实战 | 记一次某大学漏洞挖掘的失败经历

原创csz HACK学习呀
2021-02-07原文

前段时间某教育平台出来了一个新学校的证书，样子看起来十分不错，遂想整一个。

当天早上出来，中午起床的我正准备去挖一个洞，好家伙，一看该校的漏洞报送已经三页多了，其中还混杂着不少的高危中危漏洞，当下心中一凉。好家伙，手慢了，Burp一开就是干！

第一步还是常规的资产收集，渗透测试的本质。鉴于表哥们提交了那么多洞，子域名名就不看了，怕是能简单出的洞都被表哥们交完了，直接上fofa看看无域名的C段资产。

Fofa上搜索：”xx大学”

可以看到，这些都是C段的无域名资产。我们直接复制一个该段的ip，到

https://www.ip138.com/

查询该ip信息，确定教育网归属，免得挖了洞教育平台不承认。

可以看到确实为该大学资产，归属教育网，而且IP段都已经给出了，我们现在只需要通过语法210.x.x.0/24即可慢慢找出该ip段的大学的所有资产。

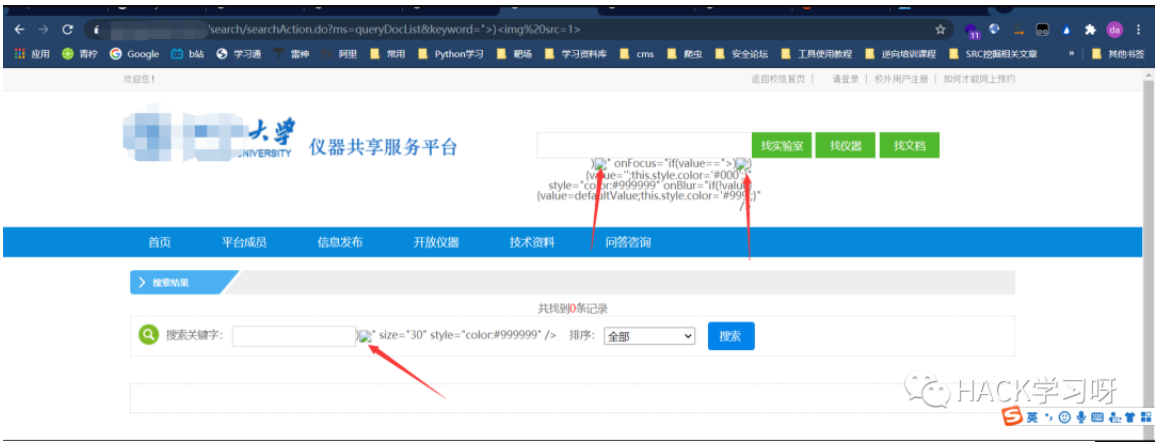
比如：

```
210.x.1.0/24
```

```
210.x.2.0/24
```

