Comment passer son site WordPress en HTTPS

Merci d’avoir d’avoir téléchargé cet article. J’espère que les conseils qu’il contient vous aideront à mettre en place le HTTPS sur votre site.

Bonne lecture et à bientôt sur WPMarmite.com

Pour commencer, sachez que le bon de réduction de 15% chez o2switch est :

WPM15

Si vous voulez me renvoyer l'ascenseur pour ce coupon, le tutoriel vidéo et tout ce dont je parle dans cette fiche récap, passez votre commande en cliquant sur ce lien.

En procédant ainsi, je toucherai une petite commission qui récompensera mon travail (sans que cela vous coûte rien).

Merci de votre soutien !

Publié par Alex le 11 juillet 2016 • 488 Commentaires

“Votre connexion à ce site n’est pas sécurisée.” Un brin interloqué, je me frotte les yeux pour bien vérifier le message que je suis en train de lire.

Mais non, pas de doute. Toujours cette même phrase placardée sur mon navigateur.

Un peu plus bas, on m’indique même que certaines informations pourraient être “dérobées par des pirates informatiques”.

Légende : **Et pas des pirates rigolos, des vraiments méchants...**

Allez, ouste, cela fait déjà beaucoup pour ce site : je ferme sa fenêtre illico presto.

Pourquoi un message aussi alarmant, véritable repoussoir à internaute ?

Simplement parce que le site WordPress sur lequel je suis en train de naviguer n’utilise pas le HTTPS, qui permet de sécuriser la connexion à un site.

Sur WPMarmite, je m’y suis mis en mai 2016. Et franchement, je ne le regrette pas du tout.

Si vous ne faites pas encore partie de la famille HTTPS, je vous invite à vous pencher sérieusement sur la question.

Pourquoi passer en HTTPS ? Comment y parvenir, et avec quels outils ? Qu’est-ce que cela change concrètement ?

C’est ce que nous allons voir dans ce nouvel article.

Accrochez vos ceintures, voici le sommaire :

Sommaire

Info : Cet article est assez long (plus de 5 000 mots). Si le sujet vous intéresse et que vous n’avez pas le temps de vous y plonger pour le moment, téléchargez-le au format PDF (en bonus, vous trouverez un code de réduction pour créer votre site chez o2switch). Cliquez ici pour le télécharger.

Qu’est-ce que le HTTPS ?

L’HTTPS (HyperText Transfer Protocol Secure), que l’on traduit en français par Protocole de transfert hypertexte sécurisé, désigne ***“un mode de sécurisation technique des données échangées entre le serveur visité et les internautes”.***

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 rôde 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).**

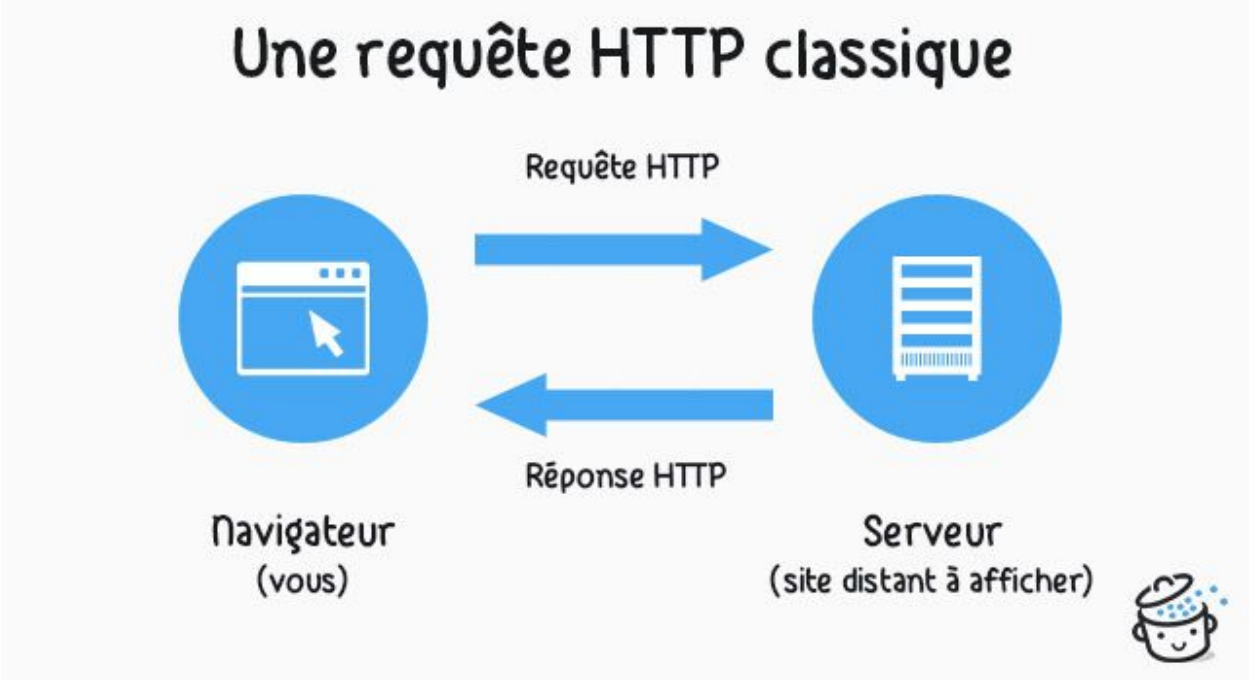
Encore mieux, vous serez certain de bien visualiser le site original, et non une version modifiée par quelqu'un qui aurait intercepté la connexion. Eh oui, beaucoup de choses sont possibles en informatique !

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.

