



OWASP et l'exigence PCI 6.5

PCI Global Paris

3 Février 2009

Sébastien GIORIA (sebastien.gioria@owasp.fr)
French Chapter Leader

Ludovic PETIT (ludovic.petit@owasp.fr)
French Chapter co-Leader

Copyright © 2009 - The OWASP Foundation
Permission is granted to copy, distribute and/or modify this document
under the terms of the GNU Free Documentation License.

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

Agenda

- L'OWASP
- Les outils, guides et publications de l'OWASP
- L'OWASP et l'exigence PCI 6.5

Le constat actuel

■ Le système d'information s'ouvre :

Welcome to OWASP
the free and open application security community

About · Searching · Editing · New Article · OWASP Categories

OWASP Overview

The Open Web Application Security Project (OWASP) is dedicated to finding and fighting the causes of insecure software. Everything here is free and open source. The OWASP Foundation is a 501c3 not-for-profit charitable organization that ensures the ongoing availability and support for our work. Participation in OWASP is free and open to all.

Join webappsec! The OWASP mail list... Get Started Find out more...
Contact OWASP owasp@owasp.org Become a Member Support our efforts...

Featured Story

Announcing the OWASP Sprajax Project - the first AJAX Security Scanner

OWASP thanks Denim Group for the donation of Sprajax, an open source security scanner for AJAX-enabled applications. Sprajax, a Microsoft .Net-based application is the first web security scanner developed specifically to scan AJAX web applications for security vulnerabilities.

"Denim Group is committed to furthering the field of application security," said Dan Cornell, principal of Denim Group, "and by donating Sprajax to OWASP, we intend to generate more discussion around security

OWASP Conferences

Register for OWASP AppSec Conference in Seattle Oct. 16-17-18

The Open Web Application Security Project

AppSec Seattle Conference

Join us for our 5th AppSec Conference October 16-18 in Seattle. Microsoft's Michael Howard will be giving the keynote and you'll hear presentations on topics like Web Services Security, PCI status, Securing AJAX, the Microsoft Secure Development Lifecycle, all the new OWASP projects, and much more. Check the full agenda.

OWASP is a not-for-profit, and the OWASP AppSec Conference is an incredible bargain (\$450, \$400 for OWASP members, and \$250 for students). You can attend one of 3 full-day training sessions on the 16th, and the main conference is two full days of presentations, posters, and discussion on the 17th and 18th. You can read all the details and then register online.

OWASP Community (add)

Google Trends Data for Buffer overflow

Google Trends

D E F

Oct 17-18 2007

2007

Map of the world showing OWASP community locations.

