Ws99

首页 管理

随笔- 10 文章- 764 评论- 46 阅读- 57万

最好的CMS：Deruv

昵称： luckc#
园龄： 11年3个月
粉丝： 150
关注： 1
+加关注

常用链接

我的随笔
我的评论
我的参与
最新评论
我的标签
更多链接

友情链接

deruv

开启HSTS让浏览器强制跳转HTTPS访问

在网站全站HTTPS后，如果用户手动敲入网站的HTTP地址，或者从其它地方点击了网站的HTTP链接，通常依赖于服务端301/302跳转才能使用HTTPS服务。而第一次的HTTP请求就有可能被劫持，导致请求无法到达服务器，从而构成HTTPS降级劫持。这个问题目前可以通过HSTS(HTTP Strict Transport Security，RFC6797)来解决。

HSTS简介

HSTS(HTTP Strict Transport Security)是国际互联网工程组织IETF发布的一种互联网安全策略机制。采用HSTS策略的网站将保证浏览器始终连接到该网站的HTTPS加密版本，不需要用户手动在URL地址栏中输入加密地址，以减少会话劫持风险。

HSTS响应头格式

```
Strict-Transport-Security: max-age=expireTime [; includeSubDomains] [; preloa
```

- 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。
- 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。
- preload，可选参数，一个浏览器内置的使用HTTPS的域名列表。

HSTS Preload List

虽然HSTS可以很好的解决HTTPS降级攻击，但是对于HSTS生效前的首次HTTP请求，依然无法避免被劫持。浏览器厂商们为了解决这个问题，提出了 `HSTS Preload List` 方案：内置一份可以定期更新的列表，对于列表中的域名，即使用户之前没有访问过，也会使用HTTPS协议。

目前这个Preload List由Google Chrome维护，Chrome、Firefox、Safari、IE 11和Microsoft Edge都在使用。如果要想把自己的域名加进这个列表，首先需要满足以下条件：

- 拥有合法的证书(如果使用SHA-1证书，过期时间必须早于2016年)；
- 将所有HTTP流量重定向到HTTPS；
- 确保所有子域名都启用了HTTPS；
- 输出HSTS响应头：
- max-age不能低于18周(10886400秒)；
- 必须指定includeSubdomains参数；
- 必须指定preload参数；

即便满足了上述所有条件，也不一定能进入 `HSTS Preload List` ，更多信息可以查看：`https://hstspreload.org/` 。

通过Chrome的 `chrome://net-internals/#hsts` 工具，可以查询某个网站是否在Preload List之中，还可以手动把某个域名加到本机Preload List。

HSTS缺点

HSTS并不是HTTP会话劫持的完美解决方案。用户首次访问某网站是不受HSTS保护的。这是因为首次访问时，浏览器还未收到HSTS，所以仍有可能通过明文HTTP来访问。

如果用户通过HTTP访问HSTS保护的网站时，以下几种情况存在降级劫持可能：

- 以前从未访问过该网站
- 最近重新安装了其操作系统

- 最近重新安装了其浏览器
- 切换到新的浏览器
- 切换到一个新的设备，如：移动电话
- 删除浏览器的缓存
- 最近没访问过该站并且max-age过期了

解决这个问题目前有两种方案：

方案一：在浏览器预置HSTS域名列表，就是上面提到的 `HSTS Preload List` 方案。该域名列表被分发和硬编码到主流的Web浏览器。客户端访问此列表中的域名将主动的使用HTTPS，并拒绝使用HTTP访问该站点。

方案二：将HSTS信息加入到域名系统记录中。但这需要保证DNS的安全性，也就是需要部署域名系统安全扩展。

其它可能存在的问题

由于HSTS会在一定时间后失效(有效期由max-age指定)，所以浏览器是否强制HSTS策略取决于当前系统时间。大部分操作系统经常通过网络时间协议更新系统时间，如Ubuntu每次连接网络时，OS X Lion每隔9分钟会自动连接时间服务器。攻击者可以通过伪造NTP信息，设置错误时间来绕过HSTS。

解决方法是认证NTP信息，或者禁止NTP大幅度增减时间。比如：Windows 8每7天更新一次时间，并且要求每次NTP设置的时间与当前时间不得超过15小时。

支持HSTS浏览器

目前主流浏览器都已经支持HSTS特性，具体可参考下面列表：

- Google Chrome 4及以上版本
- Firefox 4及以上版本
- Opera 12及以上版本
- Safari从OS X Mavericks起
- Internet Explorer及以上版本

