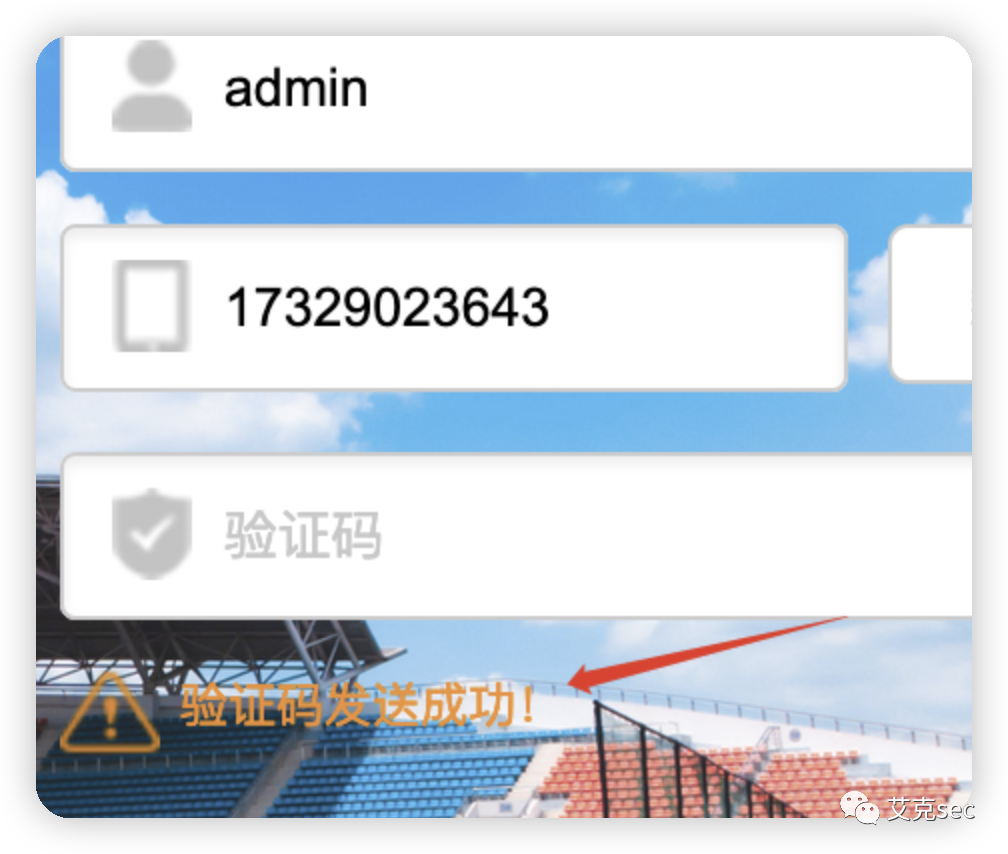
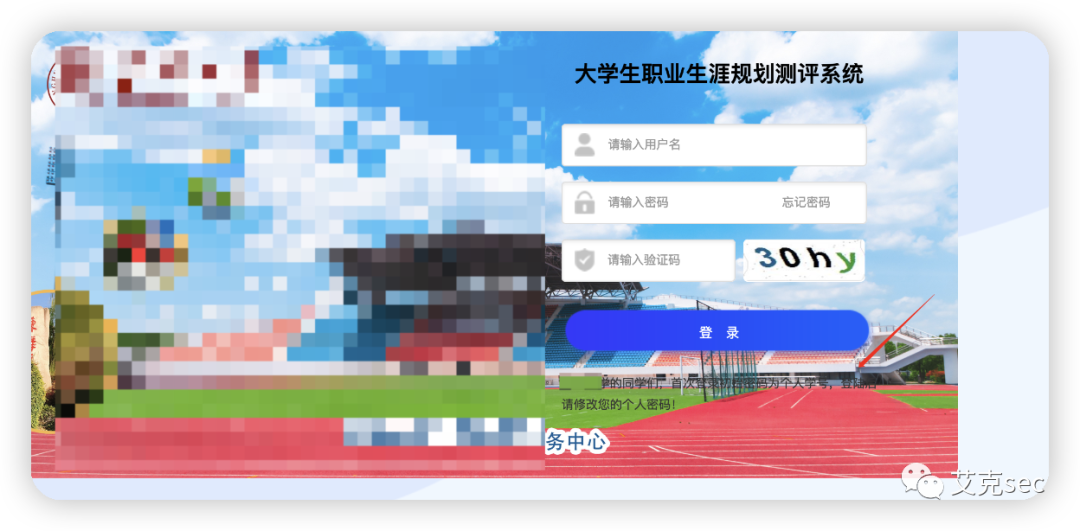
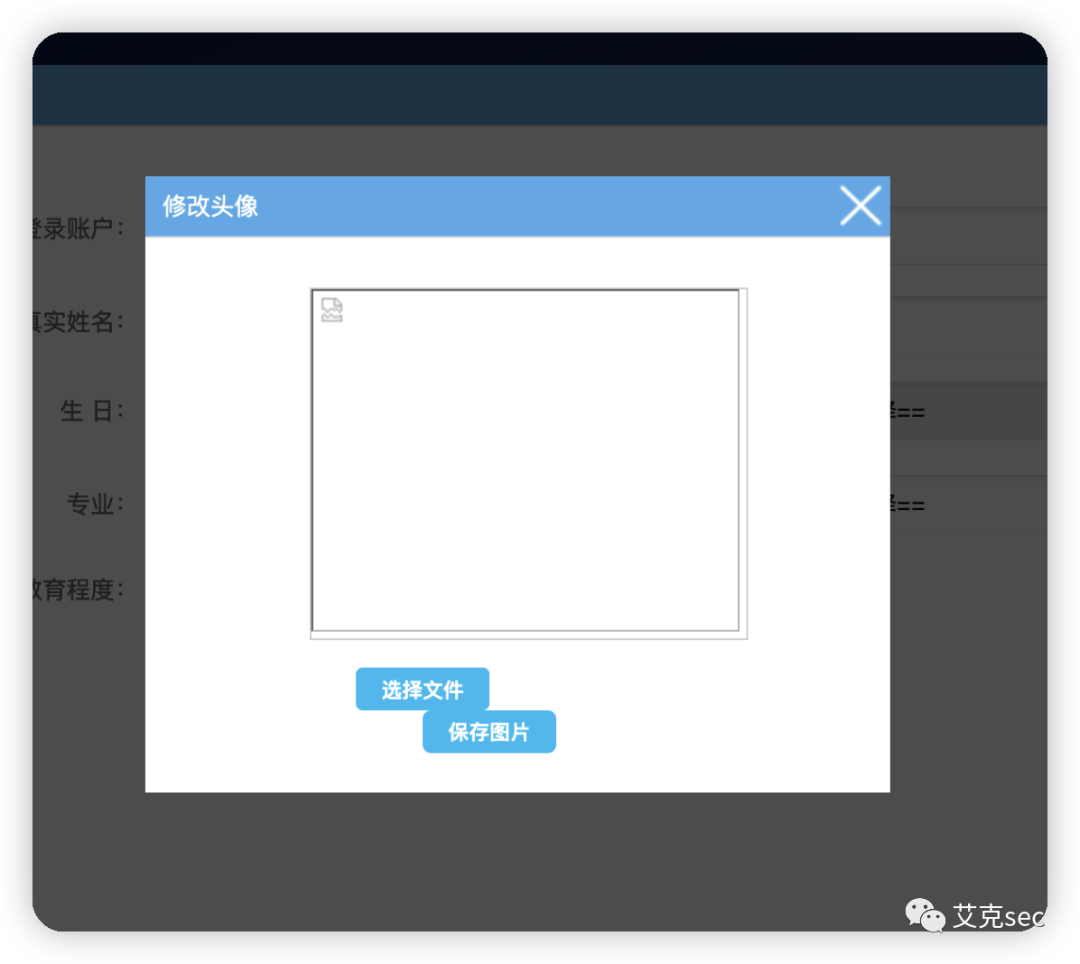
**第二套系统 ：任意用户注册&sql注入&存储XSS&未授权访问+验证码爆破->任意用户密码修改（八所学校，包括证书站和北某大学）**

