



全球软件开发大会【上海站】

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>



极客时间

重拾极客精神·提升技术认知

每天10分钟,邀请顶级技术专家,为你传道授业解惑。



扫一扫,试读专栏

主办方 **Geekbang** · **InfoQ**
极客邦科技

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



扫描关注大会官网

APSEC 2017



APSEC 2017

24th Asia-Pacific Software Engineering Conference
4-8 December 2017, Nanjing, Jiangsu, China

12月4-8日

中国南京



了解详情

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”？

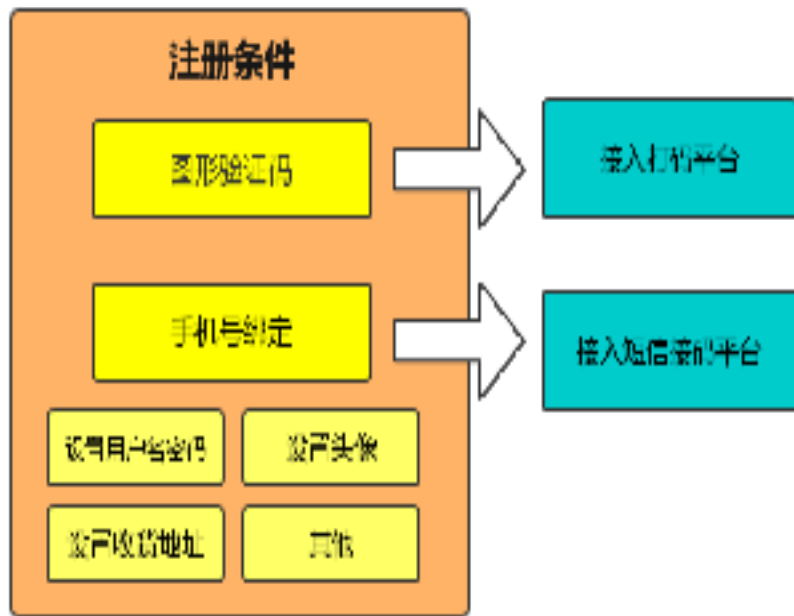


平台自己的锅

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

rid 17:11:35

啥啥啥注册就可以用了？

自由团队 17:12:07

3.这是别人的

rid 17:12:28

收费？

rid 17:19:25

还是怎么了

自由团队 17:20:34

是的 400元 注册一个小号成本6千多

自由团队 17:33:15

因为注册并方法不一样 单个过程需要4个数据 而现在的景象是 有的数据在公共的小号

自由团队 17:33:23

半成半小号注册一个

自由团队 18:04:32

