02

OPEN ORIENTED

凹 凸 实 验 室

HSTS介绍

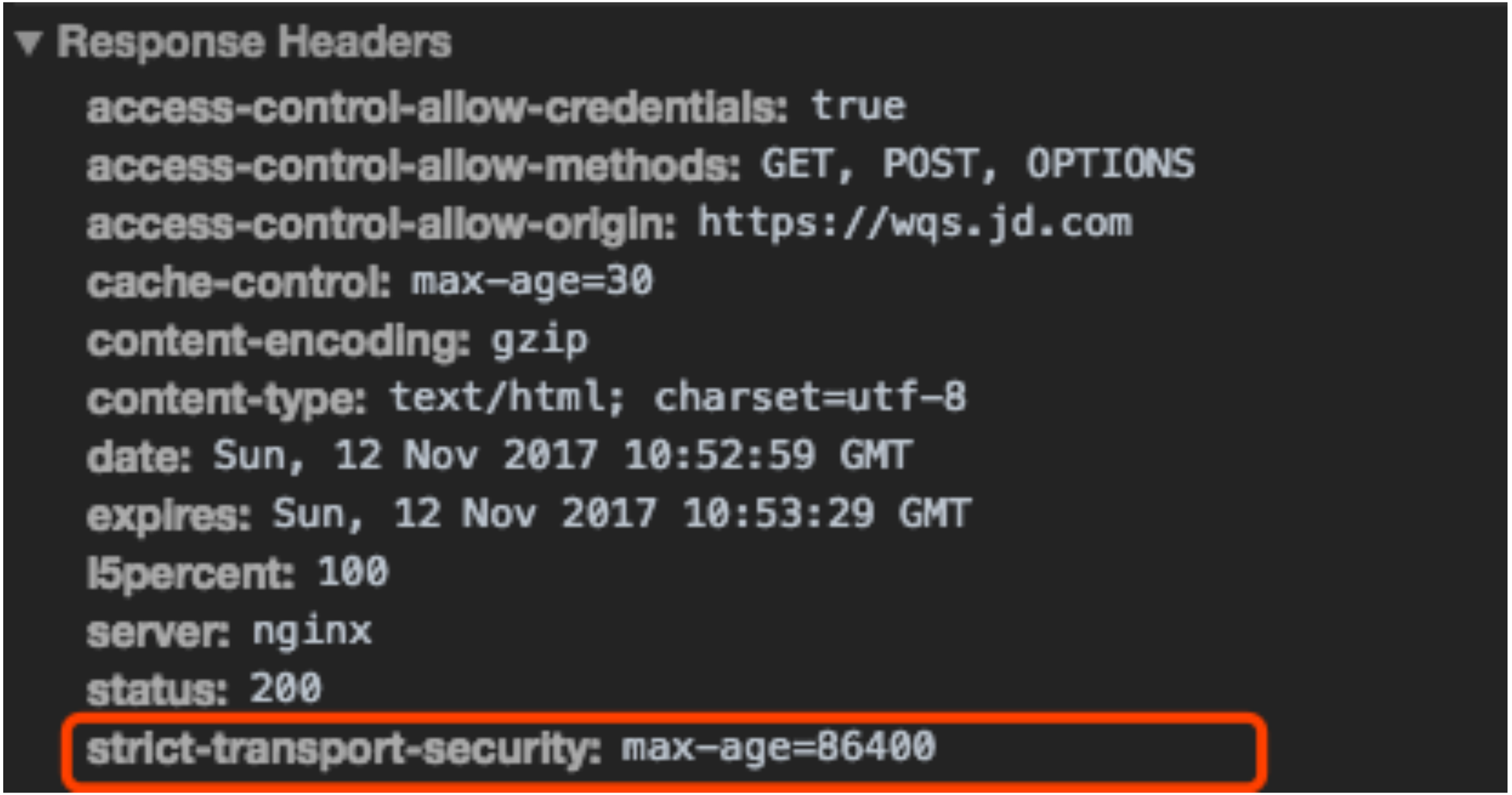
2017.11.11 cos2004

HSTS是什么

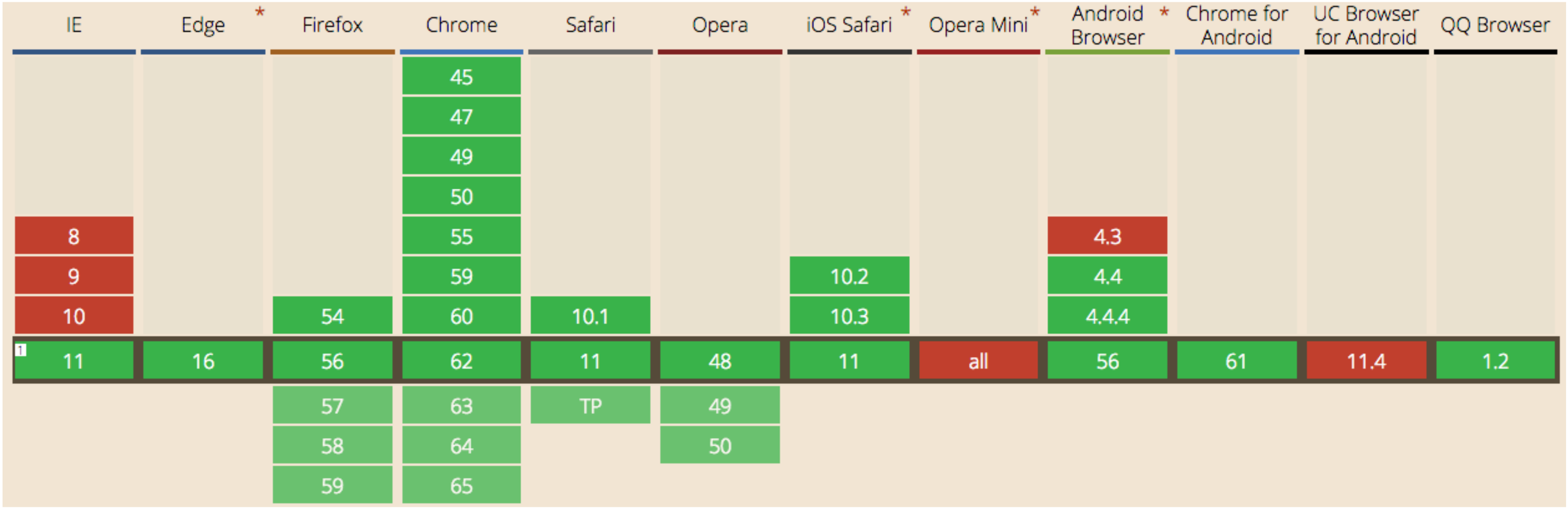
HSTS是“HTTP Strict Transport Security”（HTTP严格安全传输）的缩写

语法：

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


▼ Response Headers
access-control-allow-credentials: true
access-control-allow-methods: GET, POST, OPTIONS
access-control-allow-origin: https://wqs.jd.com
cache-control: max-age=30
content-encoding: gzip
content-type: text/html; charset=utf-8
date: Sun, 12 Nov 2017 10:52:59 GMT
expires: Sun, 12 Nov 2017 10:53:29 GMT
l5percent: 100
server: nginx
status: 200
strict-transport-security: max-age=86400

支持情况



IE	Edge *	Firefox	Chrome	Safari	Opera	iOS Safari *	Opera Mini *	Android Browser *	Chrome for Android	UC Browser for Android	QQ Browser
			45								
			47								
			49								
			50								
8			55					4.3			
9			59			10.2		4.4			
10		54	60	10.1		10.3		4.4.4			
11 [1]	16	56	62	11	48	11	all	56	61	11.4	1.2
		57	63	TP	49						
		58	64		50						
		59	65								

第1次访问(http)就被劫持怎么办?

HSTS preload计划

内置域名到chrome / safari / firefox / MS Edge等主流浏览器

提交 & 查询：https://hstspreload.org/

