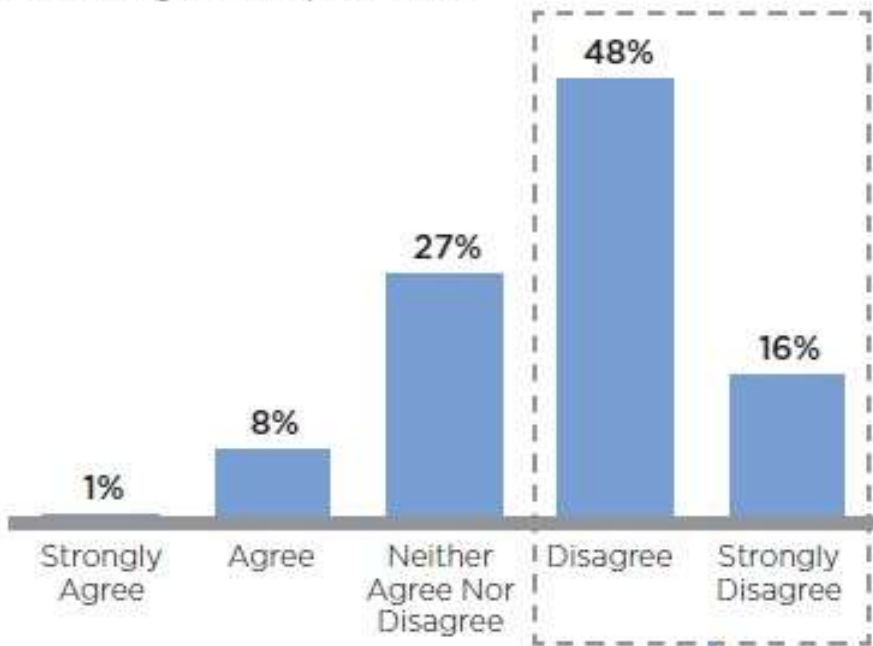


OWASP

The Open Web Application Security Project

Agreement That “Business Clients Consider Legal, Regulatory, and Records-Related Risks When Starting a New Information-Related Project”

Percentage of Respondents



n = 130.

More than 60% of respondents believe the business does not consider legal risks when starting an information- or technology-related project.

Although Legal and Information Security need to work better together, **they aren't**, and this is damaging companies' ability to manage risk.



Over 60% of General Counsel are **dissatisfied** with the way information risks are being addressed and with their involvement in information risk management.

Source: The Information Risk Executive Council (IREC)



Three criteria of sensitivity of the information commonly accepted

- **Confidentiality:** Confidentiality refers to limiting information access and disclosure to authorized users and preventing access by or disclosure to unauthorized ones.
- **Integrity:** Integrity refers to the trustworthiness of information resources.
- **Availability:** Availability refers, unsurprisingly, to the availability of information resources.

A fourth is also often used (*under different names*)

- **Traceability, Imputability, or Proof, i.e. Non-repudiation**

Stakes of Security: Status



- The **legal risk is a consequence** of operational risk
- The business risk is in fact induced by the informational risk
- Information Systems Security aims four main objectives:
 - Availability
 - Data Integrity
 - Confidentiality
 - Non-repudiation

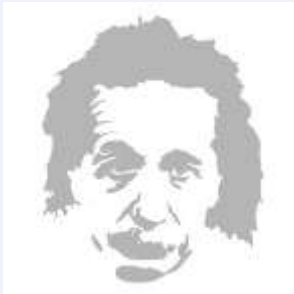
The risk assessment of information systems can make it possible to reduce both business and legal risks

