逻辑漏洞

问题：
公司新上线了一个系统，需要你对它进行测试，
如何从业务逻辑的层面对它进行测试？

学院介绍

学院宗旨：专注网安人才实战技能培养

学院官网：https://edu.hetianlab.com/

合天网安实验室：https://www.hetianlab.com/

主打课程：

《web安全》：OWASP TOP 10漏洞原理及测试

《渗透测试》：渗透测试流程及工具的使用

《安全开发》：用python写一个综合的扫描器

《CTF-PWN》：CTF中的PWN相关

《CTF-WEB》：CTF中WEB相关

目录
CONTENTS

01 业务逻辑漏洞概述

02 URL跳转漏洞

03 短信/邮箱轰炸漏洞

/01 业务逻辑漏洞概述

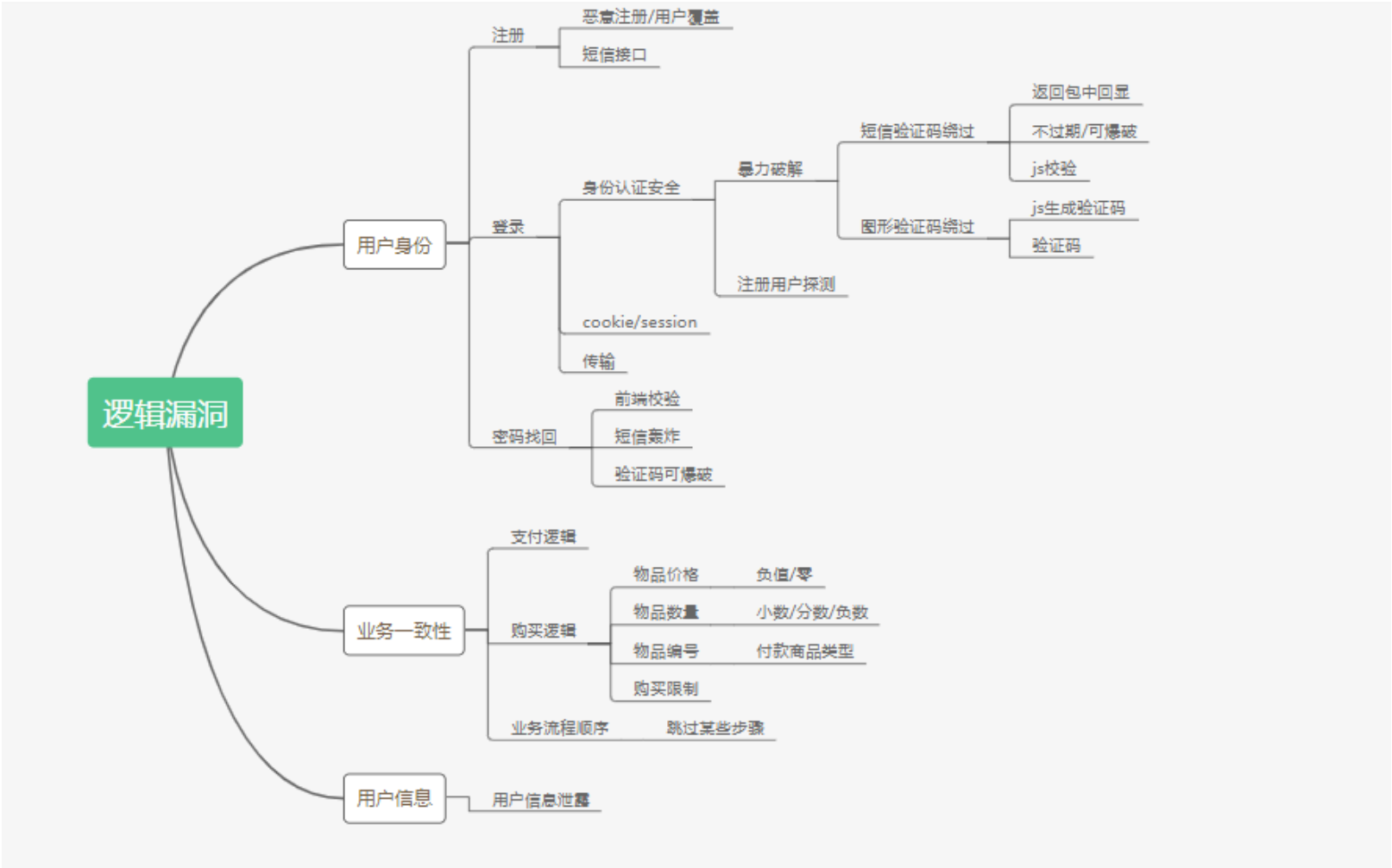
