

企业安全 攻与防

平安SRC线上沙龙系列主题活动 第六期

🕒 时间：2024.5.31 14:00-17:00

主办方



合作伙伴



外卖业务与推广功能的逻辑漏洞

月神

Theloner安全团队队长



目录

1

外卖用户端

外卖的用户端有哪些不一样的通用漏洞

2

外卖商家端

商家端存在着哪些特殊的挖洞技巧

3

推广漏洞

通杀国内所有推广业务的漏洞是如何发现的



业务逻辑漏洞

测试业务逻辑漏洞的过程中，不管用任何工具，
我们都在尝试把本地传给服务器的数据改掉。

分析业务逻辑

发现其中开发者的思维漏洞是一件很有意思的事情



外卖用户端

用户端的业务逻辑





参数叠加

营销套路：6份起购，首份1分钱，剩余5份30元

数量修改为 1 即可绕过限制

原因：后端没有对起购份数做限制，只在前端限制了

修复后可尝试用逗号的方式叠加参数进行绕过

`[{ID:1001,num1},{ID:1001,num1},{ID:1001,num1},{ID:1001,num1},{ID:1001,num1},{ID:1001,num1},{ID:1001,num1}]`

正常传的参数是：

`[{ID:1001,num6}]`



无限叠加小料

有些外卖会有小料可以选择，而小料也是容易疏忽的漏洞点。手动添加多个attrs即可无限增加、或叠加小料。

```
{
  "addr_longitude": 12534905,
  "addr_latitude": 4389861,
  "wm_poi_id": 85992236642475,
  "user_id": 1778432765,
  "foodlist": [
    {
      "spu_id": 151633512,
      "id": 172803372,
      "count": 1,
      "cart_id": 0,
      "attrs": [
        1847012552, 1847012558, 1847012550, 1847012559, 1847012549, 1847012555, 1847012561
      ]
    }
  ]
}
```

原因：后端没用对attrs参数做数量校验、重复添加校验

思路扩展：参数叠加可以用于多场景，例如开发票的订单号参数、商城额外服务参数，优惠券id等任何场景下。



```
[{"cart_id":"0","product_id":"100001","product_quantity":-1,"product_name":"盐酥鸡"}, {"cart_id":"0","product_id":"100001","product_quantity":2,"product_name":"盐酥鸡"}]
```





很多程序在校验负数的时候会疏忽，对物品单价不能为负做校验，我们只需要把参数叠加相同的然后用正负数来写即可绕过。

例如: [{ID: A, num: 2},{ID: A, num: -1}]

还有一些程序喜欢对总价格不能为负数做校验，用正负数同样能绕过

例如: [{ID: A, num: 2},{ID: B, num: -1}]



外卖商家端

外卖商家端的技巧分享



补贴类的漏洞--严重

因为补贴的漏洞都涉及到套现。



补贴类的漏洞常出现在各类促销活动中。如各种不同的城市活动、618大促、双十一大促等。

这些活动通常都有复杂的规则和玩法，其中往往就隐藏着诸多漏洞。

poicharge:0,agentcharge:100 (百分比分配)
poicharge:-100,agentcharge:200 (百分比分配)
poicharge:0,agentcharge:10 (金额分配)
poicharge:1,agentcharge:9 (金额分配)

常见的参数

✓ shippingCharge
poiCharge
agentCharge
mtCharge
brandCharge

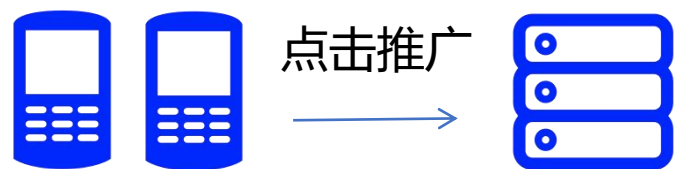


推广漏洞

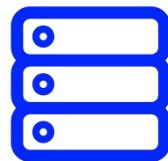
为何能做到通杀？



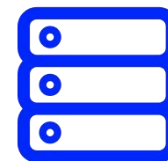




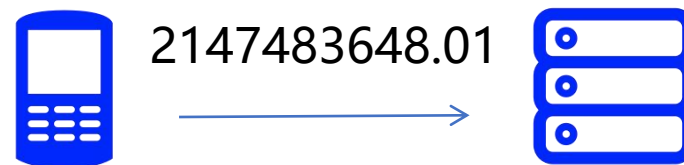
后端扣费



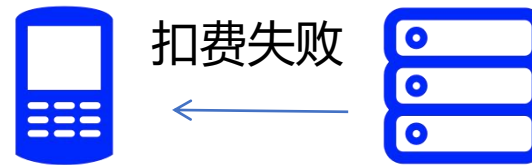
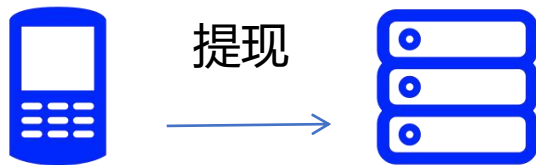
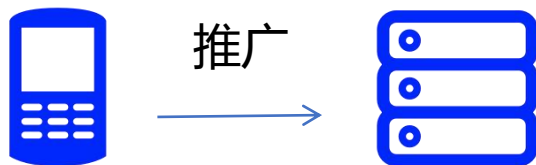
校验余额是否足够