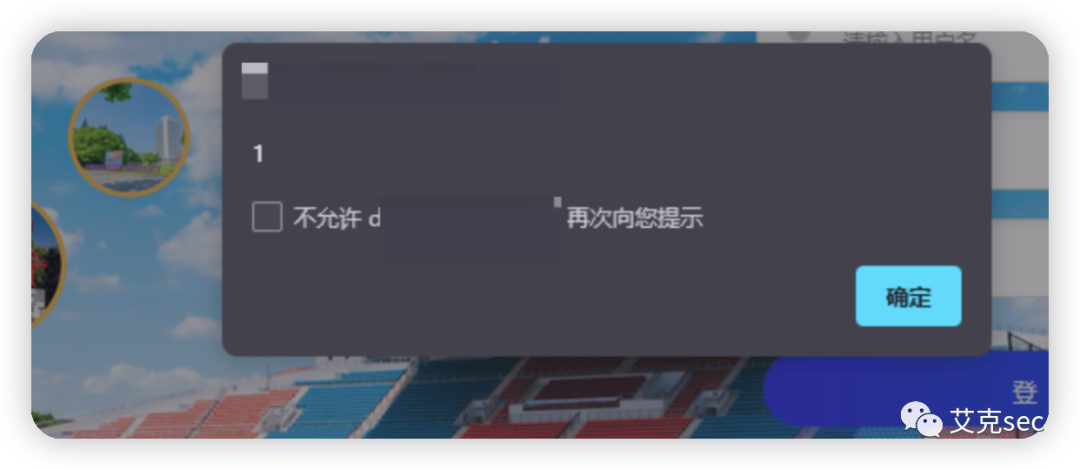
拿到系统 一个登录窗口，没有直观的注册功能，可能存在的漏洞点：弱口令，登录框sql注入(能遇到真的是天选之子) ，忘记密码逻辑缺陷 ，翻js可能存在注册功能，未授权访问。

