无间道之顺藤摸瓜

蘑菇街背后的灰色产业链

侯栋 <with.h4rdy@gmail.com>


主办方 Geekbang 极客邦科技 InfoQ
ArchSummit
全球架构师峰会 2017
12月8-9日 北京·国际会议中心


AiCon
全球人工智能技术大会2018
助力人工智能落地
2018.1.13 - 1.14 北京国际会议中心
AiCon
扫描关注大会官网

侯栋 @H4rdy

- 美联集团高级安全工程师
- 美联安全应急响应中心(MLSRC)审核大大
- 关注安全研究以及Web应用漏洞挖掘

TABLE OF **CONTENTS**

- 帐号注册的一些方法
- 权限买卖的产业链
- 套现&退款退货
- FAQ

我们先来聊一聊帐号

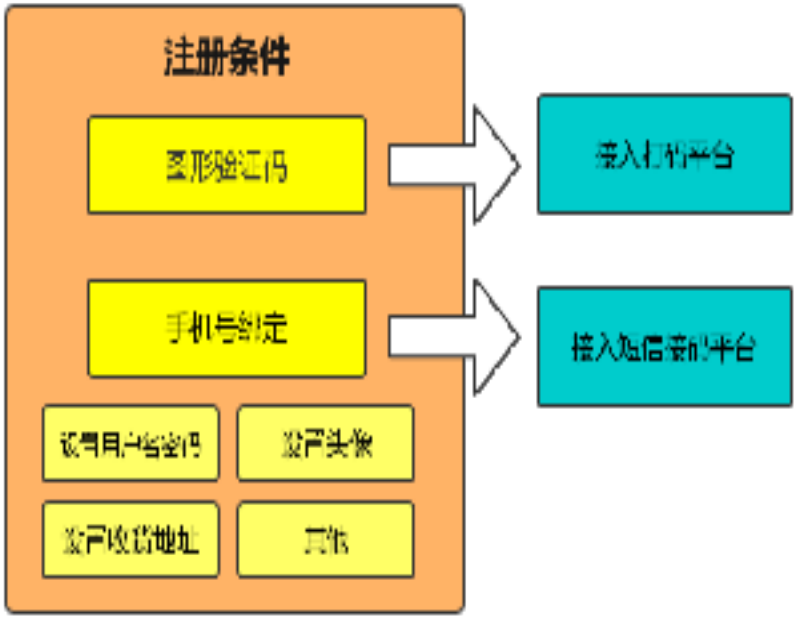
到底是”有”还是”没有”?