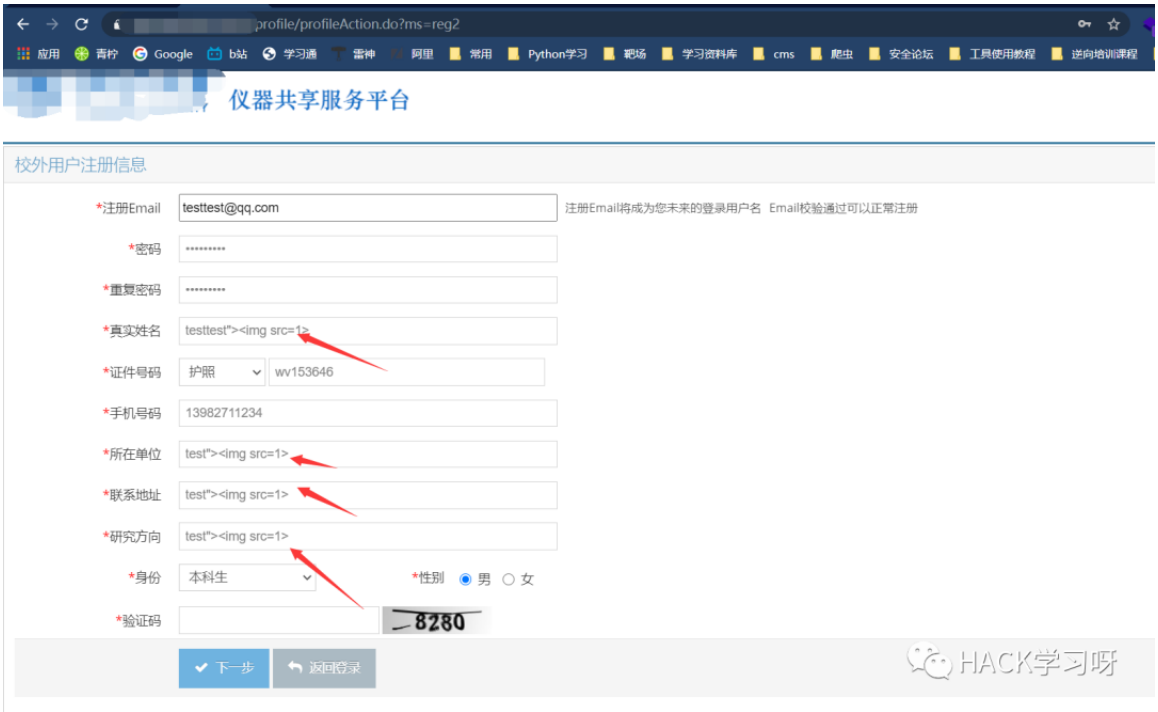
不久便找到了一个目标。

为什么选它呢，因为首页搜索框都能出Xss，足以说明这个站点的管理员安全意识并不高，想必和我不是一路人。更为重要的是，可以登录，功能点越多，出洞的概率就越大。



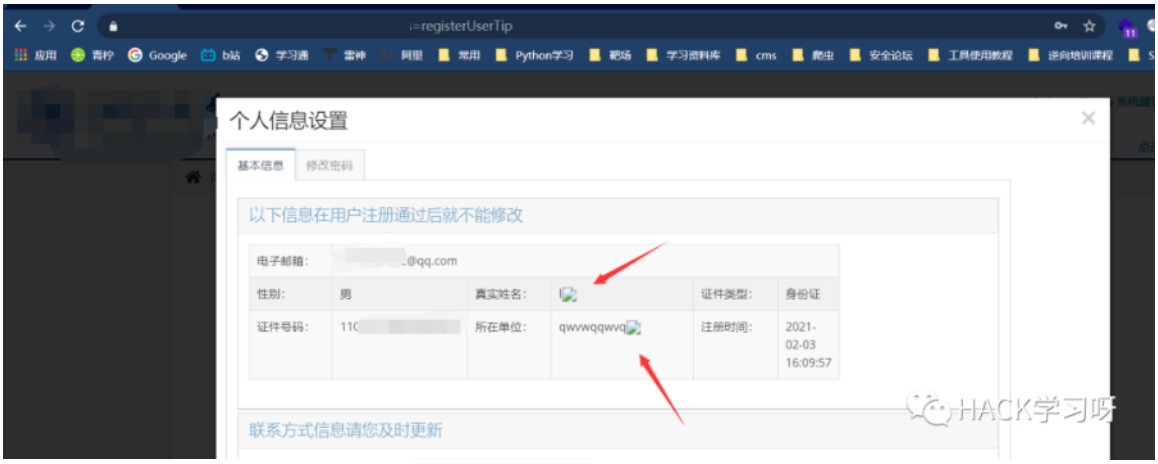
很快啊，校外用户注册一个号，登进去。

注册的时候有多个选项，其中包含了个人信息，这种个人信息一般登录进去后都会显示出来，比如说，手机号码，联系地址，证件号码等等等。这种时候直接丢xss进去。有回显的地方就有可能Xss。



