eBook Gratuit

APPRENEZ https

eBook gratuit non affilié créé à partir des **contributeurs de Stack Overflow.**

#https

Table des matières

À propos

You can share this PDF with anyone you feel could benefit from it, downloaded the latest version from: https

It is an unofficial and free https ebook created for educational purposes. All the content is extracted from Stack Overflow Documentation, which is written by many hardworking individuals at Stack Overflow. It is neither affiliated with Stack Overflow nor official https.

Use the content presented in this book at your own risk; it is not guaranteed to be correct nor accurate, please send your feedback and corrections to info@zzzprojects.com

Chapitre 1: Démarrer avec https

Remarques

Cette section fournit une vue d'ensemble de ce qu'est https et pourquoi un développeur peut vouloir l'utiliser.

Il devrait également mentionner tous les grands sujets dans https, et établir un lien avec les sujets connexes. La documentation pour https étant nouvelle, vous devrez peut-être créer des versions initiales de ces rubriques connexes.

Examples

Démarrer avec HTTPS

HTTPS *(Hypertext Transfer Protocol Secure)* est une version cryptée du protocole HTTP, le plus souvent utilisée avec des services où seuls l'expéditeur et le destinataire doivent connaître le message. Il est nécessaire si vous gérez les informations de carte de crédit et améliorez votre classement sur Google.

Pour activer HTTPS, vous devez vérifier si votre hébergeur le prend en charge. Si vous ne le savez pas, vous pouvez demander leur assistance pour obtenir de l'aide et des informations à ce sujet. Certains hébergeurs peuvent prendre de l'argent pour cela.

> **Important!** : Votre HTTPS doit utiliser sha2 ou sha3 *(sha1 est bloqué par **Chrome** , **Firefox** , **Edge** et **IE**)*

Lorsque vous avez activé HTTPS sur votre hôte Web, vous pouvez utiliser HTTPS. Mais le navigateur n'utilise pas HTTPS par défaut; Le meilleur moyen de s'assurer que tout le trafic fonctionne sur HTTPS est d'utiliser un fichier .htaccess et de l'ajouter à la racine de votre site Web.

Le fichier .htaccess

```
RewriteEngine On

# If we receive a forwarded http request from a proxy...
RewriteCond %{HTTP:X-Forwarded-Proto} =http [OR]

# ...or just a plain old http request directly from the client
RewriteCond %{HTTP:X-Forwarded-Proto} =""
RewriteCond %{HTTPS} !=on

# Redirect to https version
RewriteRule ^ https://%{HTTP_HOST}%{REQUEST_URI} [L,R=301]
```

Cela changera le http: // en https: //.

REMARQUE : .htaccess est un fichier système et ne peut pas être vu par défaut.
Comment montrer .htaccess

Lire Démarrer avec https en ligne: https://riptutorial.com/fr/https/topic/2910/demarrer-avec-https

Chapitre 2: HTTP Strict Transport Security (HSTS)

Paramètres

Paramètre	Détails
`max-age=31536000`	Temps en secondes. HSTS sera appliqué pour cette période future.
`includeSubDomains`	HSTS devrait être appliqué pour ce domaine et tous ses sous-domaines.
`preload`	Ce domaine accepte d'être inclus dans une liste de pré-chargement HSTS

Remarques

Voir également

- MDN - Sécurité de transport HTTP stricte
- Wikipedia - Sécurité de transport HTTP stricte
- Liste de préchargement HSTS

Examples

En-tête HSTS

```
Strict-Transport-Security: max-age=31536000; includeSubDomains
```

`Strict-Transport-Security` est une promesse faite au navigateur que toutes les demandes futures sur ce domaine seront sécurisées.
Pour la future période `max-age` :

- Toutes les requêtes HTTP sortantes du navigateur seront converties en HTTPS *sur le client* (pas une redirection HTTP).
- Si le certificat est invalide (par exemple, obsolète ou autoproclamé), l'utilisateur ne pourra pas le répertorier et le site restera inaccessible.

Le comportement HSTS est destiné à éliminer les attaques Man-in-the-Middle qui utilisent la suppression HTTPS, l'émission de certificats non valides (et l'attente de l'utilisateur à ajouter et à l'exception) et la redirection sur les requêtes HTTP vers une autre destination.

Liste de préchargement HSTS

```
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
```

HSTS est activé uniquement après une demande HTTPS réussie au serveur avec un certificat valide. Il y a toujours un risque pour un utilisateur débutant d'accéder au site, auquel cas une attaque de type Man-in-the-Middle est possible.
Pour sécuriser le site avant même la première demande, le domaine peut être ajouté à une liste de préchargement , déjà configurée dans les navigateurs.
Le paramètre de `preload` n'est pas utilisé directement par les navigateurs, mais les développeurs du navigateur doivent savoir que les développeurs du site ont réellement demandé à être ajoutés à la liste de préchargement.

Lire HTTP Strict Transport Security (HSTS) en ligne: https://riptutorial.com/fr/https/topic/3495/http-strict-transport-security--hsts-

Crédits

S. No	Chapitres	Contributeurs
1	Démarrer avec https	Community, finjo, RamenChef, raphinesse, TheCrazyProfessor
2	HTTP Strict Transport Security (HSTS)	Kobi