平台自己的锅

开发的锅

第三方的锅

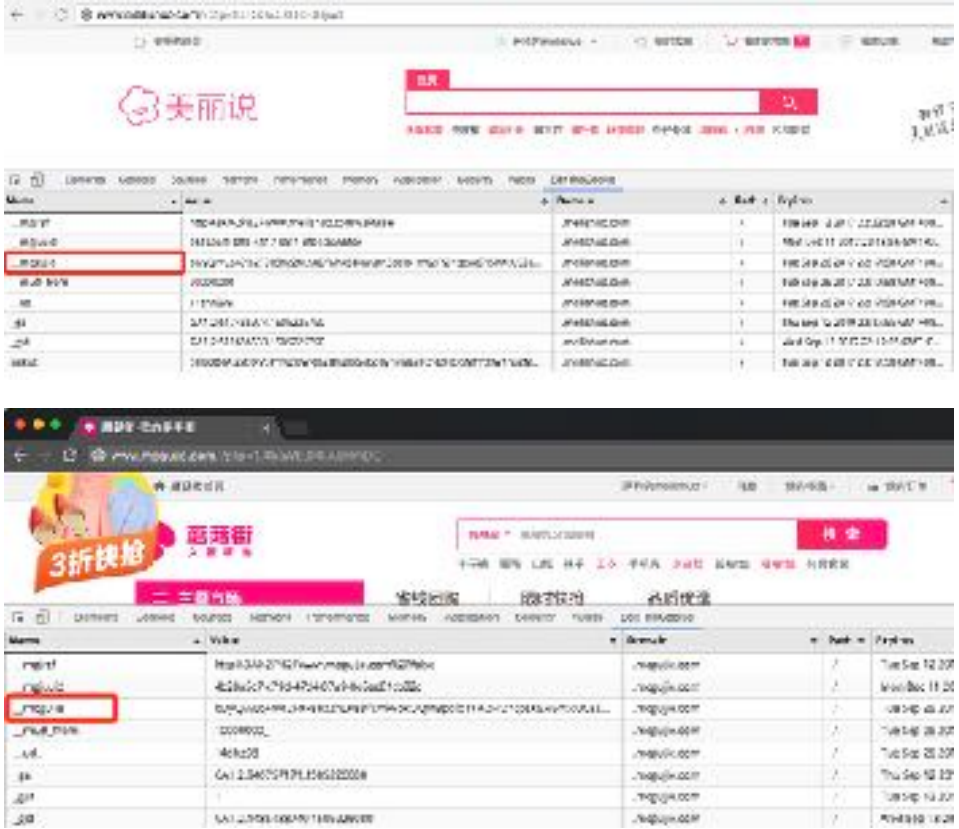
平台自己的锅



开发的锅

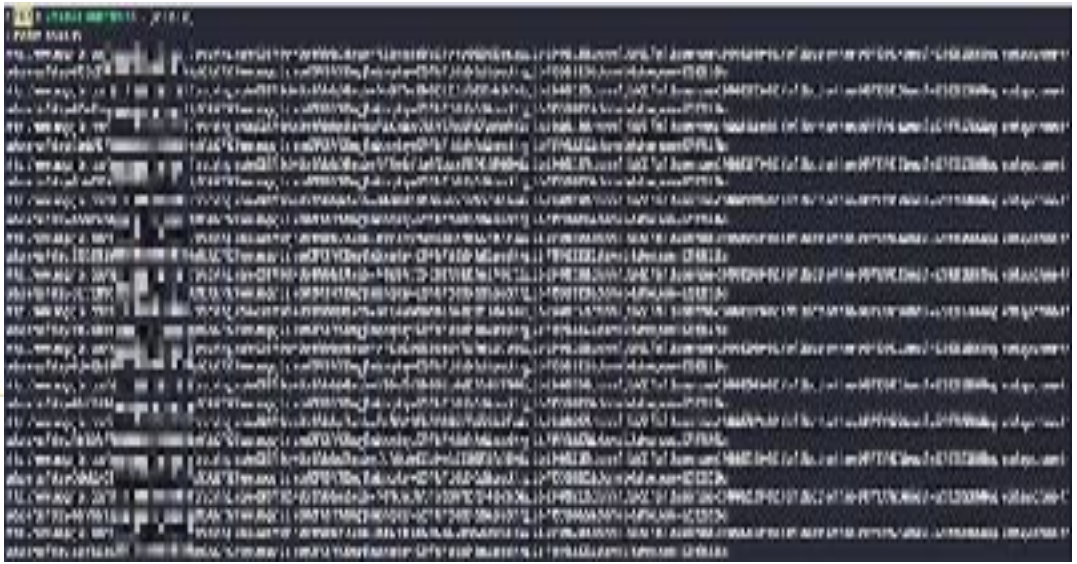
美丽说账号购买蘑菇街商品

- 直接通过登录接口登录
- 在支付环节修改订单来源
- Cookie



第三方的锅

不到20行的代码 = 5毛 * N



反查账号来源

问:注册帐号总共分几步


注册第三方账号
快捷登录模式到蘑菇街
获取返回帐号信息
http://passport.fanli.com
http://fun.fanli.com
http://paymarket.mogujie.com