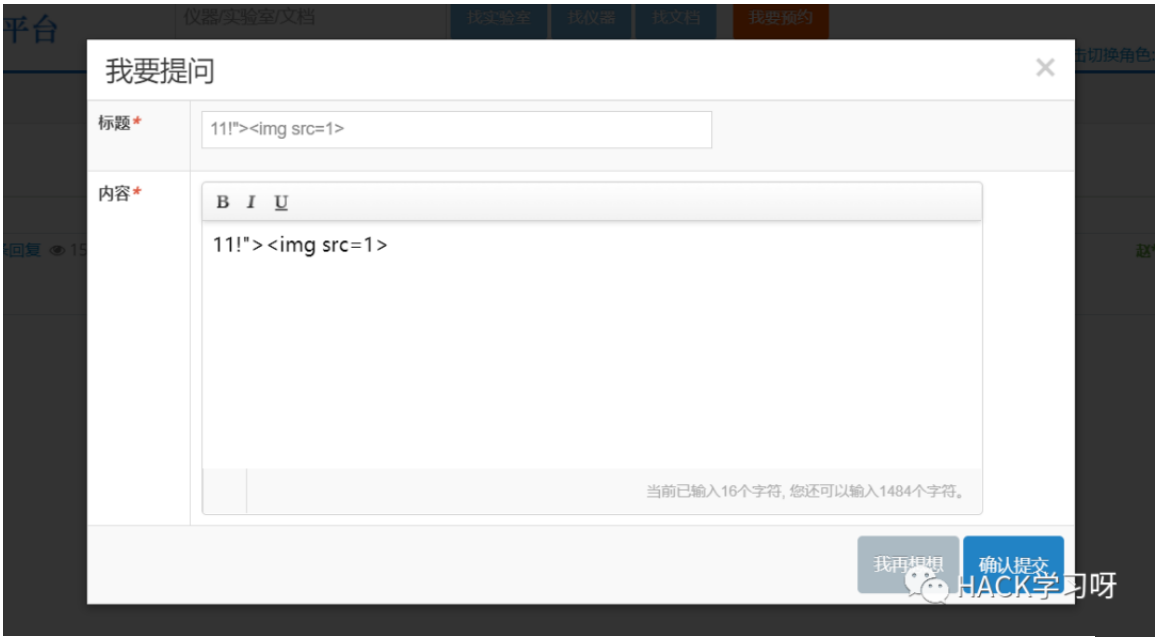
登录系统后，Xss直接回显，好家伙，一个存储型Xss出来了。

点击查看个人信息，也有。

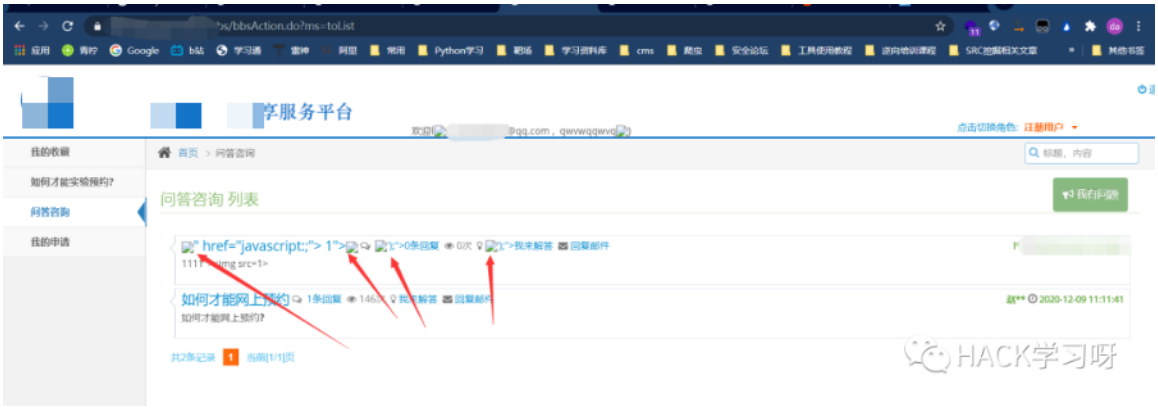


如果插入的xss代码是打cookie的，后台管理员查看我个人信息的时候就可以获取管理员cookie信息。

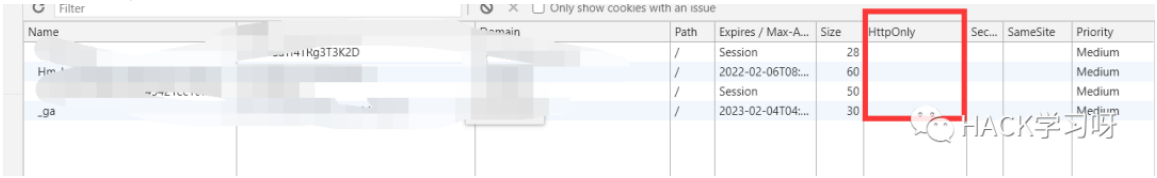
又找了一会，发现这个系统功能很少，但又发现问题咨询列表这里又存在一枚存储性Xss。



这个问题如果是公开的话，影响的几乎是所有用户。



http only未启用。可打管理员cookie是没跑了。



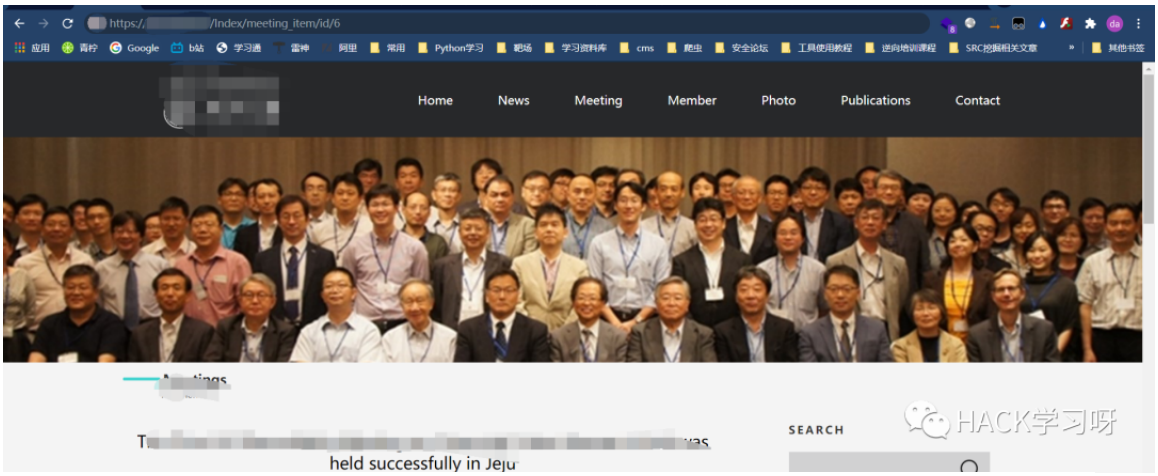
Ok，一个反射性xss，两个存储型xss。打包提交应该会有个中危吧。晚上回来一看，好家伙，就给我一分。