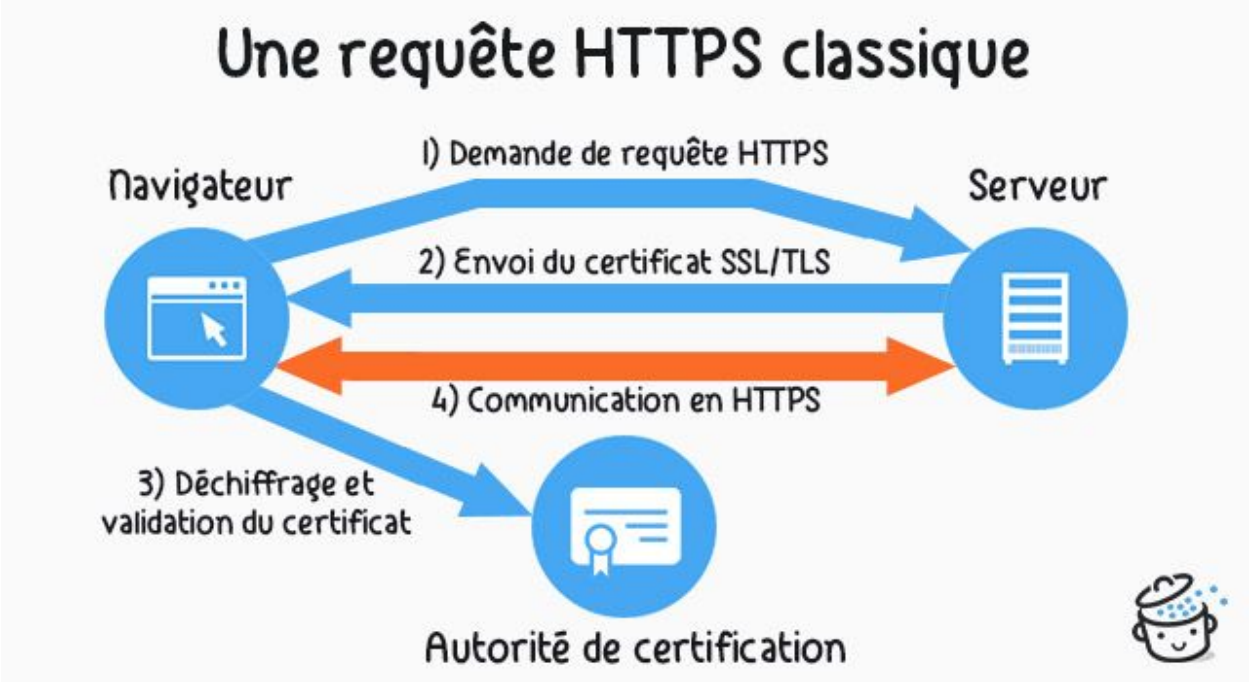


Dès que vous entrez une adresse dans votre navigateur, il envoie une requête HTTP pour demander la page. Le serveur la renvoie et le navigateur l'affiche. Plutôt facile, n'est-ce pas ?

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].

Que signifient les acronymes SSL et TLS ?

Pour mettre en place le HTTPS sur un site, vous allez avoir besoin d'**un certificat SSL/TLS, qui va permettre d'établir une connexion sécurisée en la chiffrant, et de vérifier l'identité du site** (suis-je bien connecté au site que je veux visiter ?).

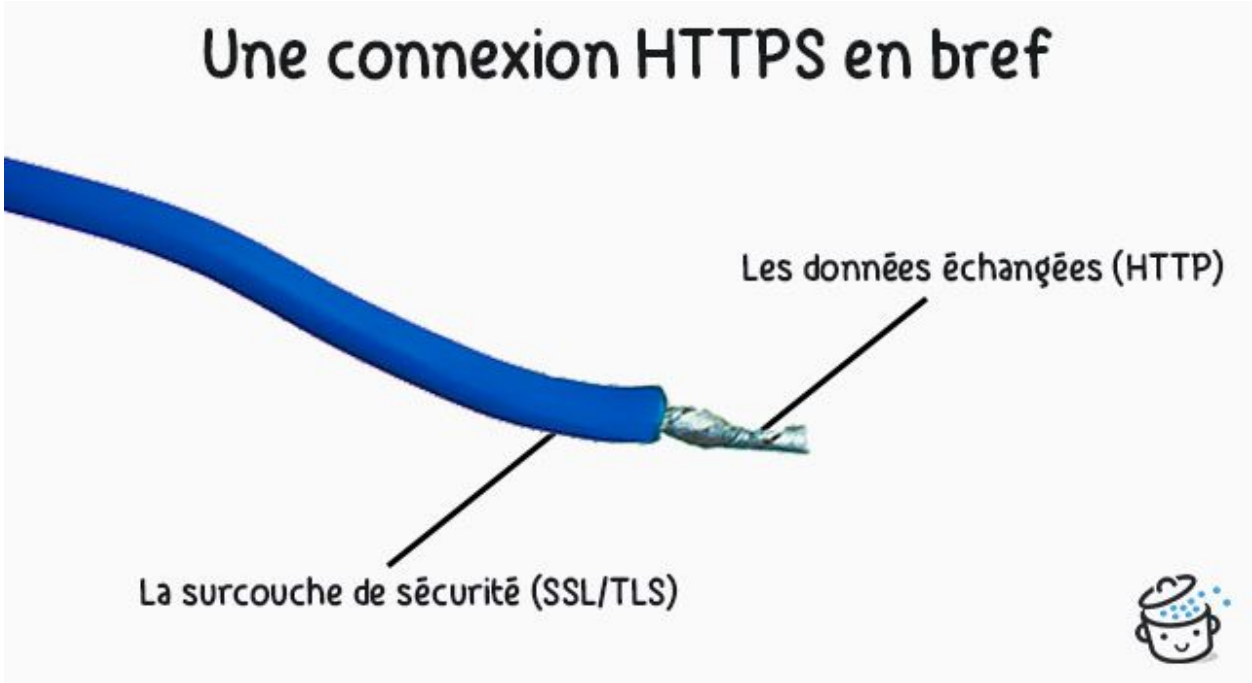


<u>Légende</u> : Tout cela se passe très vite, on n'y voit que du feu

Le certificat SSL dont je vous parle est délivré par ce que l'on appelle une autorité de certification.

Il en existe des dizaines, et les plus connues sont Comodo et GlobalSign.

Pour y voir plus clair, et de façon imagée : 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 câble 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 relais pour plus de sécurité.

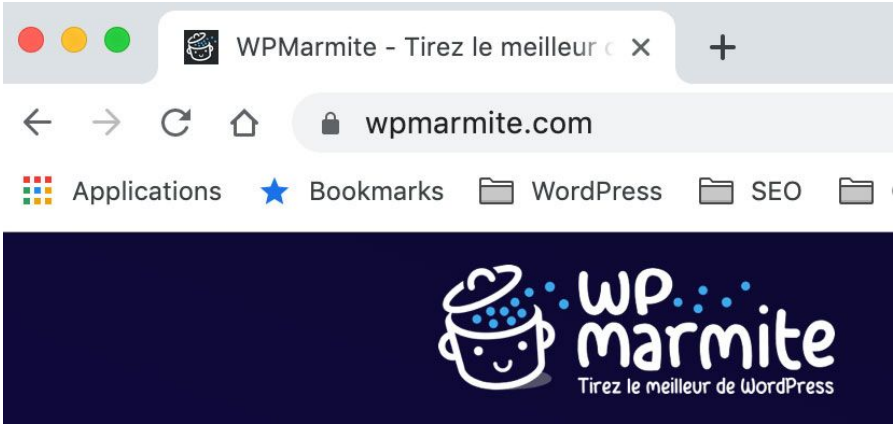
Si cela vous intéresse, vous retrouverez l'historique complet sur Wikipédia.