我们再来看一看帐号权限

蘑菇街直播

* 怎么样的视频可以通过审核呢：

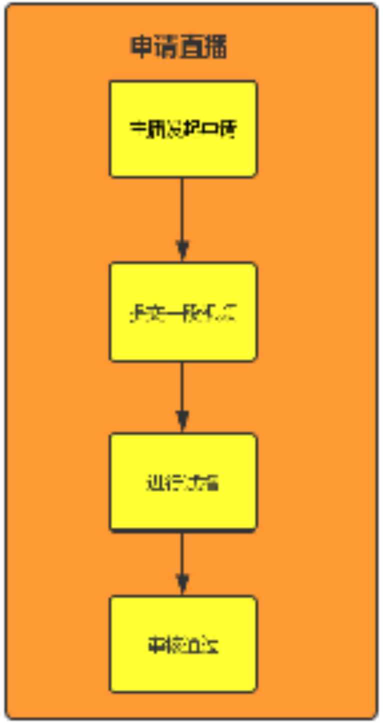
有不错的颜值和身材（非常重要，很大程度上决定你是否能通过审核），具有与商领秀能力（独特的时尚搭配），如果在其他的直播平台或者一些公众熟知的平台上有一定的粉丝影响力那就更是大大加分。

什么是蘑菇街时尚主播的标准？

1.颜值过关，这是个不光看脸的世界，所有出现在镜头前的内容（主播+布景）都要很美。

2.口才一流，思维敏捷的女神，就要会沟通。

3.了解大众的审美，对时尚趋势有自己独到的见解，并能在镜头里表现出来。



有直播权限的帐号


蘑菇街直播代开送
回复:蘑菇街可以找人代开直播马
回复:代开直播号,代开店铺
回复:代开直播号,代开店铺
蘑菇街直播代开送,当天下号,不


成员 133/169

分析

由于这个人能直接开通帐号直播权限,分析他的身份

- 他是内部员工,直接通过后台添加权限
- 他勾结内部员工通过后台添加权限
- 他是普通人,但通过某些渠道(漏洞)进行添加权限

直播权限开通流程

- 帐号在13:10:43注册了蘑菇街帐号
- 帐号在16:48:11开通了直播权限

直播权限开通方式

- 通过正常申请流程申请开通的,上传了试播视频等必要资料
- 雇佣专业的主播/模特,注册了多个帐号
- 提交试播资料去审核并开通每个帐号的直播权限

顺藤摸瓜

一个账号 → 指纹设备 → 更多账号

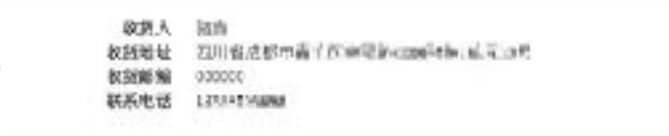
怎么解决

帐号实名制可以解决问题吗？

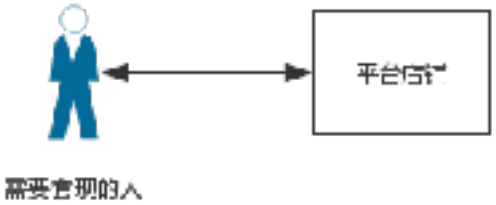
- 主播拥有直播帐号 —— 一个主播 —— A商家、B商家、C工作室
- 商家、工作室拥有直播帐号 —— 一个商家 —— A主播、B主播、C主播

最后在说说恶意的购物行为

- 在2016-11-03、2016-11-06、2017-03-05、2017-06-12购买过4次手机
- 并且均使用白付美(消费信贷产品)付款
- 4次购买手机的填写的收货地址均不相同