	等级	Rank
	低危	1

那就，在挖挖吧。

后面，又找到了一枚注入。

注入点：`https://x.x.x.x/Index/meeting_item/id/6`



直接

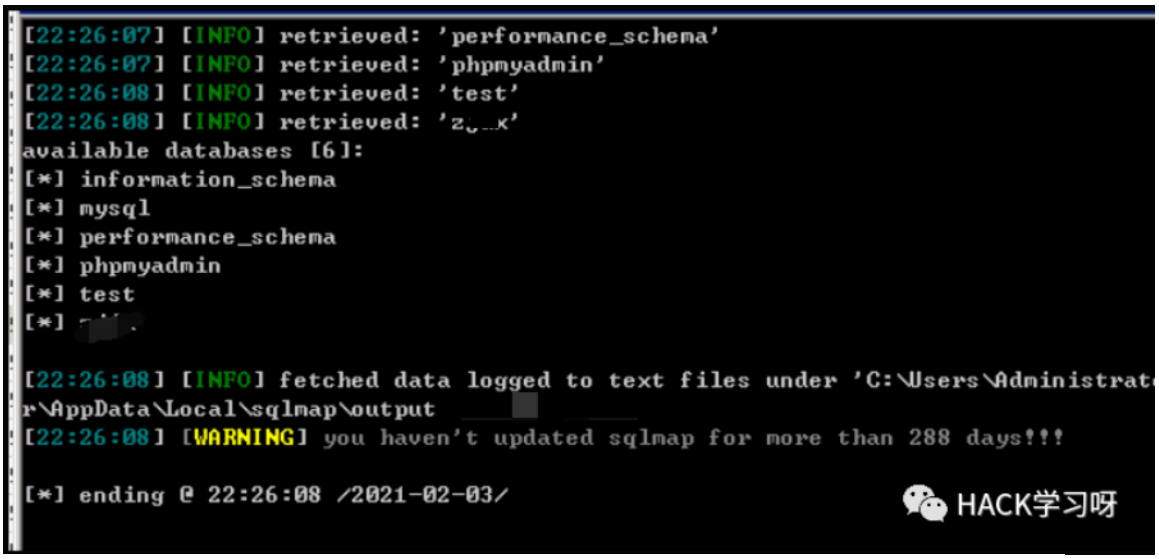
6 and 1=1 回显正常

6 and 1=2 回显错误

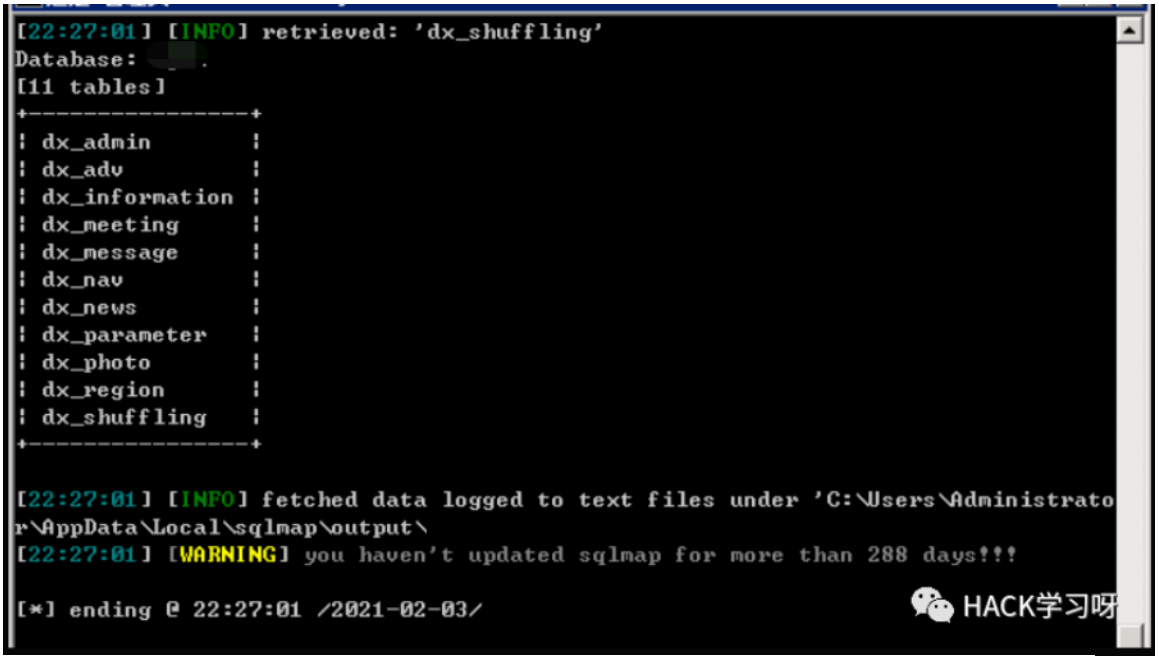
好家伙，这不明摆着有注入吗？不过让我没想到的是居然没有waf拦截。难道是伪静态传参的原因？

很快啊，sqlmap一把梭。

```
sqlmap.py -u "https:// x.x.x.x /Index/photo_item/id/6*" --dbs
```




```
sqlmap.py -u "https:// x.x.x.x /Index/photo_item/id/6*" -
D zxxxx -tables
```



