

# 让用户的数据更安全

--淘宝、天猫全网HTTPS实践

阿里巴巴集团—技术保障部 ( AIS )

李振宇 ( 震羽 )



# Geekbang

极客邦科技

整合全球最优质学习资源, 帮助技术人和企业成长  
Growing Technicians, Growing Companies

InfoQ ueue

专注中高端技术人员的技术媒体



EGO EXTRA GEEKS' ORGANIZATION  
NETWORKS

高端技术人员  
学习型社交网络



StuQ ueue

实践驱动的  
IT职业学习和服务平台



Git GEEKBANG INTERNATIONAL TRAINING 极客邦培训

一线专家驱动的企业培训服务



旧金山 伦敦 北京 圣保罗 东京 纽约 上海  
San Francisco London Beijing Sao Paulo Tokyo New York Shanghai

# QCon

## 全球软件开发大会

2016年4月21-23日 | 北京·国际会议中心

主办方 **Geekbang** & **InfoQ**  
极客邦科技

**7折** 优惠 (截至12月27日)  
现在报名, 节省2040元/张, 团购享受更多优惠

[www.qconbeijing.com](http://www.qconbeijing.com)



扫描获取更多大会信息



# 为什么要做全网HTTPS ?

The screenshot shows the Taobao.com website in a browser. The developer tools are open, displaying the DOM tree. A specific `iframe` element is selected, showing its attributes and styles. The `src` attribute is highlighted, showing a URL: `http://121.40.208.27/yeyou/3.html?aid=2863&scrolling=no`. The styles panel shows the default `user-agent` styles for an `iframe`, including `border: 2px inset`, `border-image-source: initial`, and `border-image-slice: initial`.



# 为什么要做全网HTTPS ?

The screenshot shows the Taobao.com homepage with a browser address bar displaying `https://www.taobao.com`. The page layout includes a top navigation bar with links for '我的淘宝', '购物车', '收藏夹', '商品分类', '卖家中心', '联系客服', and '网站导航'. A search bar is prominently displayed with the text '雪地里的温暖' and a '搜索' button. Below the search bar, there are various promotional banners, including one for '皮带专场' (Belt Special) and another for '气质尖头靴' (Elegant Point-toe Boots). The left sidebar contains a '淘宝特色服务' (Taobao Special Services) section with categories like '主题市场' (Theme Market) and '特色购物' (Special Shopping). The bottom of the page features a '当前热点' (Current Hotspots) section with various product recommendations and a '中国质造' (Made in China) banner. The browser's status bar at the bottom indicates '正在等待 gd1.alicdn.com 的响应...'.



# 哪些大型网站支持HTTPS ?

社交/博客/论坛 : Facebook/Twitter/LinkedIn/Blogger/  
Reddit/Tumblr/Pinterest/Instagram/Wikipedia

搜索引擎 : Google/Bing/Baidu/Haosou/Sogou

视频 : Youtube/Netflix

邮箱 : Gmail/MSN/Yahoo/Live/QQmail

支付 : Alipay/Paypal

电子商务 : Taobao/Tmall



# HTTPS是一个趋势

Chrome/Firefox : 未来会将http标记为不安全

Apple ATS : 要求新iOS9和OS X 10.11的app使用HTTPS

HTTP/2 : 必须使用HTTPS ( IE/Firefox/Chrome/Safari )