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://.

Côté visuel, les navigateurs mettent en valeur les sites dotés du HTTPS grâce à un petit cadenas placé juste avant l'adresse.

Voici l'exemple de WP Marmite avec Google Chrome :



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 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).

Pourquoi passer WordPress en HTTPS ?

HTTPS et SEO : un impact vraiment notable ?

En 2014, Google a annoncé que le HTTPS était désormais considéré comme un signal pris en compte pour le référencement des sites (parmi 200 autres critères).

Est-ce que cela peut réellement améliorer votre SEO ? Difficile à affirmer, d'autant que les avis divergent...

De mon côté, je ne peux pas vraiment vous avouer que le positionnement de WPMarmite a beaucoup progressé grâce à ça.

C'est aussi le constat qu'a fait Daniel Roch, spécialiste du SEO sur WordPress au sein de l'agence SeoMix.

Dans cet article, il indique que ***"selon nos tests et ceux de nombreux confrères, le HTTPS n'améliore pas le référencement naturel"***.

En 2016, Brian Dean, un spécialiste américain du SEO, a lui analysé 1 million de résultats de recherche Google.

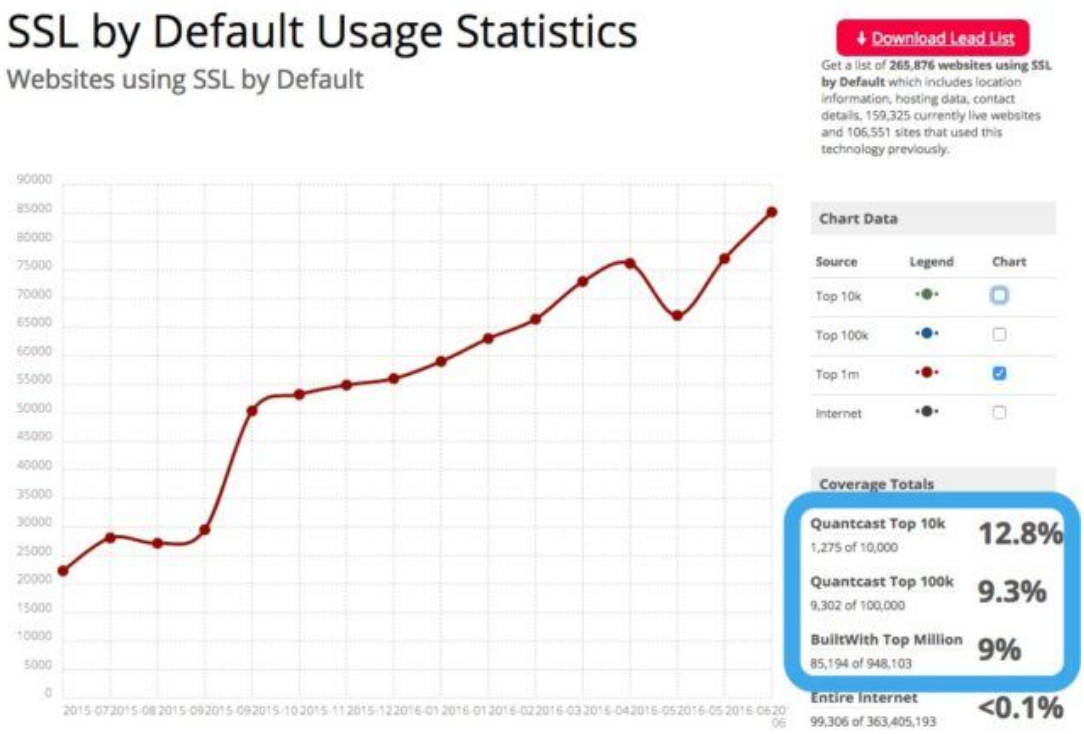
Parmi ses conclusions, il a relevé que **le HTTPS était** ***"moyennement corrélé avec un meilleur positionnement"***.

Dernier point de vue, pour clore le débat : celui d'Olivier Andrieu, l'un des pontes du référencement naturel en France.

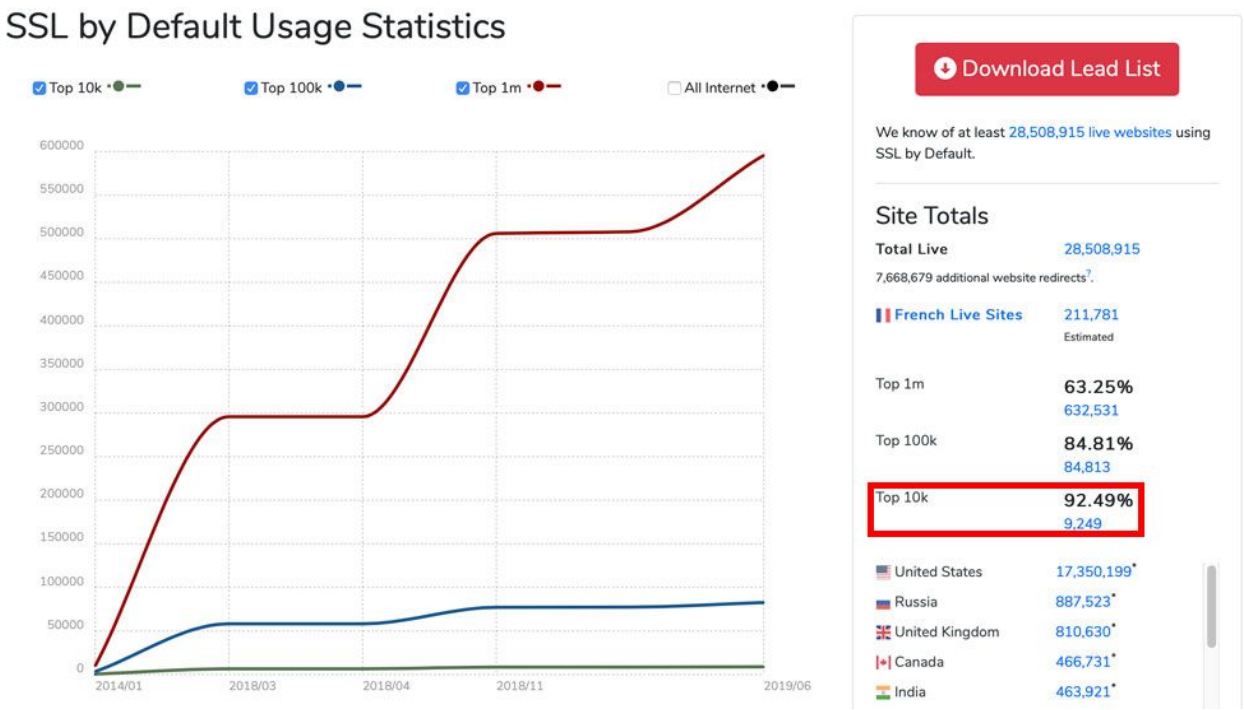
Une conférence de SEMRush sur le HTTPS hyper-intéressante rapporte ses propos : *"depuis novembre 2016, nous avons constaté que les sites web qui étaient passés au HTTPS avait amélioré leur classement dans les résultats de Google"*.