1.1 业务逻辑简述

不同的项目有不同的功能，不同的功能需要不同的代码实现，实现这些核心功能的代码就叫业务逻辑。

1.2 业务逻辑漏洞简述

业务逻辑漏洞是指由于程序逻辑不严谨或逻辑太复杂，导致一些逻辑分支不能正常处理或处理错误。

1.3 常见的业务逻辑漏洞



1.4 如何挖掘业务逻辑漏洞

确定业务流程--->寻找流程中可以被操控的环节--->分析可被操控环节中可能产生的逻辑问题--->尝试修改参数触发逻辑问题

/02 URL跳转漏洞

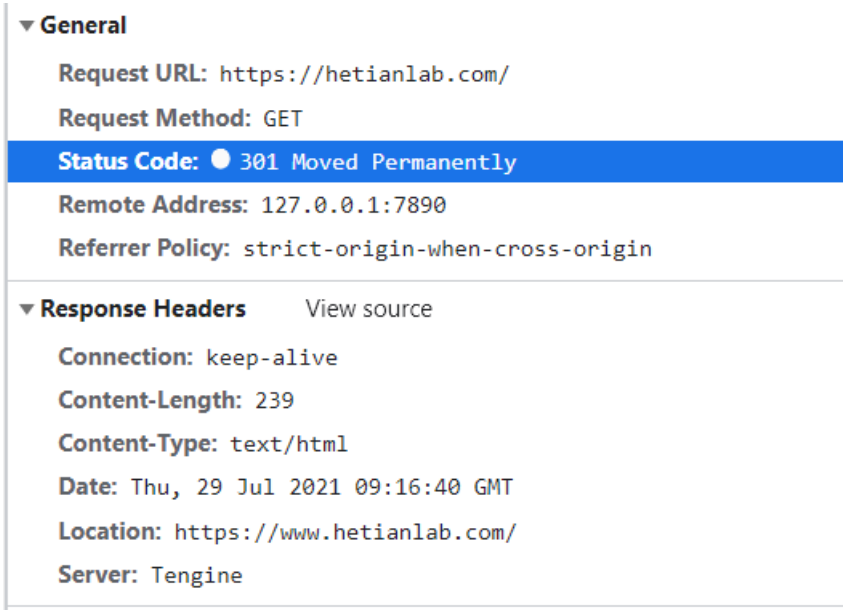
2.1 URL跳转概述

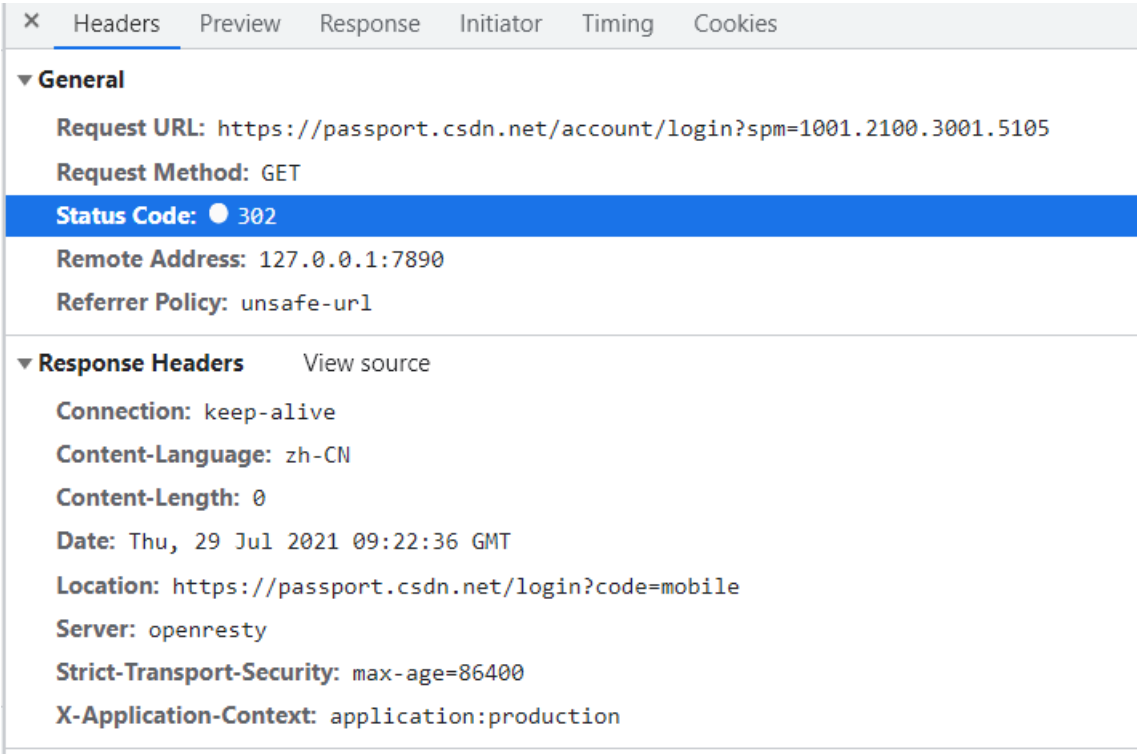