Google : 搜索排名会给HTTPS的网站加权

美国政府 : 要求2016年底所有政府网站必须是HTTPS





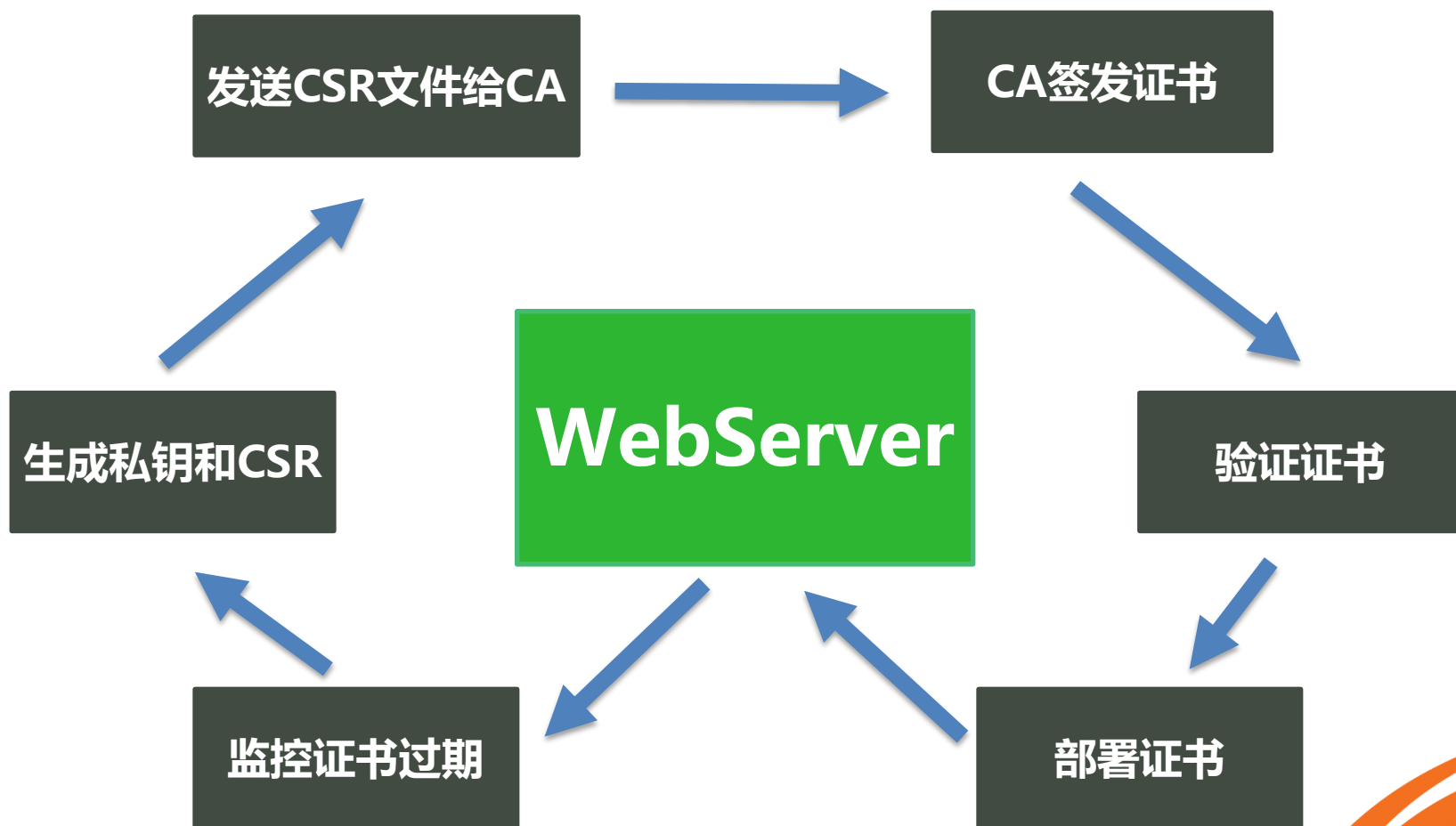
# 如何选择服务端证书？

|      | 展现  | 单域名                   | 多域名  | 泛域名                 | 多个泛域名  |
|------|---|-----------------------|--|---------------------|--|
| DV   |  | 支持                    |  | 不支持                 |  |
| OV   |  | 支持                    |  |                     |  |
| EV   |  | 支持                    |  | 不支持                 |  |
| e. g |   | <u>www.taobao.com</u> | <u>www.taobao.com</u><br><u>www.tmall.com</u><br><u>www.1688.com</u> | <u>*.taobao.com</u> | <u>*.taobao.com</u><br><u>*.tmall.com</u><br><u>*.1688.com</u> |

