跨域

从入门到工作：前后端分离

版权声明

联系方式

如果你想要购买本课程
请微信联系 xiedaimala02 或 xiedaimala03

如果你发现有人盗用本课程
请微信联系 xiedaimala02 或 xiedaimala03

跨域

面试必必必问，菜逼必定不会答

跨域关键知识

- 同源策略
  - ✓ 浏览器故意设计的一个功能限制
- CORS
  - ✓ 突破浏览器限制的一个方法
- JSONP
  - ✓ IE 时代的妥协

同源策略

什么是同源

同源定义

- 源
  - window.origin 或 location.origin 可以得到当前源
  - 源 = 协议 + 域名 + 端口号
- 如果两个 url 的
  - 协议
  - 域名
  - 端口号
  - 完全一致，那么这两个 url 就是同源的
- 举例
  - https://qq.com、https://www.baidu.com 不同源
  - https://baidu.com、https://www.baidu.com 不同源
  - 完全一致才算同源

同源策略定义

- 浏览器规定
  - 如果 JS 运行在源 A 里，那么就只能获取源 A 的数据
  - 不能获取源 B 的数据，即不允许跨域
- 举例（省略 http 协议）
  - 假设 frank.com/index.html 引用了 cdn.com/1.js
  - 那么就说「1.js 运行在源 frank.com 里」
  - 注意这跟 cdn.com 没有关系，虽然 1.js 从它那下载
  - 所以 1.js 就只能获取 frank.com 的数据
  - 不能获取 1.frank.com 或者 qq.com 的数据
- 这是浏览器的功能！
  - 浏览器故意要这样设计的

浏览器这样做的目的是啥

为了保护用户隐私！

怎么保护的?

如果没有同源策略

- 以 QQ 空间为例
  - 源为 https://user.qzone.qq.com
  - 假设，当前用户已经登录（用 Cookie，后面会讲）
  - 假设，AJAX 请求 /friends.json 可获取用户好友列表
  - 到目前为止都很正常
- 黑客来了
  - 假设你的女神分享 https://qzone-qq.com 给你
  - 实际上这是一个钓鱼网站
  - 你点开这个网页，这个网页也请求你的好友列表
  - https://user.qzone.qq.com/friends.json
  - 请问，你的好友列表是不是就把黑客偷偷偷走了？
  - 好像是哦……

问题的根源

- 无法区分发送者
  - QQ 空间页面里的 JS 和黑客网页里的 JS
  - 发的请求几乎没有区别（referrer 有区别）
  - 如果后台开发者没有检查 referer，那么就完全没区别
  - 所以，没有同源策略，任何页面都能偷 QQ 空间的数据
  - 甚至支付宝余额！
- 那检查 referer 不就好了？
  - 安全原则：安全链条的强度取决于最弱一环
  - 万一这个网站的后端开发工程师是个傻 X 呢
  - 所以浏览器应该主动预防这种偷数据的行为
  - 总之，浏览器为了用户隐私，设置了严格的同源策略

同源策略

不同源的页面之间，不准互相访问数据

你说了这么多，可有证据?

我们需要做两个网站来演示一下

步骤

- 创建目录
  - qq-com 里面有一个 server.js，用来模拟 QQ 空间
  - frank-com 里面有一个 server.js，用来模拟坏人网站
- qq-com
  - /index.html 是首页
  - /qq.js 是 JS 脚本文件
  - /friends.json 是模拟的好友数据
  - 端口监听为 8888，访问 http://127.0.0.1:8888
- frank-com
  - /index.html 是首页
  - /frank.js 是 JS 脚本文件
  - 端口监听为 9999，访问 http://127.0.0.1:9999

hosts

- 设置本地域名映射
  - 让 qq.com 映射到 127.0.0.1
  - 就可以访问 http://qq.com:8888/index.html 了
  - 让 frank.com 映射到 127.0.0.1
  - 就可以访问 http://frank.com:9999/index.html 了
- 如何设置 hosts
  - 需要用管理员权限操作
  - 老师，我没用管理员权限怎么也可以？ ——哦
  - 百度搜索 Win7 设置 hosts
  - 百度搜索 Win10 设置 hosts
  - 百度搜索 mac 设置 hosts
  - 百度搜索 Ubuntu 设置 hosts
  - 每个系统方法不同，我只演示我的系统