源代码： https://cs.chromium.org/chromium/src/net/http/transport_security_state_static.json?q=jd.com&sq=package:chromium&maxsize=6828940&l=4997

HSTS preload提交要求

1. Serve a valid **certificate**.
2. **Redirect** from HTTP to HTTPS on the same host, if you are listening on port 80.
3. Serve all **subdomains** over HTTPS.
    - In particular, you must support HTTPS for the `www` subdomain if a DNS record for that subdomain exists.
4. Serve an **HSTS header** on the base domain for HTTPS requests:
    - The `max-age` must be at least `31536000` seconds (1 year).
    - The `includeSubDomains` directive must be specified.
    - The `preload` directive must be specified.
    - If you are serving an additional redirect from your HTTPS site, that redirect must still have the HSTS header (rather than the page it redirects to).

所以子域名必须https

chrome的HSTS工具

chrome://net-internals/#hsts

可添加、删除、查询某个域名的HSTS

开发经验

HSTS 排错演示

参考资料

HSTS介绍：https://developer.mozilla.org/zh-CN/docs/Security/HTTP_Strict_Transport_Security

解决缺陷，让HSTS变得完美：https://blog.wilddog.com/?page_id=1493

THANKS

FOR YOUR WATCHING

02

OPEN ORIENTED

凹 凸 实 验 室