弱口令和sql注入我这种倒霉蛋就别想了，测试忘记密码功能点：

尝试burp修改响应包绕过验证  前端返回成功 但是处理部分是在后端一步完成的 验证码实际没有发送，无果。

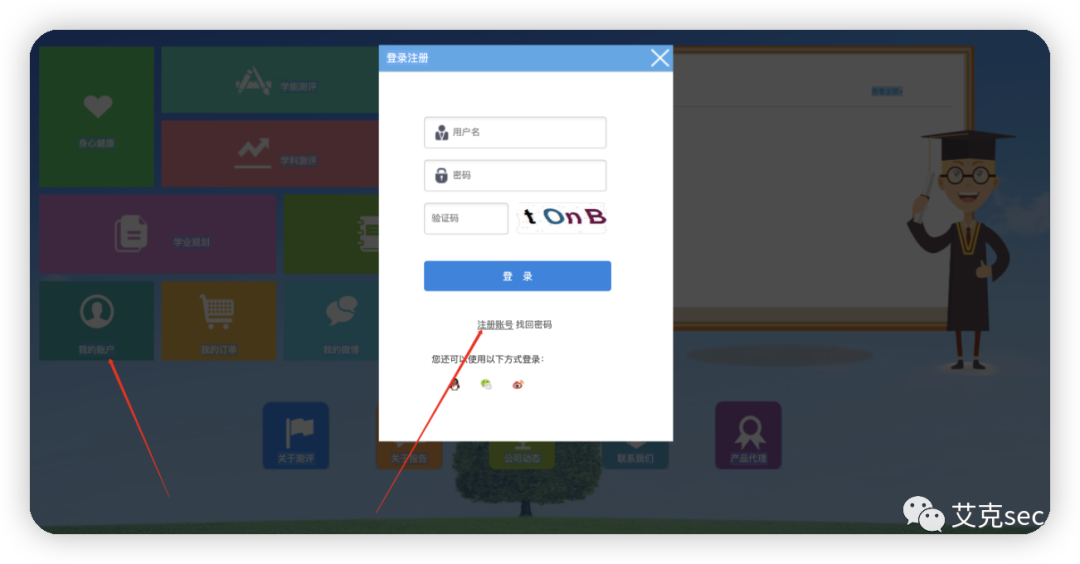
去网络空间搜索引擎看看是不是通用的系统，发现有其他学校在用 lucky 发现一个学校 写了默认账号密码