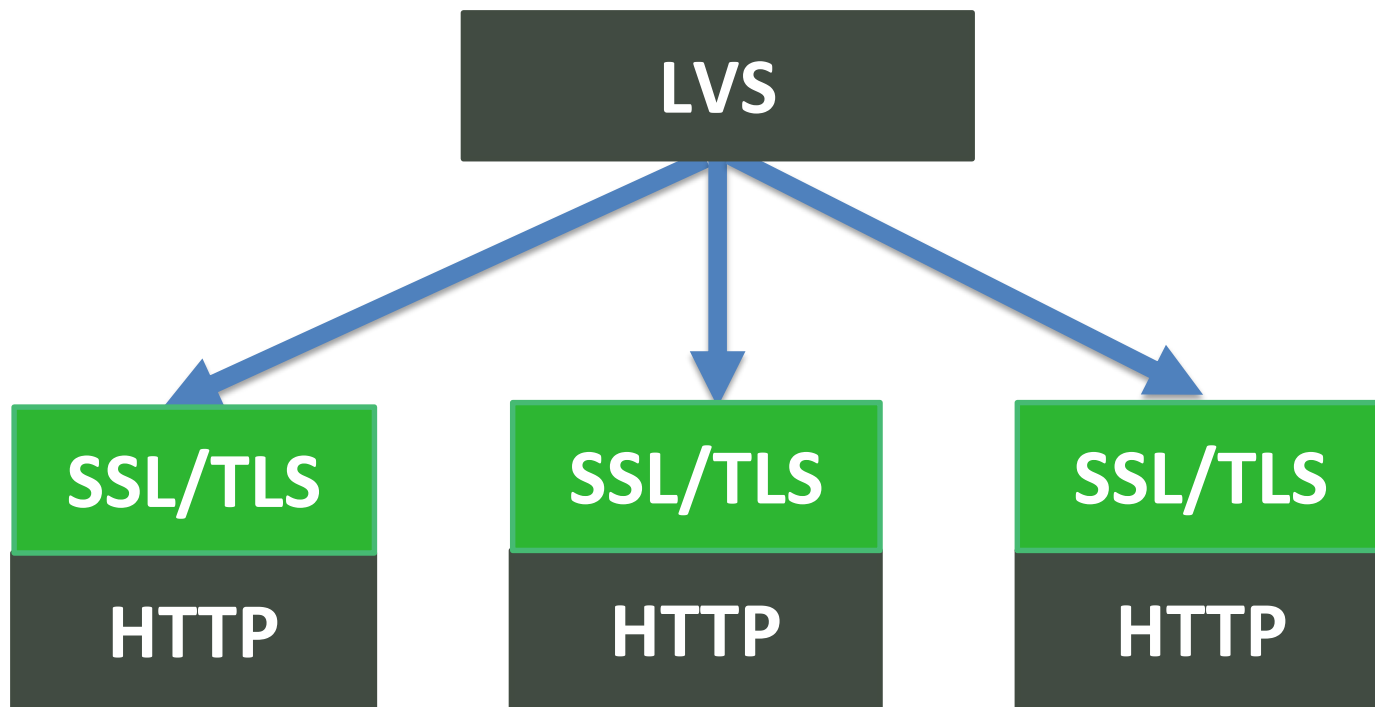




# 证书生命周期

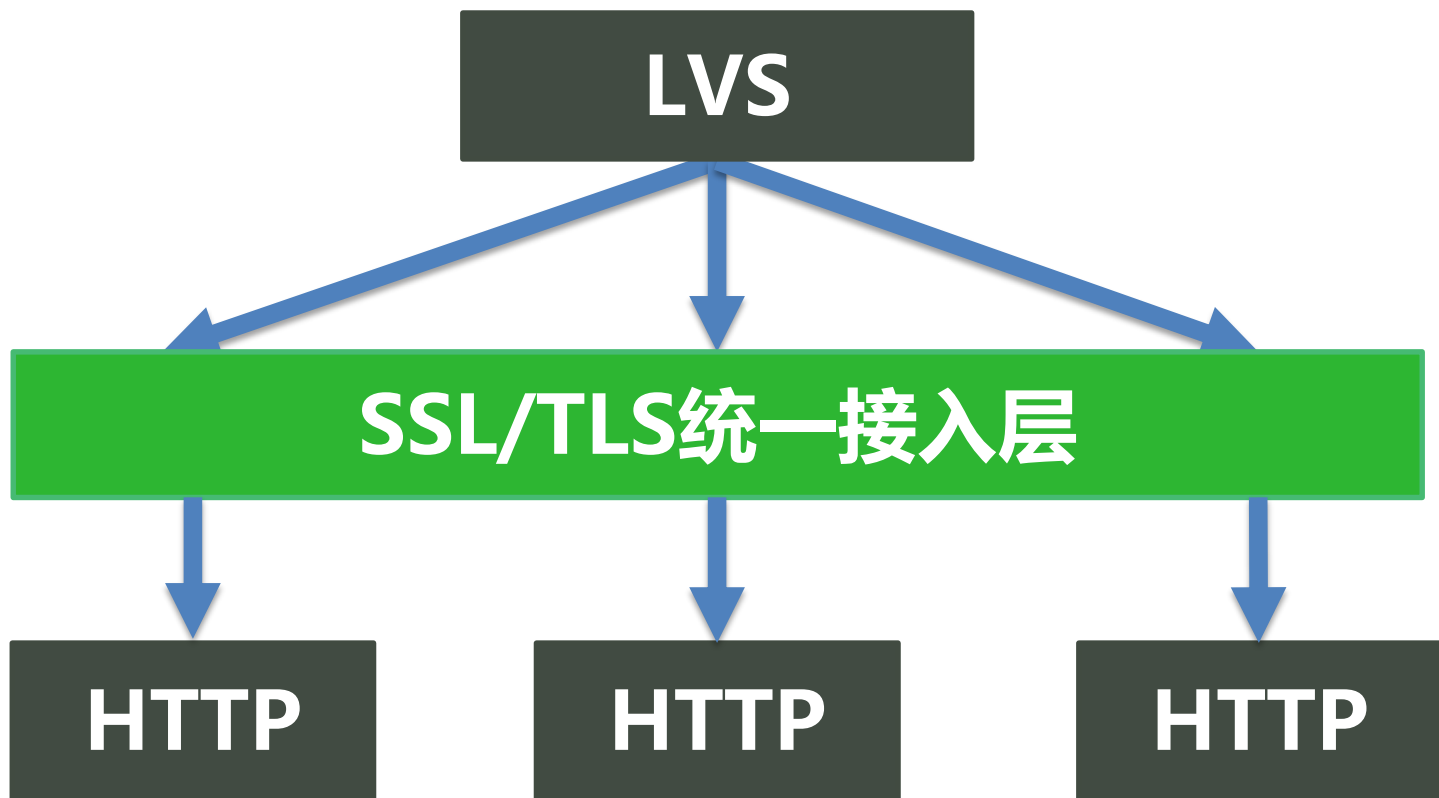


# 如何适应https带来的架构变化？



要在当前架构下支持HTTPS非常简单，但.....

# 统一是否更好？



但这种架构依旧引入了新的问题.....

