What are HSTS and the HSTS preload list?

The HSTS (HTTP Strict Transport Security) protocol is a policy / mechanism that forces a web connection over a secure HTTPS channel. In other words: without a valid SSL certificate, such a website will not load in your browser. The browser will not even show the option to ignore the SSL warning.

Implementing HSTS on your website

If you want your website always to be served over HTTPS, you can add the *Strict-Transport-Security* header. This HTTPS header carries a parameter *max-age* that defines for how long (in seconds) this requirement is valid. The optional parameter *includeSubDomains* can be added to enforce secure connections for all sub domains as well.

Example

An example of a HSTS header is the following:

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

This header defines HSTS for a period of 365 days and affects sub domains as well. In other words, next time you will visit this specific website or one of its sub domains and try to do so over an unsecured HTTP connection, your browser will throw an error.

A good source of further information is Mozilla.

Limitations

Note that the HSTS header is accepted only in case the connection is already secure. The HSTS header is ignored by the browser if the page is served over an HTTP connection. For that reason, it is important that you automatically redirect every HTTP request to HTTPS.

While the HSTS header secures against man in the middle attacks (for example when browsing through public wifi access points), there is still a risk if a website is visited for the first time: at that moment a hacker can intercept your request and remove the HSTS requirement. For that reason, ensure your first visit to the website is from a secure access point.

HSTS preload list

It is possible to enforce secure connections on a higher level, even before visiting a website for the first time: the HSTS preload list. This is a list with domain names that by default support HSTS: no case-by-case HSTS headers are required, it's just *always* HSTS. This list is managed by Google and used by all major web browsers, including Chrome, Firefox and Internet Explorer. For those interested, a full list of domains added to the HSTS preload list is available. If you want to add your website to the HSTS preload list, check the hstspreload.org website.

Not only domains can be added to the HSTS preload list, also complete top level domains (domain extensions). If a registry decides to add its extension(s) to the HSTS preload list, every domain registered under that TLD must be served over HTTPS. The first extensions using the HSTS preload list are .bank and .insurance - two extensions that have security as their unique selling point. Google Registry has also added .app and .dev to the HSTS preload list.

Revision #1
Created 2026-08-07 14:58:38 UTC by Sarath
Updated 2026-08-07 14:58:38 UTC by Sarath