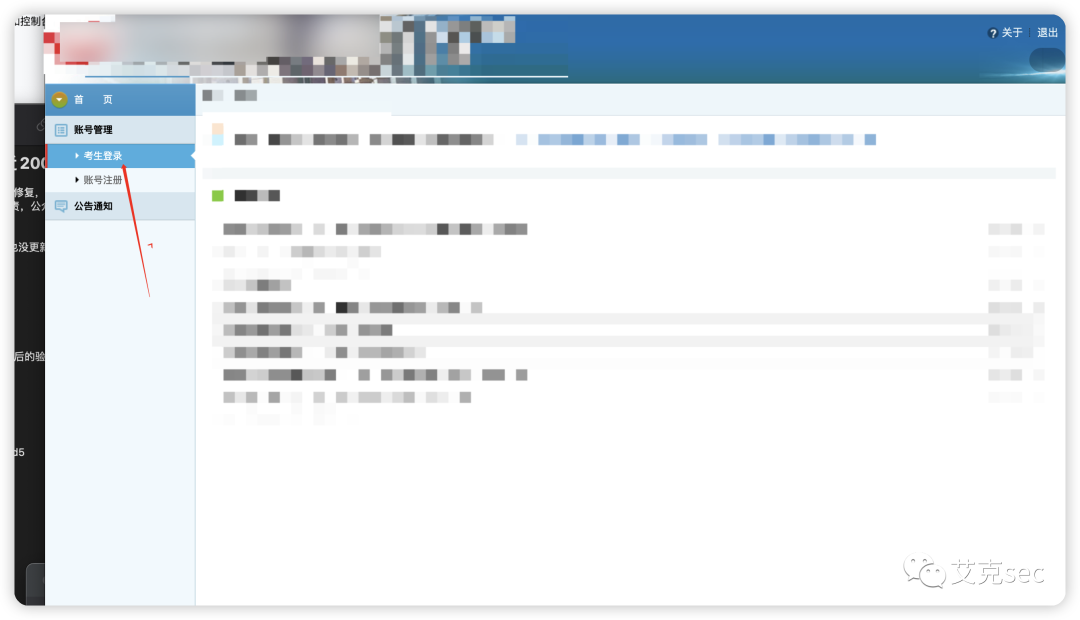
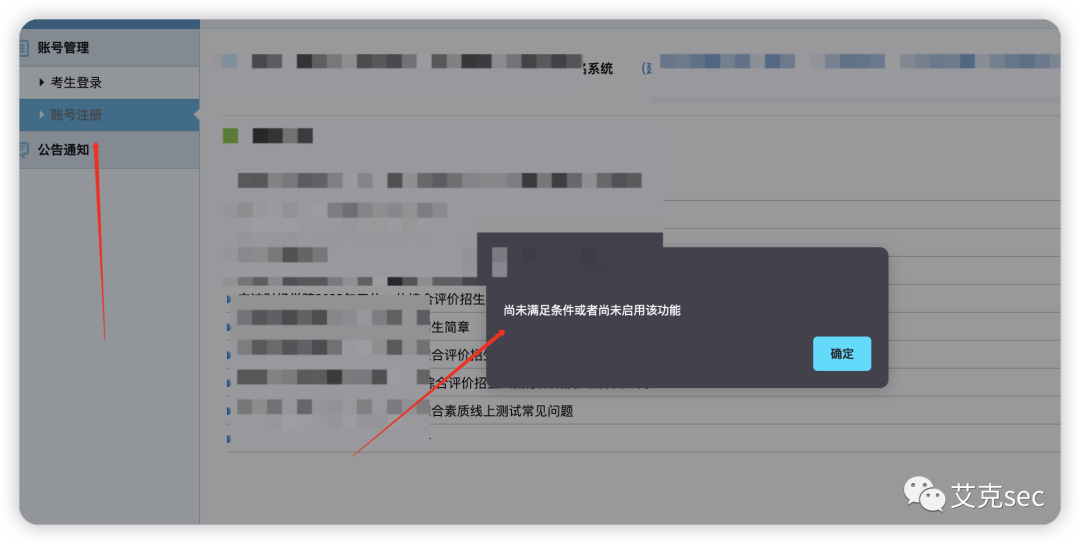
**第一套系统逻辑缺陷（二十所学校）**