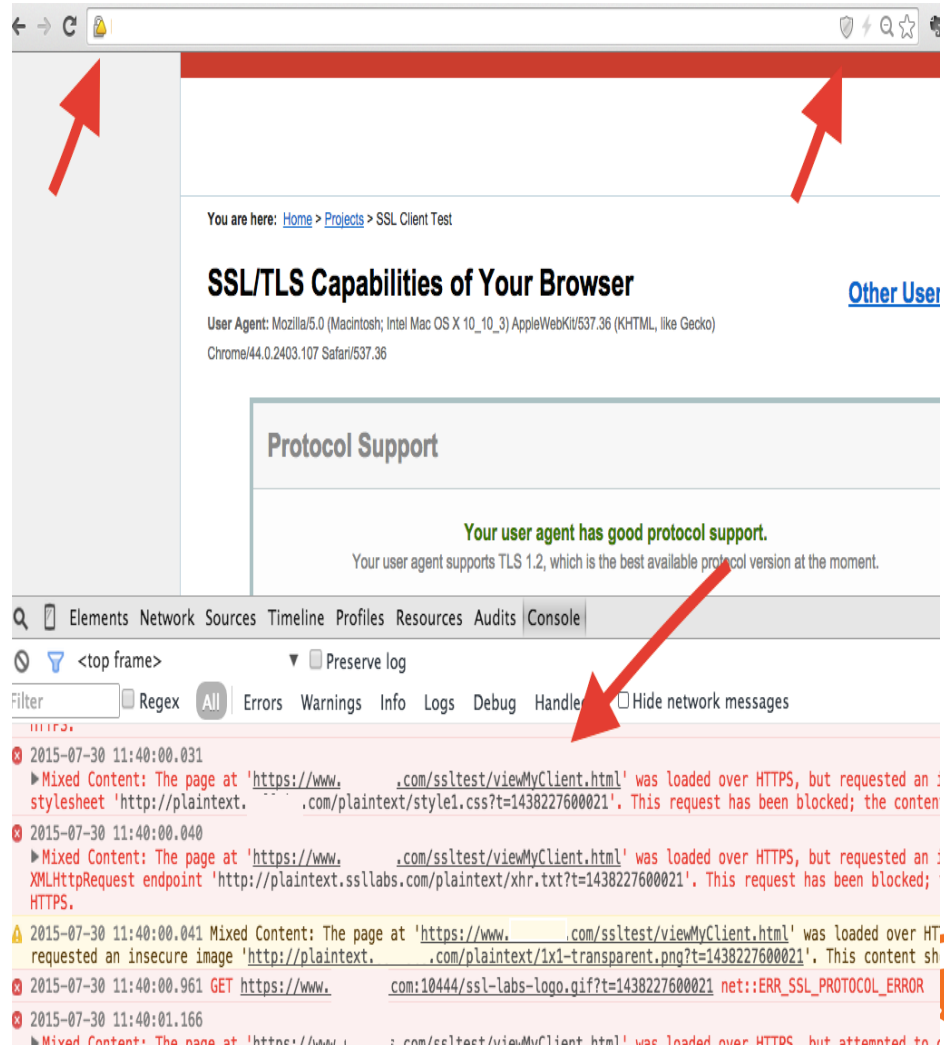


# 哪些需要改造？

盾牌：JS/CSS、异步调用、

字体、iFrame、Flash、视频

黄色三角：图片、POST



# 如何改造才能同时兼容当前用户？

http://=> //

替换逻辑简单，但是需要注意：

1. 中间件、无线app对//的识别
2. 替换底层数据源
3. 对国内部分搜索不够友好

```
view-source:https://www.taobao.com
1
2 <!DOCTYPE html><html><head><meta charset="utf-8"><link rel="dns-prefetch" href="//g.
href="//g.alicdn.com"><link rel="dns-prefetch" href="//g.alicdn.com"><link rel="dns-
href="//gtms01.alicdn.com"><link rel="dns-prefetch" href="//gtms02.alicdn.com"><link
href="//gtms03.alicdn.com"><link rel="dns-prefetch" href="//gtms04.alicdn.com"><link
href="//log.mmstat.com"><link rel="dns-prefetch" href="//p.tanx.com"><link rel="dns-
rel="dns-prefetch" href="//delta.taobao.com"><title>淘宝网 - 淘! 我喜欢</title><meta na
name="description" content="淘宝网 - 亚洲最大、最安全的网上交易平台，提供各类服饰、美容、家居、
时提供担保交易(先收货后付款)、先行赔付、假一赔三、七天无理由退换货、数码免费维修等安全交易保障服务，
name="keyword" content=""><meta http-equiv="X-UA-Compatible" content="IE=edge,chrome
content="webkit"><link href="//gtms03.alicdn.com/tps/i3/T1OjaVF14dXXa.JOZB-114-114.p
precomposed"><script src="//g.alicdn.com/secdev/pointman/js/index.js" app="taobao" c
rel="stylesheet" href="//g.alicdn.com/tb-mod/??tb-pad/1.0.1/index.css,tb-sitenav/1.0
sysinfo/1.0.0/index.css,tb-sysbanner/1.0.0/index.css,tb-double12-banner/0.0.20/index
top-spy/1.0.4/index.css,tb-birthday/1.0.2/index.css,tb-search/1.0.31/index.css,tb-lo
qr/1.0.0/index.css,tb-nav/1.0.7/index.css,tb-tanx/1.0.0/index.css,tb-promo/1.0.7/ind
notice/1.0.4/index.css,tb-member/1.0.7/index.css,tb-headlines/1.0.3/index.css,tb-con
service/0.0.9/index.css,tb-double12-belt/0.0.3/index.css,tb-belt/1.0.5/index.css,tb-
apps/1.0.8/index.css,tb-feature/1.0.4/index.css,tb-discover-goods/1.0.3/index.css,tb
discover-shop/1.0.3/index.css,tb-custom/1.0.1/index.css,tb-sale/1.0.0/index.css,tb-h
helper/1.0.0/index.css,tb-footer/1.0.0/index.css,tb-decorations/1.0.27/index.css,tb-
inject/0.0.13/index.css,tb-service/1.0.12/index.css,tb-cat/1.0.2/index.css,tb-rmdimg
ifashion/1.0.7/index.css,tb-market/1.0.2/index.css,tb-market2/1.0.3/index.css,tb-mar
market-diet/1.0.8/index.css,tb-oad/1.0.0/index.css,tb-market-furniture/1.0.5/index.
panel/1.0.4/index.css,tb-channel/1.0.1/index.css,tb-channel-travel/1.0.1/index.css,
rel="stylesheet" href="//g.alicdn.com/tb-mod/??tb-channel2/1.0.3/index.css,tb-channe
rel="stylesheet" href="//g.alicdn.com/??tb/global/3.5.28/global-min.css,tb-page/tbin
src="//g.alicdn.com/??kissy/k/1.4.14/seed-min.js,tb/global/3.5.28/global-min.js" dat
<script>window.g_config={appId:6,startDate:new Date},KISSY.config({combine:!0,packag
f{name:"ka".path:"//g.alicdn.com/ka/"}.ignorePackageNameInUri:!0,combine:!0},{name:"t
```