Vous le voyez, l'impact du HTTPS sur le SEO n'est pas encore vraiment tranché.

Une chose est sûre, cela n'empêche pas les internautes de se ruer sur le HTTPS. Jugez plutôt : en 2016, "seuls" 12,8% des 10 000 sites recevant le plus de trafic disposaient d'un certificat SSL.



Trois ans plus tard, ils sont désormais 92,49% (au moment d'écrire ces lignes) !



Comment expliquer ce regain et cette tendance de fond ? Réponse dans la partie suivante.

Passez en HTTPS pour renforcer la sécurité et la confiance de vos visiteurs

Puisque l'impact sur le SEO reste encore à démontrer (personne n'est vraiment d'accord), il est surtout devenu indispensable de disposer d'un site HTTPS pour deux raisons :

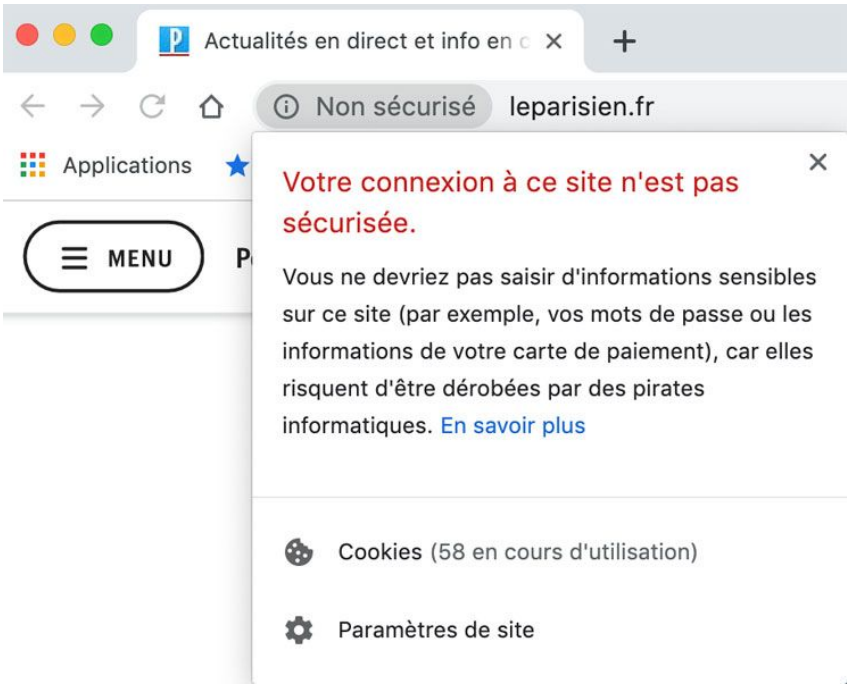
- **La sécurité**
- **L'expérience utilisateur**

Voici ce qu'indique Google sur le premier point : "Les internautes s'attendent à bénéficier d'une expérience en ligne sécurisée et confidentielle lorsqu'ils consultent un site Web. Nous vous encourageons à adopter le protocole HTTPS afin de permettre aux internautes de consulter votre site Web en toute sécurité, quel que soit son contenu."

De façon plus générale, l'objectif de Google consiste à *"rendre le web plus sécurisé"*.

Et depuis juillet 2018, l'entreprise basée à Mountain View a franchi un cap supplémentaire dans ce sens.

Son navigateur Google Chrome sanctionne en effet les sites en HTTP en indiquant à l'internaute qu'il navigue sur une page qui n'est pas sécurisée.



<u>Légende</u> : Pour le moment, le site web du quotidien régional Le Parisien ne s'est pas mis au HTTPS.

Sachant que Chrome est utilisé par 60% des internautes en France (chiffres juillet 2019), passer au HTTPS reste primordial.

Pour renforcer l'expérience utilisateur et donner confiance à vos visiteurs, vous vous doutez bien qu'un simple petit cadenas devient hyper-important.

Quand on le voit, on est de suite rassuré (même inconsciemment). C'est normal : quand on arrive sur un site que l'on ne connaît pas, on cherche à prendre ses marques.

En voyant un site au design propre, une bonne communauté et des URLs en 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).

Ce genre de sites, on a tous envie de les éviter. Parce que tomber sur des escrocs, des charlatans, et des guignols, non merci !

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

Pour enfoncer le clou, 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) !

En plus, la plupart des passerelles de paiement (type Stripe, PayPal) vous réclameront d'avoir une connexion HTTPS pour que vos visiteurs puissent procéder à des achats.

Vous le voyez : rien que pour la sécurité de votre site et la confiance de vos visiteurs, il me semble indispensable de mettre en place le HTTPS sur WordPress.

Pour être tranquille, je vous recommande d'y passer dès que 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.

Google considère cela comme *"un déplacement de site avec changement d'URL. Cela peut affecter temporairement vos chiffres de trafic."*

À présent, voyons…

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.

