Université de Bordeaux

Projet de fin d'étude

Breach, Freak & Bar Mitzvah : Attaques sur SSL/TLS

Auteur :
Tremblain Rémi

Responsable :
M. Abdel Guermouche

25 janvier 2016

Table des matières

Remerciements

Je tiens à remercier LaTeX et les tutoriels sur internet et notamment `http://www.ukonline.be/programmation/latex/tutoriel/index.php`.

Bla bla bla bla bla.

Introduction

SL/TLS est un des standards les plus repandus pour la securisation des communications sur internet. Bien que le protocole soit assez simple et robuste, de nombreuses attaques ont ete mises au point pour recuperer le contenu en clair des communications. Une premiere etape de ce projet consistera donc a faire un inventaire des diffe- rentes techniques existantes visant a attaquer SSL/TLS. Puis dans un second temps, on sinteressera aux dernieres en date, a savoir Breach, Freak et Bar Mitzvah. Ces attaques, bien quassez complexes, permettent dattaquer une communication http securisee via SSL/TLS (https) pour recuperer des informations sensibles en clair (en loccurrence les cookies dauthentification). Lobjectif sera detudier ces attaques de maniere assez fine et de les mettre en uvre (dans la mesure du possible pour ce qui est de Breach et Bar Mitzvah).

1 La première section

1.1 Une sous section

On peut mettre des mots en *italique*, en PETITES MAJUSCULES ou en `largeur fixe (machine à écrire)`.

Voici un deuxième paragraphe avec une formule mathématique simple : $e = mc^2$.

Un troisième avec des « guillemet français ».

1.1.1 Écrire en anglais

Do you speak French? Does anybody here speak french?

1.2 Lites

— Liste classique ;
— un élément ;
— et un autre élément.

1. Une liste numéroté
2. deux
3. trois

Description C'est bien pour des définitions.

Deux Ou pour faire un liste spéciale.

1.3 Références

1.4 Note de bas de page

Voici une note [1] de bas de page. Une deuxième [2] déclarée différemment. La même note [2].

1.5 Figure

1. Texte de bas de page
2. Il a deux références vers cette note

FIGURE 1 – BlogHiko | taille original

FIGURE 2 – BlogHiko | 50% de la largeur de la page

2 Citation Wikipédia

LaTeX est un langage et un système de composition de documents créé par Leslie Lamport en 198312. Plus exactement, il s'agit d'une collection de macro-commandes destinées à faciliter l'utilisation du « processeur de texte » TeX de Donald Knuth. Depuis 1993, il est maintenu par le LaTeX3 Project team. La première version utilisée largement, appelée LaTeX2.09, est sortie en 1984. Une révision majeure, appelée LaTeX2 epsilon est sortie en 1991.

Le nom est l'abréviation de Lamport TeX. On écrit souvent LaTeX, le logiciel permettant les mises en forme correspondant au logo.

Du fait de sa relative simplicité, il est devenu la méthode privilégiée d'écriture de documents scientifiques employant TeX. Il est particulièrement utilisé dans les domaines techniques et scientifiques pour la production de documents de taille moyenne ou importante (thèse ou livre, par exemple). Néanmoins, il peut aussi être employé pour générer des documents de types variés (par exemple, des lettres, ou des transparents).

Conclusion

Pour conclure, avec LaTeX on obtient un rendu impeccable mais il faut s'investir pour le prendre en main.