# 如何改造才能同时兼容当前用户？

## Tengine – sub\_filter替换模块

1. `subs_filter http://www.taobao.com https://www.taobao.com;`
2. Tengine输出替换，无需修改底层数据源
3. 只对HTTPS请求进行替换，兼容当前HTTP用户
4. 对国内搜索引擎友好

但是：

每增加一条非正则规则，服务器性能下降2%





# HTTPS一定会变慢吗？



# 切换到HTTPS之后性能变化情况

| PC PageLoad Time |          |          |           |           |
|------------------|----------|----------|-----------|-----------|
|                  | 淘宝<br>首页 | 淘宝<br>搜索 | 淘宝<br>购物车 | 聚划算<br>首页 |
| 性能提升             | 21%      | 6%       | 23%       | 16%       |
|                  | 天猫<br>首页 | 天猫<br>详情 | 天猫<br>搜索  | 聚划算<br>详情 |
| 性能提升             | 22%      | 20%      | 19%       | 30%       |





# 优化措施

- 减少握手，提高tls复用率
- SPDY3.1 & HTTP2
- 域名合并
- TCP内核优化
- 1-RTT 建连
- CDN Early Termination
- 预加载
- 算法位置调整ECDSA > RSA > ECDHE



# 减少握手，提高TLS复用率

- 单机Session Cache
- Session Ticket
- 分布式Session Cache
- TCP keepalive

• *TLS full handshake % =*

*( ! keepalive + ! session\_reused ) / total\_conn \* 100%*





# 优化措施

- 减少握手，提高tls复用率
- SPDY3.1 & HTTP2
- 域名合并
- TCP内核优化
- 1-RTT 建连
- CDN Early Termination
- 预加载
- 算法位置调整ECDSA > RSA > ECDHE



# 优化措施

- 减少握手，提高tls复用率
- SPDY3.1 & HTTP2
- 域名合并
- TCP内核优化
- False Start的1-RTT 建连
- CDN Early Termination
- 预加载
- ECDSA证书



# 优化措施

- 减少握手，提高tls复用率
- SPDY3.1 & HTTP2
- 域名合并
- TCP内核优化
- False Start的1-RTT 建连
- CDN Early Termination
- 预加载
- ECDSA证书



# 优化措施

- 减少握手，提高tls复用率
- SPDY3.1 & HTTP2
- 域名合并
- TCP内核优化
- False Start的1-RTT 建连
- **CDN Early Termination**
- 预加载
- ECDSA证书



# 优化措施

- 减少握手，提高tls复用率
- SPDY3.1 & HTTP2
- 域名合并
- TCP内核优化
- False Start的1-RTT 建连
- CDN Early Termination
- 预加载
- ECDSA证书



