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

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

```
"surchargeAmtFlag": false,
"code": "1000",
"message": "交易成功",
"billOrgName": "[redacted]",
"mobileNo": "[redacted]",
"bills": [{
}]

"surchargeAmtFlag": false,
"code": "1000",
"message": "交易成功",
"billOrgName": "[redacted]",
"mobileNo": "[redacted]",
"bills": [{
}]

"surchargeAmtFlag": false,
"code": "1000",
"message": "交易成功",
"billOrgName": "[redacted]",
"mobileNo": "[redacted]",
"bills": [{
}]

"surchargeAmtFlag": false,
"code": "1000",
"message": "交易成功",
"billOrgName": "[redacted]",
"mobileNo": "[redacted]",
"bills": [{
}]
```