亿速云的cors配置不当漏洞挖掘

最近在研究cors，这不刚找了个网站练练手，

我相信在座的各位一定都是不喜欢看原理什么的 在此也就不多赘述，直接开始吧。

简单说下cors: CORS全称Cross-Origin Resource Sharing, 跨域资源共享，是HTML5的一个新特性，已被所有浏览器支持，不同于古老的jsonp只能get请求。

但如果长满头发的程序员犯了错误，配置出错怎么办？那就，嘿嘿嘿 

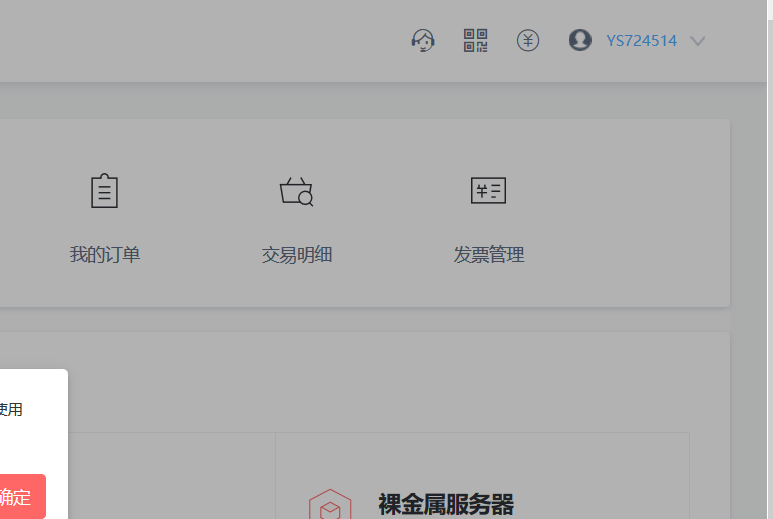
具体参照文章 <https://www.anquanke.com/post/id/97671> 讲解十分详细！

start:

官网：<https://www.yisu.com/>



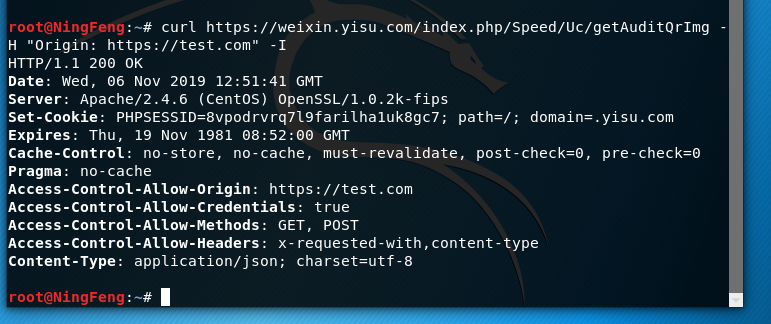
首先注册个账号这边我已经注册好了，



由此可见我的用户名是ys724514，要用curl请求看响应包。

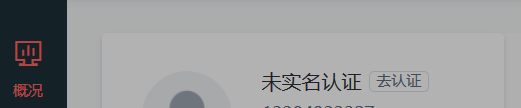
于是 启动kali，burp开干。

首先kali里用curl访问出现cors的接口

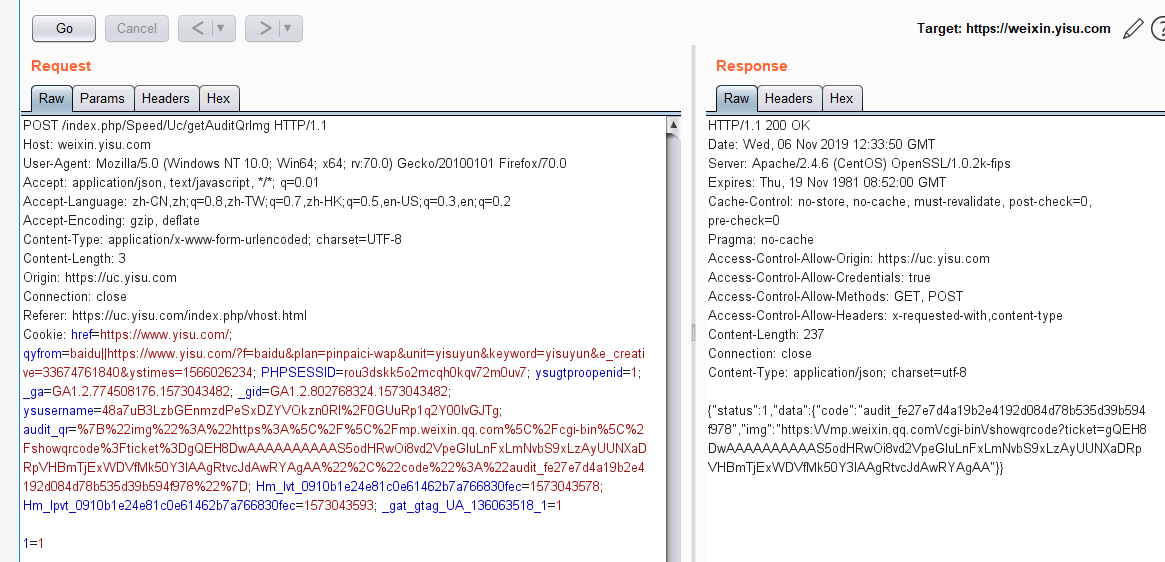


因为我这边是加了origin字段的，但他的返回包Access-Control-Allow-Origin: https://test.com

居然还是test.com 这程序员就该挨板子了啊。

开启burp 抓取