■ La sécurité



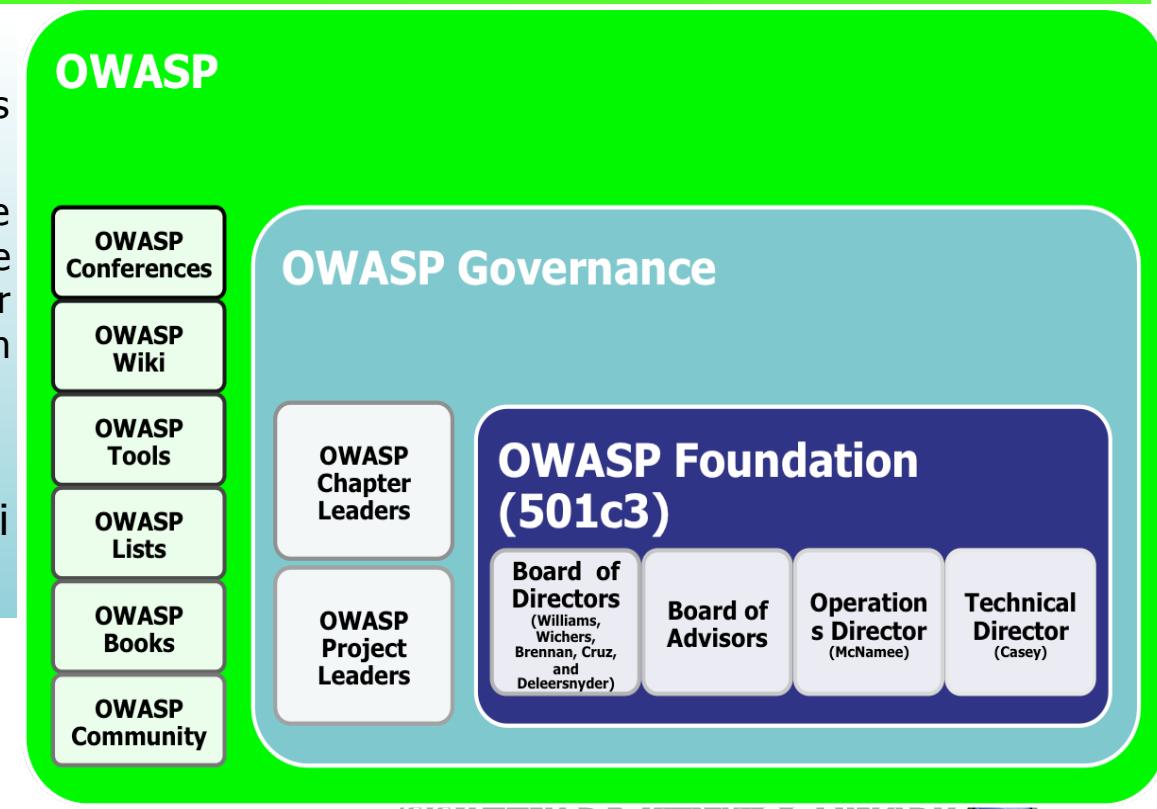
■ L'Innovation



..., l'animateur

L'OWASP (Open Web Application Security Project)

- Indépendant des fournisseurs et des gouvernements.
- Objectif principal : produire des outils, documents et standards dédiés à la sécurité des applicative.
- Tous les documents, standards, outils sont fournis sur la base du modèle open-source.
- Organisation :
 - ▶ Réunion d'experts indépendants en sécurité informatique
 - ▶ Communauté mondiale (plus de 100 chapitres) réunie en une fondation américaine pour supporter son action. L'adhésion est gratuite et ouverte à tous
 - ▶ En France : une Association.
- Le point d'entrée est le wiki
<http://www.owasp.org>



OWASP en France

Un Conseil d'Administration (Association loi 1901) :

❖ **Président**, évangéliste et relations publiques : **Sébastien Goria**

Consultant indépendant en sécurité des systèmes d'informations. Président du CLUSIR Poitou-Charentes

❖ **Vice-Président** et responsable du projet de Traduction : **Ludovic Petit**. Expert Sécurité chez SFR

❖ **Secrétaire** et Responsable des aspects Juridiques : **Estelle Aimé**. Avocate

Un Bureau :

- ❖ Le Conseil d'Administration
- ❖ **Romain Gaucher** : Ex-chercheur au NIST, consultant chez Cigital
- ❖ **Mathieu Estrade** : Développeur Apache.

Projets :

- ▶ Top 10 : traduit.
- ▶ Guide : en cours.
- ▶ Questionnaire a destination des RSSI : en cours.
- ▶ Groupe de travail de la sécurité applicative du CLUSIF.

