Comment passer son site WordPress en HTTPS

Par Alex de WPMarmite - Juillet 2016 - Suivez la WPMarmite sur Twitter

Depuis mai 2016, la Marmite est passée au HTTPS. Cela signifie que toutes les pages du site ont une URL débutant par https:// au lieu du classique http://.

Vous allez me dire : "Très bien, mais qu'est-ce que ça change concrètement ? Pourquoi as-tu fait ce choix ? En quoi est-ce important ?". Eh bien c'est ce que nous allons voir dans ce nouvel article :)

Accrochez vos ceintures, voici le sommaire !

Vous êtes toujours là ? Alors répondons à la question suivante.

Qu'est que le HTTPS, SSL et le TLS ?

Vous ne le savez peut-être pas mais lorsque vous naviguez sur un site dépourvu de HTTPS, les données que vous échangez sont en clair, c'est à dire que n'importe qui peut les lire, les analyser et les transmettre.

Bon, j'y vais un peu fort. On est d'accord que ce n'est pas le grand-père du coin qui va vous tracer (quoi que ;)).

Restreignons ce "n'importe qui" aux personnes (ou organisations) possédant de bonnes compétences techniques, certains logiciels et l'intention de vous espionner.

Même si le risque est assez faible, il n'est pas nul. Et franchement, qui aime se faire épier ?

Mais je n'ai rien à me reprocher !

Je n'en doute pas une seconde mais avouez que l'**on n'a pas le même comportement lorsque quelqu'un surveille tous nos faits et gestes**.

Cela arrive par exemple au travail, lorsque votre supérieur regarde ce que vous faites. On peut aussi vivre des situations similaires à l'école, quand le professeur passe derrière vous.

On peut dire qu'une sorte de pression psychologique s'applique sur vous (même si la personne qui passe n'en a pas l'intention) et va changer votre comportement.

Du coup, *votre liberté s'en trouve affectée*.

Sur Internet, il n'y a pas forcément quelqu'un qui rode derrière vous.
Cela est beaucoup plus subtil.

Si l'on a l'intention de vous espionner, on peut enregistrer ce que vous avez fait sur tel ou tel site. Mais surtout, on peut récupérer vos informations personnelles (emails, mots de passe, nom, adresse, déplacements, coordonnées bancaires et j'en passe).

Là, ça devient moins drôle, n'est-ce pas ?

C'est pour lutter contre tout cela que le protocole HTTPS a été mis en place. **Grâce à lui, les données que vous échangerez avec un site seront chiffrées** (c'est à dire cryptées).

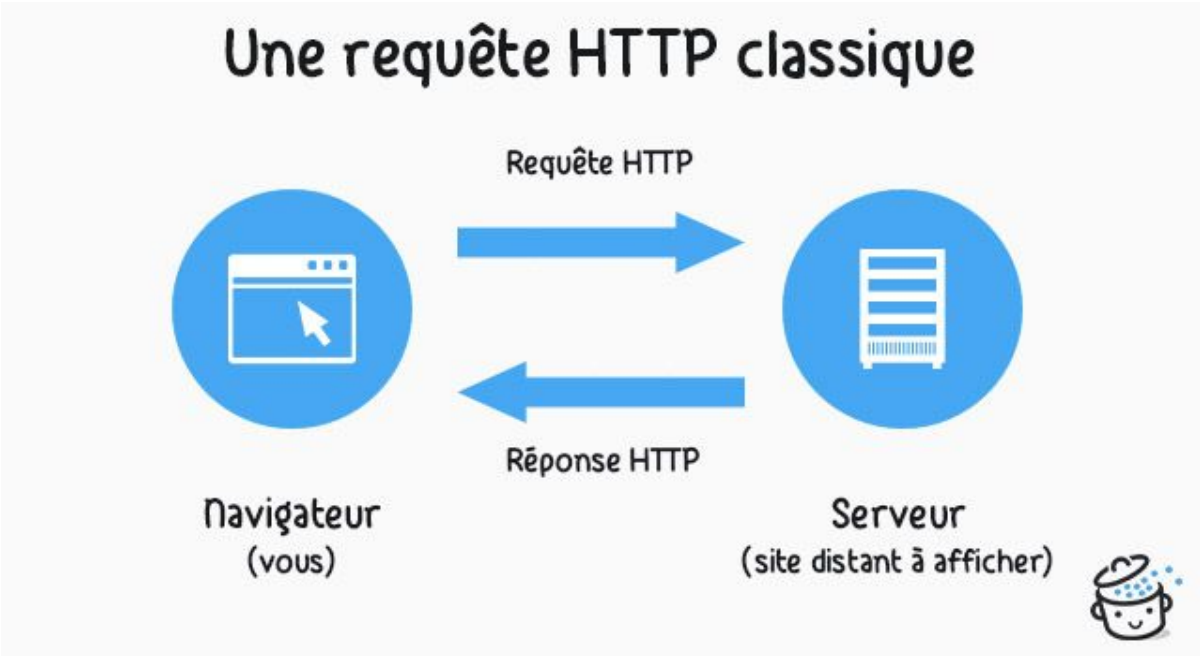
Encore mieux, vous serez certain de bien visualiser le site original et non une version modifiée par quelqu'un qui aurait intercepté la connexion. Eh oui, beaucoup de choses sont possibles en informatique !

Par contre, le HTTPS ne vous rendra pas anonyme. Il est toujours possible de savoir qui vous êtes (via votre adresse IP) et de connaître les sites que vous aurez visités

Pour résumer, on peut juste savoir que vous êtes allé sur tel site en HTTPS mais pas ce que vous y avez fait.

Comment fonctionne le HTTPS ?

Afin d'illustrer le fonctionnement du protocole HTTPS, faisons un retour rapide sur son grand frère, le protocole HTTP. Ici c'est assez simple, vous avez deux acteurs : le navigateur web (vous) et le serveur où est hébergé le site à afficher.



Dès que vous entrez une adresse dans votre navigateur, il envoie une requête HTTP pour demander la page. Le serveur la renvoie et le navigateur l'affiche. Plutôt facile, n'est-ce pas ?

Si vous voulez en savoir plus sur le fonctionnement d'un site web (et en particulier un site WordPress), jetez un oeil à l'article dédié à l'hébergement web.

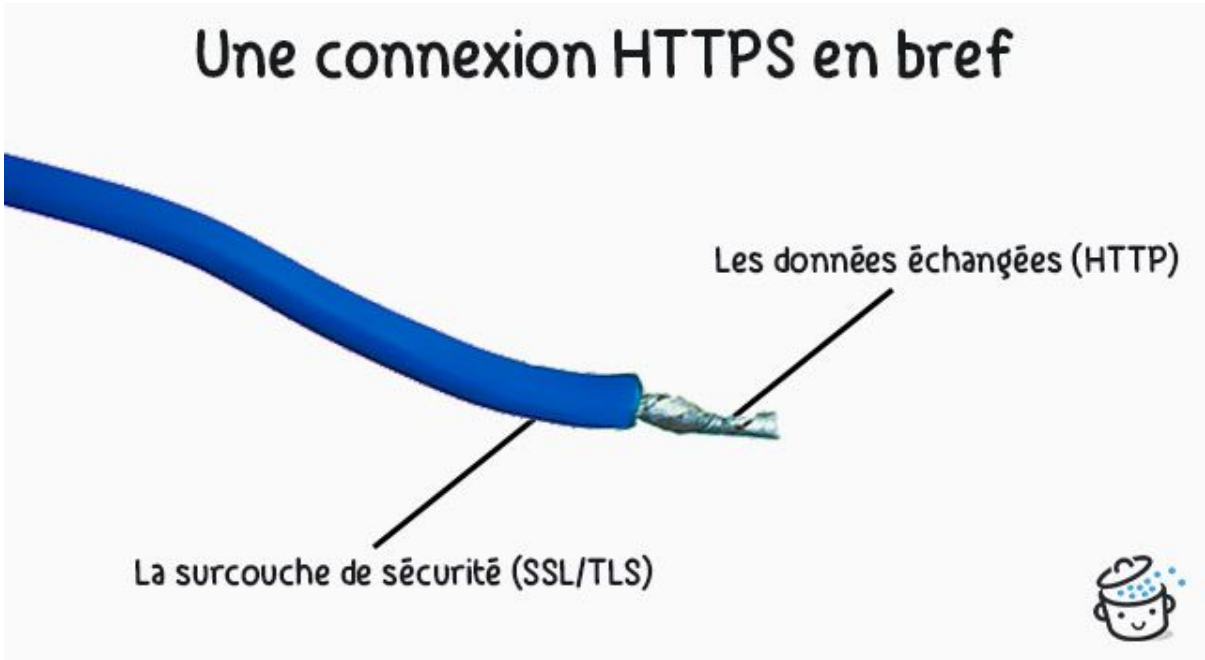
Pour le HTTPS, d'autres acteurs entrent en scène mais nous allons retenir le principal : l'autorité de certification.