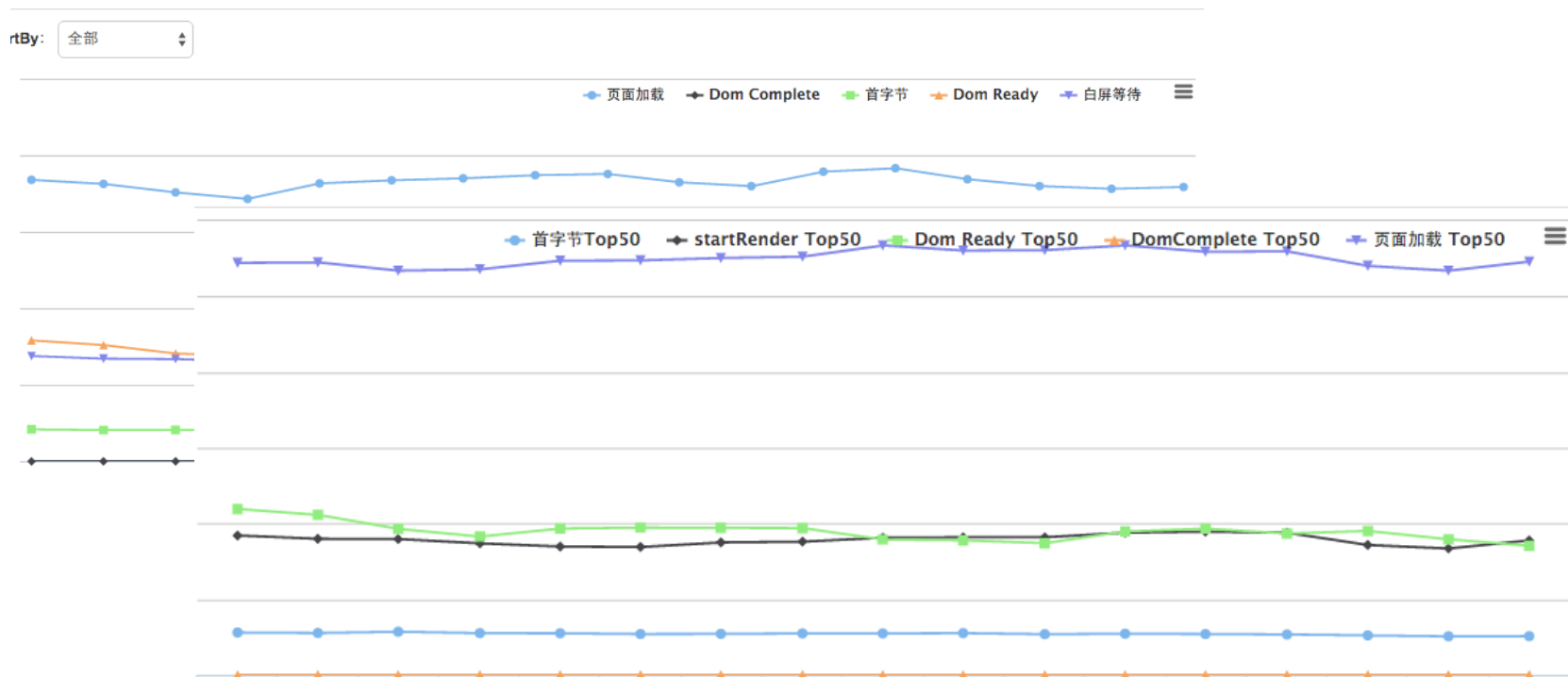
# 优化措施

- 减少握手，提高tls复用率
- SPDY3.1 & HTTP2
- 域名合并
- TCP内核优化
- False Start的1-RTT 建连
- CDN Early Termination
- 预加载
- ECDSA证书





# 获取页面加载的性能

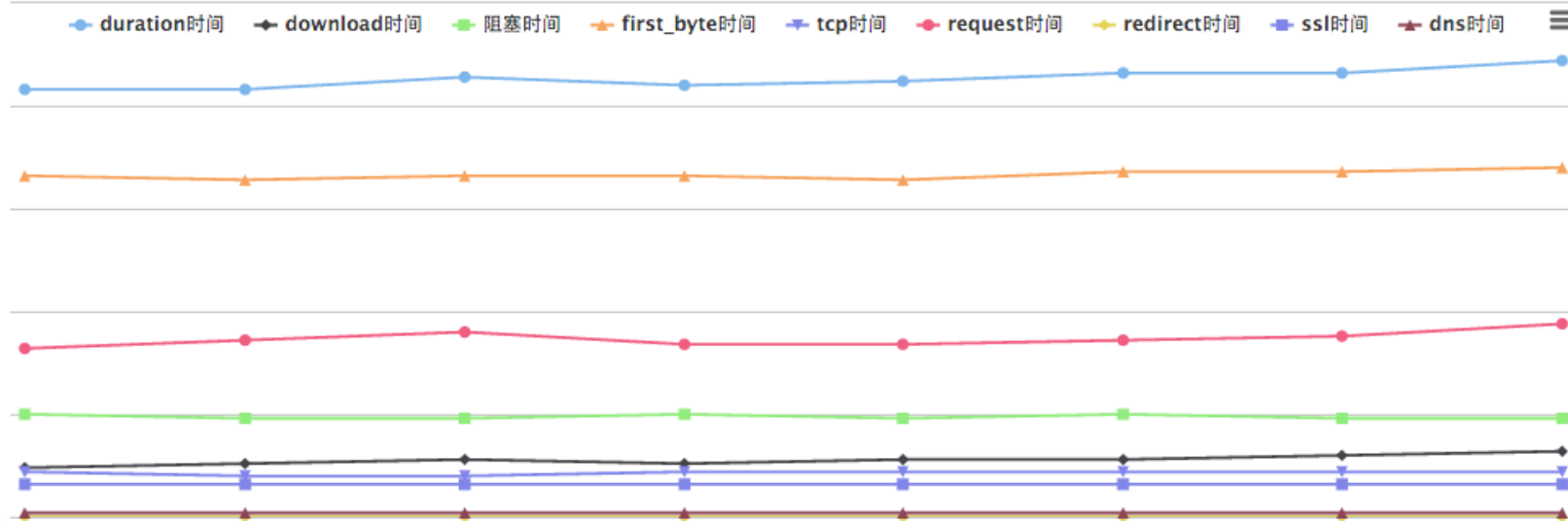


基于performance.timing的浏览器API



# 获取元素的性能数据

元素性能趋势(avg)