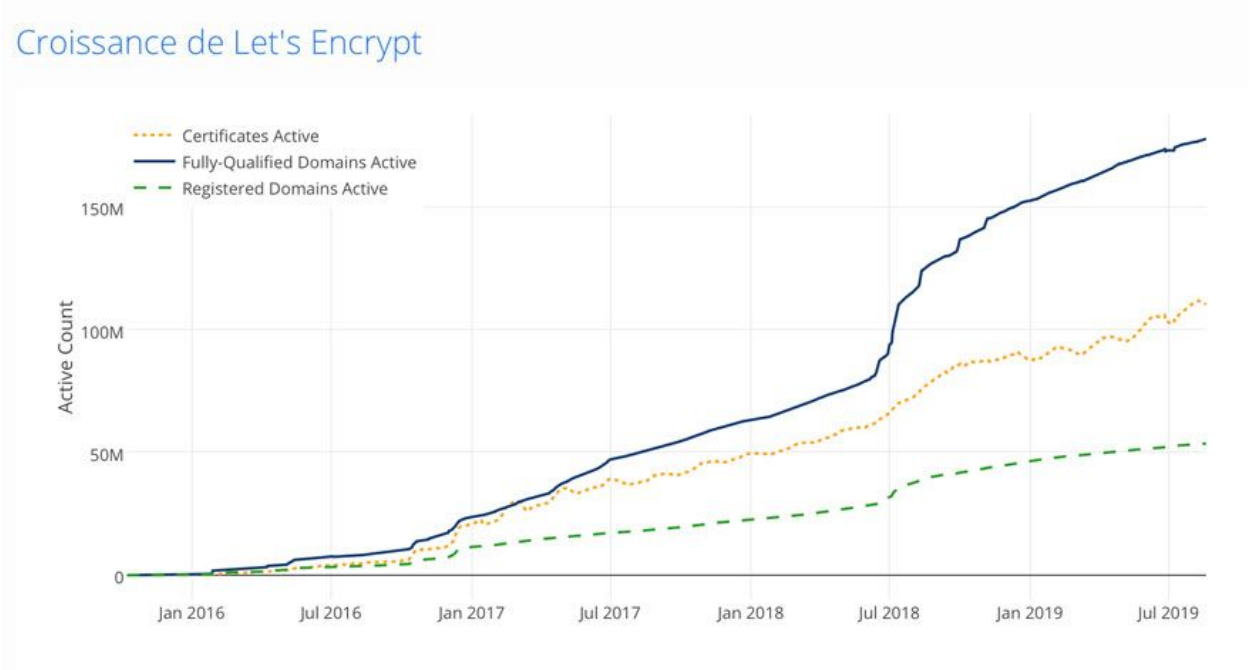
Aujourd'hui, il est toujours possible de procéder ainsi (c'est même recommandé dans certains cas) mais un nouvel acteur est apparu…

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, OVH, Shopify, 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 portefeuille.

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 1,5 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 de trois types :

- **Les certificats à validation de domaine (DV)** : Dans ce cas, l’autorité de certification vérifiera juste que vous êtes bien propriétaire du nom de domaine pour vous accorder le petit cadenas (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. A noter, à ce propos, que *“l’équipe de développeurs de Google Chrome annonce mettre fin à l’affichage spécifique supposé signaler les noms de domaines disposant d’un certificat EV”*.

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.

Note : 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 ?

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, une grande majorité d’hébergeurs proposent à leurs clients des certificats SSL gratuits générés par Let’s Encrypt.

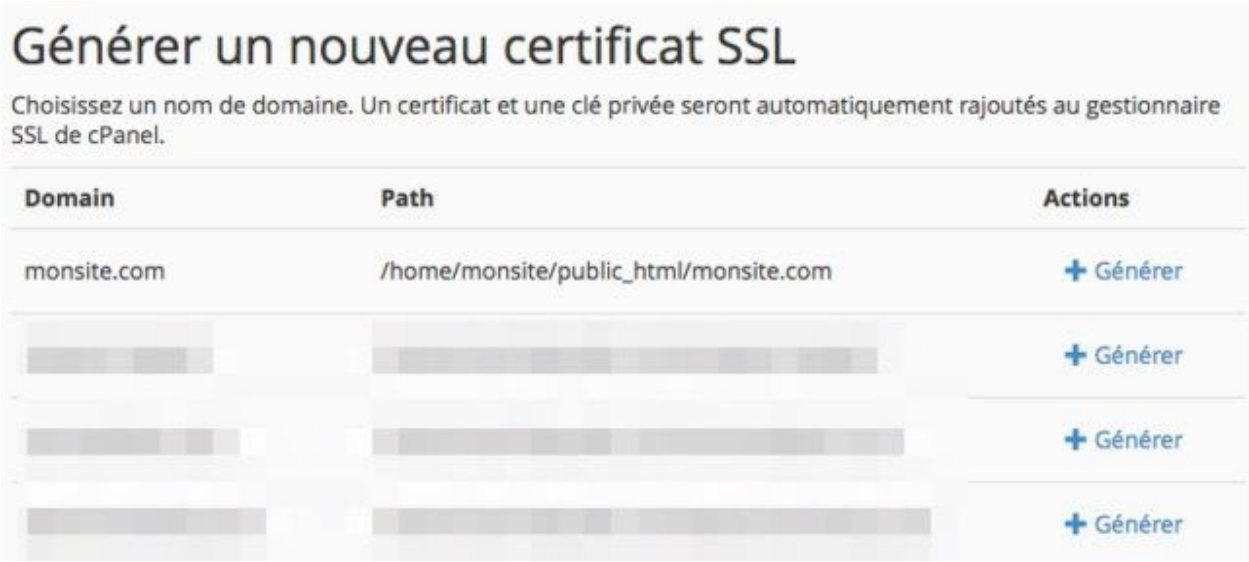
C’est le cas d’OVH, de Gandi mais aussi d’o2switch, l’hébergeur que j’ai choisi pour WPMarmite.

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 !).

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

Dans la section *Sécurité*, cliquez sur *Lets Encrypt* SSL :