Ce genre d'organisme, également appelé tiers de confiance, délivre un certificat SSL/TLS pour que les créateurs de sites puissent mettre en place le HTTPS. Il en existe des dizaines d'autorités de certification mais les plus connues sont Comodo et GlobalSign.

> Un certificat permet de chiffrer la connexion et de vérifier l'identité du site (suis-je bien connecté au site que je veux visiter ?).

Parlons rapidement des deux nouveaux acronymes cités auparavant : SSL et TLS.

On peut dire que le SSL et le TLS sont une sorte de surcouche qui va venir sécuriser une connexion HTTP classique. Un peu comme la gaine vient protéger un cable électrique si vous voulez :



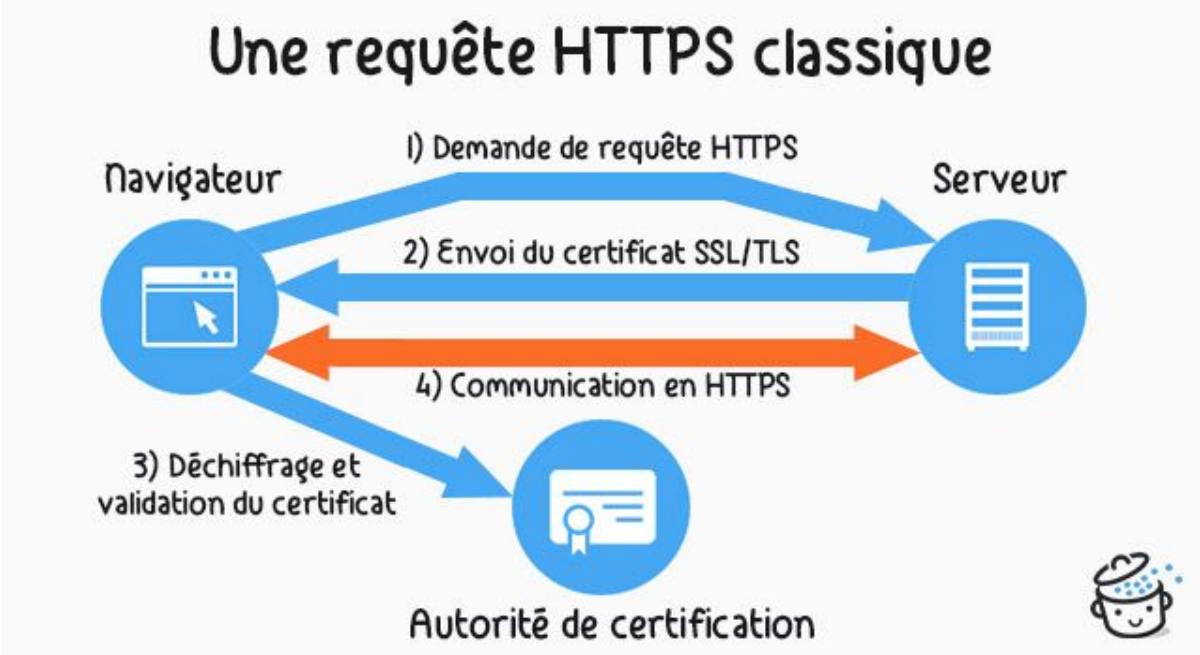
On retrouve souvent l'appellation SSL sur le web mais c'est un abus de langage.

En fait, SSL (Secure Socket Layer) est la première version de ce protocole de sécurisation. TLS (Transport Layer Security) a pris le relai pour plus de sécurité. Si cela vous intéresse, vous retrouverez l'historique complet sur Wikipédia.

Récapitulons.

> Pour bénéficier du HTTPS sur un site, nous avons besoin d'une autorité de certification qui va nous délivrer un certificat SSL/TLS.

Voici comment cela s'intègre par rapport à notre schéma précédent :



Je parie que vous ne vous doutiez pas qu'il se passait autant de choses. Et encore, j'ai dû simplifier pour que tout tienne !

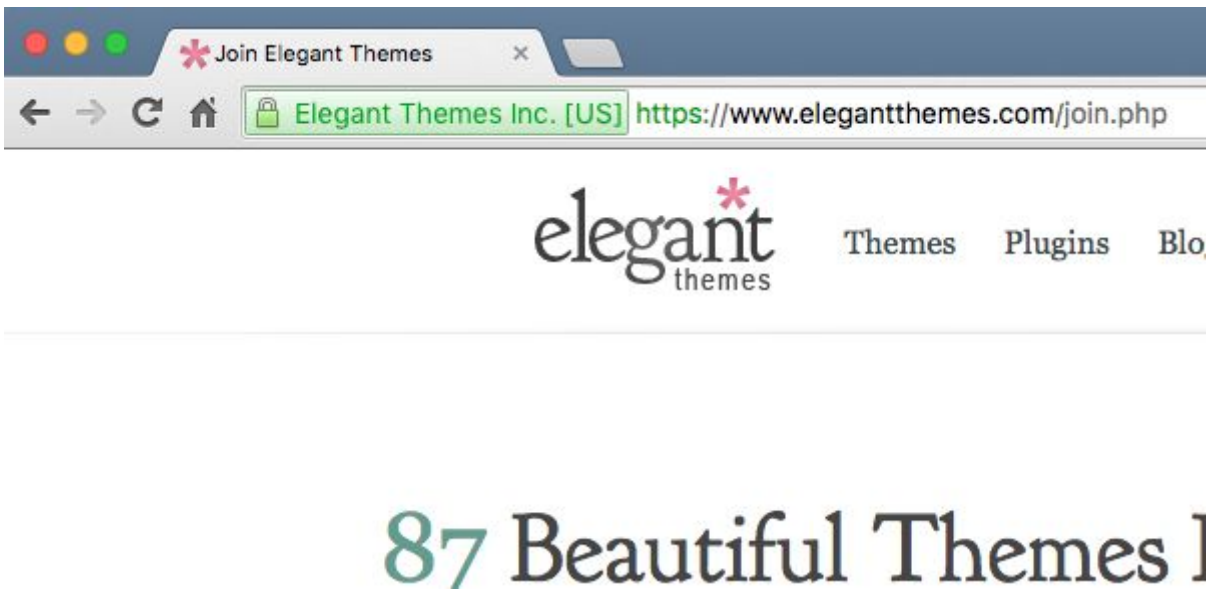
En tout cas, cela se passe très très vite. On n'y voit que du feu :)

Comment savoir si la connexion est sécurisée ?

Vous l'aurez deviné, le premier signe distinctif d'un site sécurisé est évidemment le début de son adresse (son protocole pour être plus précis) qui est passé de http:// à https://.