这次总行了吧。一个中危应该是没跑了。

第二天早晨起来一看，好家伙，直接重复。

	等级	Rank
	低危	0

既然，web挖不过你们。那老子挖公众号，这回你们不得和我抢了吧。

夜神模拟器打开，微信登录，直接搜索，XX大学，然后点击公众号，看一下有哪些。

第一个明显是学校的官方公众号，看了下也没啥可测的功能点。

第二个网上就业市场倒是有很多功能点，就决定第二个了，关注一波，进入公众号。

可以看到功能点还是不少的

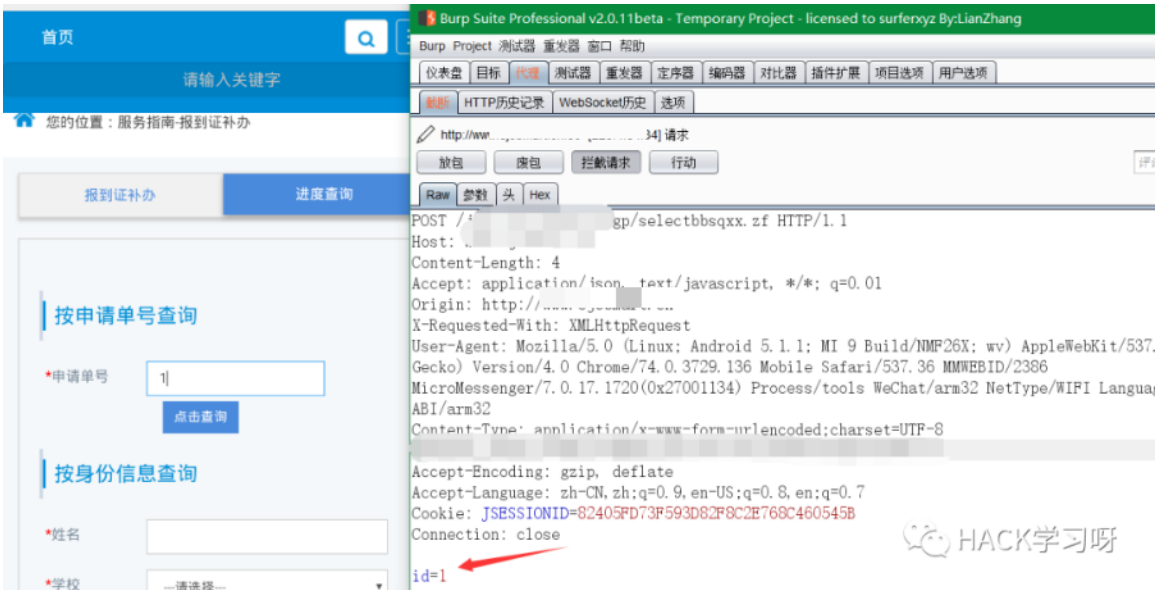
测了一圈后，发现就这个地方比较可疑：


首页
请输入关键字
您的位置：服务指南-报到证补办
报到证补办
进度查询
按申请单号查询
*申请单号
点击查询
按身份信息查询
*姓名
*学校
---请选择---
*联系电话
点击查询
查询结果
HACK学习呀