A Difficult Equation



OWASP

The Open Web Application Security Project



OBLIGATIONS OF
THE ENTERPRISE

CUSTOMER
REQUIREMENTS

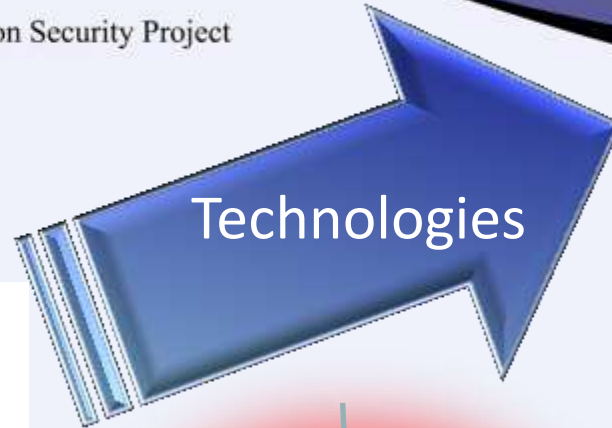
LEGAL AND REGULATION
REQUIREMENTS

Point
of Balance

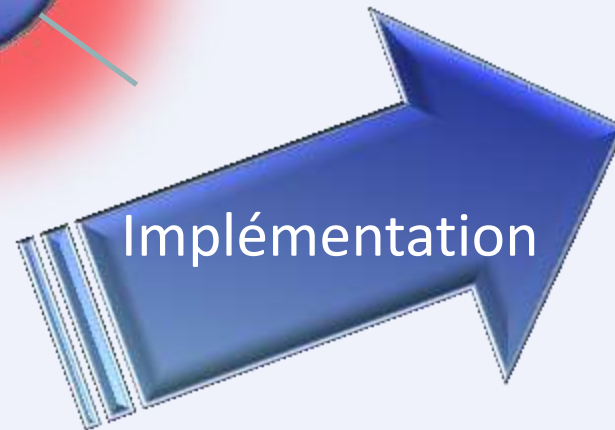
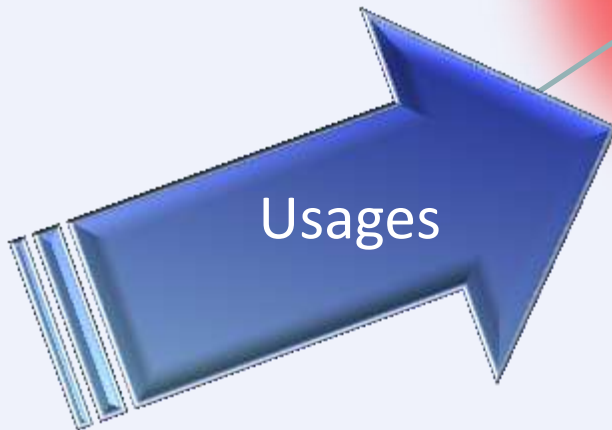
**Where is the 'Border' between
Customer Satisfaction and
Interaction with the
Authorities?**

What's at Stake?

... also for Software Makers



Anticipate Security stakes and assist businesses in their efforts to maintain a balance.

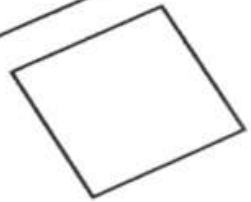




AUDIT CHECKLIST



Audit Satisfactory



**Nonconformances Found
Observations Made**

The OWASP Secure Software Contract Annex



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



OWASP

The Open Web Application Security Project

Legal Update





States of California, USA Data Breach



California was the first state in USA to enact such a law.

California Senate Bill No. 1386 became effective on 1st July 2003, amending Civil Codes 1798.29, 1798.82 and 1798.84. It is a serious bill, with far reaching implications.

Essentially, it *requires an agency, person or business that conducts business in California and owns or licenses computerized 'personal information' to disclose any breach of security (to any resident whose unencrypted data is believed to have been disclosed)*

-  The statute imposes **specific notification requirements** on companies in such circumstances.
-  The statute applies regardless of whether the computerized consumer records are maintained *in or outside* California.

European Directive 2009/136/EC




OWASP

The Open Web Application Security Project

DIRECTIVE 2009/136/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL


of 25 November 2009

amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws.