URL跳转也叫做重定向，301和302状态码都表示重定向，浏览器在拿到服务器返回的这个状态码后会自动跳转到一个新的URL地址，这个地址可以从响应的Location首部中获取。

```php
<?php
header('Location:https://www.baidu.com');
?>
```

2.2 301和302的区别

301跳转是指页面永久性移走，通常叫做301跳转，也叫301重定向，301转向。
302重定向又称之为暂时性转移，也被称为是暂时重定向。



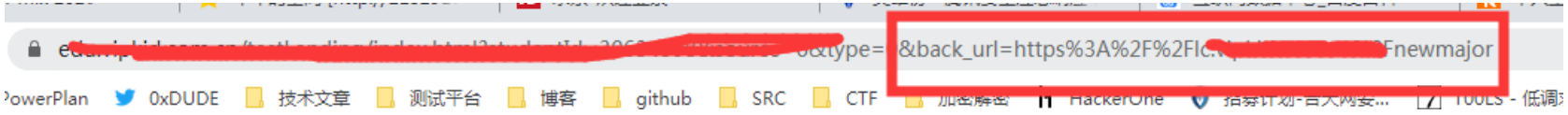


2.3 产生原因

服务端未对传入的跳转 url 变量进行检查和控制，可能导致可恶意构造任意一个恶意地址，诱导用户跳转到恶意网站。

2.4 场景举例

sso 登录、验证跳转、.....



