HP démystifie la sécurité des applications et services Web

HP est formel : à l'heure où l'évolution des solutions métiers vers un modèle hébergé se conjugue à une forte recrudescence des attaques informatiques, l'approche des entreprises doit se centrer sur la sécurisation des applications et services web, tout au long de leur cycle de vie.

Le portefeuille technologique de la multinationale américaine s'élargit en conséquence avec l'*appliance* WebInspect 10.0, automatisée et exploitable « clés en main », combinée éventuellement aux solutions HP Fortity, Quality Center et Application Lifecycle Management. Son rôle : répliquer et simuler des attaques informatiques réelles pour déceler, dans des applications finalisées ou en cours de développement, des vulnérabilités, et déterminer leurs implications potentielles sur les systèmes d'information de l'entreprise ou de ses clients/prospects.

Un fonctionnement complexe…

Opérationnelle sans contraintes particulières de mise en oeuvre, WebInspect examine de manière dynamique les failles de sécurité dans des environnements sur ou hors site. Sont intégrés, dans son analyse, des paramètres tels que les interactions entre applications et utilisateurs, les spécificités des processus métiers, les services embarqués qui font appel à des API, les systèmes d'authentification complexes ou encore les exigences de conformité vis-à-vis des standards de l'industrie.

La dimension du contexte a donc son importance, et ce jusqu'au niveau du code. Certains points de contrôle sensible sont priorisés, comme les appels Ajax en JavaScript ou les fichiers Adobe Flash, systématiquement passés au peigne fin. En associant à WebInspect la solution Fortify SecurityScope, l'analyse est encore plus approfondie, en temps réel. Ce qui améliore la réactivité des développeurs et des équipes chargées de la sécurité.

… et simple à la fois

Tous les rapports d'analyse peuvent être centralisés et restitués sous la forme d'historiques partagés, pour simplifier la mise en place de politiques de sécurité à l'échelle de l'entreprise. HP Software Security Center en constitue une extension, avec la possibilité de centraliser et comparer les résultats de tests statiques et dynamiques, ainsi que de les exporter au format XML pour l'interopérabilité avec d'autres systèmes de sécurité.

L'utilisateur est guidé dans la tâche par un processus de test interactif (Guided Scan), qui s'appuie sur une technique de reconnaissance adaptative des composants : il s'agit en l'occurrence d'apporter de la souplesse dans l'analyse, avec la prise en charge de scénarios spécifiques dans des environnements hautement personnalisés. Par exemple, des configurations de proxys erronées ou l'authentification du réseau.

Crédit illustration : kentoh – Shutterstock.com

—— **A voir aussi** ——

Quiz Silicon.fr : HP, du garage à la multinationale