买了注册机 还是买半成品的 注册机从半成半成的小号绑定手机号的

rid 17:40:25

收费，昨天半成号

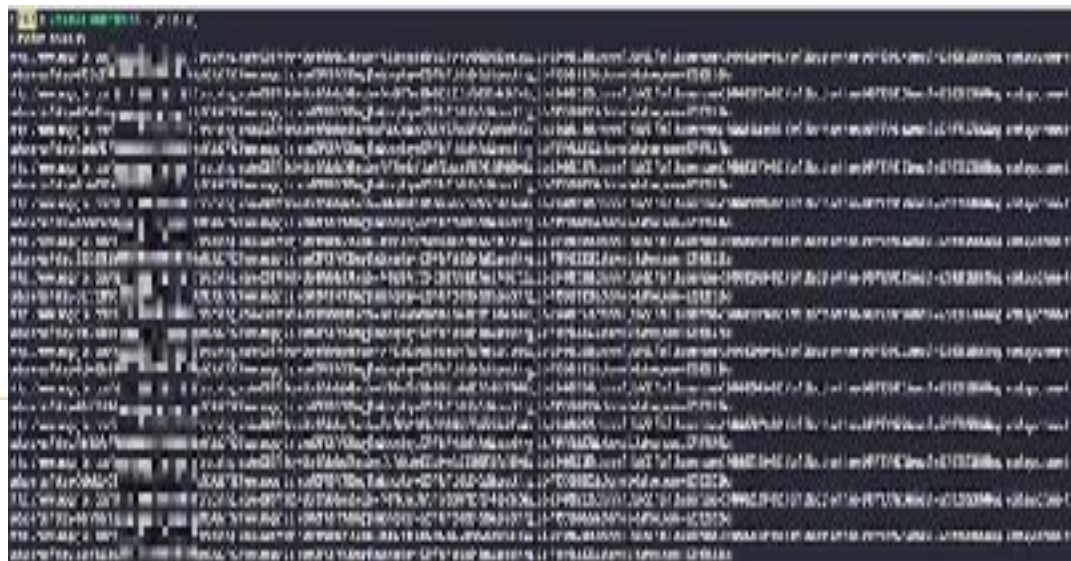
自由团队 17:42:13

fxcmrjow 编辑 17:42:13 uols 17501

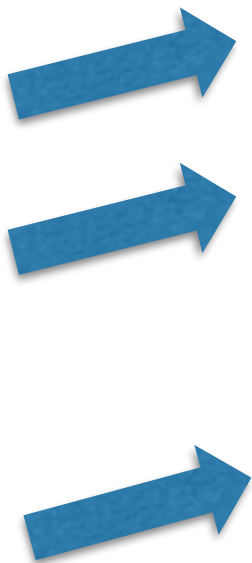
自由团队 17:42:20

你测试吧

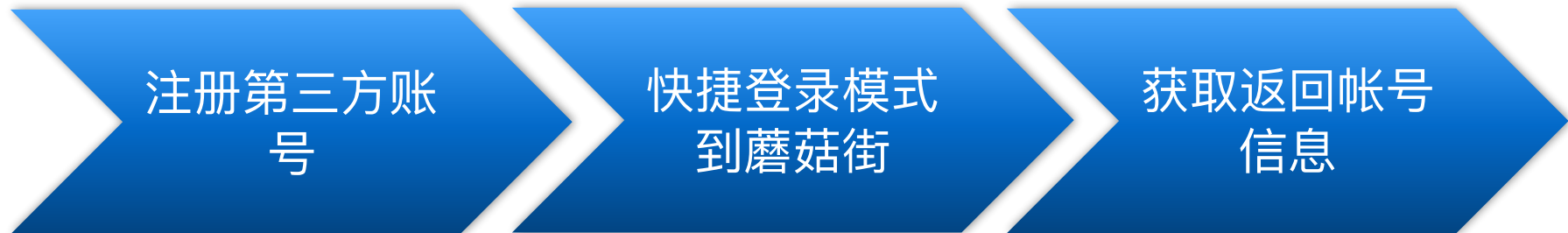
不到20行的代码 = 5毛 * N



反查账号来源



问:注册帐号总共分几步



<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

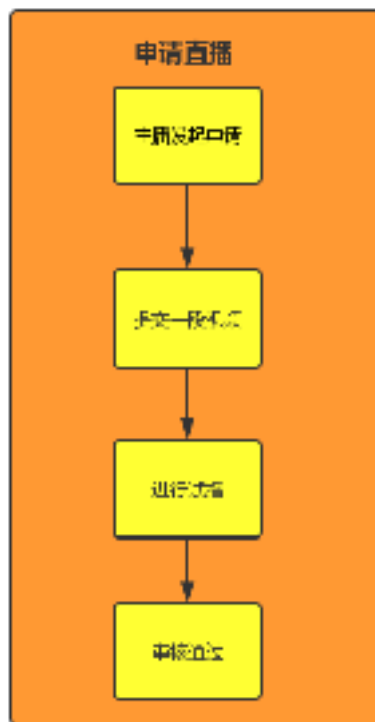


* 怎么样的视频可以通过审核呢:

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], 具有为再创造能力 (懂得时尚穿搭), 如果在其他的高雅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题的标准?

1. 把脸过关, 这是个不光看脸的世界, 所有出现在镜头的内容 (主播+布景) 都要很美。
2. 口才一流, 只想做花痴的姑娘, 赶紧去沉睡。
3. 了解大众的审美, 对时尚趋势有自己独特的见解, 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

贴吧: [用户头像] 2017-08-22

回复:蘑菇街可以找人代开直播吗

当根镜了,今天下午被骂了,难过死了...