2.5 实战中常见的触发方式

redirect
redirect_to
redirect_url
url
jump
jump_to
target
to
link
linkto
domain

2.6 绕过技巧

利用问号绕过限制：url=https://www.baidu.com?www.xxxx.me

利用@绕过限制：url=https://www.baidu.com@www.xxxx.me

利用斜杠反斜杠绕过限制：url=http://www.evil.com/www.xxxx.me

利用子域名绕过：https://www.baidu.com.xxx.com

2.7 修复/防御方法

修复该漏洞最有效的方法之一就是校验传入的跳转url参数值，判断是否为预期域名。

/03 短信/邮箱轰炸漏洞

3.1 短信轰炸概述

网站在对信息发送的次数、时间没有做限制，或者只在前端做了限制，导致可以无限制发送信息，简单的说就是发送短信/邮件的包可以无限制的发送。

3.2 漏洞产生位置

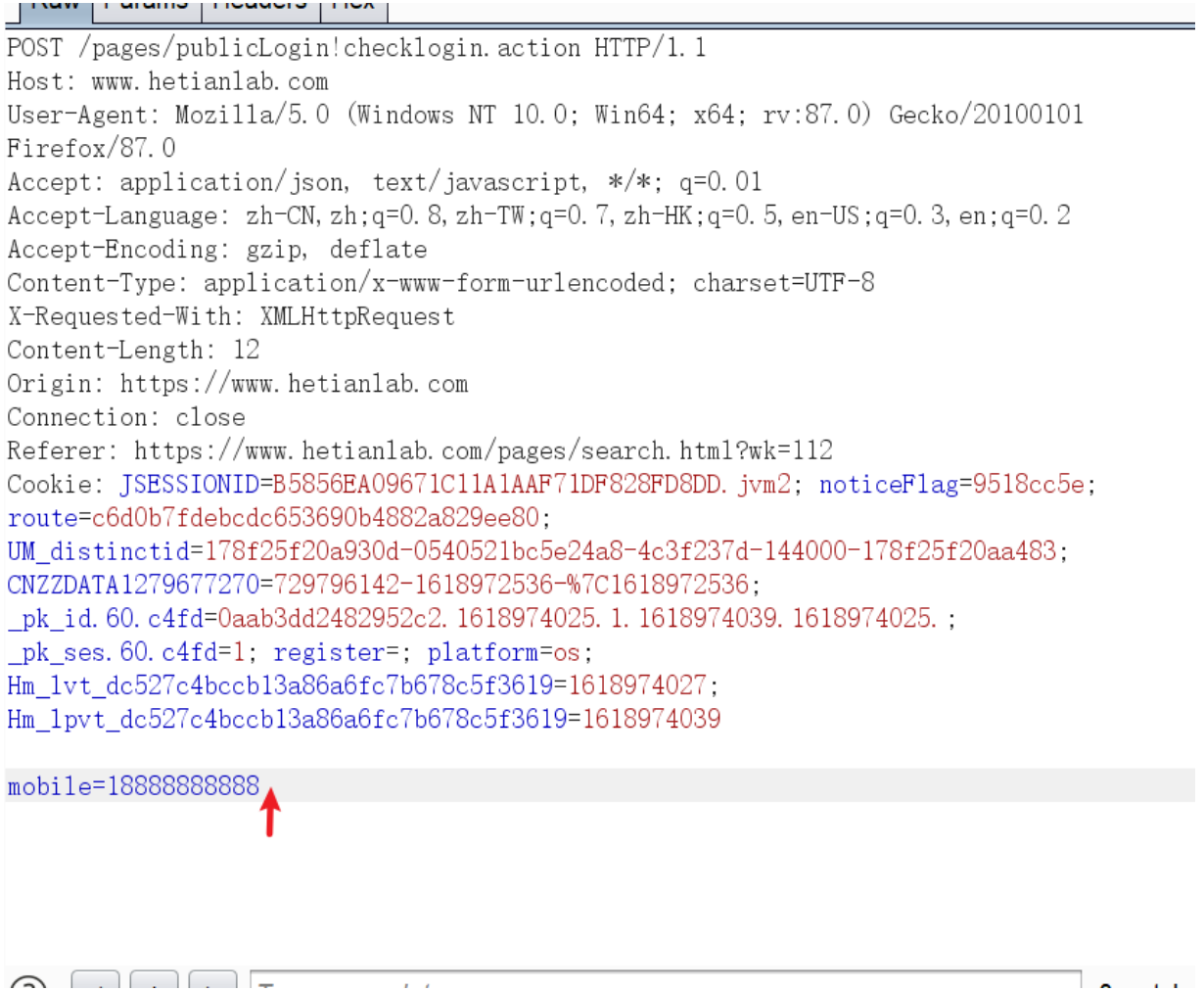
会员账号注册功能，忘记密码找回功能上，会员绑定手机邮箱功能，设置取款密码使用手机验证，或者是某项重要的操作，提现，充值等功能上需要手机短信验证码，再一个是网站活动领取奖品功能上。

