<http://blog.csdn.net/lambert310/article/details/51683775>

**什么是跨域？**

跨域，指的是浏览器不能执行其他网站的脚本。它是由浏览器的同源策略造成的，是浏览器对javascript施加的安全限制。

**所谓同源是指，域名，协议，端口均相同，不明白没关系，举个栗子：**

**http://www.123.com/index.html 调用 http://www.123.com/server.php （非跨域）**

**http://www.123.com/index.html 调用 http://www.456.com/server.php （主域名不同:123/456，跨域）**

**http://abc.123.com/index.html 调用 http://def.123.com/server.php （子域名不同:abc/def，跨域）**

**http://www.123.com:8080/index.html 调用 http://www.123.com:8081/server.php （端口不同:8080/8081，跨域）**

**http://www.123.com/index.html 调用 https://www.123.com/server.php （协议不同:http/https，跨域）**

**请注意：localhost和127.0.0.1虽然都指向本机，但也属于跨域。**

浏览器执行javascript脚本时，会检查这个脚本属于哪个页面，如果不是同源页面，就不会被执行。

**解决办法：**

**1、JSONP：**

使用方式就不赘述了，但是要注意JSONP只支持GET请求，不支持POST请求。

**2、代理：**

例如www.123.com/index.html需要调用www.456.com/server.php，可以写一个接口www.123.com/server.php，由这个接口在后端去调用www.456.com/server.php并拿到返回值，然后再返回给index.html，这就是一个代理的模式。相当于绕过了浏览器端，自然就不存在跨域问题。

**3、PHP端修改header（XHR2方式）**

在php接口脚本中加入以下两句即可：

header('Access-Control-Allow-Origin:\*');//允许所有来源访问

header('Access-Control-Allow-Method:POST,GET');//允许访问的方式