链滴

CORS 跨域发送 Cookie

作者：yiranblade

原文链接：https://ld246.com/article/1496315086438

来源网站：链滴

引言

由于默认情况下浏览器对跨域请求不允许携带Cookie，所以这次开发再与前端同学在权限验证这块踩好多坑，故将一些教训写下来，共勉！

CROS

在 2014 年 W3C 发布了 CORS Recommendation 来允许更方便的跨域资源共享，同时CORS也允我们使用额外的相应头字段来允许跨域发送Cookie。

模拟前端代码

设置withCredentials为true即可让该跨域请求携带 Cookie。 注意携带的是目标页面所在域的 Cooki 。以JQuery示例

```
$.ajax({
   type: "GET",
   url: "http://localhost:8080/seek/userinfo/#{xxxxx}",
   async:false,
   xhrFields: {
      withCredentials: true
   },
   success: function(msg){
     alert(msg.msg);

    }

});
```

模拟后端代码

此处还需要设置服务器接受跨域发送的Cookie。 否则会被浏览器的同源策略挡住：

服务器主要是设置response access-control-allow-credentials为"true"， 即可允许跨域请求携带 C okie。

相关代码如下:

```
response.setHeader("Access-Control-Allow-Origin", request.getHeader("Origin"));
response.setHeader("Access-Control-Allow-Methods", "POST, GET, OPTIONS, DELETE,PUT");

response.setHeader("Access-Control-Max-Age", "3600");
response.setHeader("Access-Control-Allow-Headers", "Origin, Content-Type, X-Auth-Token ,
uthorization");         response.setHeader("Access-Control-Allow-Credentials", "true");;
```

注意要点

跨域发送 Cookie 还要求 Access-Control-Allow-Origin不允许使用通配符事实上不仅不允许通配符而且只能指定单一域名

原文链接：CORS 跨域发送 Cookie

原文如下:

If the credentials flag is true and the response includes zero or more than one Access-Control Allow-Credentials header values return fail and terminate this algorithm. –W3C Cross-Origin esource Sharing

我采取的策略是request.getHeader("Origin")每次都获取请求的源，但是这样做的缺点也是很多的主要就是不安全，任意请求携带Cookie都可以接受，最好的就是服务端可以维护一个接受Cookie的Origin列表，验证Origin后在将其设置为Access-Control-Allow-Origin的值。

结束语

在正确配置后就可以跨域发送Cookie进行客户端与服务端之间相关的一些会话了，当然如果直接就是一域的话，那就肯定没这些问题啦，有时间再在这块深入一下^_^!

原文链接：CORS 跨域发送 Cookie