跨域 AJAX

- 正常使用 AJAX
  - ✓ 在 qq.com:8888 里运行的 JS 可以访问 /friends.json
- 黑客偷数据
  - ✓ 在 frank.com:9999 里运行的 JS 不能访问！
  - ✓ 浏览器需要 CORS
- 提问
  - ✓ 黑客的请求发成功了没有？
  - ✓ 答：成功了，因为 qq.com 后台有 log
  - ✓ 黑客拿到响应了没有？
  - ✓ 答：没有，因为浏览器不给数据给它

就没有浏览器不限制跨域么

如果不限制，就是浏览器 bug 了，快向浏览器反馈

其他新手疑问

- 为什么 a.qq.com 访问 qq.com 也算跨域?
- 答：因为历史上，出现过不同公司共用域名，a.qq.com 和 qq.com 不一定是同一个网站，浏览器谨慎起见，认为这是不同的源
- 为什么不同端口也算跨域?
- 答：原因同上，一个端口一个公司。记住安全链条的强度取决于最弱一环，任何安全相关的问题都要谨慎对待
- 为什么两个网站的 IP 是一样的，也算跨域?
- 答：原因同上，IP 可以共用。
- 为什么可以跨域使用CSS、JS和图片等?
- 答：同源策略限制的是数据访问，我们引用 CSS、JS 和图片的时候，其实并不知道其内容，我们只是在引用。不信我问你，你能知道 CSS 的第一个字符是什么吗?

现实却是：请问怎么跨域

面试官会问你，工作中也会遇到

解法一：CORS

cross-origin resource sharing, 跨域资源共享

- 问题根源
  - ✓ 浏览器默认不同源之间不能互相访问数据
  - ✓ 但是 qq.com 和 frank.com 其实都是方方的网站
  - ✓ 方方就是想要两个网站互相访问，浏览器为什么阻止
- 好吧，用 CORS
  - ✓ 浏览器说，如果要共享数据，需要提前声明！
  - ✓ 哦，那怎么声明呢？
  - ✓ 浏览器说，qq.com 在响应头里写 frank.com 可以访问
  - ✓ 哦，具体语法呢？
  - ✓ Access-Control-Allow-Origin: http://foo.example
  - ✓ 浏览器说：都得文档里，去看 MDN 文档嘛

文档现在不用看，工作要用到再看

CORS 就这么简单？！

是的，就一句话的事情。想想看，是否完美解决了问题

注意：CORS 分为简单请求和复杂请求，具体看文档

IE 说：你猜我支持不支持

哪还用猜？艹 IE 6 7 8 9

那么如果要兼容 IE，怎么办

JSONP

- 定义
  - JSONP 和 JSON 半毛钱关系都没有
  - 由于前端水平低下，错误地将其称为 JSONP
  - 具体定义看后面代码
- 我们现在面临地问题是什么
  - 程序员常常面临奇葩需求
  - 没有 CORS，怎么跨域
  - 记不记得我们可以随意引用 JS
  - 虽然我们不能访问 qq.com:8888/friends.json
  - 但是我们能引用 qq.com:8888/friends.js 啊！
  - 这有什么用？JS 又不是数据
  - 我们让 JS 包含数据不就好了……
  - 试试看吧！明天就要上线啦！

步骤

注：其它网站也可以引用friends.js获取数据了。

- frank.com 访问 qq.com

- ✓ qq.com 将数据写到 /friends.js
- ✓ frank.com 用 script 标签引用 /friends.js
- ✓ /friends.js 执行，执行什么呢?
- ✓ frank.com 事先定义好 window.xxx 函数
- ✓ /friends.js 执行 window.xxx({frinds:[...]})
- ✓ 然后 frank.com 就通过 window.xxx 获取到数据了
- ✓ window.xxx 就是一个回调啊!
- ✓ 这 TM 都能想到，人才啊!
- ✓ 这是很多前端工程师一起想出来的

优化

- xxx 能不写死吗?
  - window.xxx 能不能改其他名字?
  - 其实名字不重要，只要 frank.com 定义的函数名和 qq.com/friends.js 执行的函数名是同一个即可!
  - 那就把名字传给 /friends.js !
  - 看我改代码

再优化

- 封装！

- ✓ 初级程序员学 API，中级程序员学封装。
- ✓ 封装成 jsonp('url').then(f1, f2)

JSONP 是什么

完美回答（优缺点）

以上就是跨域的所有内容

足够大家搞定面试和工作