 Article 2 (2) (4) (c) adds a **requirement to notify Security breaches to “National Authority” and to those affected by this vulnerability**, at least if the flaw is “likely to affect negatively” their personal data

European Convention on Cyber Crime



 Came into force in Jul 2004

The Council of Europe adopted a Convention on Cyber Crime that identified and defined internet crimes:


- **Offenses against** the **Confidentiality**, **Integrity** and **Availability** of computers, data and systems (illegal access, illegal interception, data interference, system interference, misuse of devices)
- Computer-related Offenses (computer-related forgery, computer-related Fraud)
- Content-related Offenses (offenses related to child pornography)
- Offenses related to infringements of copyright and related rights

Executive Management Responsibility



All organisations need to be aware of the Convention's provisions in Article 12, Paragraph 2:

'Ensure that a legal person can be held liable where the lack of supervision or control by a natural person... has made possible the commission of a criminal offenses, established in accordance with this Convention'

 In other words, **Directors can be responsible for offenses committed** by their organisation simply because they failed to adequately exercise their *duty of care*.

European Convention on Cyber Crime



OWASP

The Open Web Application Security Project

The **Organization of American States** (OAS) and the **Asia-Pacific Economic Cooperation** (APEC) have both committed themselves to applying the European Convention on Cyber Crime.

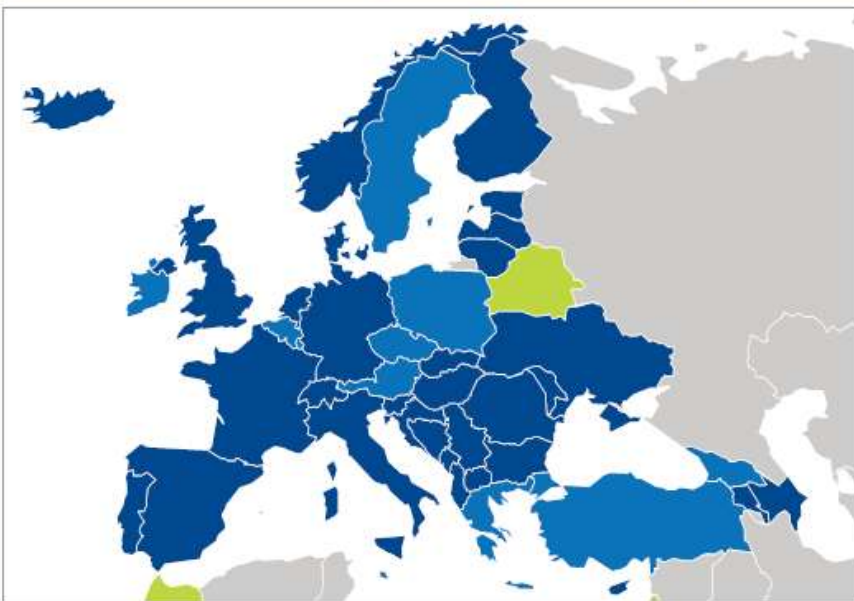
70+ countries have enacted.

http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/default_en.asp

<http://www.oas.org/en/default.asp>

<http://www.apec.org/>

Global reach of the Budapest Convention on Cybercrime



State Parties to the Convention

Signatories and States invited to accede

Cooperation also with



Source: Council of Europe
10th November 2011
www.coe.int/cybercrime

Council of Europe member states

- Albania
- Armenia
- Azerbaijan
- Bosnia and Herzegovina
- Bulgaria
- Croatia
- Cyprus
- Denmark
- Estonia
- Finland
- France
- Germany
- Hungary
- Iceland
- Italy
- Latvia
- Lithuania
- Moldova
- Montenegro
- Netherlands
- Norway
- Portugal
- Romania
- Serbia
- Slovak Republic
- Slovenia
- Spain
- «the former Yugoslav Republic of Macedonia »
- Switzerland
- Ukraine
- United Kingdom

Signatories

- Austria
- Belgium
- Canada*
- Czech Republic
- Georgia
- Greece
- Ireland
- Liechtenstein
- Luxembourg
- Japan*
- Malta
- Poland
- South Africa
- Sweden
- Turkey