Cependant, les navigateurs mettent davantage en valeur les sites dotés du HTTPS grâce à un petit cadenas vert placé juste avant l'adresse. Voici l'exemple de WP Marmite avec Google Chrome :

Pour d'autres sites, l'affichage un plus proéminent (nous verrons à quoi cela correspond plus tard dans l'article). C'est notamment le cas pour la page de commande [d'Elegant Themes](#) :



Parfois, il arrive que certaines ressources (images, fichiers CSS ou JS) d'une page en HTTPS soient chargées en HTTP, c'est à dire de manière non sécurisée.

Dans ce cas, le cadenas vert ne s'affichera pas. Le webmaster devra corriger cela pour que le site soit totalement chiffré (nous verrons comment faire un peu plus bas dans l'article).

Voilà, maintenant vous en savez un peu plus sur ce qu'est le HTTPS. Cela dit, nous venons à peine d'effleurer le sujet !

2 Arguments de plus en faveur du HTTPS

Comme vous avez pu le lire précédemment, le HTTPS permet de sécuriser la navigation des visiteurs. Tout d'abord en chiffrant la connexion, puis en lui assurant que vous êtes bien le site que vous prétendez être.

Je tiens toutefois à vous présenter deux autres avantages liés à la mise en place du HTTPS sur un site.

Le référencement sera amélioré (dans le futur)

En 2014, Google a annoncé que le HTTPS était désormais considéré comme un signal pris en compte pour le référencement des sites.

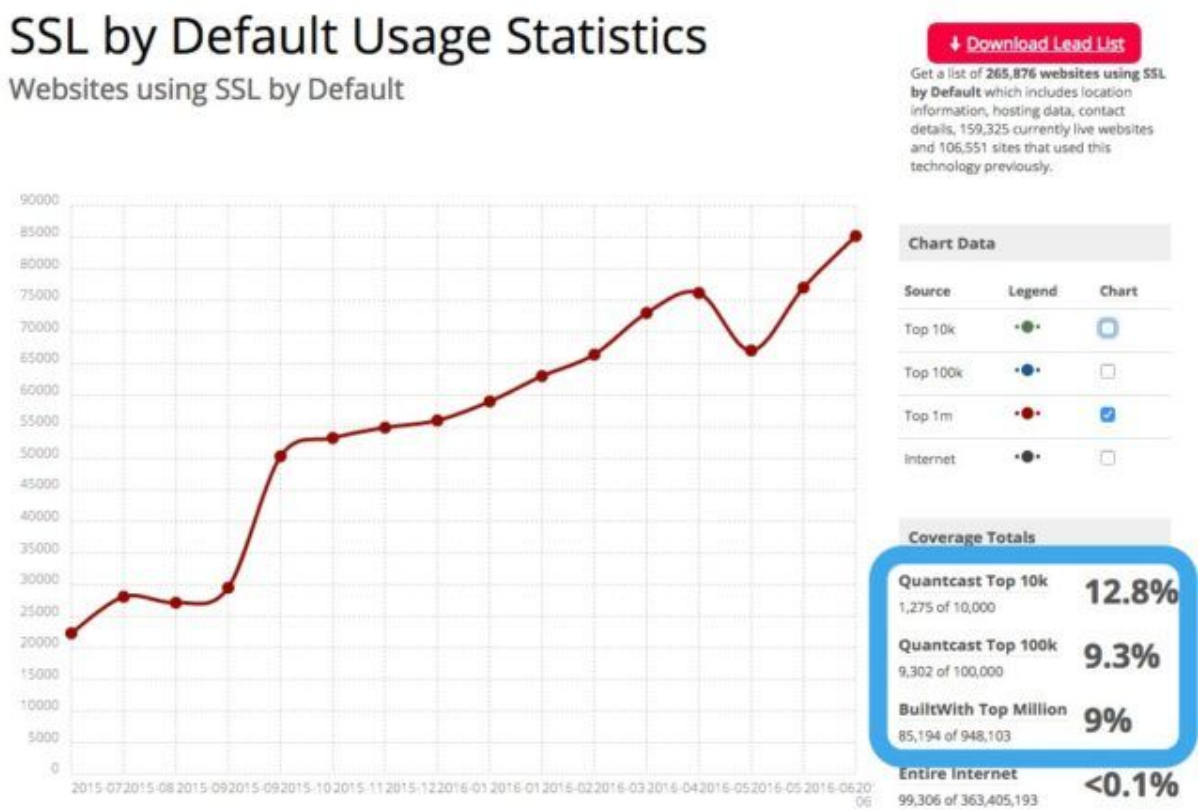
Après plusieurs semaines d'utilisation du HTTPS, *je ne peux pas vraiment vous avouer que le positionnement de la Marmite a beaucoup progressé grâce à ça.*

Toutefois, ce signal pourrait prendre plus d'importance à l'avenir. C'est pourquoi je vous recommande d'y passer si vous créez un nouveau site (au moins, vous n'aurez pas à le faire plus tard).

Si votre site est déjà en ligne depuis un certain temps, la migration sera plus délicate donc faites attention si vous décidez de vous lancer. C'est également ce que préconise Olivier Andrieu d'Abondance.com dans une vidéo de juin 2016 :

J'avais un peu peur pour la Marmite (surtout après ce que le blog a vécu par le passé) mais au final tout s'est bien passé.

Même si la corrélation entre le HTTPS et un meilleur positionnement n'est pas encore très marqué, le pourcentage des sites sécurisés augmente. 10% du top 1 million des sites y sont passés selon BuildWith :



Malgré les recommandations des experts, **je pense qu'il vaut mieux faire la transition maintenant que lorsque 90% des sites seront en HTTPS**. Il y a des chances pour que Google donne plus d'importance au HTTPS à l'avenir. D'ailleurs, il nous le dit même [sur cette page](#) :

> Google considère le protocole HTTPS comme un signal positif pour son classement. Il ne s'agit toutefois que d'un indicateur parmi tant d'autres. Il revêt moins de poids que l'aspect qualitatif d'un site. Ne vous attendez donc pas à percevoir à court terme des retombées majeures en termes de SEO en passant au HTTPS. À plus long terme, il est possible que Google accorde davantage d'importance à l'optimisation HTTPS.

Si ce premier argument ne vous a pas encore convaincu, voici le second.

On vous fera davantage confiance

À votre avis, de quoi les visiteurs ont le plus peur en ligne ?

De se faire avoir pardi ! Tomber sur des escrocs, des charlatans, des guignols !

Et autant vous le dire, il y en a des wagons...

Par contre (et heureusement), ce genre d'individu ne prend généralement pas le temps de bien faire les choses. Ils utilisent des thèmes WordPress horribles, leurs boutons d'achat se ressemblent tous et...

Leurs sites ne sont pas en HTTPS !

Si les navigateurs affichent un petit cadenas vert pour tous les sites sécurisés, ce n'est pas pour rien. **Quand on le voit, on est de suite rassuré (même inconsciemment)**.

Quand on arrive sur un site que l'on ne connait pas, on cherche à prendre ses marques. En voyant un site au design propre, une bonne communauté et des URL avec HTTPS, on se dit que l'on n'est pas tombé sur le site du zozo du coin (enfin il y a moins de chances).

Rien que pour ça, je pense que ça vaut le coup de le mettre en place.

Pour finir sur ce point, *dois-je vous rappeler que le HTTPS est indispensable pour les boutiques en ligne ?* Eh oui, il faut bien chiffrer le numéro de carte bancaire des clients (tout comme leurs identifiants de connexion et leurs autres données personnelles) !

Comment obtenir un certificat SSL/TLS ?

Auparavant, il était assez compliqué de mettre en place le HTTPS sur son site (qu'il soit sous WordPress ou non). Il fallait acheter un certificat SSL/TLS par l'intermédiaire de son hébergeur ou directement via une autorité de certification si vous avez un serveur dédié.

Quand on ne l'a jamais fait, je vous avoue que cela pouvait prendre un peu de temps. On devait nécessairement fournir une preuve de son identité pour montrer que l'on était bien le propriétaire de son site.