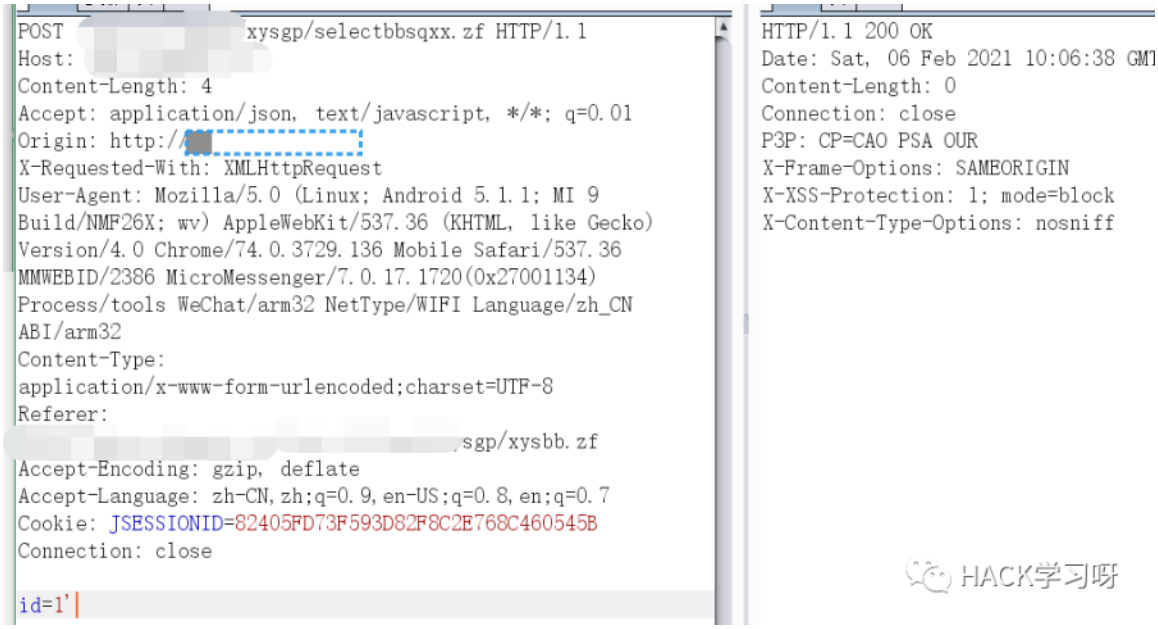
一般来讲，存在于数据库有交互的地方就有注入，而查询是很容易出问题的功能点。

直接抓个包看看。

看到这个参数名为id，我就很兴奋啊，因为出现注入最多的参数就是id。hhhh

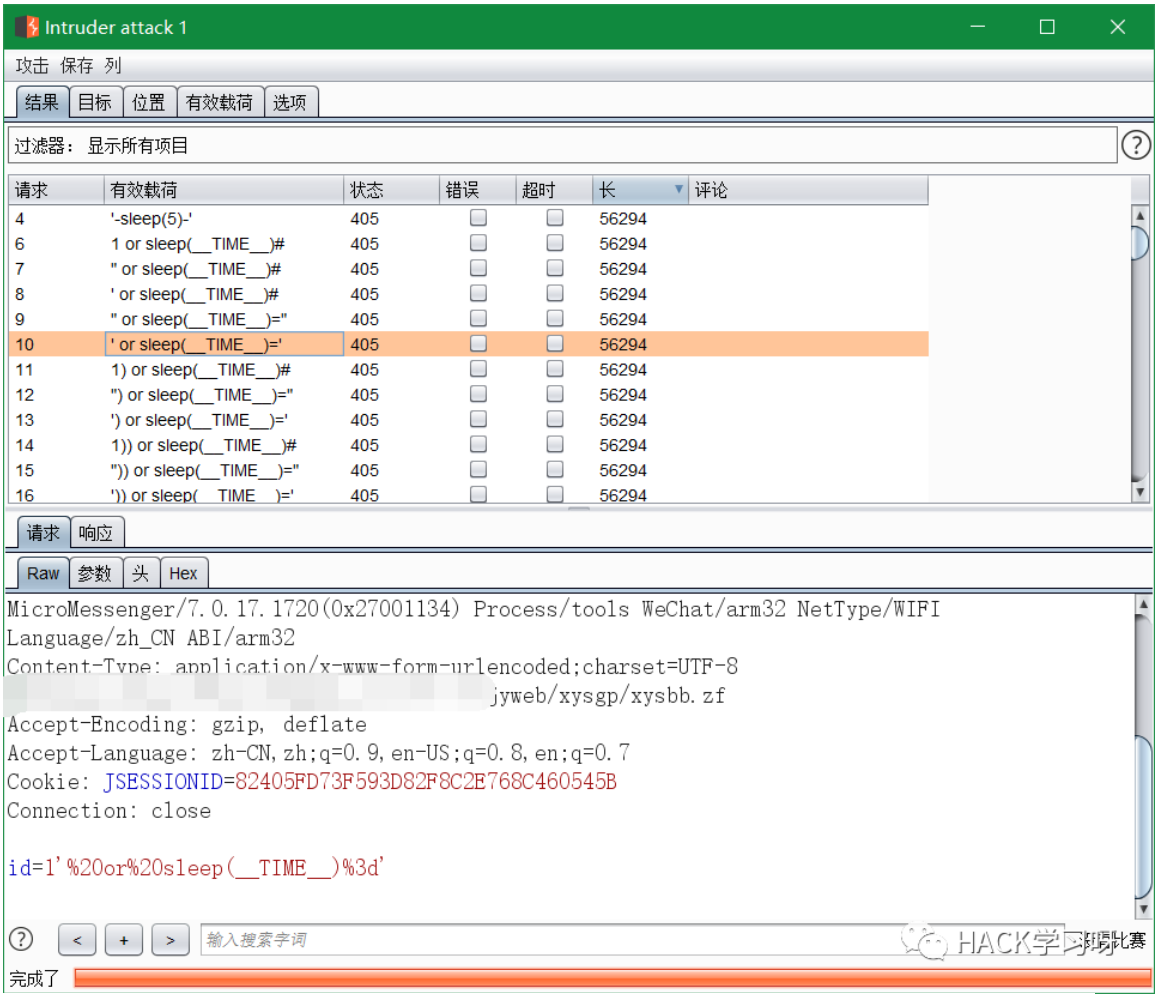


一个单引号，没反应，



出现200表示返回正常，而没有返回数据，说明没有查询结果，这时候想着fuzz一波。

看一下有没有收获。



直接405，貌似是没什么搞头。而回显200没有返回内容则是显示是没有查询结果。

这个时候就很迷惘啊，明明觉得这个有个洞，但是为什么就出不来呢。

无法闭合，sqlmap也跑不出来，也没有报错回显。开始头疼

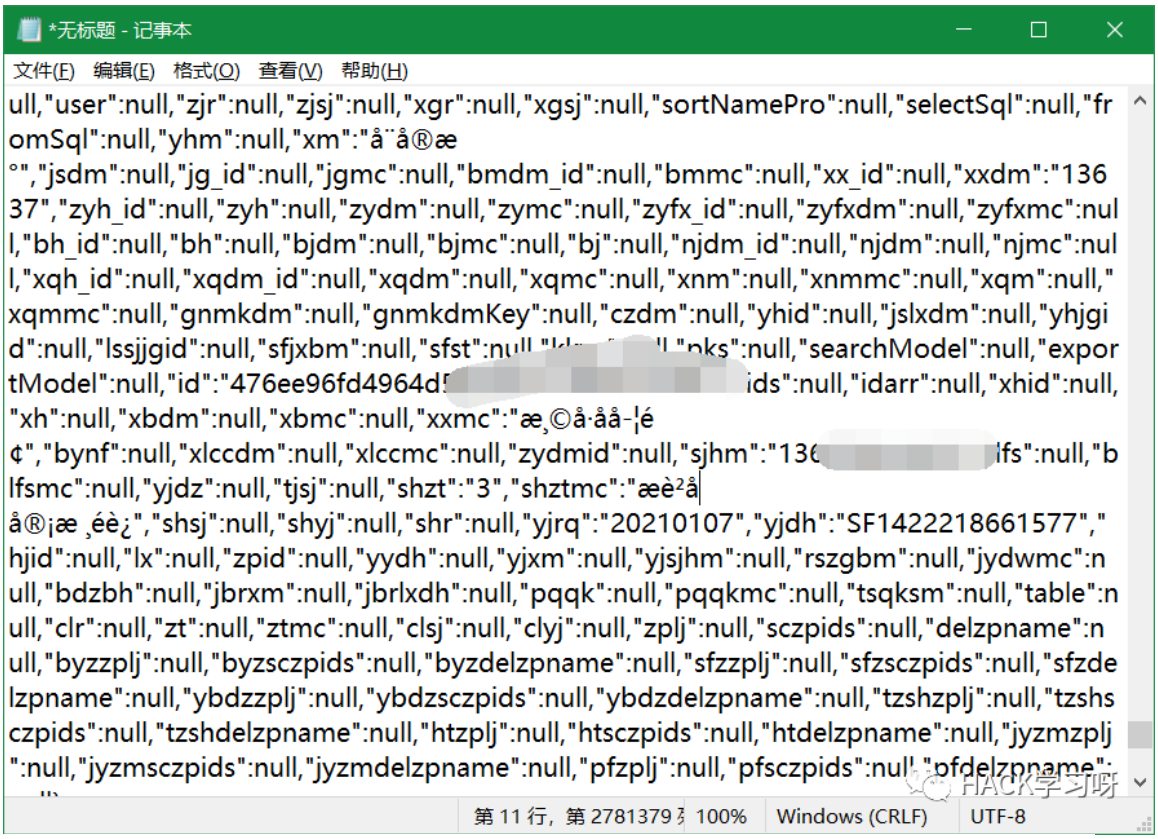
仔细想一想，这里的查询条件为申请单号，而匹配到结果是200直接返回，没有匹配到结果就是200不返回数据，假设想一下如果他的语句是
where 单号=”输入的单号”