3.3 测试方法

抓到发送短信、邮件、私信、站内信的报文，不断重放。

3.3.1 绕过技巧一

尝试在moblie参数后面加空格



3.3.2 绕过技巧二

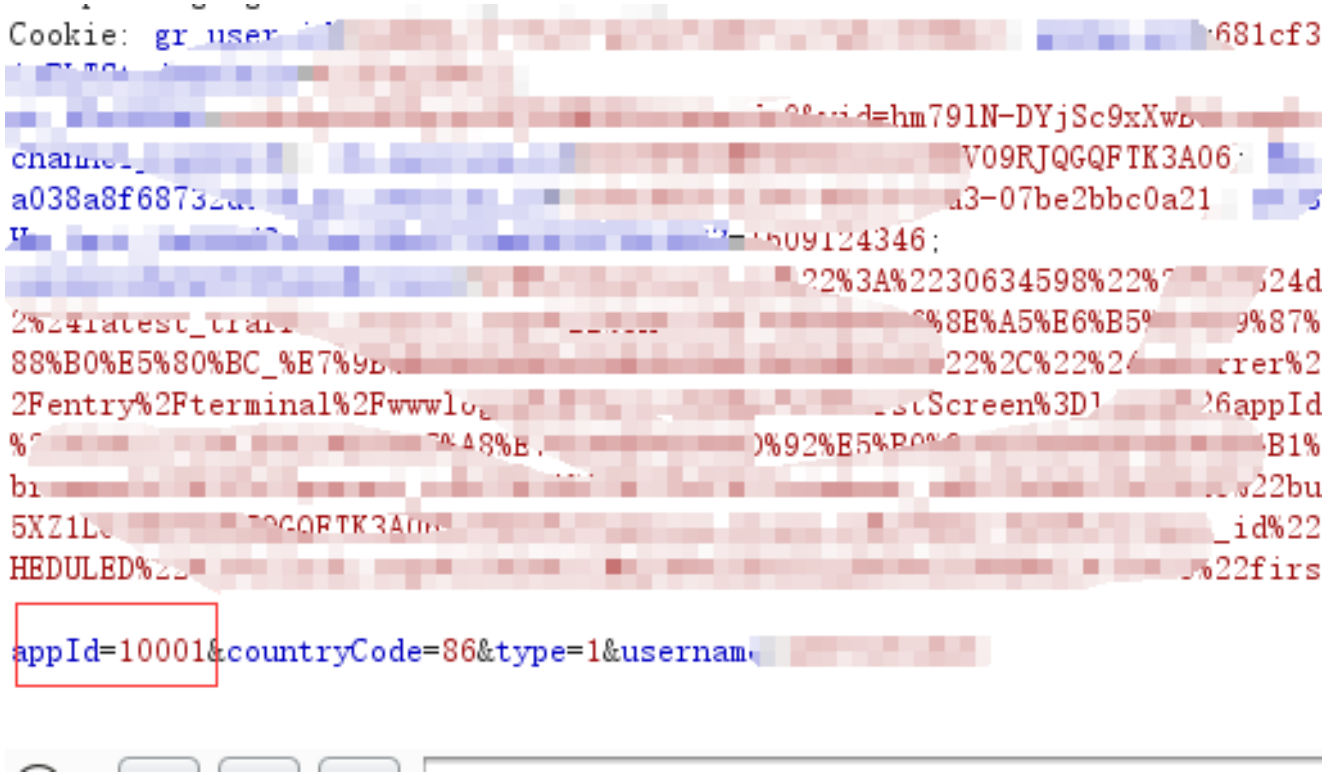
尝试对参数进行多次叠加

```
Host: m.vipfengxiao.com
Connection: close
Content-Length: 47
Accept: application/json, text/plain, */*
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWeb
like Gecko) Chrome/79.0.3945.88 Safari/537.36
Content-Type: application/json;charset=UTF-8
Origin: https://m.vipfengxiao.com
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Referer: https://m.vipfengxiao.com/user-asset/updateMobile
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8

{"mobile":"18114211234","mobile":"18114211234"}
```