*Normal me direz-vous. Sinon comment voulez-vous que l'autorité de certification vous certifie ? ^^*

Bon, c'était fastidieux mais il fallait obligatoirement passer par là.

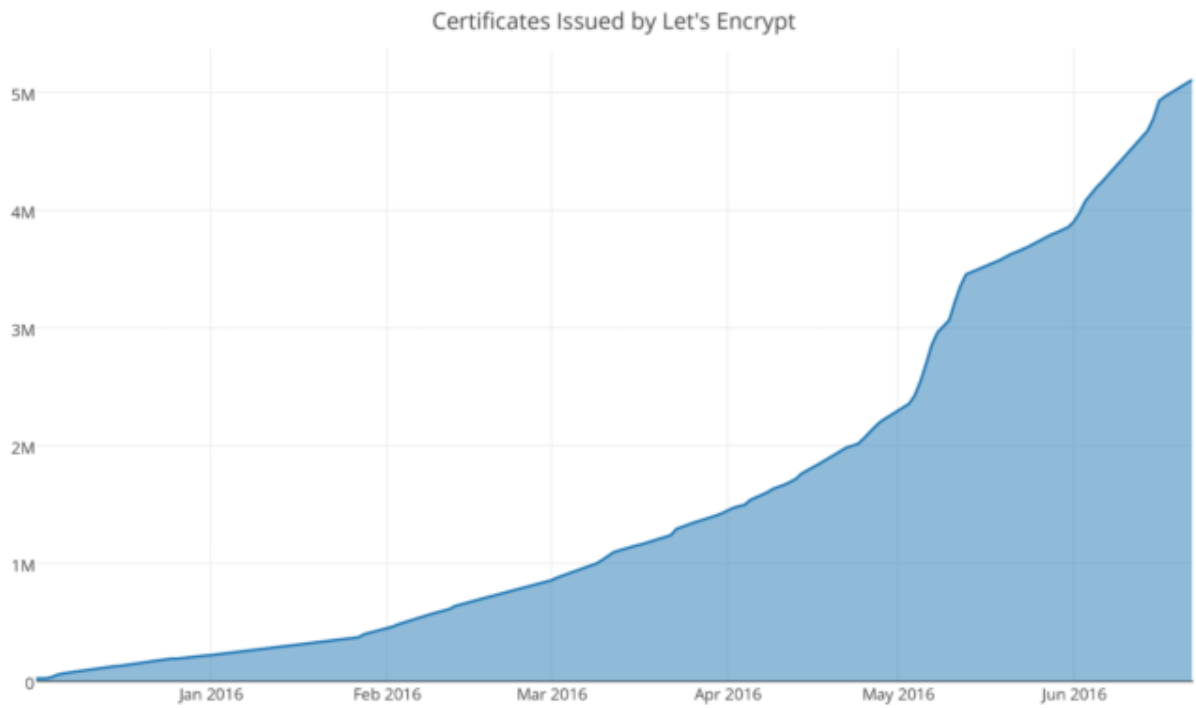
Aujourd'hui, il est toujours possible de procéder ainsi (c'est même recommandé dans certains cas) mais un nouvel acteur est apparu...

Let's Encrypt, vers un web 100% sécurisé

Let's Encrypt est une autorité de certification fournissant des certificats SSL/TLS gratuitement. Leur mission est de chiffrer le web pour le rendre plus sécurisé.

De nombreux acteurs soutiennent et financent cette initiative. On peut citer par exemple citer Facebook, Free, OVH, Automattic ou encore Google.

Depuis leur lancement en décembre 2015, le nombre de certificats qu'ils délivrent est en train d'exploser :



Cela a notamment été rendu possible grâce aux hébergeurs (OVH, Gandi, etc.) et aux plateformes comme WordPress.com qui ont intégré Let's Encrypt pour leurs utilisateurs.

Génial ! Comment faire pour installer un de leurs certificats sur mon site ?!

Pas si vite cher ami. Avant de vous montrer comment faire, il faut que je vous reparle de la première méthode. Vous savez, celle où il faut ouvrir son porte-feuille.

Les autres types de certificats SSL/TLS

Bien qu'il soit possible de sécuriser son site gratuitement avec Let's Encrypt, vous devez savoir qu'il y a un inconvénient majeur : la garantie.

En effet, si jamais un problème se pose au niveau du HTTPS et qu'un de vos clients se fait dérober des données personnelles, vous ne serez pas couvert.

On pourrait croire que cela n'arrive quasiment jamais mais parfois des failles de sécurité sont découvertes et exploitées. Ce fut par exemple le cas en 2014 avec la faille HeartBleed.

Si vous êtes un gros site et que vous gérez des dizaines de milliers de commandes, cela peut vite être problématique. Il faut donc assurer ses arrières.

C'est pourquoi il est possible de se procurer des certificats avec différents niveaux de garantie.

> Des sites comme Symantec proposent des certificats à plus de 1000€ dont la garantie monte à 1,75 millions de dollars.

Enfin je vous rassure, seules les très grandes entreprises ont besoin de ce genre de certificat SSL/TLS ;)

Si vous voulez bénéficier d'une garantie en achetant un certificat, sachez qu'il en existe trois types :

- **Les certificats à validation de domaine (DV)** : Dans ce cas, l'autorité de certification vérifiera jusque que vous êtes bien propriétaire du nom de domaine pour vous accorder le petit cadenas vert (la vérification se passe automatiquement en ligne) ;
- **Les certificats à validation de l'organisation (OV)** : Pour obtenir ce type de certificat, vous devez prouver que vous êtes la personne morale détentrice du domaine à sécuriser et fournir des documents papier comme un extrait KBIS ou une attestation de domiciliation (cela prendra donc un peu plus de temps) ;

- **Les certificats à validation étendue (EV)** : Ici, on ne rigole plus. Pour obtenir ce genre de certificat, il faudra montrer patte blanche. Les informations que vous transmettrez sur votre organisation seront vérifiées (existence légale, physique, numéro de téléphone, adresse, activité, etc) et auditées chaque année.

Ces derniers permettent de renforcer la confiance des visiteurs. Pour rappel, voici le genre de rendu que l'on peut obtenir avec les certificats EV (pour *Extended Validation*) :

Comme je vous l'ai dit, les démarches seront plus fastidieuses. Cela dit, si vous êtes une entité importante, je pense qu'il faut le faire.

Important *: Pensez à renouveler votre certificat en avance si cela ne se fait pas automatiquement. Comptez bien un mois pour être large au niveau des démarches. Sinon vous troquerez votre beau cadenas vert pour un cadenas rouge voire un avertissement du navigateur. Et ça, ce n'est pas bon du tout !*

Quel certificat SSL/TLS choisir ?

J'espère que je ne vous ai pas perdu avec toutes ces infos. Il semblerait que non puisque vous êtes encore là !

Pour répondre rapidement à la question, **dans la majorité des cas un certificat gratuit de Let's Encrypt fera largement l'affaire.**

Si vous désirez vous procurer un certificat SSL/TLS payant pour votre site (et bénéficier d'une garantie en cas de problème), la première chose à faire est de voir ce que votre hébergeur propose. Si vous n'êtes pas sur un serveur dédié, vous ne pourrez pas faire autrement.

En revanche, si vous avez accès à la configuration de votre serveur, le choix est assez vaste. Vous pouvez vous tourner vers les autorités de certifications comme Comodo, GlobalSign ou encore NameCheap (leur page de présentation est très bien faite d'ailleurs).

Gandi a mis en place un outil pour savoir quel certificat choisir. Bien sûr, ils prêchent pour leur paroisse mais cela pourra vous aider à y voir plus clair.

Dans la suite de cet article, nous allons voir...

