| | | |
|---|---|---|
| SSL Pulse | **SSL Pulse** | |
| | **Survey of the SSL Implementation of the Most Popular Web Sites** | |
| | **System Requirements**:<br>Site web accessible à l'adresse suivante : https://www.trustworthyinternet.org/ssl-pulse/ | |
| | **Développé par:** | Trustworthy Internet Movement |
| Pas de license | **Personne à contacter** | Julien.Cathalo@smals.be |

## Fonctions

SSL Pulse est un site web dédié à évaluer la sécurité pratique des implémentations de SSL. SSL Pulse permet d'une part une vue globale de la sécurité de l'implémentation de SSL sur les sites les plus populaires et d'autre part de tester un site en particulier. L'initiative vient du Trustworthy Internet Movement (TIM), organisation qui se veut neutre et qui promeut l'amélioration de la sécurité sur internet. Le TIM a été fondé par Philippe Courtot, PDG de la société Qualys (entreprise privée spécialisée dans la sécurité).

Les créateurs de SSL Pulse ont imaginé un système de notation. Le site évalue chaque serveur SSL et lui attribue une lettre qui juge sa sécurité, de A pour un site sûr à E pour un site très insécurisé. Cette lettre provient de la combinaison de deux notes :

- Une note qui évalue la validité du certificat SSL du serveur.

  Le moindre de problème de validité (certificat expiré, révoqué, pas encore valide, avec un mauvais nom de domaine ou pas « trusté ») entraînera une note totale de zéro.

- Une note qui évalue la configuration du serveur.

  Ici, de nombreux points sont examinés : versions de SSL / TLS supportées, protocoles supportés, choix des tailles de clés… Par exemple, une taille de clés trop petite entraînera une mauvaise note.

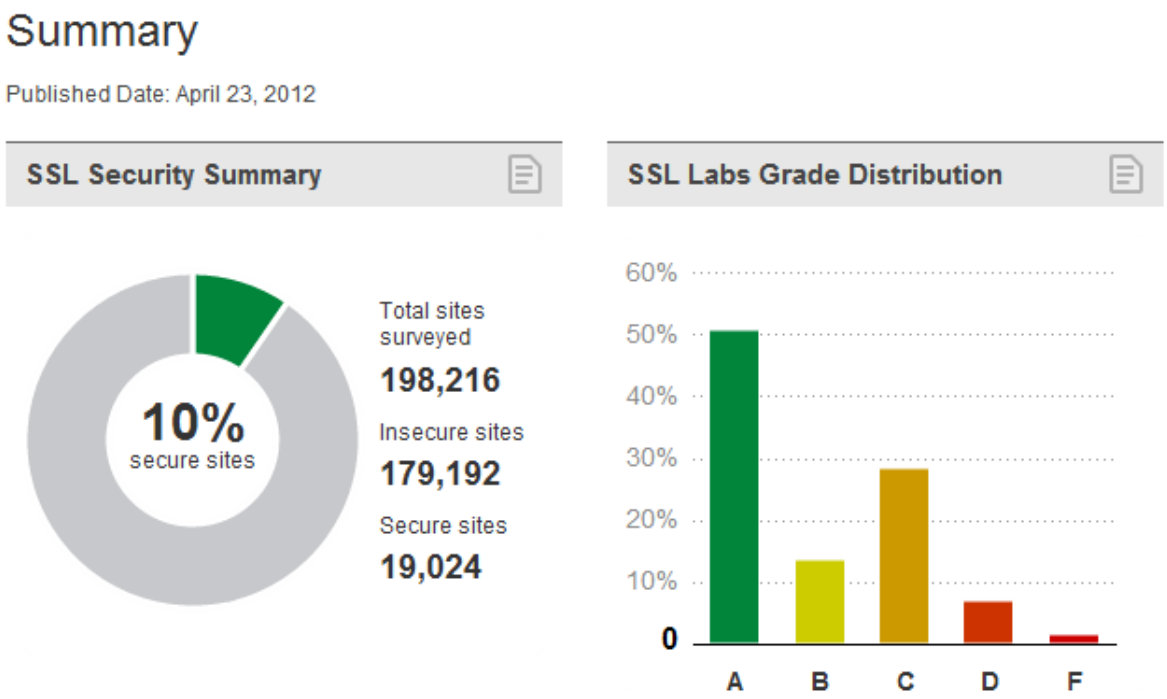
La page principale de SSL Pulse offre une vue d'ensemble des notes obtenues par une liste de 200 000 sites choisis parmi les plus populaires sur Alexa. Par ailleurs, on peut tester un site particulier en tapant l'url et SSL Pulse renvoie la note du site avec des détails expliquant les raisons de la note.

## Conclusions et Recommandations

SSL Pulse est un site clair et très simple à utiliser. Le système des notes est très incitatif : si un responsable d'un serveur constate que son site est mal noté, il sera motivé à prendre des actions. D'abord par sécurité mais peut-être aussi par souci d'image : le site SSL Labs étant public, des clients ou utilisateurs pourraient voir que le site est mal noté. L'administrateur sera ensuite guidé dans ces actions par les recommandations du site, qui fournit une documentation pertinente. SSL Labs, à condition qu'il devienne suffisamment populaire, devrait permettre une meilleure prise de conscience des étapes nécessaires pour sécuriser correctement un serveur SSL et améliorer donc globalement la sécurité sur internet.

## Tests et Résultats

Voici une vue générale des résultats de SSL Labs au 23 avril 2012. On voit (sur le graphique de gauche) que seuls 10% des sites sont considérés comme sûrs (pour être considéré sûr, un site doit être noté A et ne doit être vulnérable ni contre BEAST ni contre Insecure Renegotiation). Sur le graphique de droite, on voit la répartition des notes. Ces résultats sont assez frappants, les étapes à suivre pour obtenir un certificat valable et configurer de manière sécurisée un serveur SSL étant relativement simples. Il s'agit principalement d'un problème de prise de conscience. Il sera intéressant de voir l'évolution de ces chiffres dans le temps.




Voici un exemple de résultats du test de www.ehealth.fgov.be. On voit que le serveur obtient la meilleure note avec une remarque concernant l'attaque BEAST (le serveur, comme 73% des sites testés par SSL Labs, n'était pas encore protégé contre BEAST au moment du test).