3.3.3 绕过技巧三

利用调用接口绕过短信&邮箱轰炸限制



3.3.4 绕过技巧四

利用大小写绕过邮箱轰炸限制

```
Content-Type: application/x-www-form-urlencoded
Accept: */*
Origin: https://mail.qq.com
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://mail.qq.com/zh_CN/htmledition/ajax_proxy.html?mail.qq.com&v=140521
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8,zh-TW;q=0.7,en-US;q=0.6
Cookie: pgv_pvid=6140832990; pgv_info=ssid=s5536932822; _qpsvr_localtk=0.16952682410672382; uin=o0849310853;
RK=ecLQqaveRB; ptcz=9ac0881dd17d32336ec4cacb79650890b5047e11281737c1494eba418a460236; luin=o0849310853;
lskey=00010000eabfec017ff44354a944a865084fb0594cc3bca01df175164e3e26aaaf114643912b16cc76878eca; skey=@R1abJWLnn;
p_uin=o0849310853; pt4_token=1e1M*1knz5ptSrYWkGrMXj7qJN7KfBwAussFdXHxqwk_;
p_skey=YVzA11GHzVT7XcO*oWzyEHU539fc1NWvIfgTtujbStA_; wimrefreshrun=849310853&; qm_logintype=qq;
qm_antisky=849310853&eb65562d2c8d406c579c2da7df5bc9574d9cb0df37b6ef0937a54df362ce7bd3;
qm_device_id=Pr8s9ZQjBqk+K7D6UrFFDiv+2Kb1VpnVy+SAbmtE0OLUTkmsMCI/hPHk49qhg3djCExduLubzpvyUcIJPoQVyg==; qm_flag=0;
qqmail_alias=849310853@qq.com;
sid=849310853&5b0f2a7af0a40c9e567c098fcee0a2cd,qWVZ6QWxsR0h6V1Q3WGNPKm9Xen1FSFU1Mz1mYzFOV3ZJZmdUdHVqY1N0QV8.;
qm_username=849310853; qm_domain=https://mail.qq.com; qm_ptsk=849310853&@R1abJWLnn;
qm_ptlsk=849310853&00010000eabfec017ff44354a944a865084fb0594cc3bca01df175164e3e26aaaf114643912b16cc76878eca;
foxacc=849310853&0; ssl_edition=sail.qq.com; edition=mail.qq.com; qm_loginfrom=849310853&clientread;
username=849310853&849310853; CCSHOW=000001; new_mail_num=849310853&409; xm_uin=13102661874185349;
xm_sid=zYViaYx0cXoun0ZZADJkOAAA; xm_skey=13102661874185349&987665d8a5901119c3e10069a104448d; webp=1

b836cc9120ad32c901a824d29655c602=5b0f2a7af0a40c9e567c098fcee0a2cd&sid=jwqUwrbv0aZ1Lhx8&from_s=cnew&signtype=0&to=%22绁
虹櫍%22<849310853@Qq.com>&subject=test&content__html=<div>1234</div>&sendmailname=849310853@qq.com&savesendbox=1&actiont
ype=send&sendname=鍏戝彭鐖卞埌鍙戝姩&acctid=0
&separatedcopy=false&s=comm&hitaddrbook=0&selfdefinestation=-1&domaincheck=0&cgitm=1623415198846&clitm=1623415199288&com
tm=1623415309730&logattcnt=0&logattsize=0&timezone=28800&timezone_dst=0&cginame=compose_send&ef=js&t=compose_send.json&r
esp_charset=UTF8
```

3.3 修复方式

合理配置后台短信服务器的功能，对于同一手机号码，发送次数不超过3-5次，并且可对发送的时间间隔做限制。

页面前台代码编写时，加入禁止针对同一手机号进行的次数大于N次的发送，或者在页面中加入验证码功能，并且限制发送的时间间隔

感谢您的聆听

学习工具、资料及课程回放

扫码免费领取