主页面有登录和注册窗口，这种系统是最喜欢的，通常都是注册完进去去找功能点一一去测，系统没那么强的话还是很容易出洞的。



那当然没那么顺利，注册功能点关闭，没身份证没账号，去谷歌语法搜集了一些都没注册这个系统。



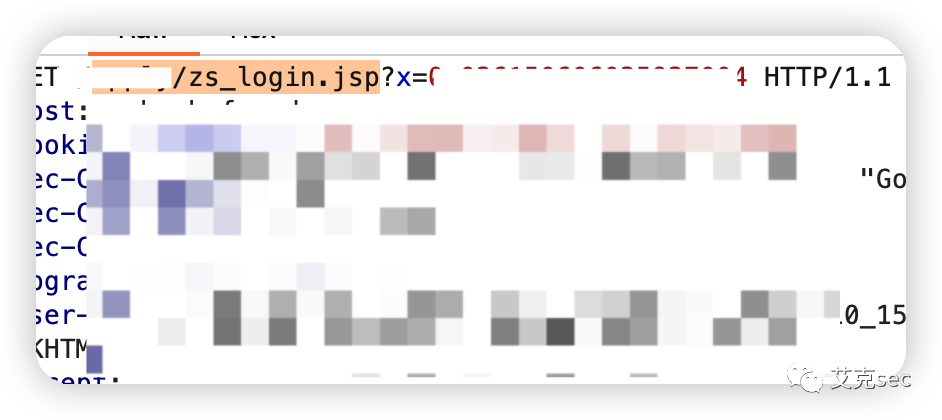
去翻js代码，看看有无留下的注册接口，可以使用



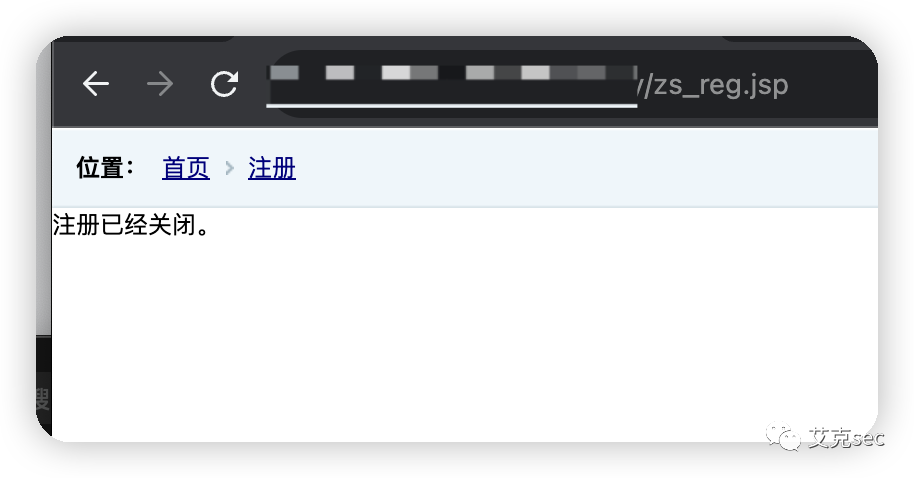
运气很差，只写了一个弹窗: (

陷入困境 扫了一些没用的目录

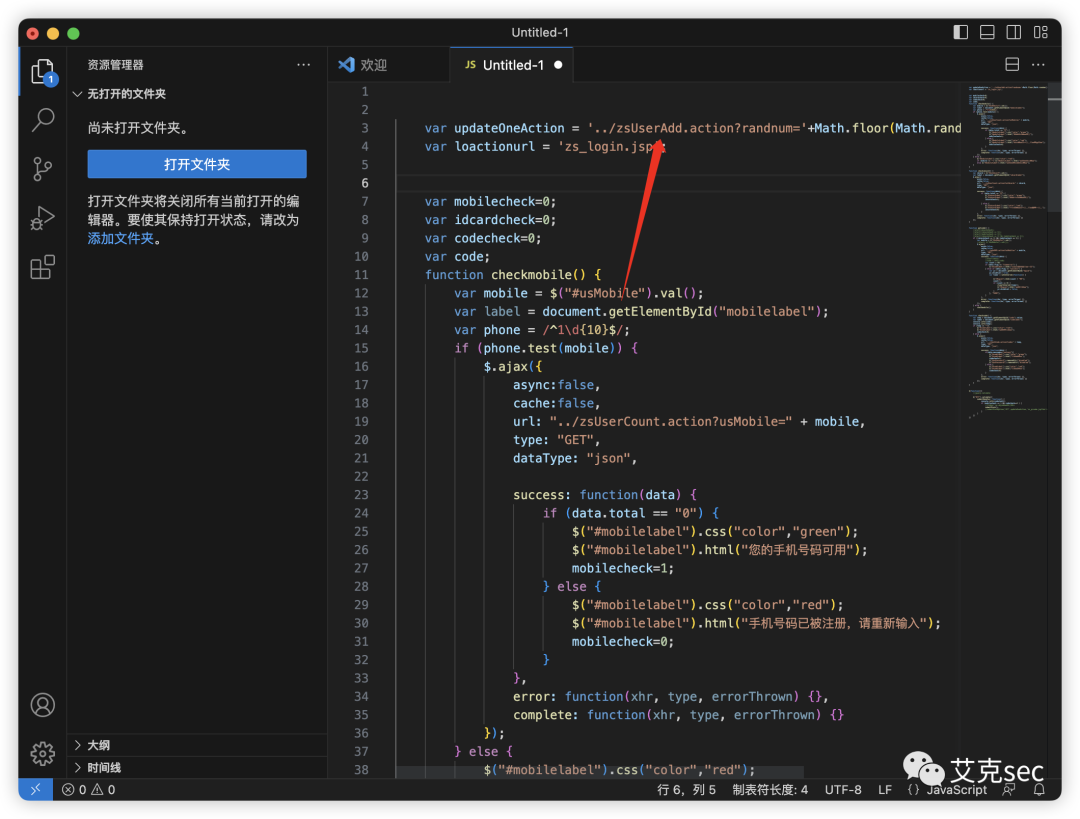
点一些仅有的功能点去burp里面看了一些请求包发现他们的目录前都加了一个zs\_



