POUR PUBLICATION IMMEDIATE

OWASP TOP 10 2010

Columbia, MD, USA – Paris, France - 19 Avril 2010 —

Depuis 2003, les experts et chercheurs en sécurité des applications du monde entire de l'Open Web Application Security Project (OWASP) suivent l'évolution de l'état des applications Web et produisent un document qui est utilisé et fait parti des standards mondiaux, que cela soit au sein des ministères, gouvernements ou standard métiers (PCI), …

L'OWASP vient de mettre à jour le document présentant les 10 risques associés à l'utilisatn des applications Web en enterprise. Ce document de 22 pages est fourni avec des exemples et des datails associés à chacun des risques, permettant aux développeurs, architectes, chef de projets, responsables d'applications et toute personne interessée par la sécurité Web de comprendre ceux-ci. Tout ce qui est diffuse par l'OWASP est libre et ouvert, vous pouvez télécharger le Top10 OWASP 2010 à l'URL suivante :

http://www.owasp.org/index.php/Top_10

Dave Wichers, membre du bureau de la fondation OWASP et COO d'Aspect Security, qui a gérer le projet depuis son début déclare : « Cette année, nous avons réorganiser le Top10 pour expliquer que nous parlons de risques et non plus uniquement de vulnérabilités. Essayer de prioriser des vulnérabilités sans leur contexte n'a pas de sens. Vous ne pouvez prendre les bonnes décisions métier sans comprendre les menaces et l'impact sur votre métier ». Ce nouveau focus sur les risques va permettre aux entreprises une meilleure compréhension et une meilleure gestion de la sécurité des applications.

Le temps est venu de prendre conscience en dehors de la communauté sécurité des risques des applications pour ceux qui en ont le plus besoin. Cette année, l'ambitieux but est de donner a tout développeur d'une application Web l'OWASP Top10 et de lui faire comprendre les problèmes.

Depuis trop longtemps, beaucoup d'entreprises s'en remettent exclusivement à un audit de vulnérabilités ou tests d'intrusion occasionnel pour s'assurer que les applications web internes et externes sont sures. Cette approche est couteuse et ne permet pas d'obtenir une couverture optimale. Comme tout autre élément de la sécurité, la sécurité des applications nécessite une visibilité transverse et globale de la stratégie de contrôle à déployer. Si votre entreprise est prête à sécuriser ses applications vous trouverez des dizaines de livres, projets, outils, forums, liste de diffusions gratuitement dans le projet OWASP. Vous pouvez aussi rejoindre un des 180 chapitre locaux pour assister à l'une de nos conférences sur la sécurité applicative.

Le Top10 2010[1] est le suivant :

A1: Injection
A2: Cross-Site Scripting (XSS)
A3: Broken Authentication and Session Management
A4: Insecure Direct Object References
A5: Cross-Site Request Forgery (CSRF)

[1] Une traduction française sera publiée rapidement.

A6: Security Misconfiguration
A7: Insecure Cryptographic Storage
A8: Failure to Restrict URL Access
A9: Insufficient Transport Layer Protection
A10: Unvalidated Redirects and Forwards

La version 2010 est basée sur une plus grande source d'informations sur les vulnérabilités applicatives que les versions précédentes. L'information est présentée de manière plus concise et claire. Elle inclue aussi des références plus fortes avec les ressources disponibles pour vous aider, en particulier les outils de l'OWAS, tels que l'Enterprise Security API (ESAPI) et l'Application Security Verification Standard (ASVS).

A PROPOS DE L'OWASP

L'OWASP (Open Web Application Security Project) est une organisation communautaire mondiale indépendante dont le principe est basé sur le volontariat et l'Open Source. Son objectif est de créer et promouvoir un référentiel documentaire cohérent de « best practices » relatifs à la sécurité des Application Web. Tous les projets et manifestations de l'OWASP sont libres et ouverts aux personnes intéressées par la sécurité des applications Web. La fondation OWASP (USA) est une organisation de type 501c3 qui permet de supporter les travaux grâce aux dons et sponsors de nos membres: Individuels, Entreprises & Ecoles/Universités.

Contact France : Sébastien Gioria (sebastien.gioria@owasp.org) && Ludovic Petit (ludovic.petit@owasp.org), Leaders du chapitre France.
Interviews (USA): Jeff Williams – OWASP Chair and Top 10 Project Founder (jeff.williams@owasp.,org)
Interviews (USA): Dave Wichers – OWASP Board Member and Top 10 Project Lead (dave.wichers@owasp.org)
Contact (USA): Lorna Alamri – Connections Committee (lorna.alamri@owasp.org)
Company Name: Open Web Application Security Project (OWASP)
Web site address: http://www.owasp.org

# # #