这样的话，闭合不了想必后面还有更多更繁杂的查询条件，或者是其他条件，比如waf，如果我直接让单号的查询内容为%的话，能不能实现把它的数据全部匹配出来呢。【%号在主流数据库里面是匹配全部字符的意思】

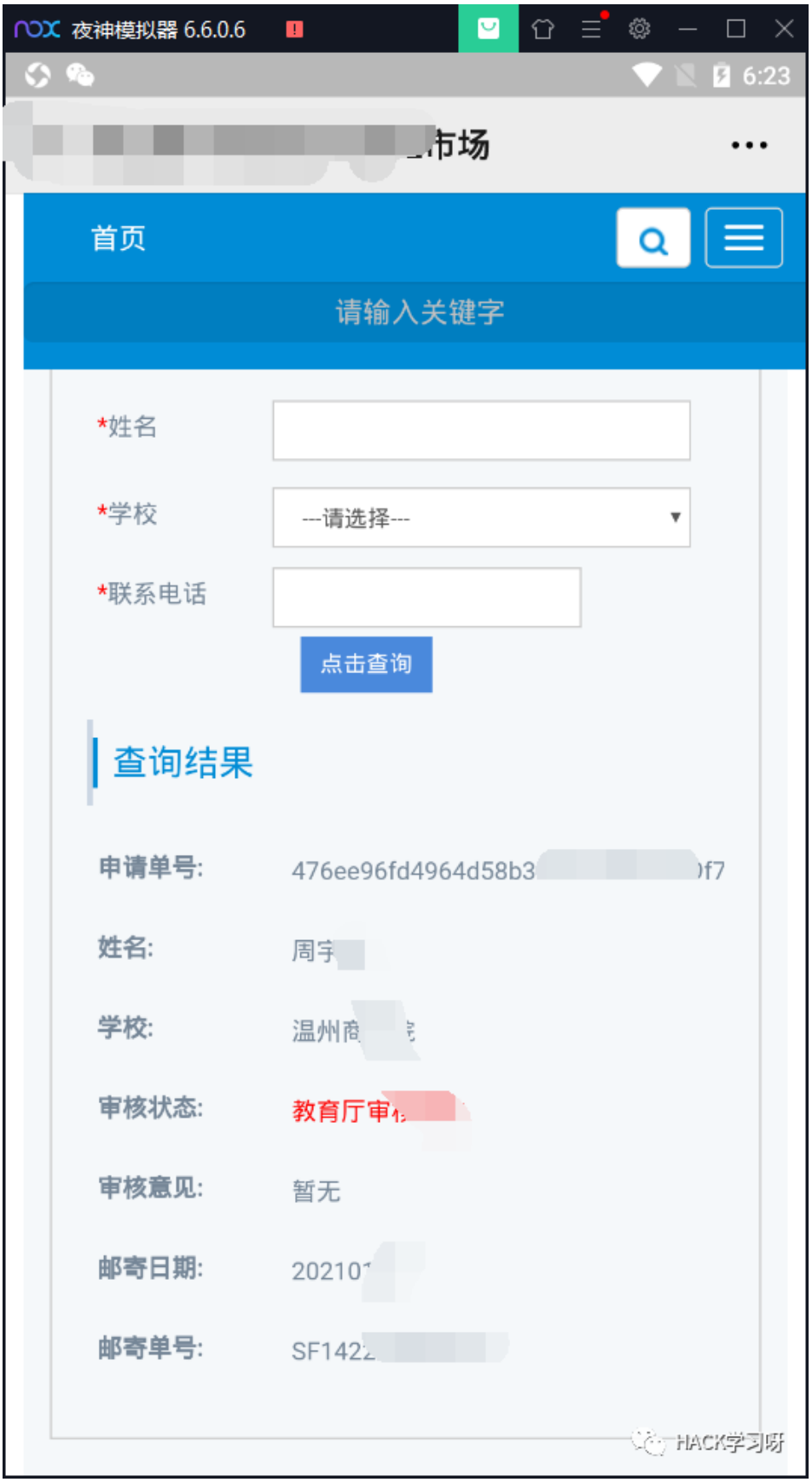
说干就干，挖洞就是要敢想敢验证才行！

Burp一下卡住，起先我还以为被waf拦截了。但随后一下就爆出了数据。
好家伙，burp都给我整的不流畅了。

将爆出的数据中的id拿去查询。


*无标题 - 记事本
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)
ull,"user":null,"zjr":null,"zjsj":null,"xgr":null,"xgsj":null,"sortNamePro":null,"selectSql":null,"fr
omSql":null,"yhm":null,"xm":"å¨å®æ
°","jsdm":null,"jg_id":null,"jgmc":null,"bmdm_id":null,"bmmc":null,"xx_id":null,"xxdm":"136
37","zyh_id":null,"zyh":null,"zydm":null,"zymc":null,"zyfx_id":null,"zyfxdm":null,"zyfxmc":nul
l,"bh_id":null,"bh":null,"bjdm":null,"bjmc":null,"bj":null,"njdm_id":null,"njdm":null,"njmc":nul
l,"xqh_id":null,"xqdm_id":null,"xqdm":null,"xqmc":null,"xnm":null,"xnmmc":null,"xqm":null,"
xqmmc":null,"gnmkdm":null,"gnmkdmKey":null,"czdm":null,"yhid":null,"jslxdm":null,"yhjgi
d":null,"lssjjgid":null,"sfjxbm":null,"sfst":null,"
ids":null,"idarr":null,"xhid":null,
"xh":null,"xbdm":null,"xbmc":null,"xxmc":"æ¸©å·åå-¦é
¢","bynf":null,"xlccdm":null,"xlccmc":null,"zydmid":null,"sjhm":"136
lfs":null,"b
lfsmc":null,"yjdz":null,"tjsj":null,"shzt":"3","shztmc":"æè²å
å®¡æ ¸é¿","shsj":null,"shyj":null,"shr":null,"yjrq":"20210107","yjdh":"SF1422218661577","
hjid":null,"lx":null,"zpid":null,"yydh":null,"yjxm":null,"yjsjhm":null,"rszgbm":null,"jydwmc":n