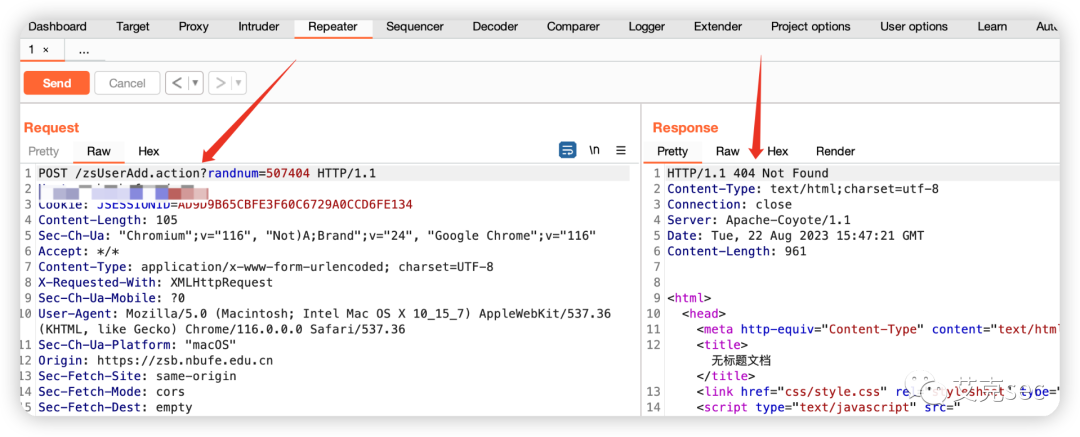
猜测了一些注册路径zs\_register zs\_reg zs\_zc 去拼接访问,找到了注册功能点，但是还是显示已经关闭