CDN : timing-allow-origin: \*





# 如何让HTTPS更安全



# 使用SHA-256证书

SHA-1已经不再安全

16年开始CA不在签发SHA-1证书

Chrome会标记SHA-1为不安全证书

XP SP2和Android2.2受影响

淘宝采用双证书解决，但不推荐

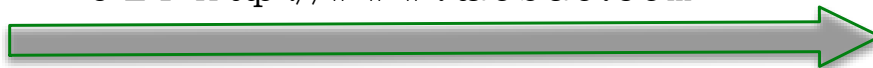
不要忘了中间证书也必须是SHA-256



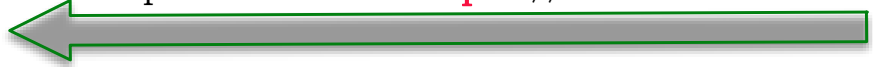
# HSTS



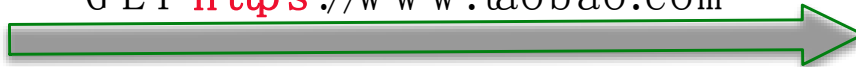
GET `http://www.taobao.com`



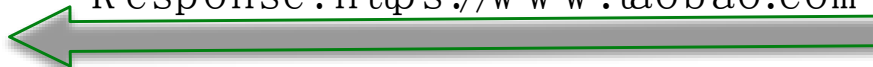
Response: 302 `https://www.taobao.com`



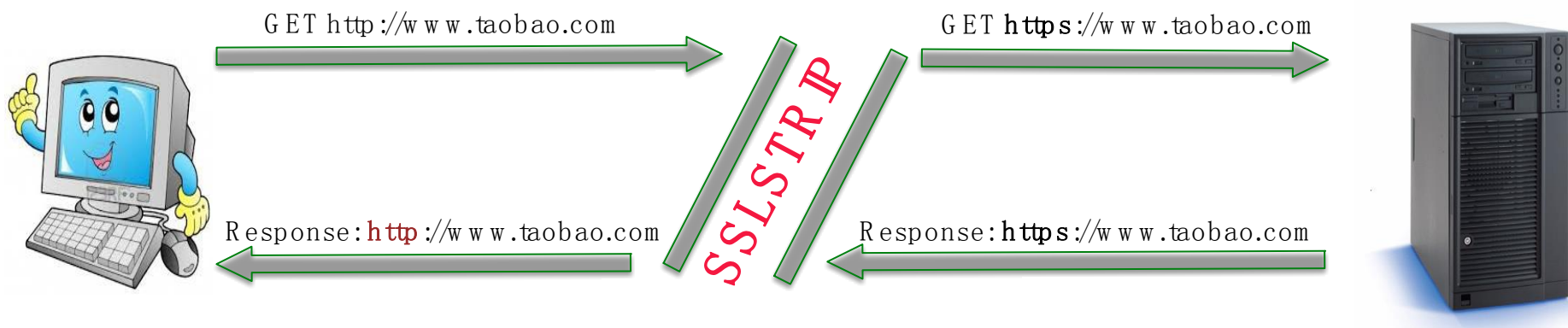
GET `https://www.taobao.com`



Response: `https://www.taobao.com`



# HSTS



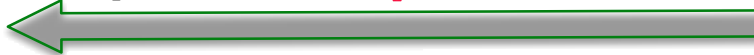
# HSTS



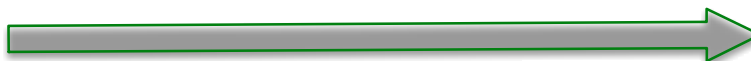
GET http://www.taobao.com



Response: 302 **http**://www.taobao.com



GET **https**://www.taobao.com



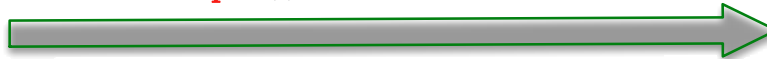
Response: **https**://www.taobao.com  
**strict-transport-security: max-age=31536000**



GET http://www.taobao.com

307 internal redirect

GET **https**://www.taobao.com



Response: **https**://www.taobao.com  
**strict-transport-security: max-age=31536000**



# TLS配置

## Modern compatibility

For services that don't need a high level of security. This configuration works with Firefox 3.6 and Safari 7.