ull,"bdzbh":null,"jbrxm":null,"jbrlxdh":null,"pqqk":null,"pqqkmc":null,"tsqksm":null,"table":n
ull,"clr":null,"zt":null,"ztmc":null,"clsj":null,"clyj":null,"zplj":null,"sczpids":null,"delzpname":n
ull,"byzzplj":null,"byzsczpids":null,"byzdelzpname":null,"sfzzplj":null,"sfzsczpids":null,"sfzde
lzpname":null,"ybdzzplj":null,"ybdzsczpids":null,"ybdzdelzpname":null,"tzshzplj":null,"tzshs
czpids":null,"tzshdelzpname":null,"htzplj":null,"htsczpids":null,"htdelzpname":null,"jyzmzplj
":null,"jyzmsczpids":null,"jyzmdelzpname":null,"pfzplj":null,"pfsczpids":null,"pfdelzpname":
HACK学习呀
第 11 行，第 2781379 列
100%
Windows (CRLF)
UTF-8

好家伙，直接出敏感信息。


夜神模拟器 6.6.0.6
6:23
市场
首页
请输入关键字
*姓名
*学校
---请选择---
*联系电话
点击查询
查询结果
申请单号:
476ee96fd4964d58b3
f7
姓名:
周宇
学校:
温州商
审核状态:
教育厅审
审核意见:
暂无
邮寄日期:
202101
邮寄单号:
SF1422
HACK学习呀

其他接口处也同样存在相同的问题，好家伙，直接交上去。美滋滋，这下证书应该稳了吧。

等了两天，终于审核了。

都通过，这下，终于可以换某大好看的证书了，感动之余，不禁与亲朋好友们奔走相告。

回来准备兑换证书嘻嘻嘻，一看归属，居然是教育厅！！！

淦，原来是我目标打偏了。

尴尬。再也不挖某大了。

对了，很多人问我，挖到自己大学的漏洞去哪里提交：

https://src.sjtu.edu.cn/

总结：

1. 挖洞要手快，不然就凉凉。
2. 与数据库有交互的地方就有可能存在漏洞，不一定非得是SQL，遇到与数据库有交互的地方就要注意是否存在漏洞。心细挖天下。
3. 测试的时候一定要想明白功能点的处理逻辑，懂了逻辑，才能更容易出洞。
4. 最重要的一点！！！一定要先搞清楚目标归属，否则就打偏！

推荐阅读：

逻辑漏洞 | 支付漏洞学习

小程序渗透 | 对酒店房间自助售货机的支付漏洞挖掘

SRC逻辑漏洞挖掘详解以及思路和技巧

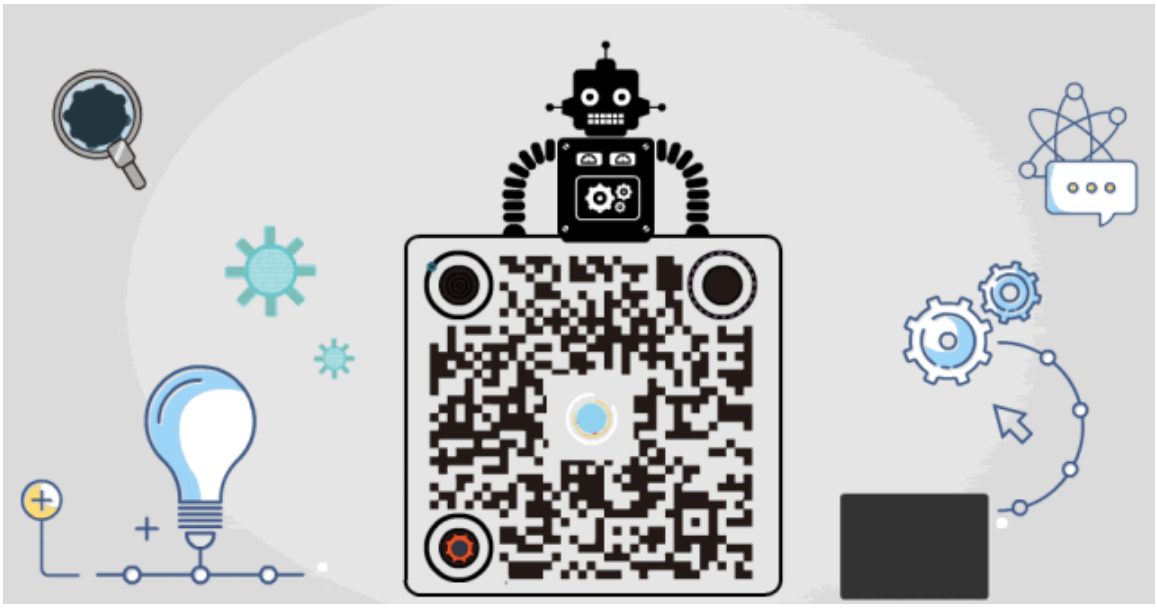
SRC漏洞挖掘经验+技巧篇

干货 | 登录点测试的Tips

漏洞挖掘 | 单点登录的网站通过Referer盗取用户授权

记一次短信验证码的"梅开五度"

点赞 在看 转发



精选留言

用户设置不下载评论