

2210697/1946Loo6

https://all.tongji.edu.cn/index.html#/



第1页, 共7页

同济大学 | 教育类招聘平台

2023/2/11 18:40

https://src.sjtu.edu.cn/post/194506/



点击创建简历并进行操作

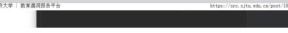


第2页, 共7页

同济大学 | 教育类招聘平台

2023/2/11 18:40

https://src.sjtu.edu.cn/post/194506/



对参数进行遍历

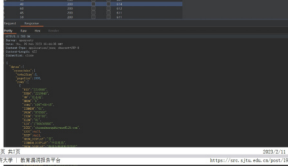


第3页, 共7页

同济大学 | 教育类招聘平台

2023/2/11 18:40

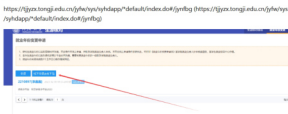
https://src.sjtu.edu.cn/post/194506/



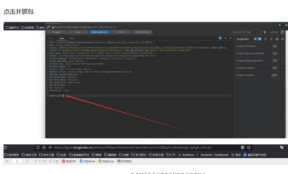
第二处漏洞: 越权

访问如下地址

https://tjyx.tongji.edu.cn/fyfw/vyn/syhdapp?default/index.do#/jymbg (https://tjyx.tongji.edu.cn/fyfw/vyn/syhdapp?default/index.do#/jymbg)



点击并截图



第4页, 共7页

同济大学 | 教育类招聘平台

2023/2/11 18:40

https://src.sjtu.edu.cn/post/194506/



登录后访问如下地址

若没有登录请点击同济统一认证登录

https://czb.tongji.edu.cn/index_cg.jsp

越权接口

czb.tongji.edu.cn/votzg/WriteMsg.jsp?msgUrlId=&msgUrlParam=5m=11140



第5页, 共7页

同济大学 | 教育类招聘平台

2023/2/11 18:40

https://src.sjtu.edu.cn/post/194506/



根据学号给别人发消息

czb.tongji.edu.cn/votzg/WriteMsg.jsp?msgUrlId=&msgUrlParam=5m=11140



czb.tongji.edu.cn/votzg/WriteMsgModal.jsp?param=11140

