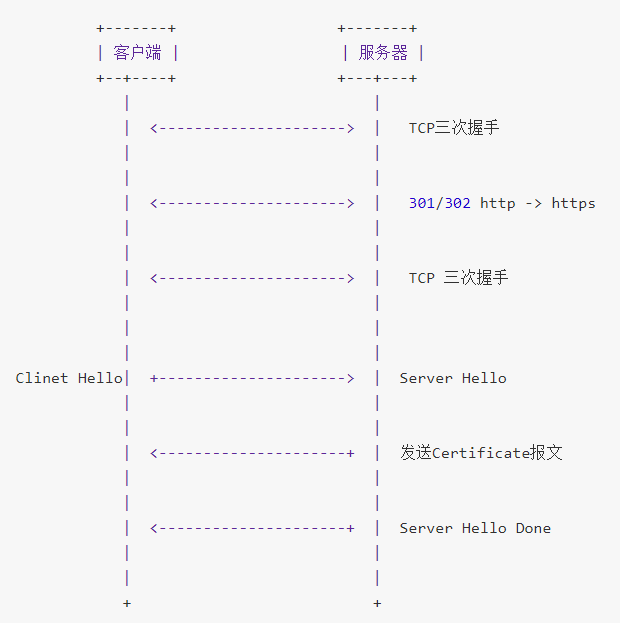
HSTS: HTTP Strict Transport Security

假设要访问的网站是全站HTTPS但未开启HSTS

1. 一般地，用户在客户端访问一个网站的时候，往往只输入域名，而不带有协议名。例如访问我的博客www.linpx.com，而不是https://www.linpx.com。
2. 输入www.linpx.com访问，客户端与服务器来一次TCP三次握手，建立连接；
3. 然后做301/302跳转到HTTPS；
4. 客户端与服务器再来一次TCP握手，重新建连；
5. 然后开始TSL（SSL）通信···

过程流图如下：



但实际上该过程中第一次TCP握手通过HTTP完成，仍然存在被攻击的可能。HSTS即为了避免此威胁。

客户端发送http请求后，服务器端发送带有HSTS头部的回应给客户端，客户端再将自身的HTTP转换为HTTPS发送，此过程无需网络请求。

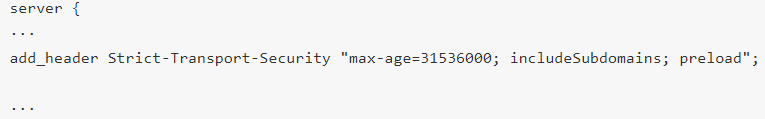
该头部如：

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

1. max-age，单位是秒，用来告诉浏览器在指定时间内，这个网站必须通过 HTTPS 协议来访问。也就是对于这个网站的 HTTP 地址，浏览器需要先在本地替换为 HTTPS 之后再发送请求
2. includeSubDomains，可选参数，如果指定这个参数，表明这个网站所有子域名也必须通过 HTTPS 协议来访问
3. preload，可选参数，预加载到浏览器缓存

该头部的配置即在自己服务器（如nginx、apache）中进行配置。

如：



但是即使使用HSTS技术，仍然存在一个问题，第一次HTTP请求仍然是不安全的。HSTS preload list的出现是为了解决这一威胁。

HSTS 必须要在浏览器访问过你的网站一次以后才会生效，如果希望提前生效，需要申请 HSTS Preloading List。

HSTS preload list是Chrome浏览器中的HSTS预载入列表，在该列表中的网站，使用Chrome浏览器访问时，会自动转换成HTTPS。Firefox、Safari、Edge浏览器也在采用这个列表。

文章基本上摘自以下博客：

<https://www.linpx.com/p/i-know-little-about-hsts.html>

<https://www.linpx.com/p/hsts-and-hsts-preload-list-enabled-applications.html>

摘录只为自我学习使用，无意抄袭。