登入后学生账号功能点很少，只有上传头像处可以上传html文件存储XSS +1  


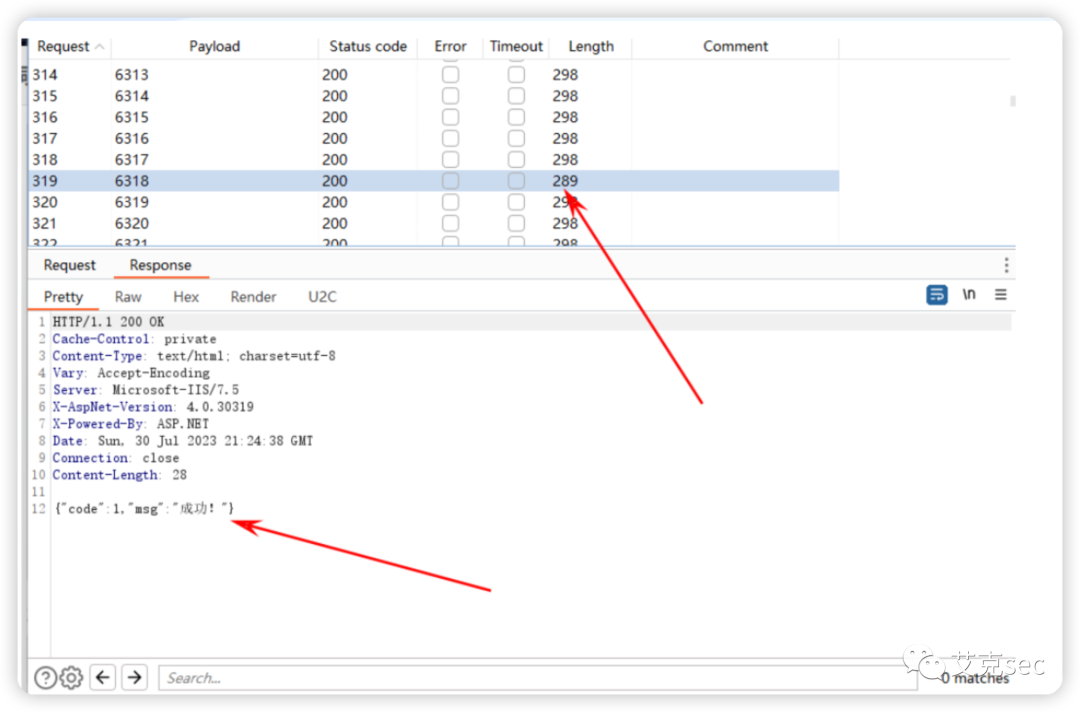
image.png

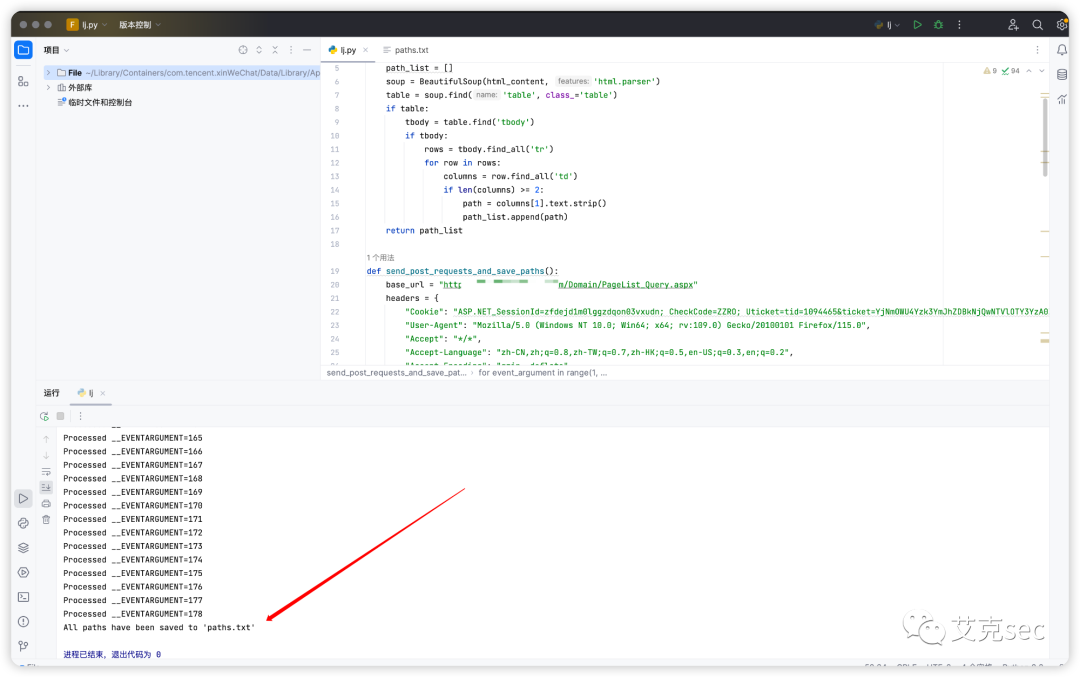