概况处的包 ，send to repeater ，go

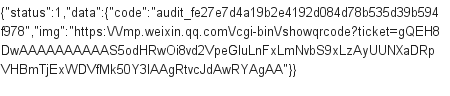


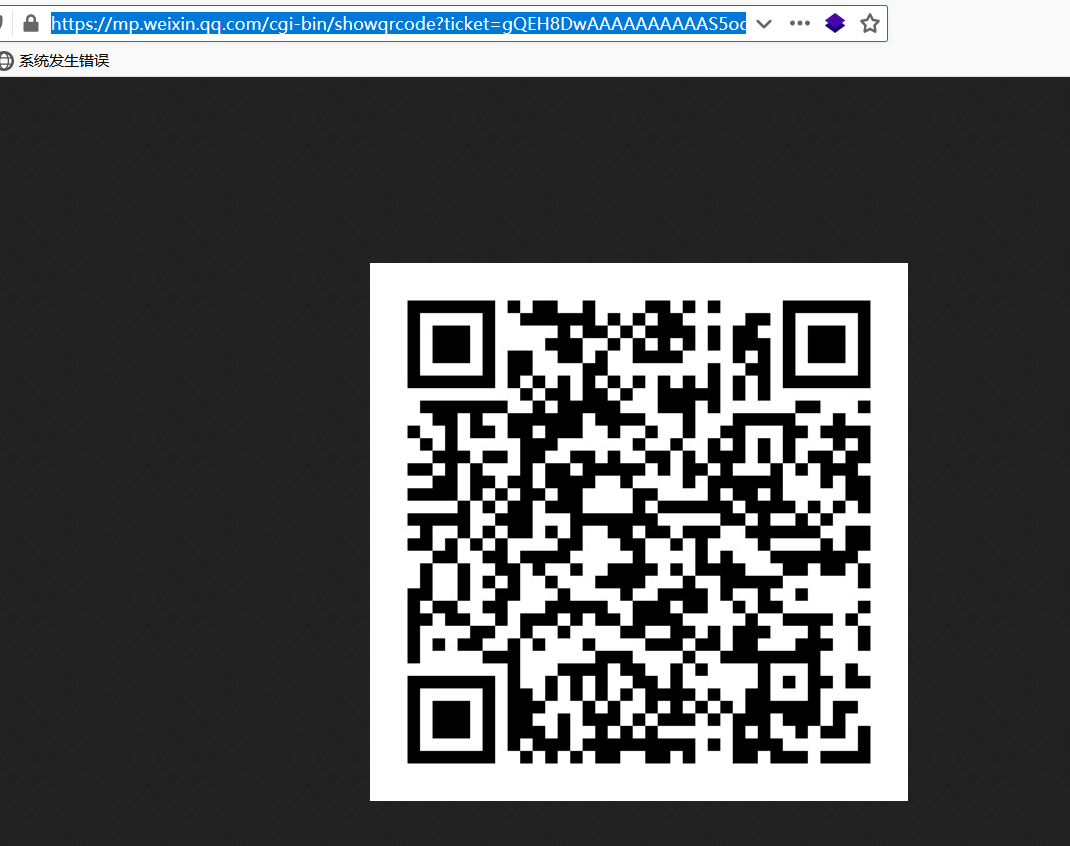
尝试放包后得到response 大家注意这个包的origin字段是和返回的

Access-Control-Allow-Origin也是相同的，这表明了什么不言而喻啊

Ok 其实刚刚curl的地址也是这个页面抓过来的 copy过去就可以了

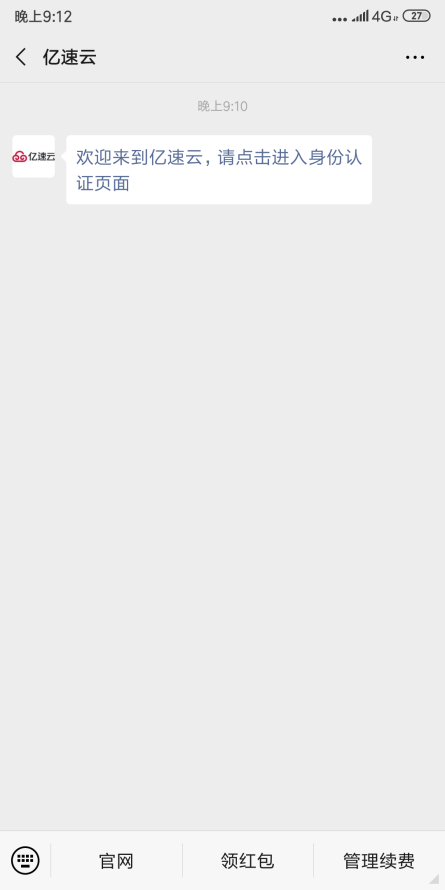
可以看到响应包返回了一个地址，我们去多余斜杠，用浏览器看看。





是一个二维码 我们扫描他试试，估计是返回用户信息的，

扫描后是关注公众号，不过不要紧 公众号里有用户信息