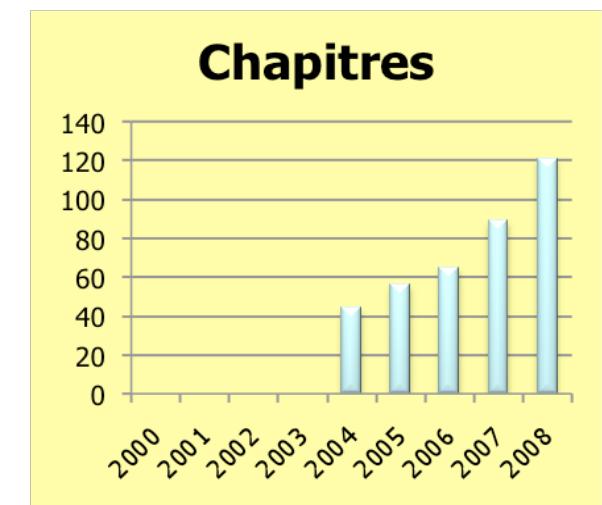
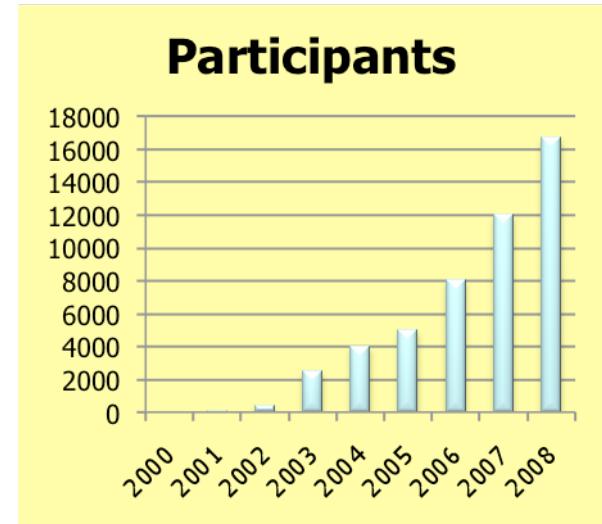
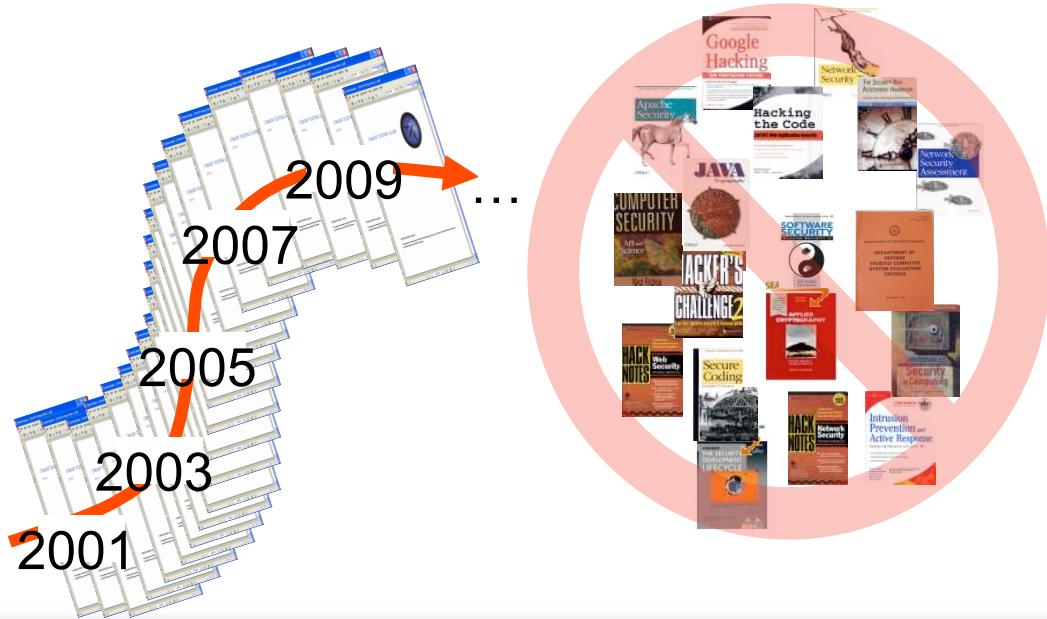
Interventions :

- ▶ Infosecurity 2007
- ▶ OSSIR
- ▶ Microsoft TechDays 2008
- ▶ Infosecurity 2008
- ▶ PCI-Global Paris 2009

Sensibilisation / Formations :

- ▶ Assurance (Java/PHP)
- ▶ Société d'EDI (JAVA)
- ▶ Opérateur Téléphonie mobile (PHP)
- ▶ Ministère de l'intérieur – SGDN
- ▶ Conférences dans des écoles
- ▶ Ministère de la santé

L'OWASP, la vie, l'univers et le reste



OWASP Conferences (2008-2009)



- Annonce et présentation du clickjacking
- Recherches sur les botnets et les malwares
- Annonce de la certification CSSLP
- Capture The Flag AppSec
- Hacking Java RMI
- Interventions du Homeland & Security
- Offshore
- Techniques de tests de vulnérabilités
- Méthodologie,
- Etc.

Conférences comparées aux BlackHat initiales :

- 2 jours de training sur les problèmes d'AppSec Avancées (WebServices, PenTesting, Defense, ...)
- 2 jours de conférences par des « black/white/gray » hackers

Agenda

- L'OWASP
- Les outils, guides et publications de l'OWASP
- L'OWASP et l'exigence PCI 6.5

Les outils de l'OWASP

- Vulnerability Scanners
- Static Analysis Tools
- Fuzzing

Automated Security Verification



- Penetration Testing Tools
- Code Review Tools

Manual Security Verification



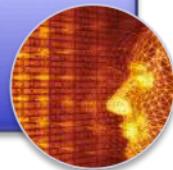
- ESAPI

Security Architecture



- AppSec Libraries
- ESAPI Reference Implementation
- Guards and Filters

Secure Coding



- Reporting Tools

AppSec Management



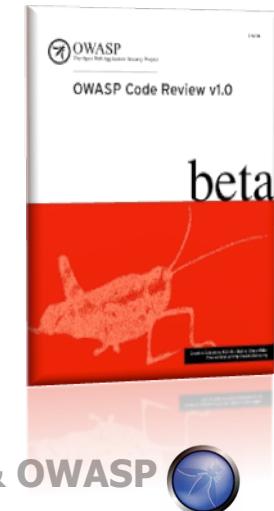
- Flawed Apps
- Learning Environments
- Live CD
- SiteGenerator

