HSTS is Zero Trust for HTTP

HSTS is the abbreviation of HTTP Strict Transport Security. This is a comment version of the RFC6797 standard, which is intended to formulate a standard so that browsers can only access a website using the https protocol. To this end, Google has also specially set up an HSTS preload application website for users to submit domain names to be included in Google Chrome's HSTS preload list, which is a list of HTTPS websites hardcoded into Google Chrome. Most Browsers (Chrome, Firefox, Opera, Safari, IE 11, and Edge) also use Google Chrome-based HSTS preload lists.

HSTS is a security measure to ensure that browsers only use https encryption to connect to websites. It is zero-trust for HTTP cleartext traffic and is supported by many websites now. The U.S. Office of Management and Budget (OMB) officially released the Federal Zero Trust Strategy on January 26, 2022, in support of U.S. Presidential Executive Order 14028, "Improving the Nation's Cybersecurity," to enable federal government agencies network security architecture adapts to the principles of zero trust. In the "Encrypting HTTP Traffic" section, all government agencies are required to use HTTPS in all Internet-accessible web services and APIs, and to ensure that government websites support https encryption, from 2020 major browsers automatically HSTS preload all new registered .gov domains, and has announced that the entire U.S. government .gov domain name will eventually be prepended to HTTPS-only access, this requirement will improve security and zero trust for U.S. government agencies at all levels. This measure is also a zero trust in whether government agencies can consciously implement the https encryption policy, because after this measure is taken, the browser will not use the http protocol to access, and if the SSL certificate is not deployed to implement https encryption, the website cannot be accessed.

Of course, to implement mandatory https encryption, users only need to set the automatic redirection of http access to https access when deploying the SSL certificate on the website, and it is not necessary to submit the website domain name to the HSTS preloading database. To allow browsers based on the Chromium to automatically use https to access websites, you just need to simply add a line of code like this to the Nginx server configuration file:

add_header Strict-Transport-Security "max-age=31536000; includeSubdomains; preload"

Since HSTS preloading is hardcoded, not only will the preloading list be very long, but the newly added website domain name will not take effect until the next update, which is a very inefficient solution, but still a worthwhile solution.

The author hereby appeals: In order to ensure the security of China government websites and protect the e-government service confidential information, it should also be mandatory to use https to access government websites with .gov.cn domain names. All websites with .gov.cn domain names cannot be accessed through http, only https access. This enforcement can further require https encrypted access only using the SM2 encryption algorithm. Of course, no need to use HSTS preload method, we can have more efficient and simpler ways.

Richard Wang

Feb. 8, 2022
In Shenzhen, China