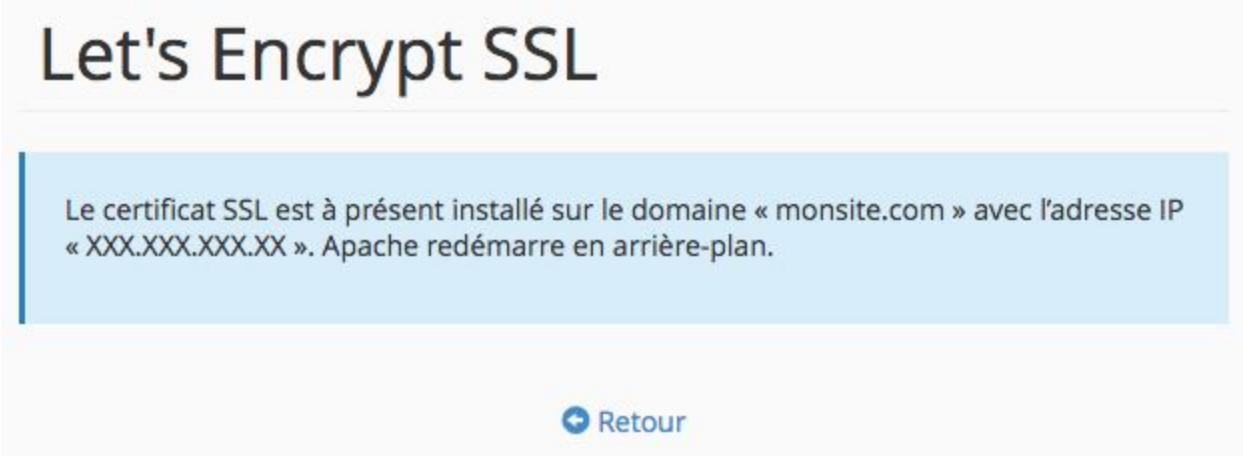
Cliquez ensuite sur le lien *+ Générer* en face du domaine que vous comptez sécuriser :



