

时间	单位	作者	等级	Rank
2023-02-28 11:15:45	浙江大学 (/list/firm/3987)		中危	2

存在sql注入

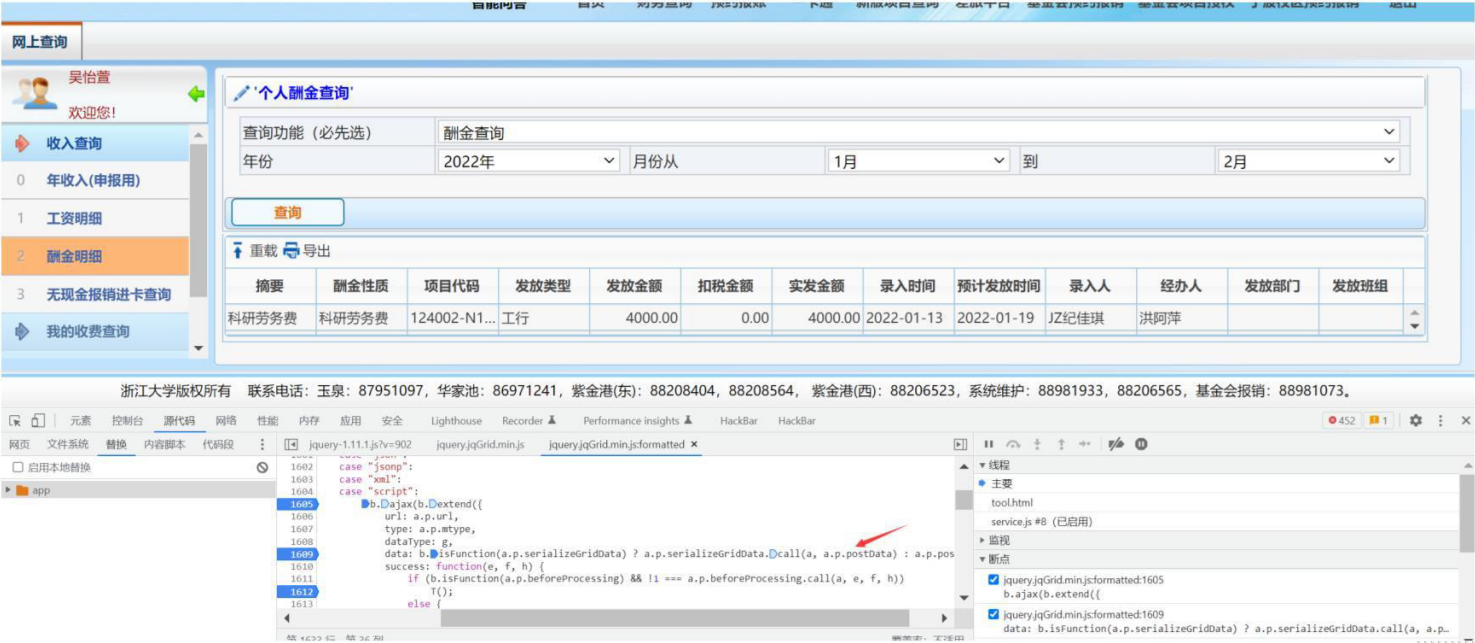
url:http://cwcx.zju.edu.cn/WFManager/login.jsp (http://cwcx.zju.edu.cn/WFManager/login.jsp)