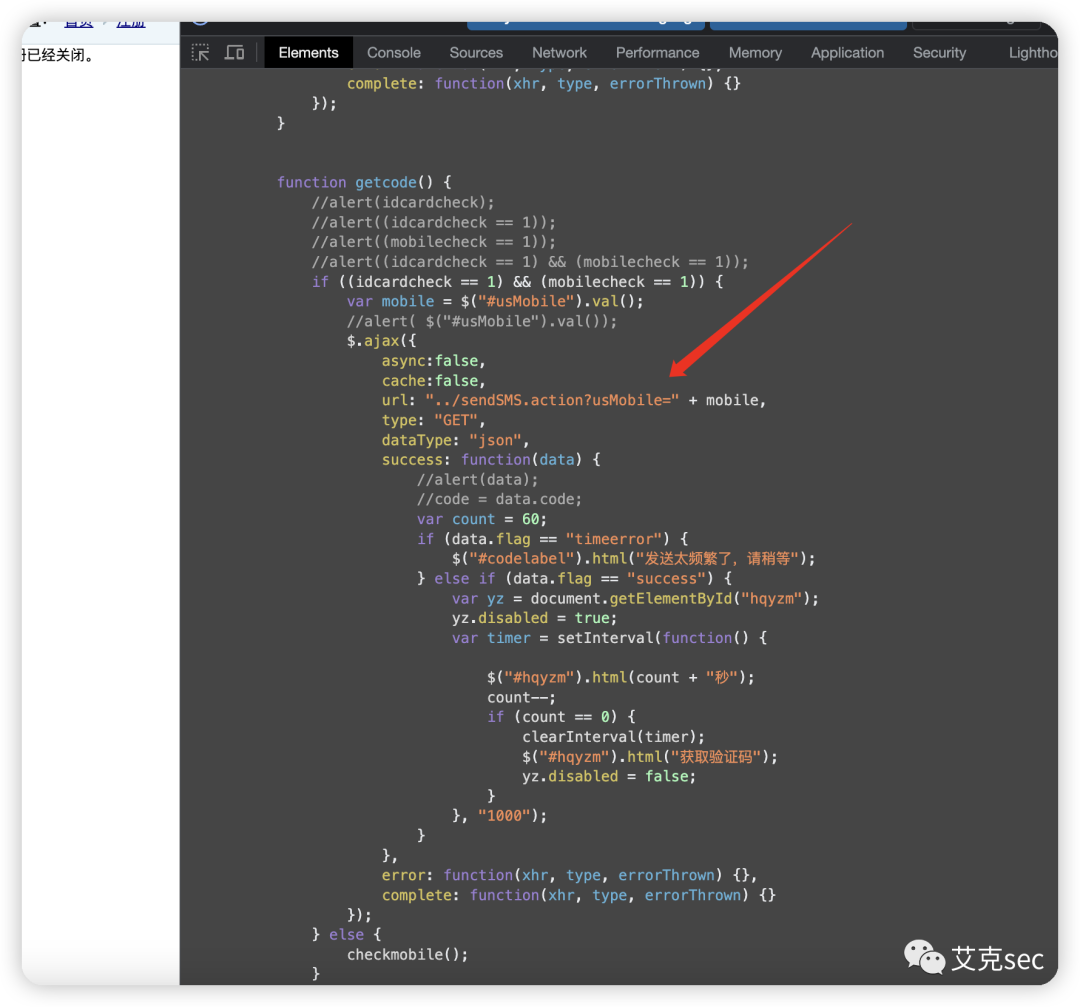
老样子去看js代码，这次就比较好运了，很多接口都写在了js里面，审计js代码，准备构造请求包，去注册一个账号