States invited to accede

- Argentina
- Australia
- Chile
- Costa Rica
- Dominican Republic
- Mexico*
- Philippines
- Senegal



- Antigua and Barbuda
- Bahrain
- Bangladesh
- Belarus
- Benin
- Bolivia
- Botswana
- Brazil
- Brunei Darussalam
- Cambodia
- Cameroon
- Colombia
- Congo, Republic of
- Cook Islands
- Cote d'Ivoire
- Dominica
- Ecuador
- Egypt
- El Salvador
- Fiji
- Gabon
- Ghana
- Grenada
- Guatemala
- Haiti
- Honduras
- India
- Indonesia
- Jamaica
- Korea, Republic of
- Laos
- Lebanon
- Malaysia
- Maldives
- Marshall Islands
- Mauritius
- Micronesia
- Morocco
- Nauru
- Nicaragua
- Niger
- Nigeria
- Pakistan
- Palau
- Panama
- Papua New Guinea
- Paraguay
- Peru
- Samoa
- Singapore
- Solomon Islands
- Sri Lanka
- St Kitts and Nevis
- St Vincent and the Grenadines
- Tanzania
- Thailand
- Tonga
- Togo
- Trinidad and Tobago
- Tuvalu
- Uruguay
- Vanuatu
- Vietnam

Non Council of Europe member states

- United States*

* observer countries

What about France? 1/2



- **Reporting** of violations of personal data to the CNIL
- **New obligation to notify** security breaches or the integrity of Networks and Services
- **Consequences** in case of non-compliance with legal obligations

The Commission Nationale de l'Informatique et des Libertés (CNIL) is responsible for ensuring that information technology remains at the service of citizens, and does not jeopardize human identity or breach human rights, privacy or individual or public liberties.

<http://www.cnil.fr/english/the-cnil/>



Article 38 de l'ordonnance du 24 août 2011 (aka 'Telecom Packet): l'obligation d'une notification des failles de sécurité

«En cas de violation de données à caractère personnel, le fournisseur de services de communications électroniques accessibles au public avertit, sans délai, la Commission nationale de l'informatique et des libertés. Lorsque cette violation peut porter atteinte aux données à caractère personnel ou à la vie privée d'un abonné ou d'une autre personne physique, le fournisseur avertit également, sans délai, l'intéressé. »

Penalties in case of breach of the duty to report under the jurisdiction of the CNIL

- 150 K€, 300 K€ for repeat offenses

Brand Impact!



Possibility of publication of the CNIL's decision




According the French Penal Code

- **Fraudulent access** and **maintaining** in an Information System (*Art. 323-1 C. Pénal*)
- **Obstacle** to the functioning of an information system (*Art. 323-2 C. Pénal*)
- **Fraudulent introduction** of data into an information system (*Art. 323-3 C. Pénal*)



Legal risks in connection with the fraudulent use of Information Systems:

 **Reminder:** Any Commercial Web Application Service is part of an Information System

Why: Because we are talking about **Information Security**, which means... **Legal Compliance!**



The Responsible of the Data Processing is required to take any useful precautions, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données et, notamment empêcher qu'elles soient déformées, endommagées ou que des tiers non autorisés y aient accès. (Article 34 de la Loi 78-17 du 6 janvier 1978 modifiée - CNIL)

Article 226-17 du Code Pénal : *Le fait de procéder ou de faire procéder à un traitement de données à caractère personnel sans mettre en œuvre les mesures prescrites à l'article 34 de la loi n° 78-17 du 6 janvier 1978 précitée est puni de cinq ans d'emprisonnement et de 300 000 Euros d'amende.*

What is this obligations?



Take any useful precautions

- In regard of the nature of Data
- And the risks presented by the Processing
- To preserve data security and, in particular, prevent that they are
 - Modified
 - Tampered
 - or that unauthorized third parties have access

Privacy Security within the Enterprise



- 👉 The **CEO** is **criminally responsible** of the Data Processing
 - France: Obligations under the law of 6 Jan 1978 (modified in 2004)

- 👉 **Criminal Risk in case of Delegation of Authority**
... for each person part of the Chain!

