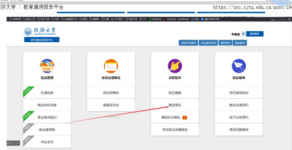
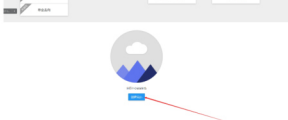
2210897/1996Lxx946

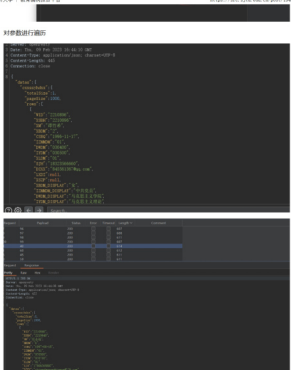
https://all.tongji.edu.cn/index.html#/





点击创建简历并且进行跳包

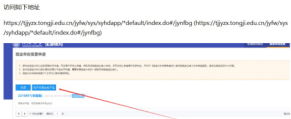
对参数进行篡改



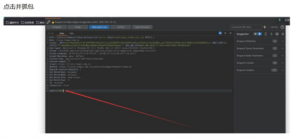
第二处漏洞：越权

访问如下地址

https://tjyjxx.tongji.edu.cn/jyfw/xys/syhdapp/*default/index.do#/jynfbg (https://tjyjxx.tongji.edu.cn/jyfw/xys/syhdapp/*default/index.do#/jynfbg)



点击并抓包



登录后访问如下地址

若没有登录跳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/xetzgj/WriteMsg.jsp?msgUrlId=&msgUrlParam=1m=11140

根据学号给别人发消息

czb.tongji.edu.cn/xetzgj/WriteMsg.jsp?msgUrlId=&msgUrlParam=1m=11140

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