基础版套现方式



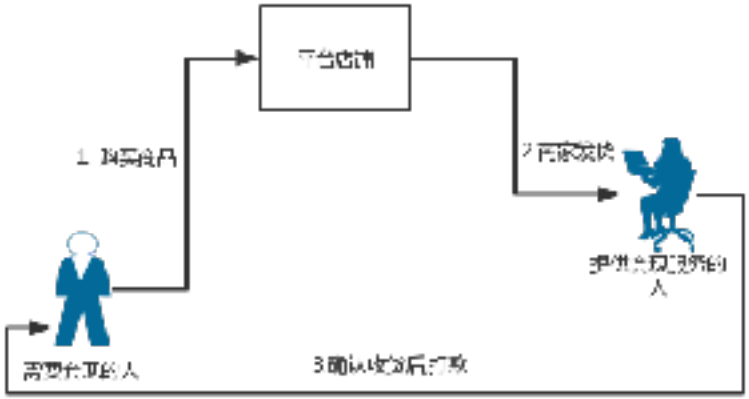
【群】我[redacted] 17/7/7 13:16:15

@全体成员 7.7，所有业务开工，套现找群上，安全又靠谱

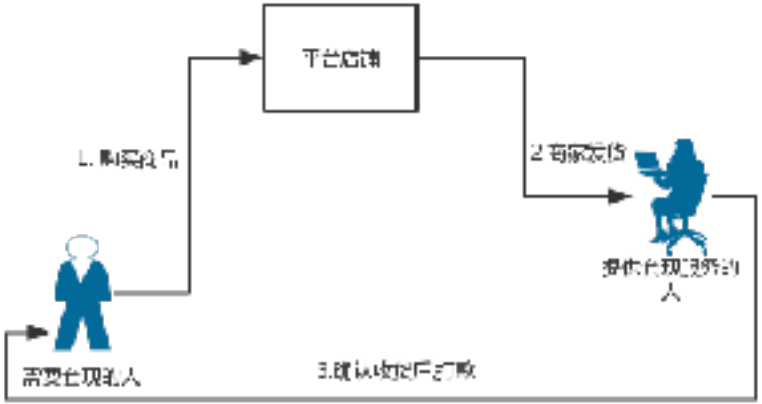
【群】[redacted] 17/7/7 14:28:26

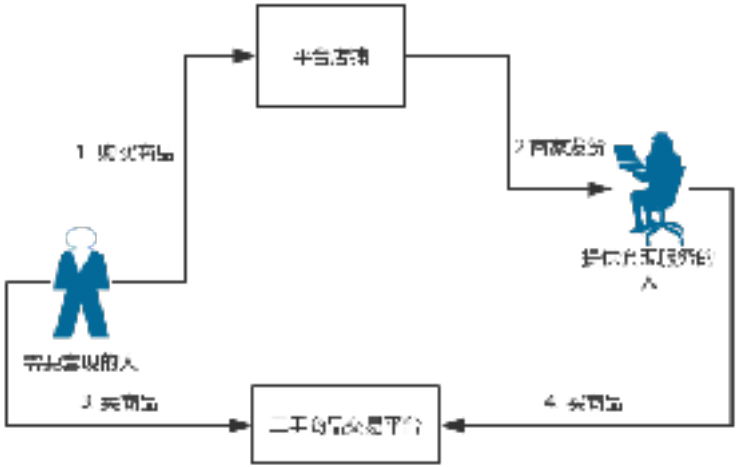
@全体成员 大量收信用住，不怕死的酒店来了，我们搞死他，速度砸单子过来

高级版套现方式



顶配版套现方式





申请退货退款

- 使用低价快递进行退货退款 → 套运险费
- 使用虚拟单号进行退货退款 → 免费获得商品

申请仅退款

- 卖家发货后申请仅退款
  - 恶意消耗卖家的运费险保费
  - 申请"未按约定时间发货"赔付
  - 免费获得商品
- 主动购买仿品进行维权申请仅退款 → 免费获得商品

Thanks!

INTERNATIONAL SOFTWARE DEVELOPMENT CONFERENCE

关注QCon微信公众号
获得更多干货!