

# 有没有开放的API接口（直接用js调用的）？

互联网   JavaScript   API

关注者  
15

被浏览  
1,812

## 有没有开放的API接口（直接用js调用的）？

问一下，有没有开放的API接口，是那种不需要后台转发，直接js调用没有跨域问题的！显示全部

- 关注问题
- 写回答
- 邀请回答
- 好问题
- 添加评论
- 分享
- 

6 个回答

默认排序

 **Ayon Lee**  
Web 爱好者，GitHub 与知乎专栏: hyurl

4 人赞同了该回答

很多开放平台 api 都是这样的吧，比如地图，有跨域问题是因为没有加入白名单，或者服务端本身就不支持跨域访问。你有这问题说明还不了解同源策略的原理。

同源策略是浏览器的一套防治跨域访问和潜在威胁的手段，它只限制了对所需资源加载，然而实际上服务器却可能丝毫不做限制，例如你是用 api 跨域登陆一个网站，你在浏览器上看到报同源策略限制不允许加载，但实际上服务端那边却可能已经登陆成功，并将 cookie 什么的下发给了客户端，只是浏览器拒绝接受它们。

如果服务端要让客户端同意跨域加载它的资源，那么它就语言设置 Access-Control-Allow-Origin 这一类头字段，如果服务器是完全开放的，那么它可以将这个头设置为 \*，如果只对白名单开放，那么可以在请求收到后动态设置这个头为请求发起的源域名。但无论是那种方法，看起来好像是服务端决定了决定了资源是否应该被加载，然而却恰好相反，在同源策略中，服务端其实处于被动地位，它要通过设置请求头来告诉浏览器它希望自己的资源不要被屏蔽。否则即使服务器完整的进行了相关操作，例如登录，浏览器还是要拒绝它的响应内容。

我个人觉得，同源策略是一个失败的策略，一方面，在规范上，它没有明确说明服务端的责任（实际上根本没说）。另一方面，同源策略根本看不出来能用来解决什么问题，除了带来不便。如果一个网站希望它不要访问外域资源，因为可能不安全，但是同源策略实际上丝毫不能限制网站对外访问，只要它在相应头加上一Access-Control-Allow-Origin 这一类字段，网站就能肆无忌惮的访问它。而在服务端，因为没有明确服务端的责任，所以服务端以为同源限制是客户端的工作，因此服务端不做任何处理，所以也就是为什么虽然你在浏览器看不到登录的结果，但实际上服务端已经登录成功。

在 NPM 上有一个名为 cors 的包，被用来通过自动设置 Access-Control-Allow-Origin 这一类相应头，下载量很大，但实际上这个包完全不限制客户端的跨域请求行为，只是被动地告诉客户端自己的资源希望被加载。出现这种问题（BUG）的原因，就在同源策略自身上，因为它没有告诉服务器应该怎么处理和限制跨域请求行为。如果一个服务端认为其他源可能存在危险而限制访问，那么它就应该有一套策略来限制客户端的请求，而不是设置个什么响应头。

编辑于 2019-09-01

赞同 4   1 条评论   分享   收藏   喜欢   ...


 **包勇明**  
前端工程师

NEI 是一个接口管理平台，在上面可以定义接口（包括请求地址、请求方式、请求参数、响应结果等），定义好的接口也提供了在线 Mock 接口，可以直接通过 JS 调用，没有跨域问题，因为 NEI 后端已经处理好了，也就是给 Mock 接口加了可以跨域请求的响应头信息。

比如官方的Todo Demo中的接口：nei.netease.com/api/api...

编辑于 2019-09-03

赞同   1 条评论   分享   收藏   喜欢   ...

 **龙腾道默默地**  
数据结构即业务逻辑。

如果你问的是能跨任何域的前端技术，那么没有浏览器扩展等的辅助，这是不可能的。

如果你问的是主流网站有没有提供这种端口，而不是只能可视化访问的，那么还是有的，其中比较有代表性的是GitHub。

发布于 2019-09-03

赞同   添加评论   分享   收藏   喜欢   ...



有没有开放的API接口（直接用js调用的）？



chenmingmeng

1 人赞同了该回答

今日头条开放的是内容对接入口，你的网站和微信的内容导入今日头条。

查看追问

发布于 2019-09-04

▲ 赞同 1 ▼ ● 添加评论 ➦ 分享 ★ 收藏 ♥ 喜欢 ...



林一二

想开发自动生成的无限世界

如果你是需**要** BaaS（后端即服务），试试 SoLiD，中文介绍见 [learnsolid.cn](#)，文档里也有关于同源策略设计的解释 [为互联网应用授权：关于同源策略的背景知识](#)。

同源策略是为了防止自己家的服务被黑客嵌入在钓鱼网站里调用，所以是服务端来做这个控制，服务端知道和自己相适配的前端有哪几个，就都放在白名单里。

所以同源策略是浏览器听服务端的话，不听客户端 JS 的话。如果让客户端 JS 来控制，那么钓鱼网站的 JS 会很自然地会要求浏览器关闭同源策略，然后盗取你在别的网站上的 cookie。

编辑于 2019-09-01

▲ 赞同 ▼ ● 添加评论 ➦ 分享 ★ 收藏 ♥ 喜欢 ...



夏天的西瓜

有

发布于 2019-10-28

继续浏览内容



知乎

发现更大的世界

打开



Chrome

继续