AppSec Education



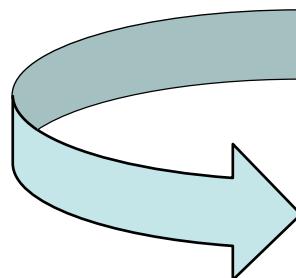
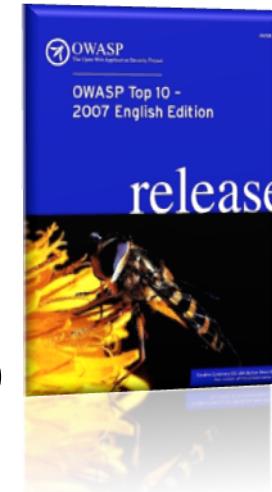
Les publications

- Toutes les publications sont disponibles sur le site de l'OWASP: <http://www.owasp.org>
- L'ensemble des documents est régi par la licence GFDL (GNU Free Documentation License)
- Les documents sont issus de différentes collaborations :
 - ▶ Projets universitaires
 - ▶ Recherche & développements des membres



Les publications majeures

- Le TOP 10 des vulnérabilités applicatives
- Le guide de conception d'applications Web sécurisées
- La FAQ de la Sécurité des Applications
- Le Guide du *PenTester*
- Le *Code Review Guide*



**En refonte complète sur 2009 pour
une meilleure intégration a
destination des différents publics**

Le Top10 2007

A1: Cross Site Scripting (XSS)

A2: Failles d'injection

A3: Execution de fichier malicieux

A4: Référence directe non sécurisée à un objet

A5: Falsification de requête inter-site (CSRF)

A6: Fuite d'information et traitement d'erreur incorrect

A7: Violation de gestion de session ou de l'authentification

A8: Stockage cryptographique non sécurisé

A9: Communications non sécurisées

A10: Manque de restriction d'accès à une URL



OWASP

The Open Web Application Security Project
<http://www.owasp.org>

www.owasp.org/index.php?title=Top_10_2007

probabilistic

© 2009 - S.Gioria & OWASP



12

Agenda

- L'OWASP
- Les outils, guides et publications de l'OWASP
- L'OWASP et l'exigence PCI 6.5

L'exigence PCI 6.5

Develop all web applications (internal and external, and including web administrative access to application) based on secure coding guidelines such as the Open Web Application Security Project Guide. Cover prevention of common coding vulnerabilities in software development processes, to include the following: Note: The vulnerabilities listed at 6.5.1 through 6.5.10 were current in the OWASP guide when PCI DSS v1.2 was published. However, if and when the OWASP guide is updated, the current version must be used for these requirements.

Les failles d'injection

■ 6.5.1 : Cross Site Scripting

XSS permet à des attaquants d'exécuter du script dans le navigateur de la victime afin de détourner des sessions utilisateur, défigurer des sites web, potentiellement introduire des vers, etc

■ 6.5.2 : Failles d'injections

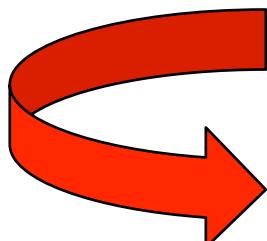
L'injection se produit quand des données écrites par l'utilisateur sont envoyées à un interpréteur en tant qu'élément faisant partie d'une commande ou d'une requête. Les données hostiles de l'attaquant dupent l'interpréteur afin de l'amener à exécuter des commandes fortuites ou changer des données

■ 6.5.3 : Execution de fichier malicieux

Un code vulnérable à l'inclusion de fichier à distance permet à des attaquants d'inclure du code et des données hostiles, ayant pour résultat des attaques dévastatrices, telles la compromission totale d'un serveur.

■ 6.5.5 : Falsification de requête inter-site (CSRF)

Une attaque CSRF force le navigateur d'une victime authentifiée à envoyer une demande pré-authentifiée à une application web vulnérable, qui force alors le navigateur de la victime d'exécuter une action hostile à l'avantage de l'attaquant.