Comment mettre en place Let's Encrypt chez o2switch

Aujourd'hui, de plus en plus d'hébergeurs proposent à leurs clients des certificats SSL gratuits générés par Let's Encrypt. C'est le cas d'OVH, de Gandi mais aussi d'o2switch, l'hébergeur que j'ai choisi pour la Marmite.

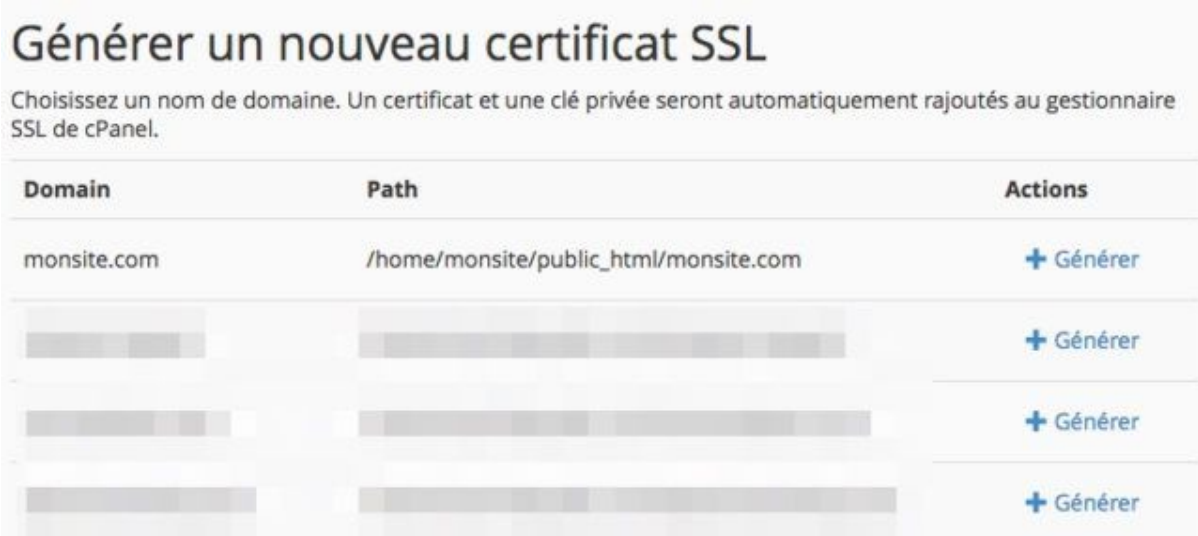
Je vous propose donc de voir comment installer le HTTPS si vous êtes client chez eux (si ce n'est pas le cas, allez voir ce qu'ils font (aff), ça vaut le coup !).

Et grâce à la Marmite, bénéficiez de 15% de réduction avec le code WPM15.

Une fois que vous aurez un compte chez eux et que vous aurez un ou plusieurs nom de domaine de liés, rendez-vous dans votre cPanel.

Dans la section *Sécurité*, cliquez sur *Let's Encrypt* :

Cliquez ensuite sur le lien *+ Générer* en face du domaine que vous comptez sécuriser :

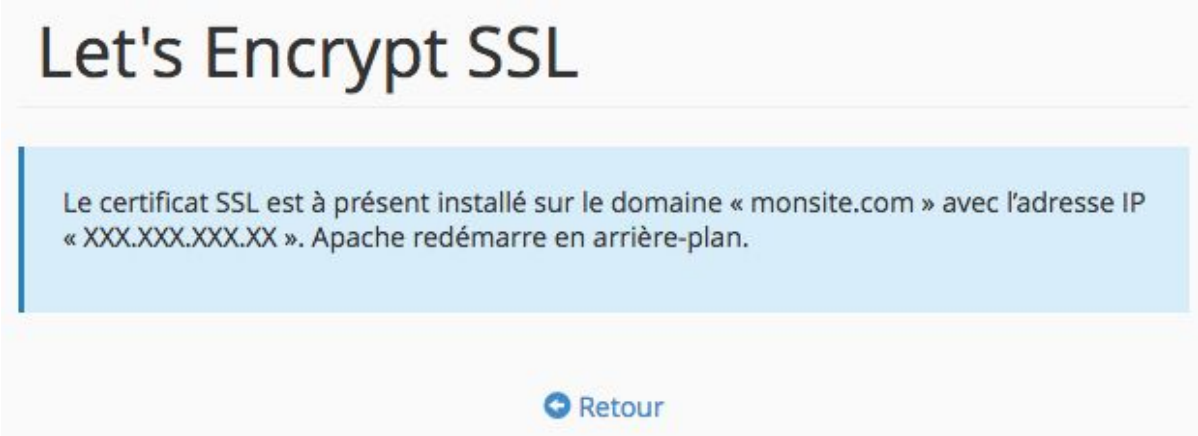


Sur la page suivante, sélectionnez éventuellement la version avec les *www*. Vous n'êtes pas forcé de le faire étant donné que nous ferons des redirections pour emmener les visiteurs sur la version HTTPS :

Vous pouvez aussi installer un certificat sur votre boite email (si vous avez déjà un site, il faudra mettre à jour vos clients de messagerie). Quand vous aurez tout ce qu'il vous faudra, cliquez sur *Activer !*.

Et voilà, c'est terminé !

Le message suivant apparaîtra pour vous le confirmer :



Si vous avez déjà configuré un certificat classique, vous apprécierez la rapidité de mise en place :)

Notez qu'o2switch renouvellera automatiquement le certificat chaque année. Contrairement aux certificats classiques, vous n'aurez pas à vous en charger.

9 choses à faire absolument après l'activation du HTTPS

Très bien, le certificat est actif sur votre nom de domaine. Pourtant la configuration n'est pas encore terminée.

La liste de tâche diffère légèrement si vous partez d'un site vierge ou s'il s'agit d'une migration de HTTP vers HTTPS mais if faudra toujours commencer par...

1. Tout rediriger vers le site en HTTPS

Eh bien oui, maintenant que vous avez un site sécurisé autant en faire profiter vos visiteurs.

Pour l'instant, votre site est à la fois accessible via HTTP et via HTTPS. Il faut que tout renvoie vers le HTTPS sinon vous aurez des problèmes de contenu dupliqué.

Certains hébergeurs proposent de gérer au niveau de leur console d'administration mais vous pouvez aussi faire ça dans le fichier .htaccess.

Je vous ai déjà montré comment procéder dans cet article mais voici le morceau de code à inclure (en l'adaptant à votre nom de domaine bien sûr) :

```
# Redirection vers HTTPS
RewriteCond %{SERVER_PORT} ^80$ [OR]
RewriteCond %{HTTPS} =off
RewriteRule ^(.*)$ https://monsite.com/$1 [R=301,L]

# Redirection du www vers non-www en HTTPS
RewriteCond %{HTTP_HOST} ^www\.monsite\.com [NC]
RewriteRule ^(.*)$ https://monsite.com/$1 [R=301,L]
```

Notez que dans mon cas, je n'utilise pas le *www*. Il faudra le modifier si vous utilisez *www* dans l'adresse de votre site.

Une fois que vous aurez l'impression que tout fonctionne, entrez votre nom de domaine dans cet outil pour vérifier que les redirections sont bien configurées (tout doit être au vert).

C'est très pratique car dans le cas de la Marmite, cela m'a permis de réaliser que les redirections n'étaient pas si directes que ça. En fait :

- **https://www.**wpmarmite.com redirigeait vers :
- **http://**wpmarmite.com qui redirigeait vers :
- **https://**wpmarmite.com

et que :

- **http://www.**wpmarmite.com redirigeait vers :
- **http://**wpmarmite.com qui redirigeait vers :
- **https://**wpmarmite.com

Alors que chaque adresse doit rediriger directement vers *https://wpmarmite.com*. Trop de redirections peuvent heurter votre positionnement dans les moteurs de recherches.

Ça serait dommage de se tirer une balle dans le pied n'est-ce pas ?