Vous pouvez aussi installer un certificat sur votre boîte 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 tous les 3 mois. 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 tâches diffère légèrement si vous partez d’un site vierge, ou s’il s’agit d’une migration de HTTP vers HTTPS, mais il 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]
```

Si votre site utilise le *www*, il faudra utiliser le code suivant pour la redirection :

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

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

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

C'est très pratique car dans le cas de WPMarmite, 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 désiriez utiliser HTTPS ou non, il vous faudra mettre en place des redirections, sinon aurez des problèmes de contenus dupliqués.*

Attention si vous êtes chez 1&1 : Si une erreur du genre de « cURL error 35: error:140770FC:SSL routines:SSL23_GET_SERVER_HELLO:unknown protoc » se produit, essayez de supprimer les redirections et ça devrait fonctionner.

2. Remplacer les URLs en HTTP

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

Rassurez-vous, nous n'allons pas faire cela à la main, mais avec un script que WPMarmite 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).

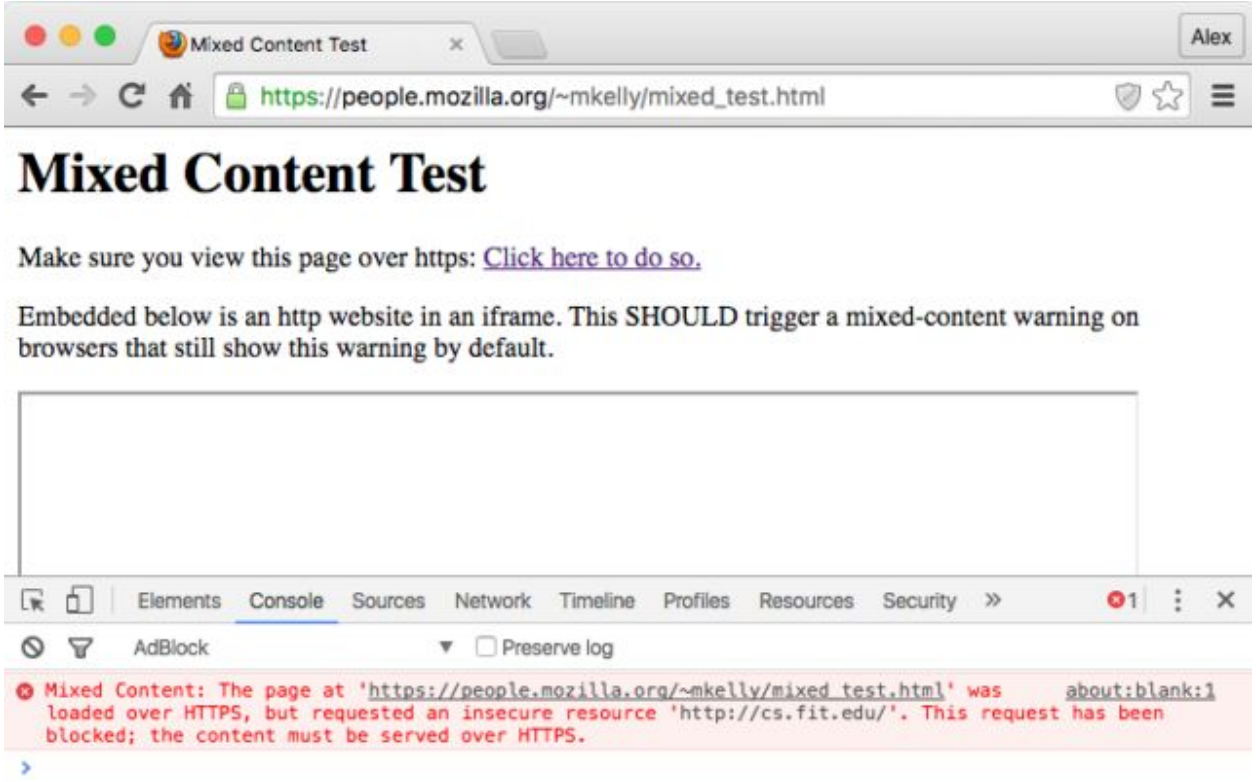
On pourrait être tenté de penser que ce n'est pas bien grave mais en fait si, car la page ne sera pas entièrement sécurisée.

Résultat des courses, le précieux cadenas 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.

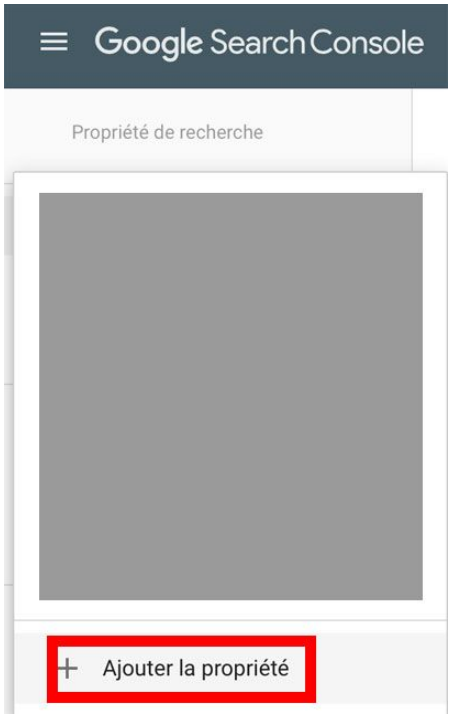
Vous n'aurez qu'à ajouter un « s ».

6. Mettre à jour votre site dans Google Search Console

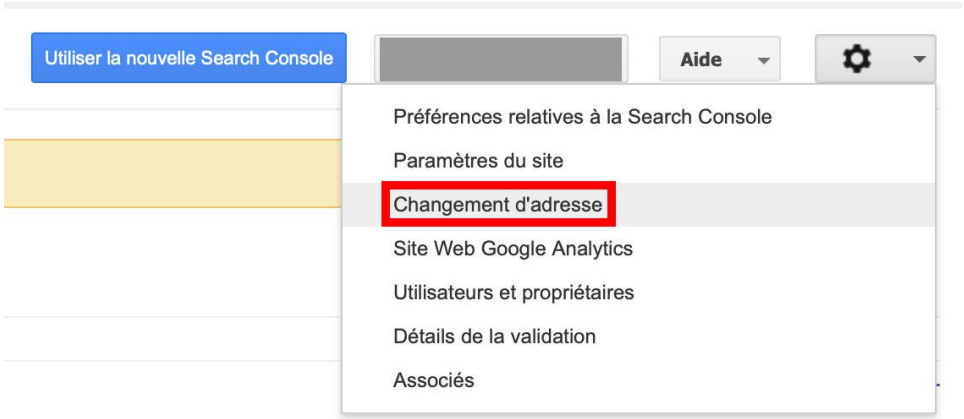
La Google Search Console (GSC) est un outil incontournable pour tous les webmasters. Il permet de mieux gérer votre site et de suivre votre référencement en fournissant tout un tas d'infos (erreurs sur votre site, analyse de la recherche, liens, état de l'indexation, erreurs d'exploration etc.).

Si vous l'utilisez, il va falloir signifier à Google votre passage au HTTPS en ajoutant ce que l'on appelle une nouvelle propriété (un nouveau site, en quelque sorte) car *"la Search Console traite séparément les protocoles HTTP et HTTPS"*.

Pour ce faire, choisissez *Ajouter la propriété* dans le menu situé en haut, à gauche, de la nouvelle Search Console.



Si vous utilisez l'ancienne version de la GSC, vous pouvez aussi utiliser la fonction *Changement d'adresse* présente dans l'engrenage, une fois que vous avez sélectionné votre site.



Ensuite, laissez-vous guider.

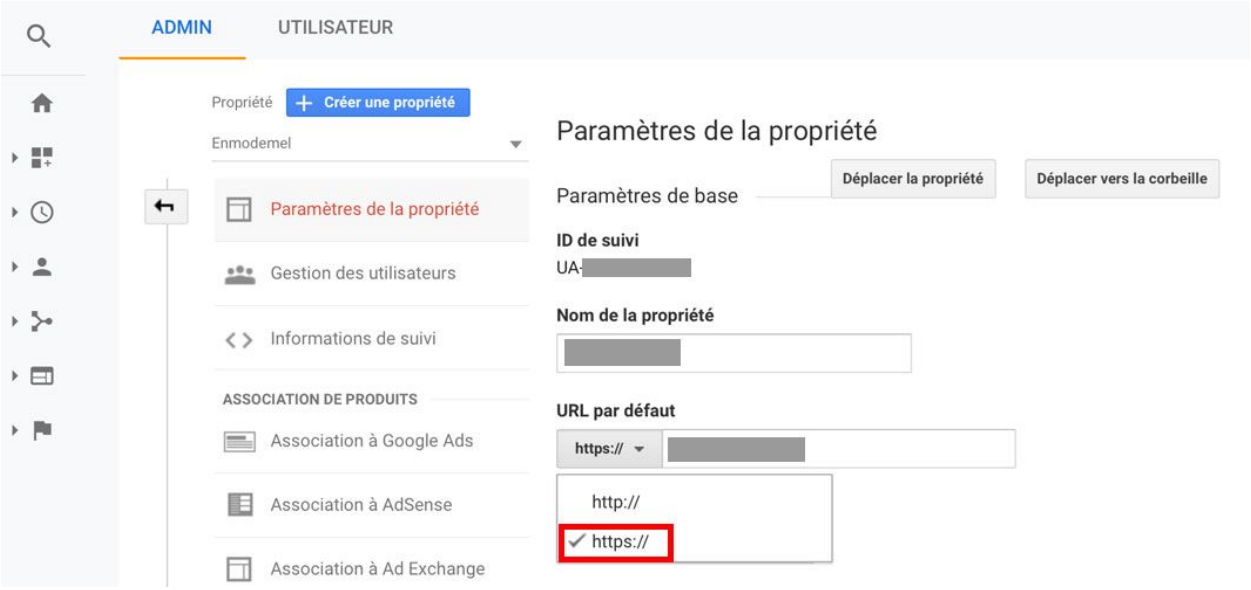
7. Mettre à jour Google Analytics

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

Google Analytics est un outil statistique qui vous donne accès à tout un tas d'informations concernant le trafic de votre site.

Comme la GSC, il est très utile et gratuit, donc ne vous en privez pas.

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



8. Attention aux compteurs des boutons de partage

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

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

***Légende* : 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 WPMarmite s’en sort plutôt bien.

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

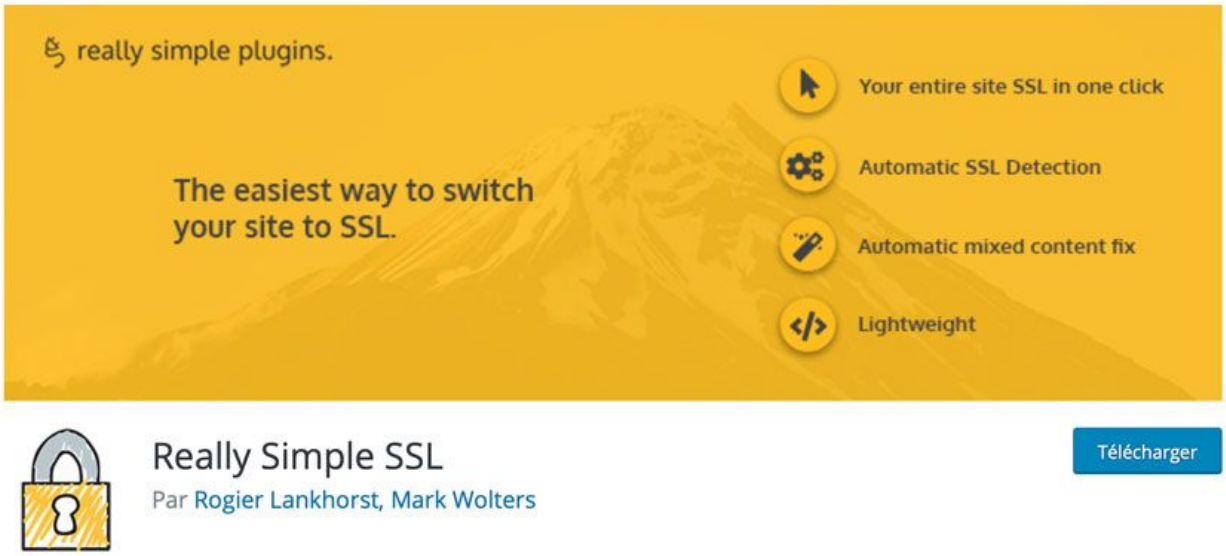
Note : Je vous ai présenté 9 points de contrôle généraux et incontournables mais, de façon générale, pensez à signaler à tous les outils que vous utilisez que votre site est désormais accessible en HTTPS. La plupart du temps, cela sera possible à réaliser via leurs réglages.

Et les extensions WordPress liées au HTTPS, alors ?

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

Certains d'entre-eux proposent des fonctionnalités intéressantes, mais d'autres sont totalement inutiles. Regardons cela de plus près.

Really Simple SSL



Really Simple SSL est tout simplement l'extension la plus populaire sur notre sujet du jour (une version pro est aussi disponible avec davantage de fonctionnalités)..

Elle cumule plus de 3 millions d'installations actives (soit plus qu'Elementor qui en compte 2 millions !) et possède une note de 5 étoiles.

Parmi ses atouts : **sa facilité d'utilisation**. Elle se configure rapidement (en fait, je n'ai rien eu à faire) et elle est très légère.

Du coup, pas besoin de toucher à des fichiers ou autres : je vous la recommande si vous ne voulez pas vous salir les mains.