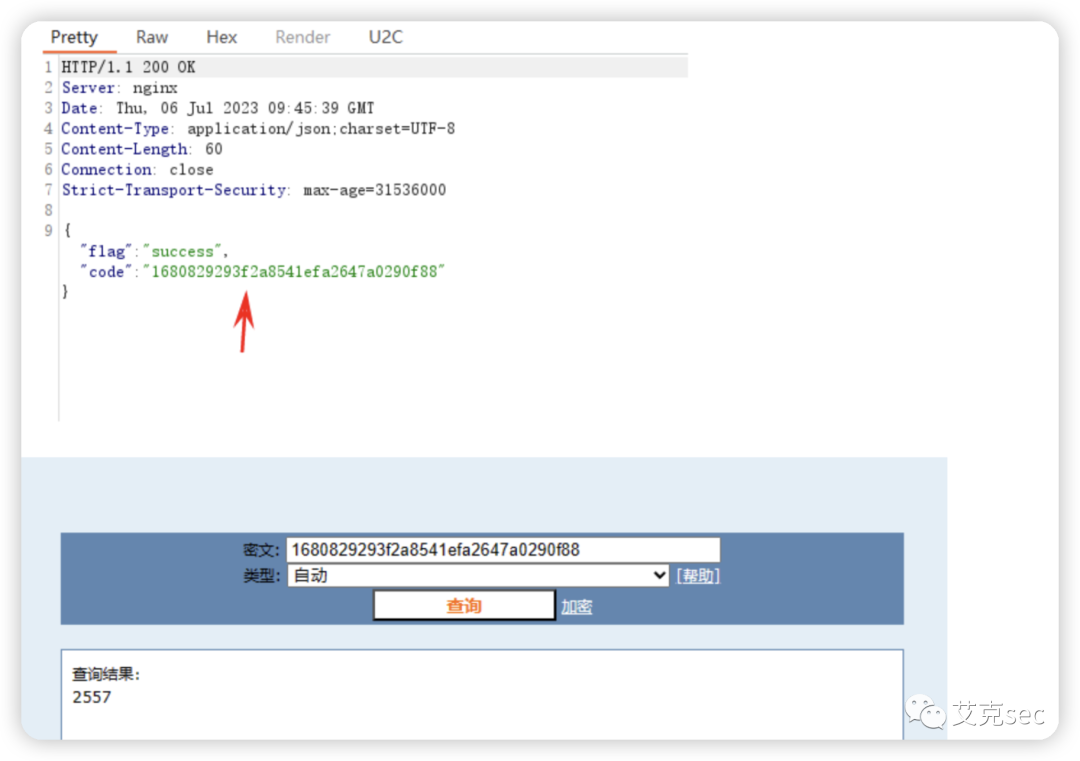
好家伙 注册接口直接给删了？跳了好几个目录去试了 确实是404，继续看js代码



发生验证码接口



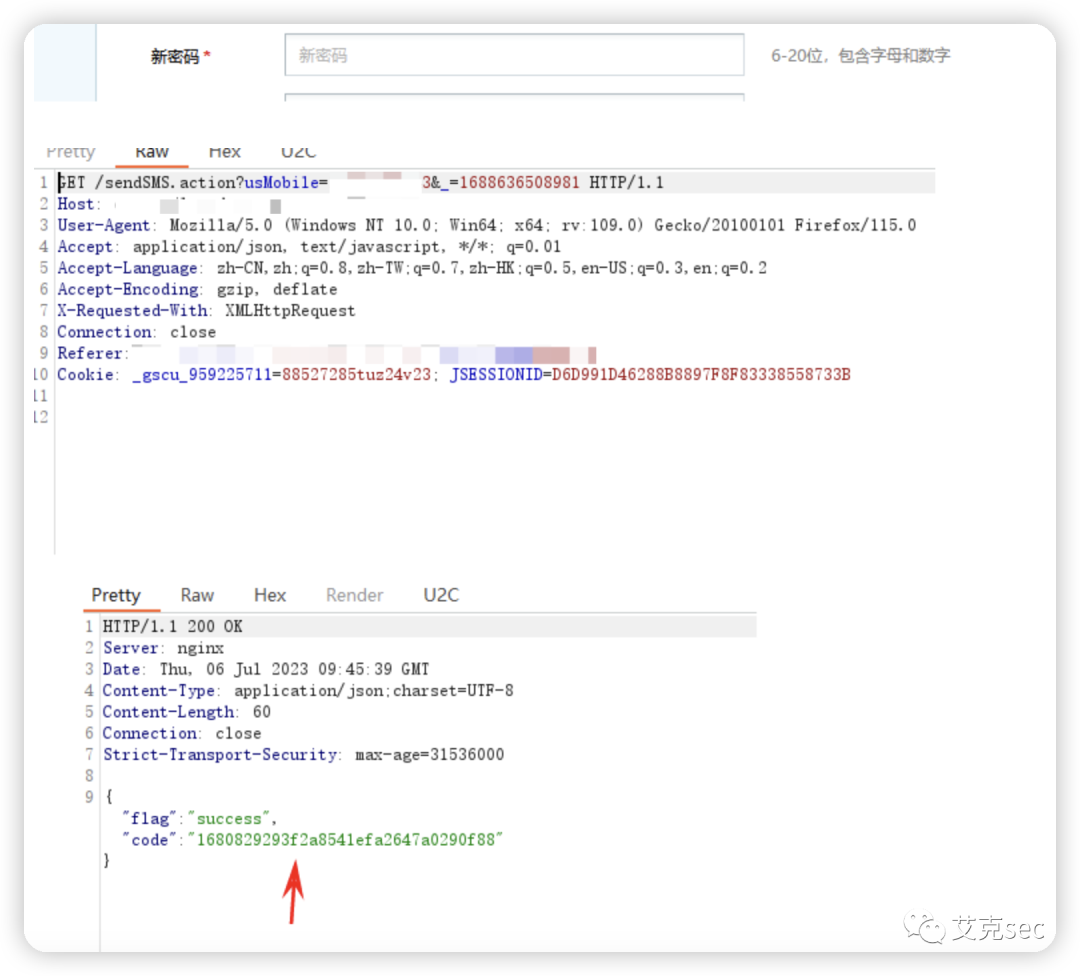
可用，直接回显出md5加密后的验证码，可用，但是注册功能关的，这时候怎么办，别忘了登录处还有个找回密码，发送验证码是不是同一个接口呢