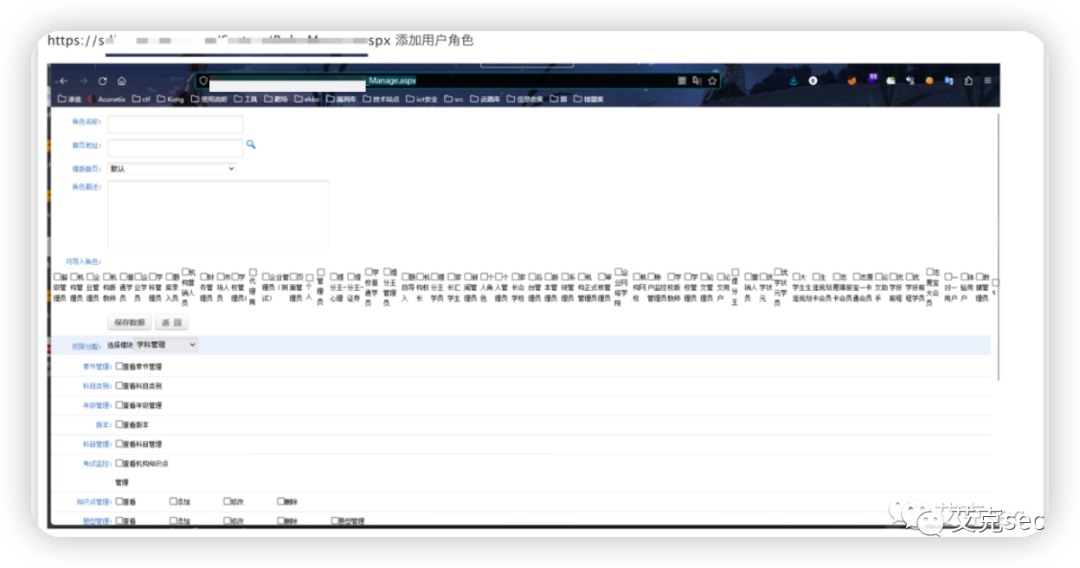
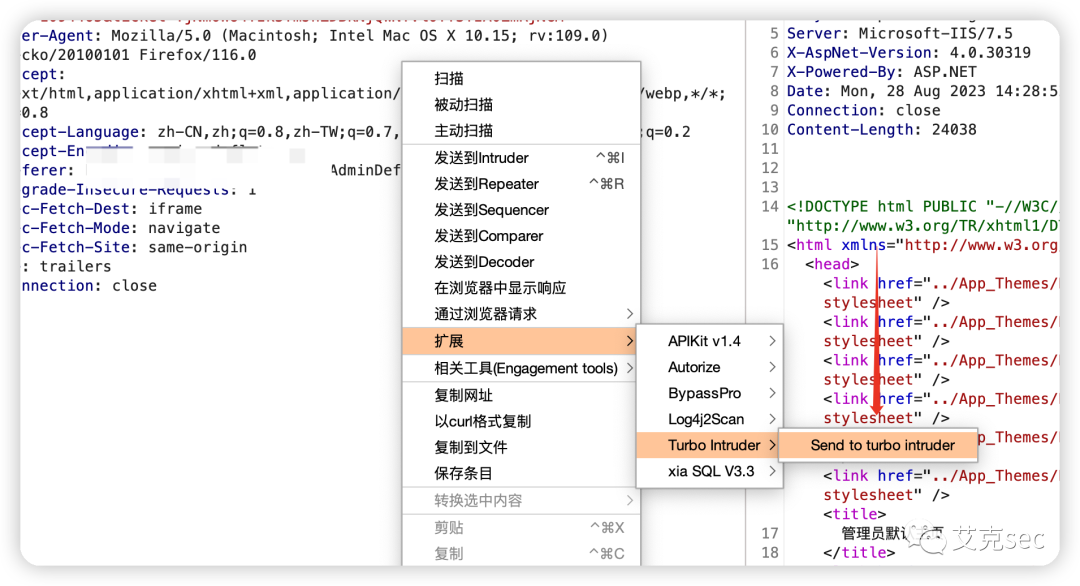
虽然才1rank 但是是通用系统，加起来 = getshell  ^ 就这点rank还得写一个个报告那太亏了，继续测试

