OWASP Top Ten 2007

Le but principal du Top Ten des vulnérabilités est d'éduquer les développeurs, designers ou architectes d'infrastructures contenant des applications ou services web, sur les conséquences des vecteurs d'attaques web les plus connues. Le Top 10 propose des méthodes simples pour protéger contre ces vulnérabilites. Un bon début pour vos développements d'applications sécurisées.

A1. Cross site scripting (XSS)

A2. Injection flaws

A3. Malicious file execution

A4. Insecure direct object reference

A5. Cross site request forgery

A6. Information leakage and improper error handling

A7. Broken authentication and session management

A8. Insecure cryptographic storage

A9. Insecure communications

A10. Failure to restrict URL Access

Informations sur la traduction française du Top 10 au Stand B2, Infosecurity.

Les projets OWASP

Chaque projet OWASP est dirigé par des responsables en charge des tâches et de la roadmap. Ces mêmes responsables sont tenus de constituer les équipes et de promouvoir leurs projets. Un certain nombre de documents sont publiés par l'OWASP:

OWASP Appsec FAQ
Liste de questions les plus fréquentes sur la sécurité des applications Web

OWASP Code review
Recommandations à destination des développeurs d'applications Web

OWASP Guide
Guide de la sécurité des applications Web et Web Services

OWASP Testing Guide
Les procédures de tests et contrôles d'applications Web

OWASP Legal
Aspects légaux de la sécurité des applications Web

OWASP Tools
Document indépendant sur les outils de sécurité applicative

OWASP Ajax security guide
Document sur la sécurité des applications utilisant du javascript (web 2.0)

Les Outils OWASP

OWASP Webgoat
Environnement de test et de formation sur la sécurité des applications web.

OWASP Webscarab
Outil de test de sécurité pour les applications Web et Web Services.

OWASP Live CD
Cd-rom contenant des outils utiles pour la sécurité des applications Web.

OWASP Live Education
Compilation de matériel de formation sur la sécurité des applications Web.

Participer a l'OWASP

Sites Web
http://www.owasp.org
http://www.owasp.org/index.php/France

Devenir Membre
http://www.owasp.org/index.php/Membership

Les Listes de Diffusion
https://lists.owasp.org/mailman/listinfo

Les Projets
http://www.owasp.org/index.php/Category:OWASP_Project

Bee Ware sponsor de l'OWASP, Infosecurity 2007

Sponsorisé par Bee Ware, éditeur de solutions de sécurité applicative Web, XML et Web Services, l'OWASP sera présent sur le salon Infosecurity au stand B02 et assurera également l'introduction de la table ronde «Modernité des Services Publics - Nouvelles Architectures SOA» co-organisée par Bee Ware et le journal e.Administration.

A propos de Bee Ware

Bee Ware est le premier fournisseur de solutions Appliance de déploiement sécurisé des applications Web.
Nos clients utilisent i-Watch pour surveiller le trafic Web, i-Sentry pour protéger les applications et les services Web contre les attaques connues et inconnues et i-Trust pour mettre en oeuvre aisément le Web Single Sign On.
Construites sur des standards ouverts
(Open Standards), les solutions Appliance de Bee Ware, primées par l'industrie, garantissent la sécurité, les performances et la continuité d'activité au sein des entreprises les plus exigeantes.

BeeWare
Delivering Confidence in Web Applications

A propos de l'OWASP

L'OWASP (Open Web Application Security Project) est une organisation communautaire mondiale ouverte et indépendante. Elle a pour objectif d'organiser, promouvoir, développer et maintenir des applications sûres.
Tous les projets et manifestations de l'OWASP sont libres et ouvertes aux personnes intéressées par la sécurité des applications Web.

L'OWASP est une organisation d'un nouveau genre, sa liberté par rapport aux influences commerciales lui permet de fournir des informations pratiques et non influencées a propos de la sécurité des applications Web.

L'OWASP n'est lié a aucune société commerciale, bien qu'elle puisse fournir des informations à propos des technologies de ces dernières sociétés.

Comme beaucoup d'organisations Open Source, l'OWASP produit différents contenus et outils dans un esprit collaboratif et ouvert.

OWASP
The Open Web Application Security Project

OWASP Chapitre Français

au

Salon Infosecurity

CNIT - Paris

21-22 novembre 2007

www.owasp.org
www.owasp.org/index.php/France