身份证写够18位即可 打开burp抓包 拦截返回包修改 total为1 绕过前端判断账号是否存在



任意用户密码修改到手 。

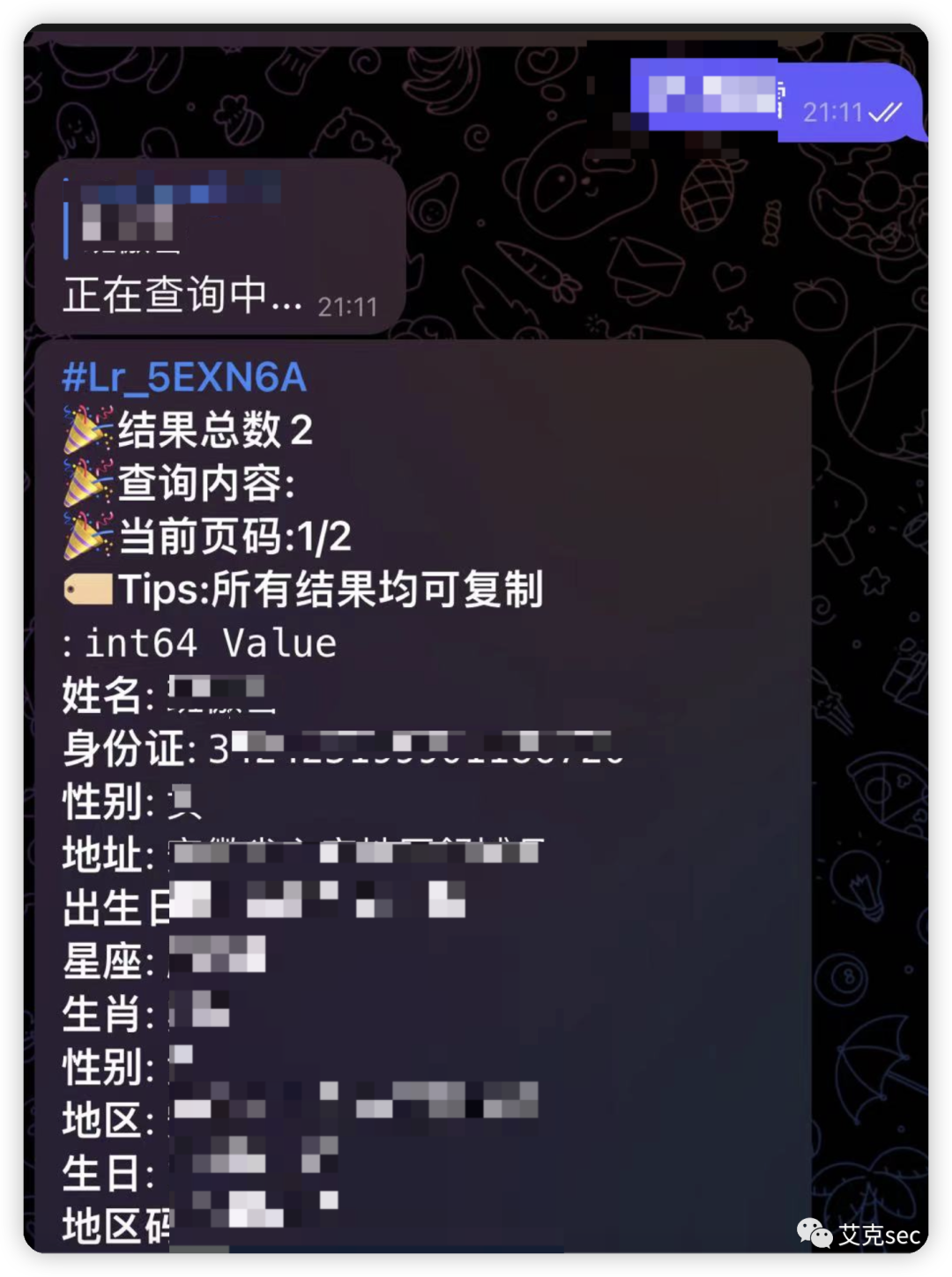


想进去进一步测试其他功能点，但是这个漏洞的前提是得知道账号，没账号咋办，那当然是白帽的最高境界 社会工程学攻击^

找到了一个公告接口，遍历了一下参数，找到了一个表格，但是只有姓名和身份证前后四位 中间的是 \*  2023年报考，推测都是0504的，用burp跑了一些生日，无果。