Attention : Si vous êtes chez OVH, vous devez savoir qu'ils ont activé Let's Encrypt par défaut sur tous leurs hébergements. Que vous désirez utiliser HTTPS ou non, il vous faudra mettre en place des redirections sinon aurez des problèmes de contenus dupliqué !

2. Remplacer les URL en HTTP

Si vous ne créez pas un nouveau site, il va falloir mettre à jour toutes les URL en HTTP vers HTTPS.

Rassurez-vous nous n'allons pas faire cela à la main mais avec un script que la Marmite vous a déjà présenté dans son tutoriel sur la migration : j'ai nommé Search and Replace DB !

Je vous rappelle brièvement comment procéder (faites tout de même une sauvegarde avant au cas où !) :

- **Téléchargez le script** et décompressez-le sur votre ordinateur ;
- **Placez-le à la racine de votre site** en renommant son dossier (par exemple "kjhdqiuyrezeaz") ;
- **Indiquez l'adresse de votre site SANS HTTPS** dans le champ *replace* : http://monsite.com (et sans / à la fin !) ;
- **Indiquez l'adresse de votre site AVEC HTTPS** dans le champ *with* : https://monsite.com (et toujours pas de / à la fin !) ;
- **Cliquez sur *dry run*** pour voir si ça fonctionne bien ;
- **Cliquez sur *live run*** pour tout remplacer dans votre base de données ;
- **Cliquez sur *delete me*** pour supprimer le script de votre serveur.

Une fois l'exécution du script terminée, tous les liens insérés dans vos articles, pages, menus et dans les réglages du site seront désormais en HTTPS.

Pour vous en convaincre, connectez-vous à votre site et allez dans *Réglages > Général*. Vous devriez voir que les adresses ont été mises à jour :

Votre site est toujours vivant ? Alors on continue !

3. Vérifier les ressources chargées par le thème

Bon ici, je vous avoue que ça se corse un peu. Parfois, il arrive que le thème charge toujours des fichiers (CSS, JS ou autre) en HTTP au lieu de HTTPS. On appelle ça les contenus mixtes (mixed content en anglais).

On pourrait être tenté de penser que ce n'est pas bien grave mais en fait si, car la page ne sera pas entièrement sécurisée.

Résultat des courses, le précieux cadenas vert risque de ne plus être affiché par votre navigateur (et exposera votre visiteur à des attaques).

À qui la faute ?

À l'auteur du thème ! (ou à vous si vous l'avez bidouillé n'importe comment)

Pour régler ça, il va falloir mettre les mains dans le code et corriger les ressources chargées en HTTP. Vous pourrez vous aider de l'inspecteur de code de votre navigateur pour traquer les contenus mixtes (via l'onglet console).

Comme vous pouvez le voir ci-dessus, le contenu mixte n'est pas chargé par le navigateur (en l'occurrence un iframe).

Pour en savoir plus sur ce problème et comment les détecter, jetez un oeil à cet article du Journal du Net qui est très bien fait.

> Rendez-vous également en fin d'article pour découvrir des extensions pour corriger ce problème quasi automatiquement.

4. Forcer le HTTPS dans l'administration

Ce n'est pas parce que l'on fournit une version du site en HTTPS aux visiteurs qu'il faut s'en passer dans l'administration, n'est-ce pas ?

Normalement, ça devrait déjà être le cas grâce aux redirections mises en place précédemment mais vous pouvez insérer ce code dans le fichier wp-config.php pour forcer cela :

```
// Forcer le HTTPS dans l'administration
define('FORCE_SSL_ADMIN', true);
```

Au moins, vous serez certain que WordPress se charge bien en HTTPS.

5. Mettre à jour le fichier robots.txt

Continuons avec l'édition de fichiers avec robots.txt. Ce fichier normalement situé à la racine de votre site permet de dire aux robots d'indexation ce qu'ils peuvent faire sur votre site.

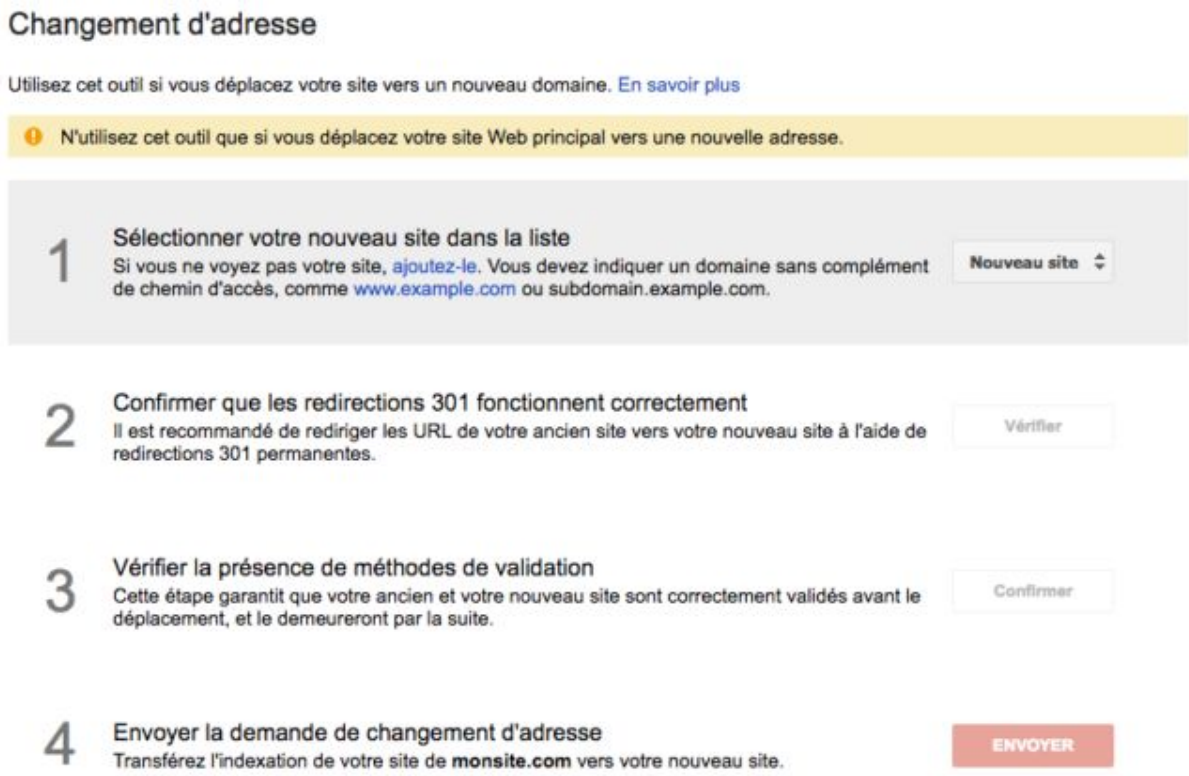
Ici, il n'y a pas grand chose à faire à part mettre à jour l'adresse du sitemap de votre site. Vous n'aurez qu'à ajouter un "s" :)

6. Mettre à jour votre site dans Google Search Console

La Marmite n'a pas encore abordé le sujet en détail mais Google Search Console sert à suivre l'indexation de votre site par Google. C'est donc un outil incontournable pour tous les webmasters !

Si vous l'utilisez, il n'est malheureusement pas possible de spécifier que votre site est désormais en HTTPS. Il faudra suivre les instructions de Google pour ajouter votre site.

Pour cela, cliquez sur l'engrenage en haut à droite de GSC (Google Search Console), cliquez sur *Changement d'adresse* et laissez-vous guider.



