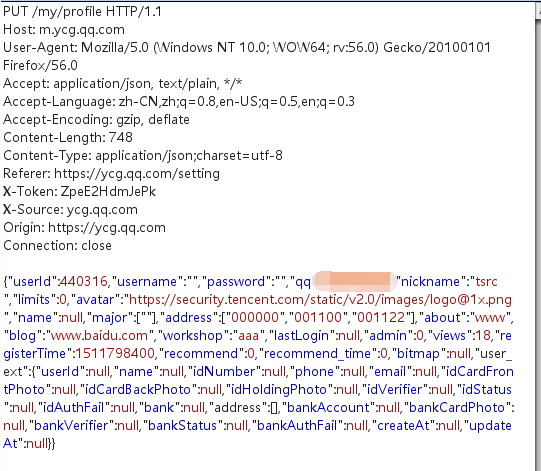
<https://ycg.qq.com/setting>

记忆中这个站点是可以引入第三方资源的 想来试试401钓鱼

结果发现网站改版了 ！

还是先来到记忆中可引入第三方资源的地方 保存个人信息头像处

数据包如下 一个put请求

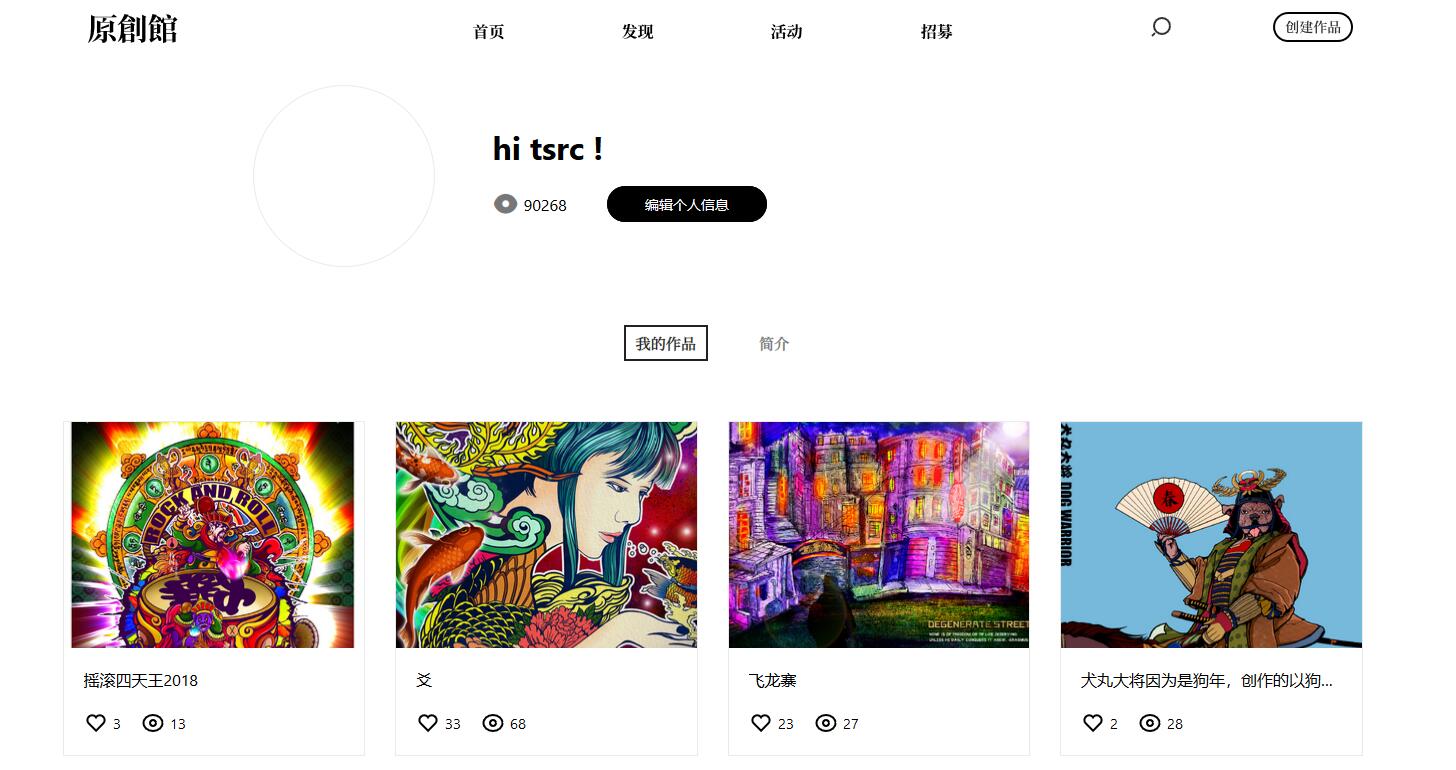


开始将userId改成他人的 其他不动 发现他的信息就被我改了 以为只是个简单的越权。。

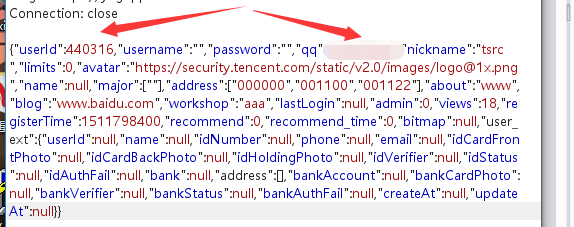
后来再看看 还有个username password参数 难道还可以设置账号密码？

随便输入了 username和password之后 就put上去了 重新登录 也没发现 需要账号密码啊 始终是qq登录

但当我点开我个人信息的时候 惊讶的发现 我的信息变成别人的了！！



再回来看下数据包 恍然大悟



这里userId与qq号绑定

所以就是 你想登录哪个用户 你就将他的id与你qq号绑定就完了！！