最终靠sgk查名字，找到了 （不得不感慨信息泄漏太严重了，查了几个都能查到，互联网人人裸奔）



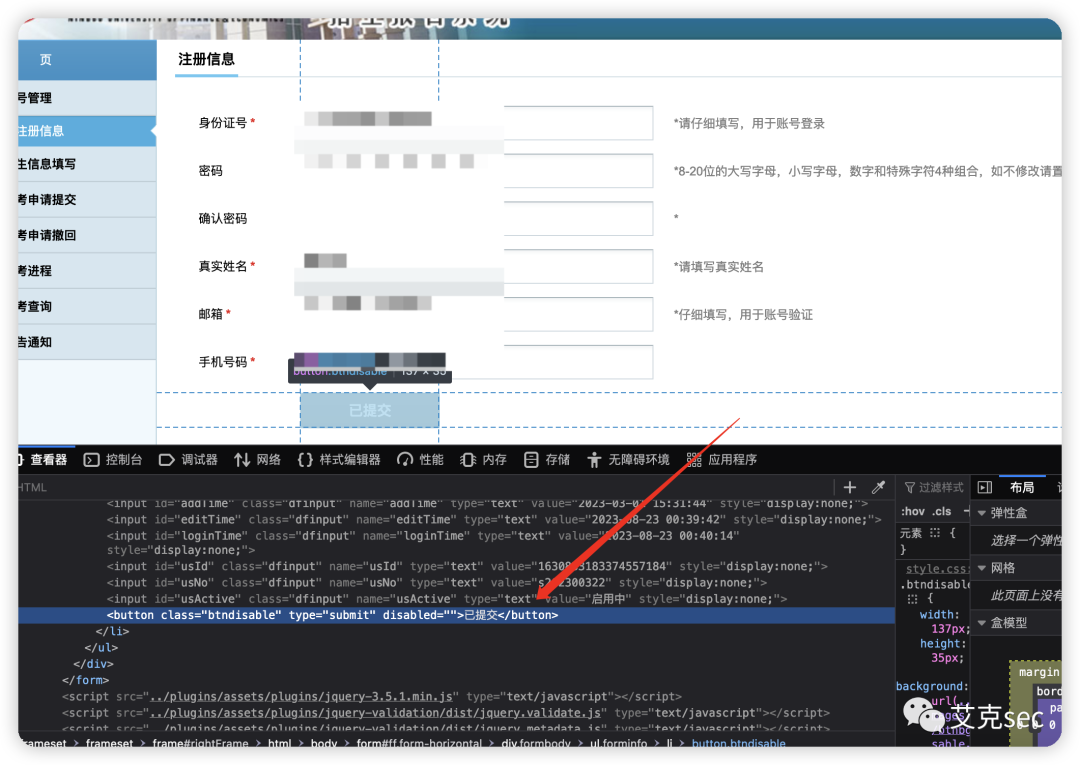
配合上面的漏洞，成功修改密码（一些高权限用户最好不要修改，影响了业务会找你，这个是已经考完试的学生账号，无妨）