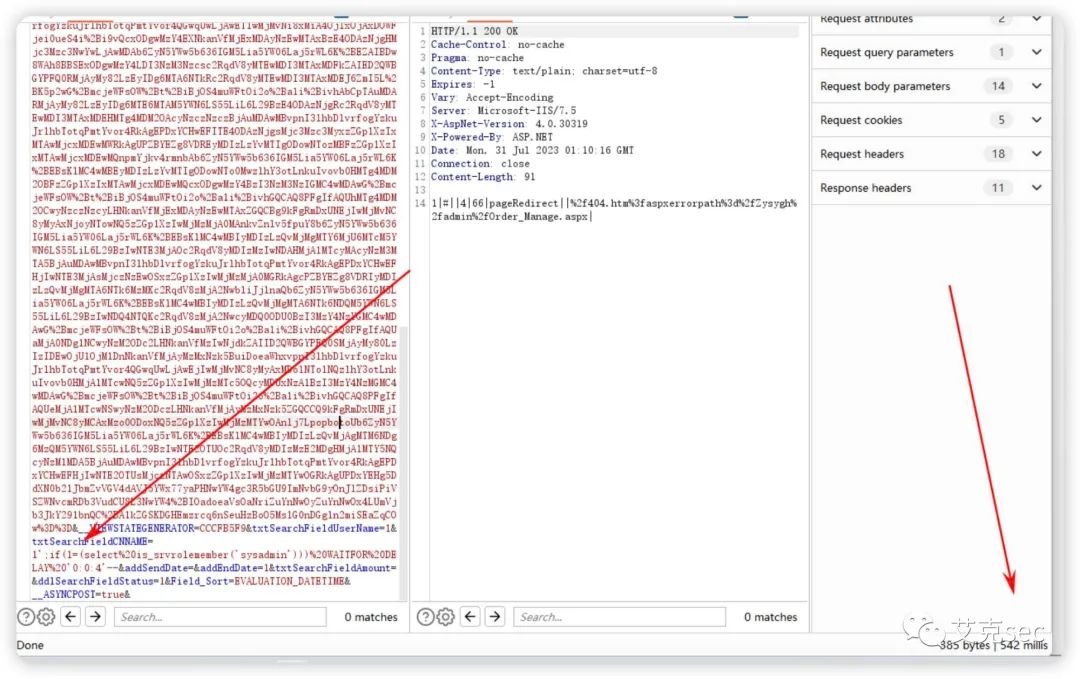
网络空间搜索引擎中找到了一个用户个人中心，是企业的域名 ui和学校的ui很相似，看起来是一个让用户体验的系统，很明显很大可能就是供应商。

