

## Qualys, auditer la qualité des certificats SSL des sites Web

### Internet

Posté par : JPilo

Publié le : 3/8/2010 0:00:00

De nouveaux travaux de recherche présentés à **Black Hat USA 2010** renseignent sur l'état de l'utilisation du protocole SSL sur Internet.

Qualys annonce **un test SSL gratuit des sites Web** disponible sur Qualys SSL Labs. Qualys SSL Labs offre des ressources pour mettre SSL à profit et sécuriser les sites Web ainsi que les transactions en ligne.

Gratuit, ce test SSL en ligne examine la chaîne de certification SSL d'un site Web pour vérifier qu'elle est de confiance et qu'elle participe activement à la sécurité des communications sur Internet. En marge de cette annonce, les résultats d'une étude menée en 2009 sur quelque 120 millions de noms de domaine enregistrés utilisant plus de 800 000 certificats SSL seront présentés en direct le 29 juillet pendant la conférence Black Hat USA 2010.



**SSL est un protocole de sécurité qui protège les sites Web** en chiffrant les informations sensibles pendant les transactions en ligne. Même s'il s'agit d'un protocole fiable, certains déploiements peuvent poser des problèmes, notamment au niveau de la configuration et de la validation du certificat, ce qui rend alors SSL inutile et compromet la sécurité sur Internet. Qualys SSL Labs et le nouveau test SSL en ligne permettent à un tout utilisateur, technicien ou non, d'évaluer ses déploiements SSL pour mieux utiliser ce protocole et protéger ses sites contre d'éventuelles attaques.

« SSL est un protocole fiable qui sert de fondement à la sécurité d'Internet, mais qui n'est tout simplement pas configuré correctement sur la plupart des sites, » déclare **Ivan Ristic**, directeur technique chez Qualys qui est à l'origine de SSL Labs. « Qualys SSL Labs est une initiative de recherche non lucrative pour comprendre comment SSL est utilisé afin d'améliorer ce protocole et d'aider les utilisateurs à le configurer et à l'utiliser correctement. »

**Grâce à ce nouveau test en ligne gratuit**, un utilisateur peut tester la chaîne de certification SSL d'un site Web pour vérifier si cette dernière est fiable et qu'elle sécurise les communications via Internet. Il est également possible de faire une analyse complète de la configuration du certificat SSL pour détecter les faiblesses de configuration et les problèmes de performance. Pour ce faire, il suffit de saisir l'URL du site Web pour que le test évalue tous les serveurs hébergeant ce site. Les résultats du test attribuent une note numérique au service SSL dans plusieurs catégories ainsi qu'une note alphabétique qui évalue la configuration SSL. Afin d'améliorer cette note, Qualys SSL Labs fournit des recommandations et des ressources pour mieux utiliser SSL.

Une note numérique finale allant de 0 à 100 et une note alphabétique délivrées à la fin du test renseignent sur la puissance du déploiement SSL sur le site Web testé.

Et **Ivan Ristic** de déclarer « Notre objectif chez SSL Labs est d'aborder les aspects rarement mentionnés du protocole SSL, d'en promouvoir une utilisation correcte et d'inviter quiconque à s'impliquer dans la sécurité ».

### Points forts des travaux de recherche abordés lors d'une session à Black Hat USA :

☞ Seule une fraction de l'ensemble des sites Web utilise SSL

☞ Seuls 70% des certificats sont valides

☞ La moitié de tous les sites supporte encore le protocole SSLv2

☞ Environ 38% des sites SSL sont bien configurés et 62% ne le sont pas

☞ Environ 32% des sites continuent de pâtir de la vulnérabilité liée à la renégociation

### Disponibilité

Ivan Ristic présentera le nouvel outil SSL en ligne ainsi que ses travaux d'analyse sur les certificats SSL réalisés à travers le monde lors d'une session spéciale le 29 juillet à 10h00 (heure d'été du Pacifique) à l'occasion de Black Hat USA 2010.

Pour en savoir plus sur SSL et sur l'utilisation de ce [nouvel outil de test SSL gratuit](#). Pour accéder sur ce test SSL avec d'autres utilisateurs, rendez-vous sur [le site de la communauté Qualys](#).