

漏洞案例介绍

该功能点位于缴账单的查询接口，当输入指定地区的手机号时，即可绕过限制，实现遍历订单

具体案例

可以看到下图查询订单处存在“密码”及“验证码”限制



The screenshot shows a mobile application interface for bill payment. On the left is a sidebar with two main options: '充话费' (Recharge) and '缴账单' (Pay Bill), with the latter being selected. The main content area contains the following fields:

- 手机号码:** A text input field for the phone number.
- 查询月份:** A date range selector showing '2022' year, '01' month, and '06' month.
- 密 码:** A password input field.
- 验 证 码:** A verification code input field next to a CAPTCHA image displaying the number '4389'.

Below these fields is a blue button labeled '立即查询' (Query Immediately). At the bottom, there is a red text notice: '如您手机已成功办理携号转网业务，[请点击](#)更换正确的出账机构'.

但输入指定地区的手机号时，上述限制失效，接着即可爆破后四位批量获取订单信息



 充话费

 缴账单

手机号码:

查询月份:

2022 ▼ 年 01 ▼ 月

 -

2022 ▼ 年 06 ▼ 月

立即查询

如您手机已成功办理携号转网业务，[请点击](#)更换正确的出账机构

```
1  "surchargeAmtFlag": false,|
2  "code": "1000",
3  "message": "交易成功",
4  "billOrgName": " ",
5  "mobileNo": " ",
6  "bills": [{
21 }]
22
23 "surchargeAmtFlag": false,
24 "code": "1000",
25 "message": "交易成功",
26 "billOrgName": " ",
27 "mobileNo": " ",
28 "bills": [{
43 }]
44
45 "surchargeAmtFlag": false,
46 "code": "1000",
47 "message": "交易成功",
48 "billOrgName": " ",
49 "mobileNo": " ",
50 "bills": [{
65 }]
66
67 "surchargeAmtFlag": false,
68 "code": "1000",
69 "message": "交易成功",
70 "billOrgName": " ",
71 "mobileNo": " ",
72 "bills": [{
87 }]
```