确认资产

提交当中中记补充将一认证账号 账号为漏洞2当中登录的账号 密码为：lyl011109 请审阅

漏洞1 任意用户注册

https://webvpn.nankai.edu.cn/http/77726476706e69737468656262573742/1a1ae13d27666301e2f5d8fe2c905/hygl/Others/New_user.aspx

输入学号 1910079 自动带出用户手机号 + 姓名 存在注册用户信息风险

为：

填写完成后即可进行直接注册登录信息当中

漏洞2 垂直越权admin

账号 1910077 密码 000000 登录系统当中

右键查看源代码 发现菜单地址

发现存在权限架构

访问 https://webvpn.nankai.edu.cn/http/77726476706e69737468656262573742/1a1ae13d27666301e2f5d8fe2c905/hygl/Others/Hysgrwh.aspx

可进行管理员操作

进行删除改 减整用户对审批会议情况 或删除用户对应权限

即可证明已经实现了越权操作

漏洞3

在漏洞2当中给点漏洞3的方式 可获取如下用户的手机号

977282
977094
978053
977273
978053
931072
977273
977273
978053
977094
977094