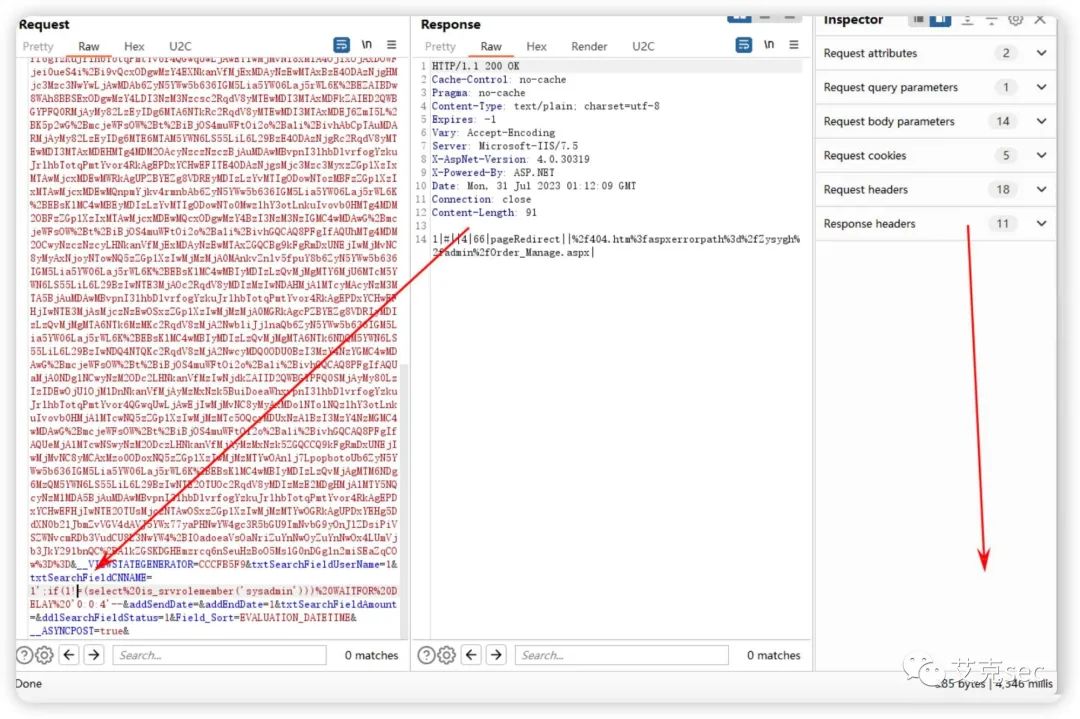
找到了供应商的注册功能点，注册一个账号

提示注册成功，去看burp流量包发现了一个敏感参数经验丰富的师傅已经知道在注册功能点出现这个参数意味这什么了 将这个参数改为1重新发包注册一个账号，直接登入到了供应商后台这里就有了所有学校用户的信息，找到管理员账号和手机号，配合上面的找回密码模块爆破四位验证码 任意用户密码修改 +1

image.pngimage.png

后台找到了一个有意思的页面, 写了系统的全部接口，全部扣下来跑下未授权岂不是美滋滋可惜返回包不是json还不是一页全部回显，这种得写个爬虫，为了rank！冲结合chatgpt写的，成功全部爬出（gpt确实好用）用burp插件跑一下，成功跑出来了很多未授权支付设置！（后来看到这个系统是卖测评的每日流水3000+）给黑灰拿到就惨了

然后就去后台点点点，然后去burp翻数据包，看看哪些地方传参了 测一测。

堆叠延迟注入+1

1';  
if(1=(select%20is\_srvrolemember('sysadmin')))%20WAITFOR%20DELAY%20'0:0:4'--`

这个注入语句是查询该数据库权限是否为高权限，如果不是的话延时4s，如果是的话可以getshell，可惜不是，但是是sqlserver数据库是有办法提权然后shell的。 因为是在hw休息的时候挖的，有点累了就没搞了，后面回头再想搞的时候已经修了。。。

这套系统学校少但是洞多，刷了70分左右，总结一下  当在一个站点没思路的时候看看能不能从通用的其他站点或者供应商下手。

感谢各位师傅能看到文末，觉得写的不错的话可以点个关注，因为最近在学习代码审计相关的内容，后面也会常更新，黑盒真是坐牢～