登入进去继续测试

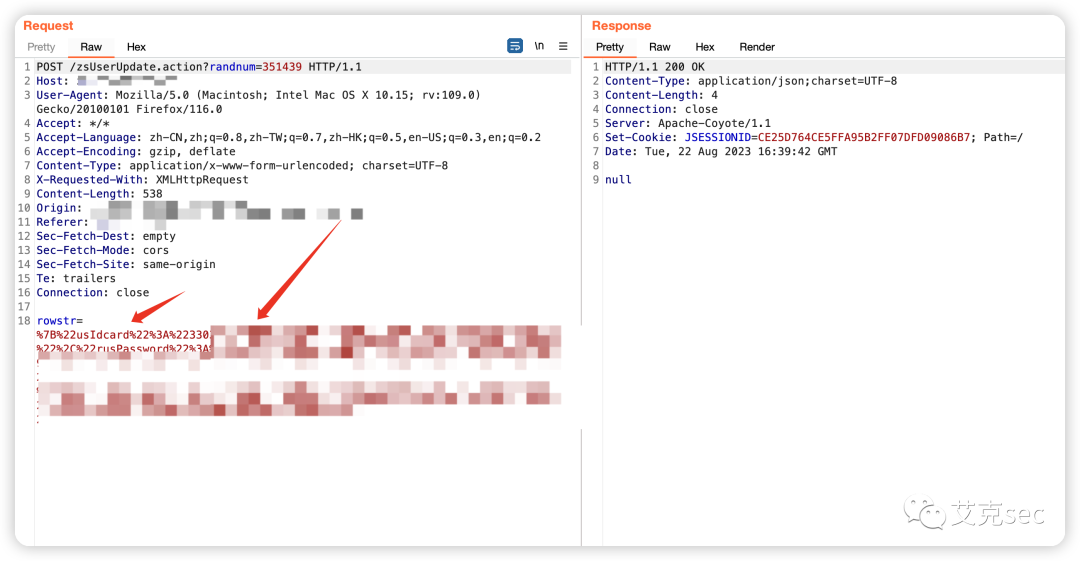
漏洞一 未授权修改任意用户密码

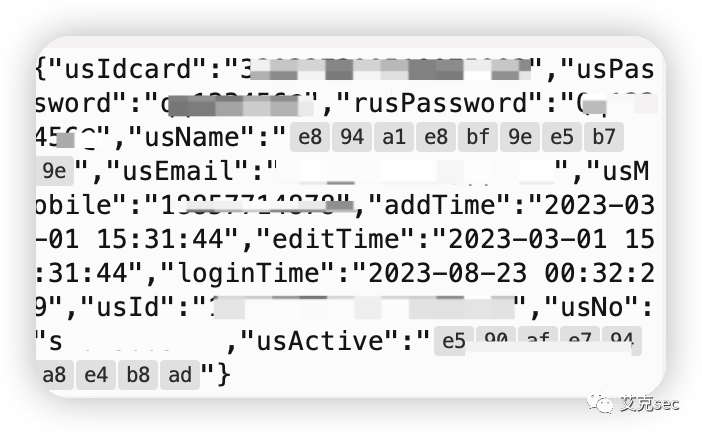
    按钮为灰色的，不能点击 修改js代码



<button type="submit" class="btnenable">提交</button>

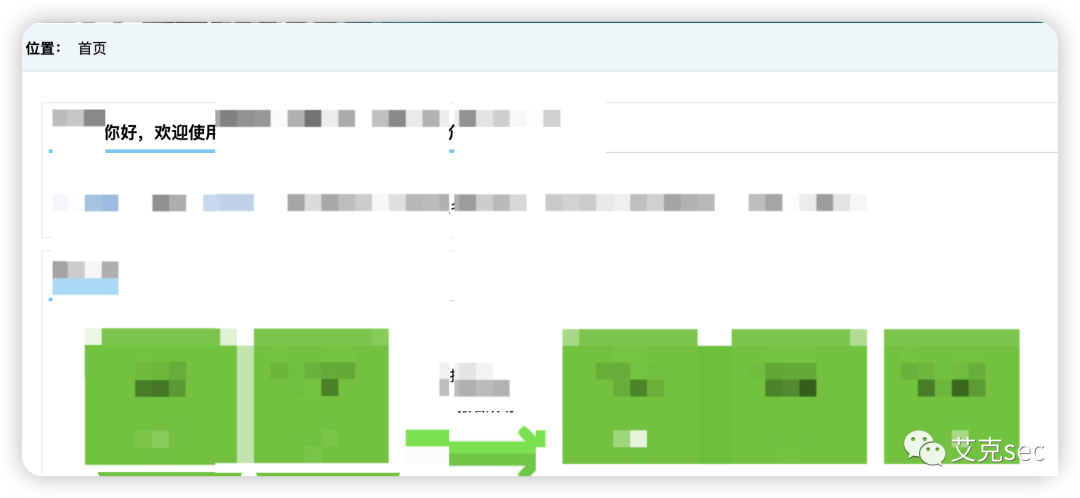
提交抓数据包 找到决定用户的那个参数，判断是否存在越权（这个接口我删了cookie还能访问 未授权加一）





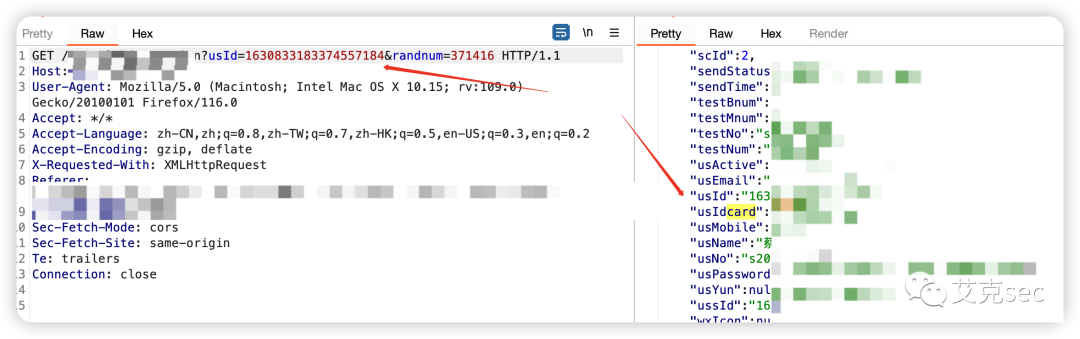
因为有密码字段，可以越权修改密码 利用起来危害还是挺大的 同样的方法，又找了一个账号登入，先判断一下是哪个参数决定账号

用另一个账号只替换usId，发包，登入成功



get 未授权任意用户账号密码修改

有一个未授权接口 可以看到用户的所有信息，如果usid有规律的话，可以遍历出所有用户信息，可惜是时间戳加9位随机数



后续测了上传点和参数注入均无果

第一套系统就到此为止了 因为利用条件是需要知道账号，而账号又是身份证，比较苛刻，给分较低 刷了60分左右

感谢各位师傅们能看到文末，麻烦点一下订阅，一起学习共同进步～ 下次更新第二套系统。