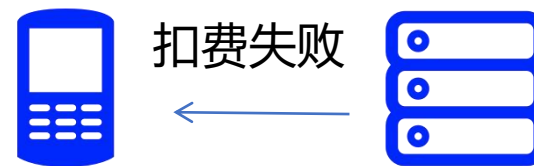
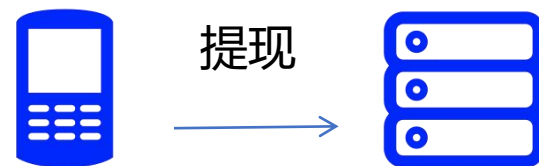
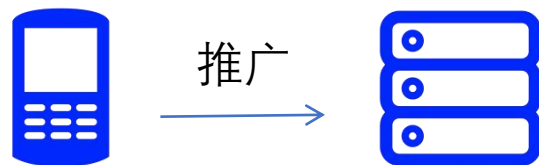
1、创建推广时一般业务都会对金额做校验，所以我们可以选择用int类型最大值来绕过校验



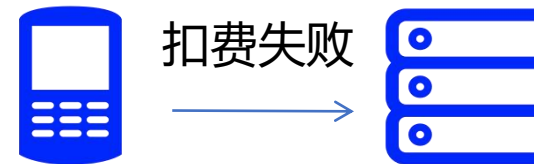
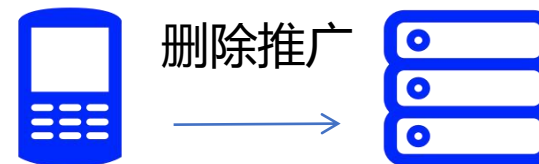
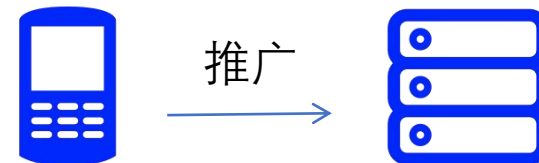
2、充值后在提现（基本通杀）



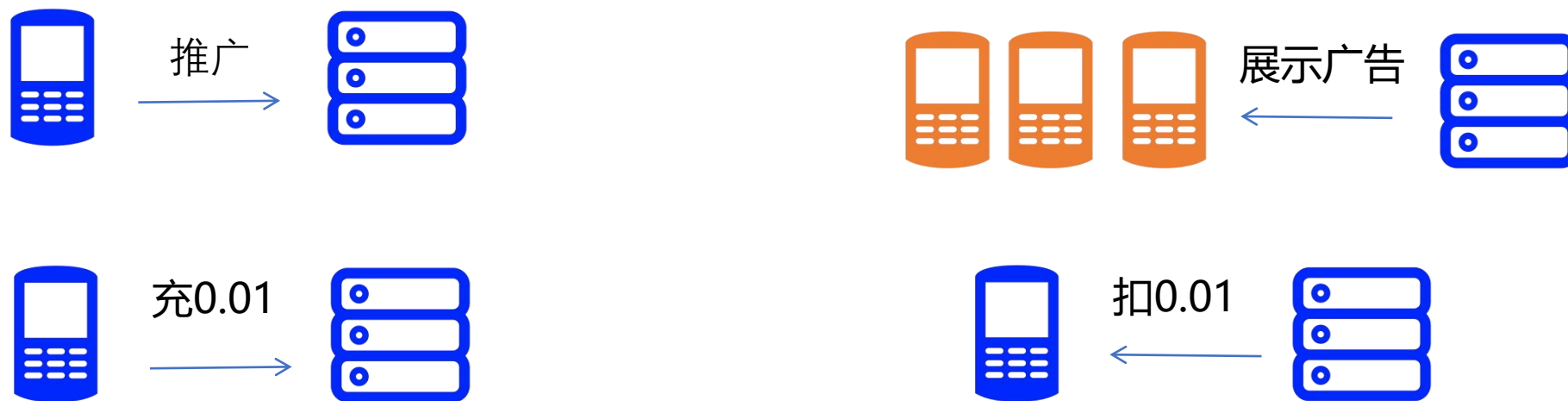
3、余额转入子账号（基本通杀）



4、开启推广后中断推广



5、保持最低余额推广，余额为0.01，单次点击价格为99



推广逻辑首先要了解业务流程，才能找到流程中的逻辑漏洞，这就是逻辑漏洞的魅力，找到一个开发者思维上的漏洞，你会发现每一个开发者所开发的业务逻辑是完全一样的，这样就做到了通杀所有SRC业务了。

还有6种绕过方式希望大家可以根据以上内容自己深入研究一下

彩蛋

内存挖掘漏洞



关注Theloner安全团队公众号，
不定期更新技术文章



很多不走http协议的功能其实漏洞都非常多
因为http协议的功能白帽子和内部都测过很多遍了。

比如越权覆盖直播推流，越权发消息，越权关闭会议，越权踢人，但只是越权吗？



月神

09-21 12:50:56

马哥这个漏洞你怎么看



Pony马化腾

09-21 12:50:55

这个漏洞一定要给这个叫月神的小伙子严重，我马化腾说的，耶稣也拦不住



月神

09-21 12:51:04

谢谢马哥