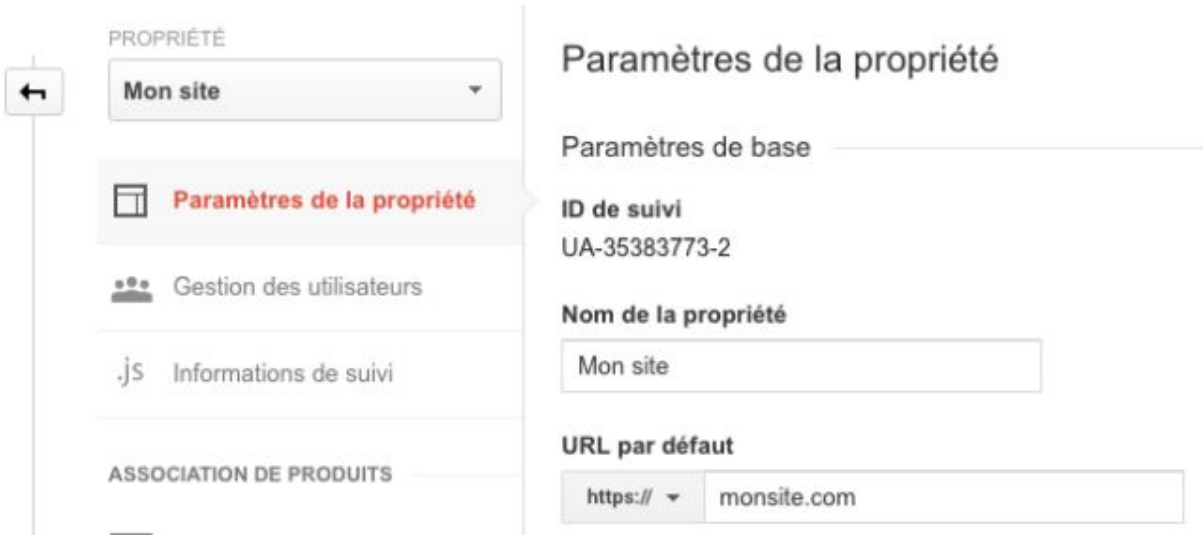
Nous aurons l'occasion de revenir plus en détail sur GSC prochainement. Abonnez-vous à la newsletter pour être prévenu ;)

7. Mettre à jour Google Analytics

Eh oui, il ne faut pas l'oublier celui-là ! Ça a failli m'arriver avec la Marmite...

Contrairement à GSC, vous n'aurez pas à supprimer votre site pour le rajouter ensuite (sinon vous perdriez toutes vos statistiques !).

Pour dire à Google Analytics que votre site utilise désormais le HTTPS, rendez vous dans *Admin > Propriété (de votre site) > Paramètre de la propriété* et sélectionnez https:// pour le champ URL par défaut :



Allez, reprenez votre souffle, on arrive bientôt au bout de cet article (bravo vous venez de parcourir plus de 3500 mots !).

8. Attention aux compteurs des boutons de partage

Inévitablement, vous si vous utilisez les boutons de partage officiels de Facebook, Twitter ou autre, les compteurs vont être réinitialisés.

En effet, les URL n'étant plus les mêmes, **pour les réseaux sociaux il ne s'agit plus du même partage !**

Vous allez perdre tous vos partages sociaux...

C'est bête mais vous ne pouvez rien y faire si vous utilisez les boutons officiels. Il ne vous restera plus qu'à obtenir de nouveaux partages pour vos contenus (d'où l'intérêt de passer au HTTPS le plus rapidement possible).

Toutefois, sachez qu'il vous reste une chance de les récupérer.

L'extension premium Social Warfare, vous donnera la possibilité d'afficher le bon nombre de partages pour vos contenus (HTTP + HTTPS).

9. Tester votre certificat SSL/TLS

Enfin, quel que soit le certificat que vous aurez choisi, sachez que vous avez la possibilité de le tester sur ce site. Cela prend un peu de temps mais à la fin vous aurez un tableau présentant les statistiques importantes ainsi qu'une note globale.

Vous pouvez voir que la Marmite s'en sort plutôt bien :)

Ce test vous permettra de vous assurer que vous n'êtes pas vulnérable à certaines failles SSL.

Et les extensions WordPress liées au HTTPS alors ?

Il est vrai qu'il existe pas mal d'extensions pour optimiser des sites en HTTPS sur le répertoire officiel.

Certaines d'entre-elles proposent des fonctionnalités intéressantes mais d'autres sont totalement inutiles. Regardons cela de plus près :

WordPress HTTPS

Je ne pense pas me tromper en disant qu'il s'agit de l'extension qui est la plus recommandée. Pourtant, elle n'a pas été mise à jour depuis 3 ans (oui, ça pique) et elle a déclenché une erreur lorsque je l'ai installée.

Malgré tout, elle semble fonctionner correctement.

Elle permet notamment de :

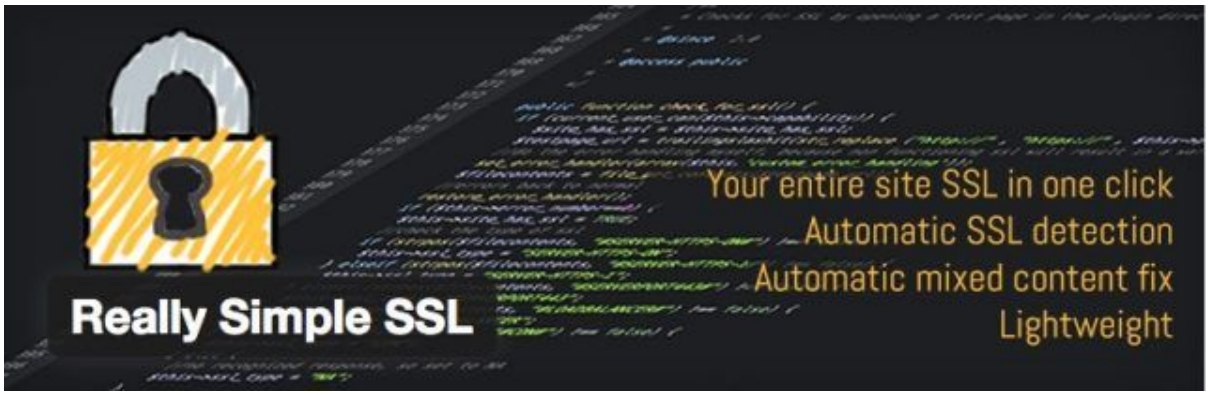
- Rediriger les pages chargées en HTTP vers leur version HTTPS (chose inutile dans notre cas car nous avons géré cela précédemment dans le fichier .htaccess) ;
- Ne pas charger les éléments indisponibles en HTTPS ;
- Charger des ressources externes via leurs serveurs sécurisés (par exemple Gravatar) ;
- Se servir du HTTPS sur certaines pages ou articles.

Cette dernière fonctionnalité peut s'avérer intéressante si vous ne désirez pas perdre vos compteurs de partage. Vous pourrez garder vos pages et articles populaires en HTTP et passer tout le reste en HTTPS.

Je suis cependant septique à l'idée d'employer cette extension étant donné que l'auteur ne semble pas décidé à la mettre à jour.

Voir cette extension sur le répertoire officiel (mais je ne vous la recommande pas)

Really Simple SSL



Cette extension est celle qui est la mieux maintenue à jour. Elle est également très légère et se configure rapidement (en fait, je n'ai rien eu à faire !).

Comme pour l'extension précédente, Really Simple SSL permettra de rediriger les pages chargées en HTTP vers HTTPS (jusque là, rien d'extraordinaire).