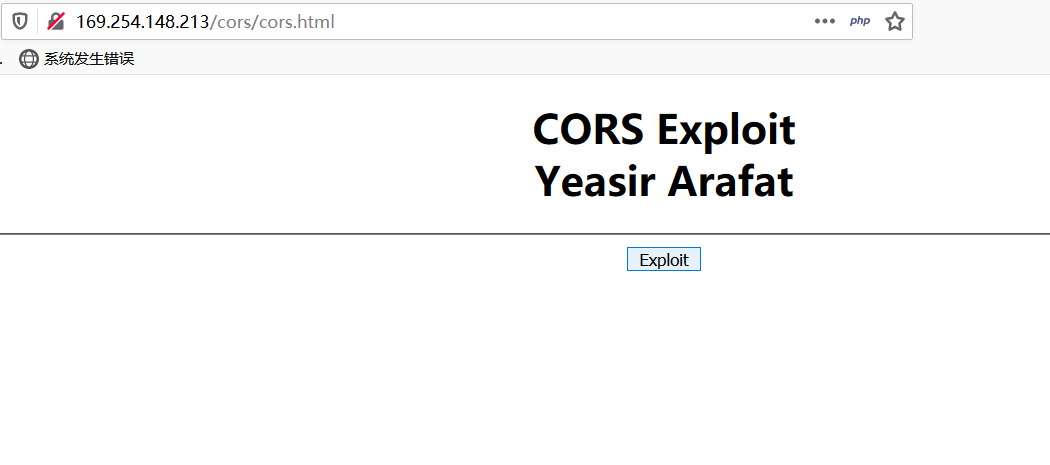


可以看到 用户是ys724514

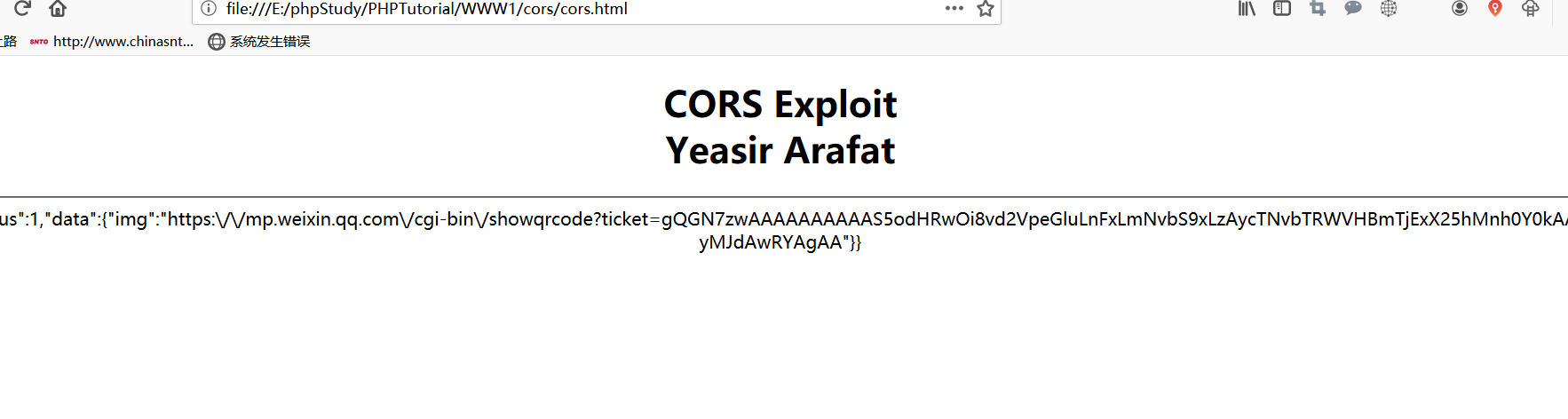
此时可以编写一波poc



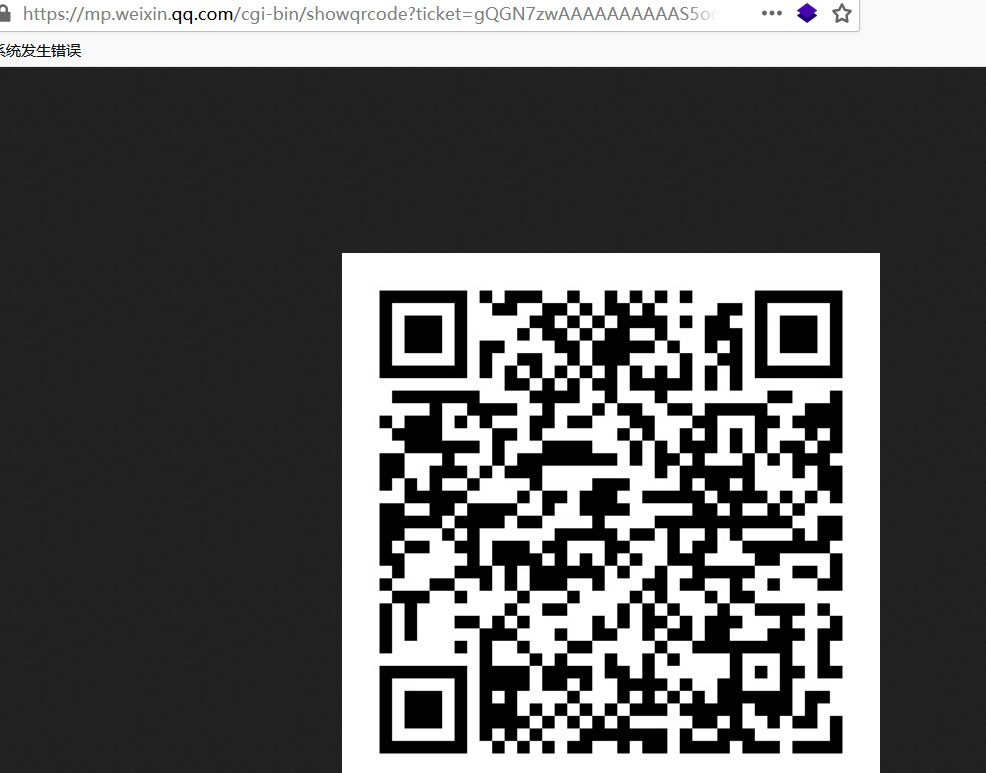
把最重要的部分改为他的接口即可 接下来部署好服务器 模拟黑客给用户发送这个页面 用户打开的效果！



用户点开之后是这样的 ，然后我们点击exploit 即可获取用户的二维码！



可以看到已经成功获取了，是跟原二维码一模一样的 黑客进行扫描即可获取用户数据。



不妨设想 我刚刚没有进行实名认证 若受害者是位实名用户，那危害 不言而喻啊。

Ok，分享结束，其实本例站点的类似接口还挺多的 大家可以去找找 好的拜拜！