- Ciphersuite: ECDHE-RSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-GCM-SHA384:DHE-RSA-AES128-GCM-SHA256:DHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES128-SHA256:ECDHE-RSA-AES256-SHA384:ECDHE-RSA-AES128-SHA:ECDHE-RSA-AES256-SHA384:ECDHE-RSA-AES128-SHA:ECDHE-RSA-AES256-SHA384
- Versions: TLSv1.1, TLSv1.2
- RSA key size: 2048
- DH Parameter size: 2048
- Elliptic curves: secp256r1, secp384r1, secp521r1
- Certificate signature: SHA-256, SHA-384, SHA-512
- HSTS: max-age=15724800

## Intermediate compatibility (default)

For services that don't need compatibility with legacy clients (mostly WinXP), but still need to support a wide range of client versions (Firefox 1, Chrome 1, IE 7, Opera 5 and Safari 4).

- Ciphersuite: ECDHE-RSA-AES128-GCM-SHA384:ECDHE-RSA-AES256-GCM-SHA384:DHE-RSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES128-SHA256:ECDHE-RSA-AES256-SHA384:ECDHE-RSA-AES128-SHA:ECDHE-RSA-AES256-SHA384:DHE-RSA-AES128-SHA256:DHE-RSA-AES256-SHA384:ECDHE-RSA-AES128-SHA256:DHE-RSA-AES128-SHA256:DHE-RSA-AES256-SHA384:ECDHE-RSA-AES128-SHA256:DHE-RSA-AES256-SHA384:ECDHE-RSA-AES128-SHA256:DHE-RSA-AES256-SHA384
- Versions: TLSv1, TLSv1.1, TLSv1.2
- RSA key size: 2048
- DH Parameter size: 2048
- Elliptic curves: secp256r1, secp384r1, secp521r1
- Certificate signature: SHA-1, SHA-256, SHA-384, SHA-512

## Old backward compatibility

This is the old ciphersuite that works with all clients back to Windows XP/IE6. It should be used as a last resort only.

- Ciphersuite: ECDHE-RSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES128-SHA256:ECDHE-RSA-AES256-SHA384:DHE-RSA-AES128-GCM-SHA256:DHE-RSA-AES256-GCM-SHA384:DHE-RSA-AES128-SHA256:DHE-RSA-AES256-SHA384:ECDHE-RSA-AES128-SHA256:ECDHE-RSA-AES256-SHA384:ECDHE-RSA-AES128-SHA:ECDHE-RSA-AES256-SHA384:ECDHE-RSA-AES128-SHA:ECDHE-RSA-AES256-SHA384:DHE-RSA-AES128-SHA256:DHE-RSA-AES256-SHA384:ECDHE-RSA-AES128-SHA256:DHE-RSA-AES256-SHA384:ECDHE-RSA-AES128-SHA256:DHE-RSA-AES256-SHA384:ECDHE-RSA-AES128-SHA256:DHE-RSA-AES256-SHA384
- Versions: SSLv3, TLSv1, TLSv1.1, TLSv1.2
- RSA key size: 2048
- DH Parameter size: 1024 (see [Pre-defined DHE groups](#))
- Elliptic curves: secp256r1, secp384r1, secp521r1
- Certificate signature: SHA-1 (windows XP pre-sp3 is incompatible with sha-256)

[https://wiki.mozilla.org/Security/Server\\_Side\\_TLS](https://wiki.mozilla.org/Security/Server_Side_TLS)

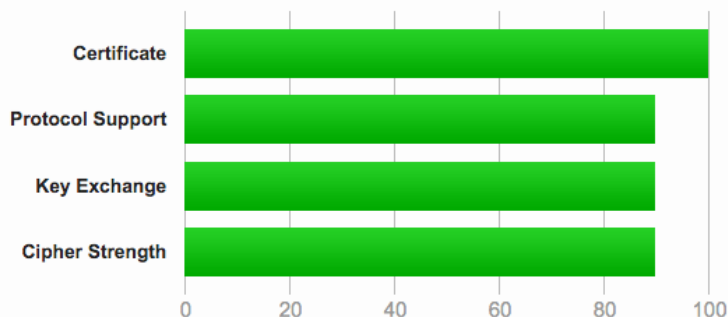




# https://www.ssllabs.com

## Summary

### Overall Rating



Visit our [documentation page](#) for more information, configuration guides, and books. Known issues are documented [here](#).

This server uses SSL 3, which is obsolete and insecure. Grade capped to B. [MORE INFO »](#)

This server accepts RC4 cipher, but only with older protocol versions. Grade capped to B. [MORE INFO »](#)

The server does not support Forward Secrecy with the reference browsers. [MORE INFO »](#)

This server supports TLS\_FALLBACK\_SCSV to prevent protocol downgrade attacks.

This server supports HTTP Strict Transport Security with long duration. [MORE INFO »](#)





# 11.11 HTTPS保障

## 风险点和监控

- DNS、网络设备、负载均衡、发布、OCSP server
- 服务器/客户端性能、访问量、tls新建比率

## 预案

- 降级、限流和防攻击

## 压测

- 评估模型、模拟瞬间峰值


## 异地容灾




# QA

李振宇 : [tony.lizy@alibaba-inc.com](mailto:tony.lizy@alibaba-inc.com)



 @阿里技术保障



 @阿里技术保障