账号 22160173

密码 xuan.15613001609

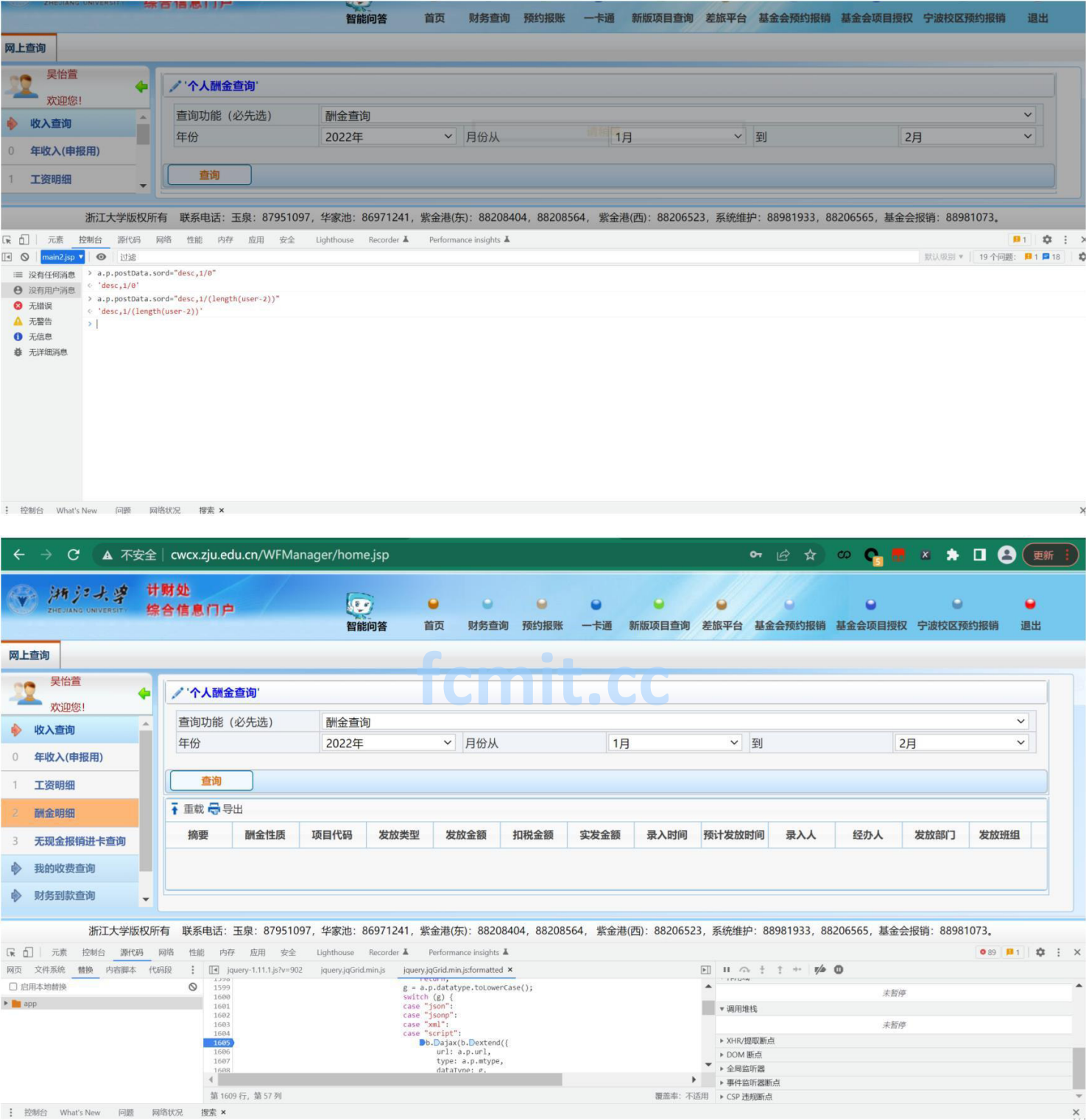


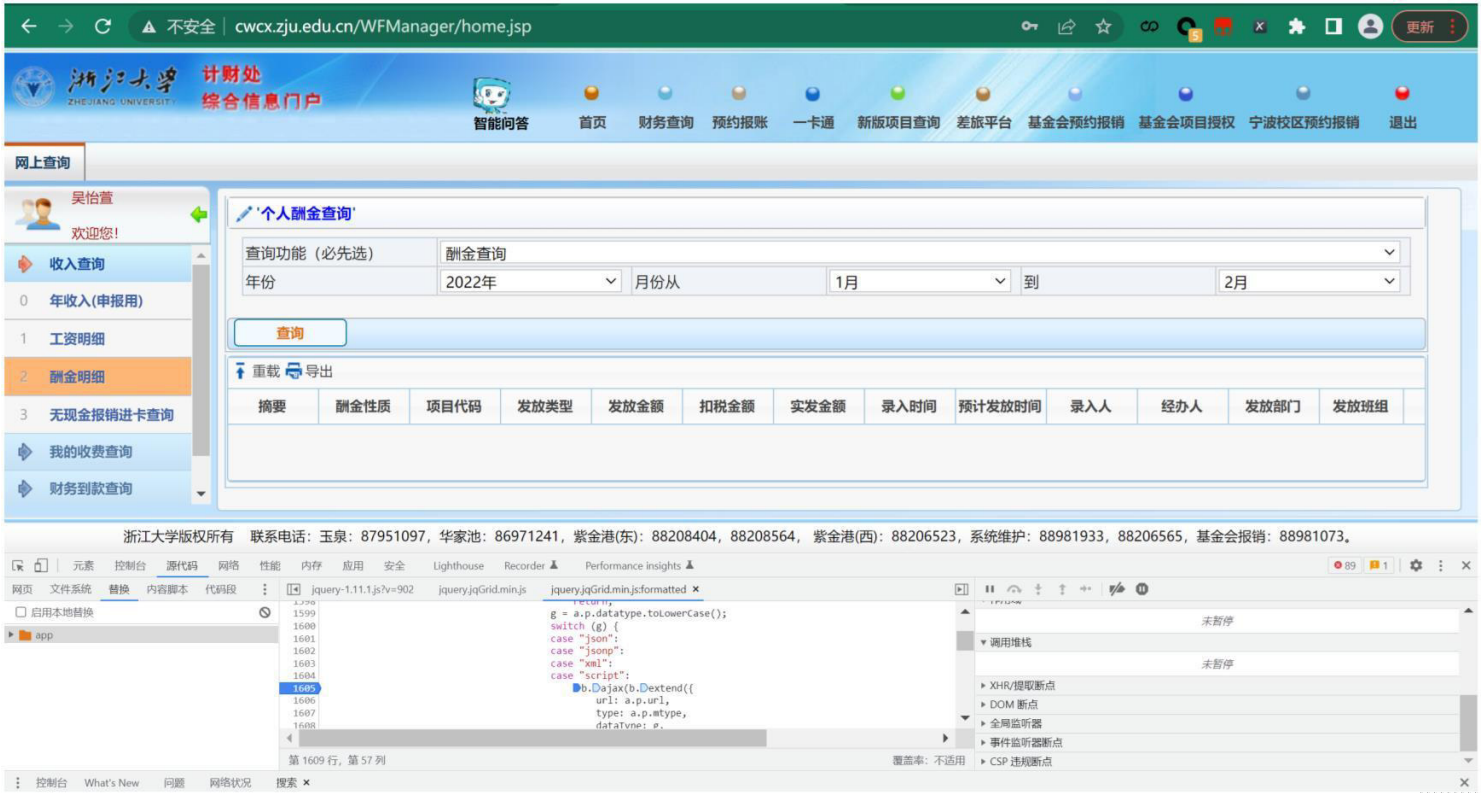
js是http://cwcx.zju.edu.cn/WFManager/jquery/jquery.jqGrid.min.js?v=902



此处下上断点

当判断user字段为2是，发现回显不正常（下图为不正常截图），接着猜解





当user为5时



发现页面回显正常，长度为5

吴怡萱
欢迎您!

收入查询

0 年收入(申报用)

1 工资明细

2 薪金明细

3 无现金报销进卡查询

我的收费查询

财务到账查询

我的财务信息

个人薪金查询

查询功能(必先选)

薪金查询

年份

2023年

月份从

1月

到

2月

查询

重载

导出

摘要	薪金性质	项目代码	发放类型	发放金额	扣税金额	实发金额	录入时间	预计发放时间	录入人	经办人	发放部门	发放班组
校级外设奖...	劳务	288850-54...	工行	5000.00	0.00	5000.00	2023-01-13	2023-01-18	邓晓韵	陈如萍		
2022年研究...	专项奖助学...		工行	5000.00	0.00	5000.00	2023-01-13	2023-01-21	邓晓韵	邓晓韵		
红冲	劳务		工行	-5000.00	0.00	-5000.00	2023-01-13	2023-01-18	王辉			
2021-2022...	学业奖学金	188310-54...	工行	1000.00	0.00	1000.00	2023-01-12	2023-01-18	王辉			
总计				6000.00	0.00	6000.00						

浙江大学版权所有 联系电话: 玉泉: 87951097, 华家池: 86971241, 紫金港(东): 88208404, 88208564, 紫金港(西): 88206523, 系统维护: 88981933, 88206565, 基金会报销: 88981073。

元素 控制台 源代码 网络 性能 内存 应用 安全 Lighthouse Recorder Performance insights HackBar HackBar

main2.jsp 过滤

778 条消...> a.p.postData.sord="desc,1/0"< "desc,1/0"

没有用户...> a.p.postData.sord="desc,1/(length(user-4))"< "desc,1/(length(user-4))"

775 个错...> a.p.postData.sord="desc,1/(length(user-4))"< "desc,1/(length(user-4))"

无警告

无信息

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

fcmit.cc