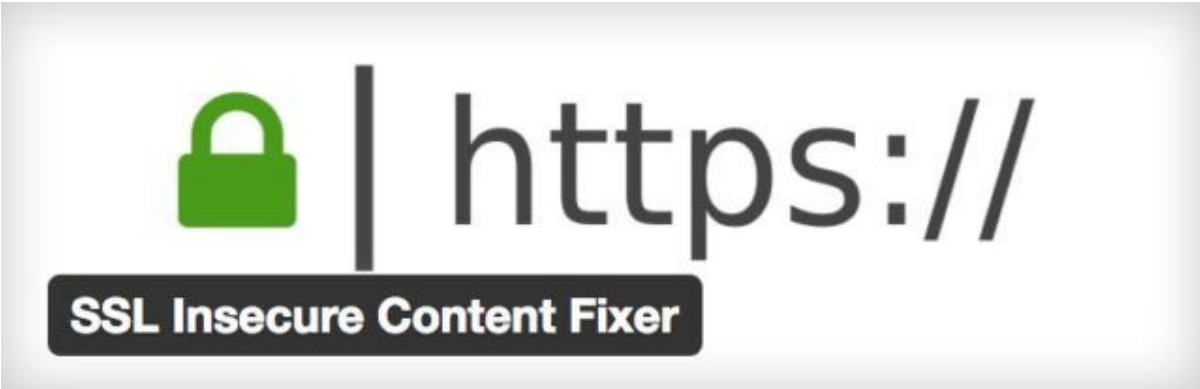
Là où ça devient plus intéressant, c'est au niveau de la gestion du contenu mixte. Vous vous rappelez, ce sont ces éléments qui ne sont pas chargés en HTTPS sur les pages et qui empêchent l'apparition du petit cadenas vert.

Eh bien cette extension remplace dynamiquement les adresses des ressources pour qu'elles soient chargées correctement.

Le seul cas où cela ne pourrait pas fonctionner serait où la ressource à afficher serait placée sur un autre serveur ne disposant pas d'un certificat SSL. Il vous faudrait alors rapatrier cette ressource sur votre site et mettre à jour son adresse.

Voir cette extension sur le répertoire officiel (une version pro est aussi disponible avec davantage de fonctionnalités)

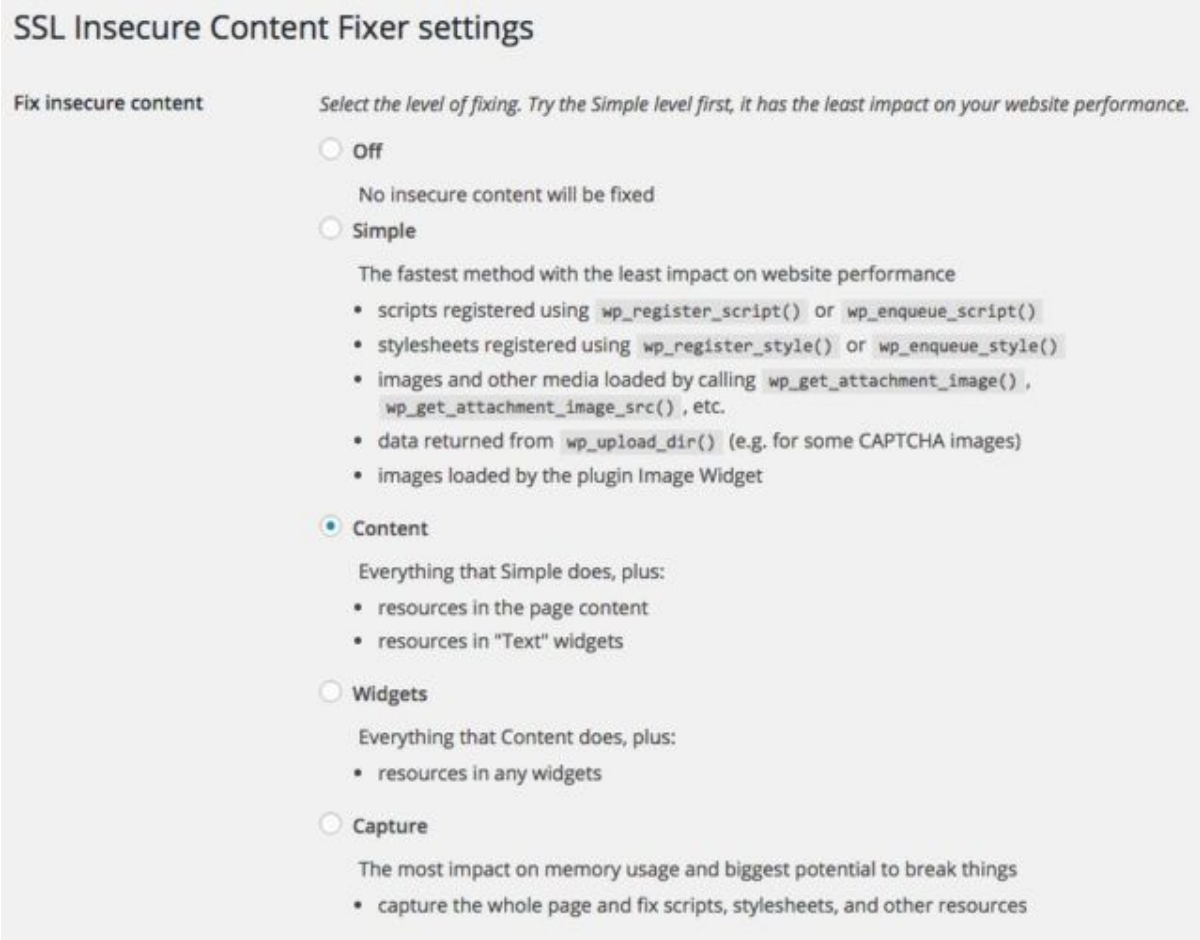
SSL Insecure Content Fixer



Si vous avez décidé de gérer les redirections au niveau du fichier **.htaccess**, il ne vous reste plus qu'à gérer les éventuels problèmes de contenus mixtes.

Ça tombe bien, une extension a été développée exclusivement pour ça : SSL Insecure Content Fixer.

Une fois que vous l'aurez installée, vous pourrez définir le niveau de correction à employer sur votre site :



Vous pourrez choisir entre :

- **Off** : Pour ne rien corriger (vous n'aurez donc pas de cadenas vert) ;
- **Simple** : Pour corriger la plupart des problèmes ;
- **Content** : Pour analyser et corriger vos publications et widgets textes ;
- **Widgets** : Pour analyser et corriger les ressources de n'importe quel widget ;
- **Capture** : C'est le mode barbare. Cela analysera le contenu et les ressources de toutes vos pages et les corrigera (par contre, cela sera gourmand en ressources).

Personnellement, je vous conseille de sélectionner *Content*. Si vous avez encore des soucis, essayez avec les niveaux suivants.

Si le problème persiste toujours, vous n'aurez pas d'autre choix que de régler cela manuellement. Ouvrez l'inspecteur de code, allez dans l'onglet

Console, repérez d'où vient le problème et corrigez-le dans votre thème ou votre contenu.

Voir cette extension sur le répertoire officiel (je vous la recommande si vous ne voulez pas trop vous salir les mains).

Conclusion : Restez sur vos gardes

Ça y est, vous avez à présent un site sécurisé grâce à un certificat SSL/TLS. Vos visiteurs peuvent donc accéder à votre site en HTTPS.

Grâce à vous, ils seront certain de bien avoir accès à votre site (et non pas une version modifiée par un malfrat du web) et personne ne pourra savoir qu'ils feront sur votre site (sauf vous bien sûr).

Cependant, le HTTPS ne fait pas tout !

Par exemple dans le cas d'une boutique en ligne, si vos clients utilisent des mots de passe foireux, on pourra toujours tenter d'accéder à leur compte afin de passer des commandes en leur nom.

Pour lutter contre ça, vous pouvez leur générer automatiquement des mots de passe, changer l'adresse de la page de connexion et limiter les tentatives de connexion.

Il y a bien d'autres choses à faire pour sécuriser son site, nous aurons l'occasion d'en reparler prochainement !

Comptez passer au HTTPS prochainement ? Et si vous l'avez déjà fait, pour quel certificat avez-vous opté ? Utilisez-vous une

extension en complément ? Dites-moi tout en commentaire sur la Marmite ;)