Elle permet de rediriger les pages chargées en HTTP vers HTTPS de façon automatique (jusque là, rien d'extraordinaire).

Là où ça devient plus intéressant, c'est au niveau de la gestion du contenu mixte.

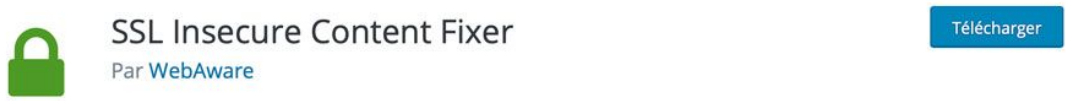
Vous vous rappelez, ce sont ces éléments qui ne sont pas chargés en HTTPS sur les pages, et qui empêchent l'apparition du petit cadenas vert.

Ce plugin remplace dynamiquement les adresses des ressources pour qu'elles soient chargées correctement.

Le seul cas où cela ne pourrait pas fonctionner serait lorsque 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

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 (+ de 300 000 installations actives).

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

Réglages de SSL Insecure Content Fixer

Corriger le contenu non sécurisé

Choisir le niveau de correction. Essayez en premier le niveau Simple, qui a le plus faible impact sur les performances d'un site.

○ **Désactiver**

Aucun contenu ne sera sécurisé

◉ **Simple**

La méthode la plus rapide avec un faible impact sur les performances du site

- scripts enregistrés avec `wp_register_script()` ou `wp_enqueue_script()`
- stylesheets enregistrés avec `wp_register_style()` ou `wp_enqueue_style()`
- images et autres médias chargés avec `wp_get_attachment_image()` , `wp_get_attachment_image_src()` , etc.
- données venant de `wp_upload_dir()` (ex. pour certains codes CAPTCHA)
- images chargées par le plugin Image Widget

○ **Contenu**

Tout ce que le niveau Simple offre, plus :

- ressources du contenu de la page
- ressources dans le widget « Texte »

○ **Widgets**

Tout ce que le niveau Contenu offre, plus :

- ressources dans n'importe quel widget

○ **Capture**

Tout sur la page, de l'en-tête au pied de page :

- Capture la totalité d'une page, corrige les scripts, stylesheets et autres ressources
- exclut les appels AJAX, pour éviter certains problèmes de compatibilité et de performance

○ **Tout capturer**

Le plus grand potentiel pour casser des choses, mais parfois nécessaire

- Capture la totalité d'une page, corrige les scripts, stylesheets et autres ressources
- inclut les appels AJAX, qui peuvent causer des problèmes de compatibilité et de performance

Vous pourrez choisir entre :

- **Désactiver** : Pour ne rien corriger (vous n'aurez donc pas de cadenas) ;
- **Simple** : Pour corriger la plupart des problèmes ;
- **Contenu** : Pour corriger vos publications et widgets Texte, en plus de l'option Simple ;
- **Widgets** : Pour corriger les ressources de n'importe quel widget, en plus de l'option Contenu ;
- **Capture** : Pour corriger la totalité d'une page (scripts, feuilles de style et autres ressources), en excluant les appels AJAX.
- **Tout capturer** : C'est le mode barbare. Cela analysera le contenu, les scripts, les ressources et les appels AJAX de toutes vos pages et les corrigera (par contre, cela sera gourmand en ressources et peut causer des problèmes de compatibilité).

Personnellement, je vous conseille de sélectionner *Contenu*. 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]

WordPress HTTPS

On termine ce petit tour de table des extensions avec WordPress HTTPS. Avec plus de 100 000 installations actives, elle fait partie des plugins les plus utilisés sur le sujet.

Son principal souci, et il est de taille : elle n'a pas été testée avec plus de trois mises à jour majeures de WordPress, ce qui est assez embêtant.

Pour rappel, les mises à jour sont notamment importantes pour continuer à assurer la sécurité de votre site.

Si WordPress HTTPS a déclenché une erreur lorsque je l'ai installée, elle a ensuite semblé 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 sceptique à l'idée d'employer cette extension étant donné que l'auteur ne semble pas décidé à la mettre à jour.

Du coup, je ne vous la recommande pas.

Voir cette extension sur le répertoire officiel

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 WordPress en HTTPS.

Comme vous l'avez vu, l'impact sur le SEO reste encore à démontrer.

Par contre, l'influence sur l'expérience utilisateur et la sécurité n'est plus à prouver.

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 votre site. Si cet aspect vous intéresse, vous pouvez également consulter la série de vidéos Le Point Sécu, sur la chaîne YouTube de WPMarmite.

Sinon, de votre côté, 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.