What about the subcontracting?

- ✓ **Enterprise**: Data owner = **Accountable**
- ✓ **Subcontractor**: Data processor = **Accountable**

Proposed European Regulation on the protection of personal data



Will to harmonization of the regulations at EU level by the use of a Regulation, for greater harmonization of rules between actors and countries:

- Same framework for all players regardless of their location:
 - The proposed regulation provides that EU rules apply to any provider that handles data from a EU user
- Same framework throughout Europe:
 - The choice of a Regulation, not a Directive, reduces the risk of differences in interpretation between Member States (national transposition not required).
- Same framework, whatever the activity of the controller

New obligations for the persons in charge of the treatment



OWASP

The Open Web Application Security Project

- **Privacy by design**, impact analysis and documentation:
 - Principles of “*privacy by design*” and “*accountability*”: new internal governance rules for companies to integrate the protection of personal data in the design of the product / service.
- **Reporting** of violations of personal data



Art. 79 - Penalties:

- A 2% annual turnover fine
 - ✓ Administrative penalties may be up to 2% of total revenues
- 1 000 000 Euros

*A 2% annual turnover fine would have meant
1.2 Billion dollars in 2008 for a company like Microsoft!*

Issues for the Enterprise & Consequences



All these acts can have serious consequences for the Company

- **Financial** Consequences
- Consequences on the **Reputation**
- **Brand** impact
- **Criminal** Consequences for the Executives
- Proceedings to the civil courts: **Claims for damages by customers**

Criminal Consequences (France)



- 👉 Article 226-17 of the Penal Code *also* charges the disclosure of information... to the spied!
- The **Enterprise** (i.e. **the Spied**) is **responsible of consequences** caused to third parties
- The **people 'accountable'** (*IT, Security, or the CTO, even the CEO*) **can be personally involved**
 - ✓ Law 'Godfrain' - Penalty: **2 months to 5 years / 300 € to 300 K€**
 - ✓ Protection of information / Negligence: **5 years / 300 K€**



OWASP

The Open Web Application Security Project

What about Software Makers, Developers?

Don't forget!



A Software Maker, a Developer, is recognized as a **subject-matter expert** in its field.

As such, Software Makers and Developers
have a **Duty to Advise**
... including about Web Application Security.



EC wants software makers held liable for code

After identifying gaps in EU consumer protection rules, the European Commission is proposing that software makers give guarantees about the security and efficiency of their code.

http://news.cnet.com/8301-1001_3-10237212-92.html



Should developers be sued for security holes?

Dr Richard Clayton, security researcher at the University of Cambridge, is arguing for regulations that remove the developer's right to waive any responsibility for security flaws in their software.

It's an argument that has already won support from officials across Europe, with a **House of Lords committee (UK) recommending such a measure be implemented in 2007** and European Commissioners arguing for the requirement in 2009 - however agreements to this effect have not been passed.

<http://www.publications.parliament.uk/pa/ld200607/ldselect/ldsctech/165/165i.pdf> (see page 38, Vendor liability)

<http://www.techrepublic.com/blog/european-technology/should-developers-be-sued-for-security-holes/1109>

Here is the Question



Developers, Software makers **held liable for code?**

❖ From a **global point of view** and in essence, **YES**.

❖ From a **Legal point of view**: **YES, you could**.

- Depends on the circumstances
- Depends on the Contract
- Depends on the eventual License
- Depends on the Product
- Depends on the Customer (reputation, business, large account, etc.)

So, is your Software company concerned?
(Answers below from lawyers specialized in IT)



YES, you could also be held liable in case of Security Breach in a Customer's Information System, *as well as the company concerned.*



The Knowledge is wealth,
Knowledge must flow



OWASP

The Open Web Application Security Project

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

Abraham Lincoln



Teamwork



TEAM stands for... **T**ogether **E**ach **A**chieves **M**ore

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



Ludovic Petit

Ludovic.Petit@owasp.org

+33 (0) 611 726 164