**Confidentialité
Intégrité
Disponibilité**

La fuite d'information

■ 6.5.6 : Fuite d'information et traitement d'erreur incorrect

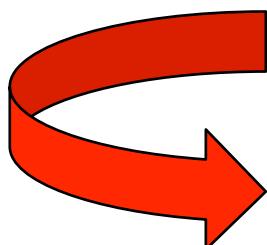
Les applications peuvent involontairement divulguer des informations sur leur configuration, fonctionnements internes, ou violer la vie privée à travers toute une variété de problèmes applicatifs. Les attaquants utilisent cette faiblesse pour subtiliser des données sensibles ou effectuer des attaques plus sérieuses.

■ 6.5.9 : Communications non sécurisées

Les applications échouent fréquemment à chiffrer le trafic de réseau quand il est nécessaire de protéger des communications sensibles.

■ 6.5.10 : Manque de restriction d'accès à une URL.

Fréquemment, une application protège seulement la fonctionnalité sensible en empêchant l'affichage des liens ou des URLs aux utilisateurs non autorisés. Les attaquants peuvent utiliser cette faiblesse pour accéder et effectuer des opérations non autorisées en accédant à ces URL directement.



**Confidentialité
Intégrité**



La mauvaise gestion de l'authentification

■ 6.5.4 :Référence directe non sécurisée à un objet

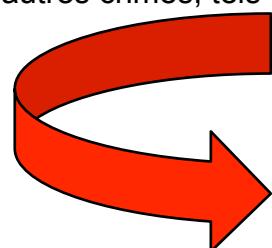
Une référence directe à un objet se produit quand un développeur expose une référence à un objet d'exécution interne, tel qu'un fichier, un dossier, un enregistrement de base de données, ou une clef, comme paramètre d'URL ou de formulaire. Les attaquants peuvent manipuler ces références pour avoir accès à d'autres objets sans autorisation.

■ 6.5.7 : Violation de la gestion de l'authentification et des sessions

Les droits d'accès aux comptes et les jetons de session sont souvent incorrectement protégés. Les attaquants compromettent les mots de passe, les clefs, ou les jetons d'authentification identités pour s'approprier les identités d'autres utilisateurs.

■ 6.5.8 :Stockage cryptographique non Sécurisé.

Les applications web utilisent rarement correctement les fonctions cryptographiques pour protéger les données et les droits d'accès. Les attaquants utilisent des données faiblement protégées pour perpétrer un vol d'identité et d'autres crimes, tels que la fraude à la carte de crédit.



**Confidentialité
Intégrité**

Des Solutions !

■ Des bibliothèques :

- Les filtres (Java/PHP) : http://www.owasp.org/index.php/Category:OWASP_Filters_Project
- OWASP CSRF Guard, http://www.owasp.org/index.php/CSRF_Guard

■ OWASP Enterprise Security API (ESAPI)

- Un framework de sécurité open-source pour les développeurs.
- Classes Java et .NET.

Couverture de l'ESAPI

OWASP Top Ten

A1. Cross Site Scripting (XSS)

A2. Injection Flaws

A3. Malicious File Execution

A4. Insecure Direct Object Reference

A5. Cross Site Request Forgery (CSRF)

A6. Leakage and Improper Error Handling

A7. Broken Authentication and Sessions

A8. Insecure Cryptographic Storage

A9. Insecure Communications

A10. Failure to Restrict URL Access

OWASP ESAPI

Validator, Encoder

Encoder

HTTPUtilities (Safe Upload)

AccessReferenceMap, AccessController

User (CSRF Token)

EnterpriseSecurityException, HTTPUtils

Authenticator, User, HTTPUtils

Encryptor

HTTPUtilities (Secure Cookie, Channel)

AccessController



Des méthodes

■ Comprehensive, Lightweight Application Security Process (**CLASP**)

- ▶ Couvre le cycle de vie logiciel dans sa globalité
- ▶ Adaptable à tout processus de développement

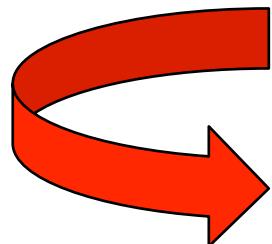
■ The Software Assurance Maturity Model (**SAMM**)

- ▶ L'ensemble des activités de sécurité est regroupé en 4 groupes.



Pas de recette Miracle

- Sensibiliser et Former les développeurs au développement sécurisé !
- Auditer et Tester son code !
- Vérifier le fonctionnement de son Application !



***La sécurité est d'abord et avant tout
affaire de bon sens, le maillon faible
restant... l'Humain***

Merci

Questions



"Si vous pensez que l'éducation coûte cher, essayez donc l'ignorance"

Abraham Lincoln