EBook Gratis

APRENDIZAJE

https

Free unaffiliated eBook created from
Stack Overflow contributors.

#https

Tabla de contenido

Acerca de

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

Capítulo 1: Empezando con https

Observaciones

Esta sección proporciona una descripción general de qué es https y por qué un desarrollador puede querer usarlo.

También debe mencionar cualquier tema grande dentro de https y vincular a los temas relacionados. Dado que la Documentación para https es nueva, es posible que deba crear versiones iniciales de los temas relacionados.

Examples

Empezando con HTTPS

HTTPS *(Protocolo de transferencia de hipertexto seguro)* es una versión cifrada del protocolo HTTP, que se utiliza con más frecuencia en conexión con servicios en los que solo el remitente y el destinatario deben conocer el mensaje. Se requiere si maneja la información de la tarjeta de crédito y mejorará su rango en Google.

Para habilitar el protocolo HTTPS , debe verificar si su proveedor de alojamiento web lo admite; si no sabe, puede solicitar ayuda e información al respecto. Algunos servidores web pueden tomar algo de dinero para ello.

> **¡Importante!** : Su HTTPS necesita usar sha2 o sha3 *(sha1 está bloqueado por **Chrome** , **Firefox** , **Edge** e **IE**)*

Cuando haya habilitado HTTPS en su servidor web, puede usar HTTPS. Pero el navegador no usa HTTPS como predeterminado; La mejor manera de asegurarse de que todo el tráfico se ejecute en HTTPS es usar un archivo .htaccess y agregarlo a la raíz de su sitio web.

El archivo .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]
```

Esto cambiará el http: // a https: //.

NOTA : .htaccess es un archivo del sistema y no se puede ver de forma predeterminada. Cómo mostrar .htaccess

Lea Empezando con https en línea: https://riptutorial.com/es/https/topic/2910/empezando-con-https

Capítulo 2: Seguridad de transporte estricta de HTTP (HSTS)

Parámetros

Parámetro	Detalles
`max-age=31536000`	Tiempo en segundos. HSTS se aplicará para este período de tiempo futuro.
`includeSubDomains`	HSTS debe aplicarse para este dominio y todos sus subdominios.
`preload`	Este dominio acepta ser incluido en una lista de precarga HSTS

Observaciones

Ver también

- MDN - Seguridad de transporte estricta de HTTP
- Wikipedia - Seguridad de transporte estricta de HTTP
- Lista de precarga HSTS

Examples

Cabecera HSTS

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

`Strict-Transport-Security` es una promesa para el navegador de que todas las solicitudes futuras a este dominio serán seguras.
Para el período de tiempo futuro `max-age` :

- Todas las solicitudes HTTP salientes del navegador se convertirán a HTTPS *en el cliente* (no una redirección HTTP).
- Si el certificado no es válido (por ejemplo, desactualizado o autodenominado), el usuario no podrá incluirlo en la lista blanca y el sitio permanecerá inaccesible.

El comportamiento de HSTS está destinado a eliminar los ataques Man-in-the-Middle que utilizan la eliminación de HTTPS, la emisión de certificados no válidos (y la expectativa de que el usuario agregue una excepción) y la redirección de las solicitudes HTTP a otro destino.

Lista de precarga HSTS

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

HSTS se activa solo después de una solicitud HTTPS exitosa al servidor con un certificado válido. Todavía existe el riesgo de que un usuario nuevo acceda al sitio, momento en el que es posible un ataque Man-in-the-Middle.
Para que el sitio sea seguro, incluso antes de la primera solicitud, el dominio se puede agregar a una lista de precarga , ya configurada en los navegadores.
El parámetro de `preload` no es usado directamente por los navegadores, pero es una indicación para los desarrolladores del navegador que los desarrolladores del sitio realmente solicitaron ser agregados a la lista de precarga.

Lea Seguridad de transporte estricta de HTTP (HSTS) en línea:
https://riptutorial.com/es/https/topic/3495/seguridad-de-transporte-estricta-de-http--hsts-

Creditos

S. No	Capítulos	Contributors
1	Empezando con https	Community, finjo, RamenChef, raphinesse, TheCrazyProfessor
2	Seguridad de transporte estricta de HTTP (HSTS)	Kobi