HSTS部署

服务器开启HSTS的方法是：当客户端通过HTTPS发出请求时，在服务器返回的超文本传输协议响应头中包含 `Strict-Transport-Security` 字段。非加密传输时设置的HSTS字段无效。

最佳的部署方案是部署在离用户最近的位置，例如：架构有前端反向代理和后端Web服务器，在前端代理处配置HSTS是最好的，否则就需要在Web服务器层配置HSTS。如果Web服务器不明确支持HSTS，可以通过增加响应头的机制。如果其他方法都失败了，可以在应用程序层增加HSTS。

HSTS启用比较简单，只需在相应头中加上如下信息：

```
Strict-Transport-Security: max-age=63072000; includeSubdomains;preload;
```

`Strict-Transport-Security` 是Header字段名， `max-age` 代表HSTS在客户端的生效时间。
`includeSubdomains` 表示对所有子域名生效。preload是使用浏览器内置的域名列表。

HSTS策略只能在HTTPS响应中进行设置，网站必须使用默认的443端口；必须使用域名，不能是IP。因此需要把HTTP重定向到HTTPS，如果明文响应中允许设置HSTS头，中间人攻击者就可以通过在普通站点中注入HSTS信息来执行DoS攻击。

Apache上启用HSTS

```
$ vim /etc/apache2/sites-available/hi-linux.conf

# 开启HSTS需要启用headers模块
LoadModule headers_module /usr/lib/apache2/modules/mod_headers.so

<VirtualHost *:80>
  ServerName www.hi-linux.com
  ServerAlias hi-linux.com
...
 #将所有访问者重定向到HTTPS，解决HSTS首次访问问题。
  RedirectPermanent / https://www.hi-linux.com/
</VirtualHost>
```

```
<VirtualHost 0.0.0.0:443>
...
# 启用HTTP严格传输安全
  Header always set Strict-Transport-Security "max-age=63072000; includeSubdo
...
</VirtualHost>
```

重启Apache服务

```
$ service apche2 restart
```

Nginx上启用HSTS

```
$ vim /etc/nginx/conf.d/hi-linux.conf

server {
   listen 443 ssl;
   server_name www.hi-linux.com;
   add_header Strict-Transport-Security "max-age=63072000; includeSubdomains;
...
}

server {
   listen 80;
   server_name www.hi-linux.com;
   return 301 https://www.hi-linux.com$request_uri;
...
}
```

重启Nginx服务

```
$ service nginx restart
```

IIS启用HSTS

要在IIS上启用HSTS需要用到第三方模块，具体可参考：https://hstsiis.codeplex.com/

测试设置是否成功

设置完成了后，可以用 `curl` 命令验证下是否设置成功。如果出来的结果中含有 `Strict-Transport-Security` 的字段，那么说明设置成功了。

```
$ curl -I https://www.hi-linux.com
HTTP/1.1 200 OK
Server: nginx
Date: Sat, 27 May 2017 03:52:19 GMT
Content-Type: text/html; charset=utf-8
...
Strict-Transport-Security: max-age=63072000; includeSubDomains; preload
X-Frame-Options: deny
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff
...
```

对于 `HSTS` 以及 `HSTS Preload List` ，建议是只要不能确保永远提供HTTPS服务，就不要启用。因为一旦HSTS生效，之前的老用户在 `max-age` 过期前都会重定向到HTTPS，造成网站不能正确访问。唯一的办法是换新域名。

参考文档

http://www.google.com
http://t.cn/RSzfyBb
https://yuan.ga/hsts-strict-https-enabled-site/
https://imququ.com/post/sth-about-switch-to-https.html
http://www.ttlsa.com/web/hsts-for-nginx-apache-lighttpd/
http://www.jianshu.com/p/66ddc3124006

更多精彩热文:

- Prometheus入门
- Nginx配置文件安全分析工具——Gixy
- 推荐两款实用工具——hcache和SQLPad
- 配置Nginx反向代理WebSocket
- 基于Upsync模块实现Nginx动态配置

分类: WEB_SCHEMA, Nginx

luckc#
关注 - 1
粉丝 - 150
+加关注

1 0

posted @ 2017-06-05 13:46 luckc# 阅读(7983) 评论(0) 编辑 收藏 举报