[什么是同源策略？如何解决跨域问题？ - 掘金 (juejin.cn)](https://juejin.cn/post/6904070281048883208)

**什么是同源策略**

同源即同协议，同域名，同端口。

同源策略是浏览器的一个安全功能，用于隔离潜在恶意文件的重要安全机制。不同源的客户端脚本在没有明确授权情况下，不能读写对方的资源。

**为什么会存在跨域？如何解决跨域问题？**

浏览器的同源策略造成了跨域。

1代理（生产环境不发生跨域，开发环境发生跨域）

2.JSONP

当需要跨域请求的时候，不利用AJAX，而是生成一个script元素去请求服务器，因为浏览器不阻止script元素的请求，这样请求可以到达服务器。服务器拿到请求后，响应一段JS代码，这段代码实际上是个函数调用，把浏览器所需要的数据作为参数传递到函数中，从而间接得传递到客户端。但是只能支持get请求

3.CORS（Cross-Origin-Resource-Share）

cors是基于http1.1的跨域解决方案，如果浏览器要跨域访问服务器的资源，需要获得服务器的允许。

根据不同的请求，cors规定了三种不同的交互模式。

1.简单请求，如果ajax跨域请求被浏览器判定为简单请求，就会在请求头添加Origin字段，Origin字段会告诉服务器是哪个源地址在跨域请求。服务器收到请求后，如果允许请求跨域，则会在响应头中添加Access-Control-Arrow-Origin字段。2如果浏览器不认为这是个简单请求（复杂请求）。浏览器发送预检请求，询问浏览器是否可以。（预检请求请求方法是OPTIONS 没有请求体，请求头包含Origin，请求的源，Access-Control-Request-Method：后续请求得方法，Aceess-Control-Request-Header：后续请求头）如果浏览器允许，则会在响应头中添加Access-Control-Allow-Origin，Access-Control-Allow-Method，Access-Control-Allow-Headers，Access-Control-max-age告诉浏览器，多少秒内对于同样的请求源，方法，头，都不需要发送预检请求。之后就是浏览器发送真实消息，服务器发送真实响应

3.附带身份凭证，请求头中添加cookie字段，服务器响应时，如果响应头中有Access-Control-Allow-Credentials：true，说明服务器允许这样的请求

**简单请求、复杂请求？**

简单请求跨域方法只能是head，post，get。请求头中只能有Accept，Accept-language,content-language，last-event-id，content-type只能为application/x-www-form-urlencoded,multipart/form-data,text/plain