

## 确认资产

提交当中书记补充统一认证账号 账号为漏洞2当中登录的账号 密码为: 1y011109 请等待



## 漏洞1 任意用户注册

https://webvpn.nankai.edu.cn/http/77726476706e69737468656265737421a1ae13d27666301e2f5dd9e2c905/hygl/Other/New\_user.aspx

输入学号 1910079 自动带出用户手机号 + 姓名 存在泄露用户信息风险

Registration form for the Meeting Management System. It includes fields for '职工编号' (Employee ID), '职工姓名' (Employee Name), '联系电话' (Contact Number), '密码' (Password), and '密码确认' (Confirm Password). A '注册' (Register) button is at the bottom. To the right, there's a warning message: '为了您的密码更加安全 1、长度 2、包含大写字母、小'.

Registration form for the Meeting Management System. It includes fields for '职工编号' (Employee ID), '职工姓名' (Employee Name), '联系电话' (Contact Number), '密码' (Password), and '密码确认' (Confirm Password). A '注册' (Register) button is at the bottom.

Registration form for the Meeting Management System. It includes fields for '职工编号' (Employee ID), '职工姓名' (Employee Name), '联系电话' (Contact Number), '密码' (Password), and '密码确认' (Confirm Password). A '注册' (Register) button is at the bottom.

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 1910079 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/77726476706e69737468656265737421a1ae13d27666301e2f5dd9e2c905/hygl/Other/Hysprnh.aspx

姓名	学号	手机号	姓名	学号	手机号	姓名	学号	手机号	姓名	学号	手机号
1	1910079	13826476706	2	1910079	13826476706	3	1910079	13826476706	4	1910079	13826476706
5	1910079	13826476706	6	1910079	13826476706	7	1910079	13826476706	8	1910079	13826476706
9	1910079	13826476706	10	1910079	13826476706	11	1910079	13826476706	12	1910079	13826476706

可进行管理员操作

进行增删改 调整用户的审批会议等级 或删除用户的对应权限

即可证明已经实现了越权操作

姓名	学号	手机号	姓名	学号	手机号	姓名	学号	手机号	姓名	学号	手机号
1	1910079	13826476706	2	1910079	13826476706	3	1910079	13826476706	4	1910079	13826476706
5	1910079	13826476706	6	1910079	13826476706	7	1910079	13826476706	8	1910079	13826476706
9	1910079	13826476706	10	1910079	13826476706	11	1910079	13826476706	12	1910079	13826476706

## 漏洞3

在漏洞2当中结合漏洞1的方式 可获取如下用户的手机号

977202  
977094  
978053  
977273  
978053  
931072  
977273  
977273  
977202  
977094  
977094

Registration form for the Meeting Management System. It includes fields for '职工编号' (Employee ID), '职工姓名' (Employee Name), '联系电话' (Contact Number), '密码' (Password), and '密码确认' (Confirm Password). A '注册' (Register) button is at the bottom.

温馨提示:

为了您的密码更加安全, 建议您的密码遵循以下原则

1、长度应至少6位;