贴吧: [用户头像] 2017-08-22

回复:代开直播号,代开店铺

她一个小程序员表直播,有直播权限,有意者以

贴吧: [用户头像] 2017-06-

回复:代开直播号,代开店铺

妈的,智商,老子给你变卖了,有本事拿证据来告

贴吧: [用户头像] 2017-08-17

蘑菇街直播代开送,当天下号,不

蘑菇街直播代开送,当天下号,不要和代开视频!

贴吧: [用户头像] 2017-06-1



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

关联设备 (设备数量: 6)

设备类型	设备名称	首次使用时间	最后使用时间	关联数
ANDROID	小米手机	2017-08-01 10:00	2017-08-01 10:00	1
ANDROID	小米手机	2017-08-01 10:00	2017-08-01 10:00	1
ANDROID	小米手机	2017-08-01 10:00	2017-08-01 10:00	1
ANDROID	小米手机	2017-08-01 10:00	2017-08-01 10:00	1
IOS	iPhone	2017-08-01 10:00	2017-08-01 10:00	1
IPAD	iPad	2017-08-01 10:00	2017-08-01 10:00	1

关联用户 (用户数量: 11)

用户名	用户名称	用户类型	最近使用时间	最近登录时间	关联数
admin	admin	管理员	2017-08-01 10:00	2017-08-01 10:00	11
admin	admin	管理员	2017-08-01 10:00	2017-08-01 10:00	10
admin	admin	管理员	2017-08-01 10:00	2017-08-01 10:00	9
admin	admin	管理员	2017-08-01 10:00	2017-08-01 10:00	8
admin	admin	管理员	2017-08-01 10:00	2017-08-01 10:00	7
admin	admin	管理员	2017-08-01 10:00	2017-08-01 10:00	6
admin	admin	管理员	2017-08-01 10:00	2017-08-01 10:00	5
admin	admin	管理员	2017-08-01 10:00	2017-08-01 10:00	4
admin	admin	管理员	2017-08-01 10:00	2017-08-01 10:00	3
admin	admin	管理员	2017-08-01 10:00	2017-08-01 10:00	2
admin	admin	管理员	2017-08-01 10:00	2017-08-01 10:00	1

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

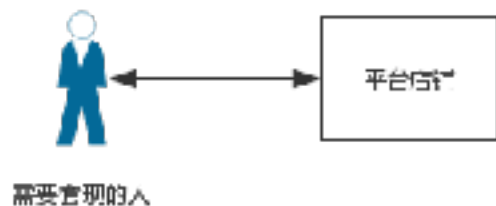
最后在说说恶意的购物行为

- ▶ 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

收货人 周南
收货地址 四川省成都市青羊区...
收货邮编 610000
联系电话 13784146666



基础版套现方式



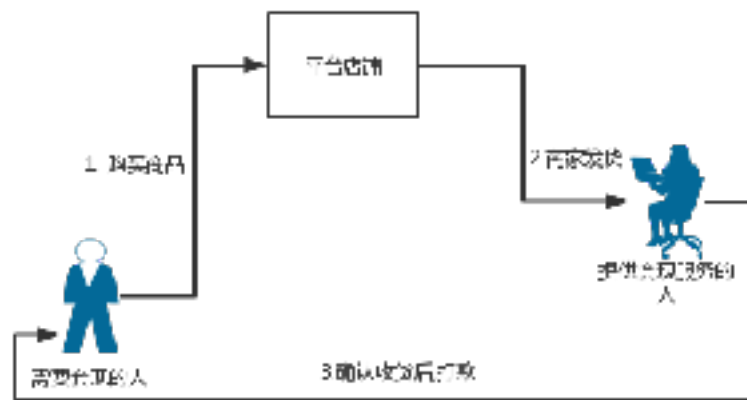
【群1】我[头像] [头像] [头像] [头像] [头像] [头像] [头像] [头像] [头像] [头像] 17/7/7 13:16:15

@全体成员 7.7，所有业务开工，套现找群上，安全又靠谱

【群1】我[头像] [头像] [头像] [头像] [头像] [头像] [头像] [头像] [头像] [头像] 17/7/7 14:28:26

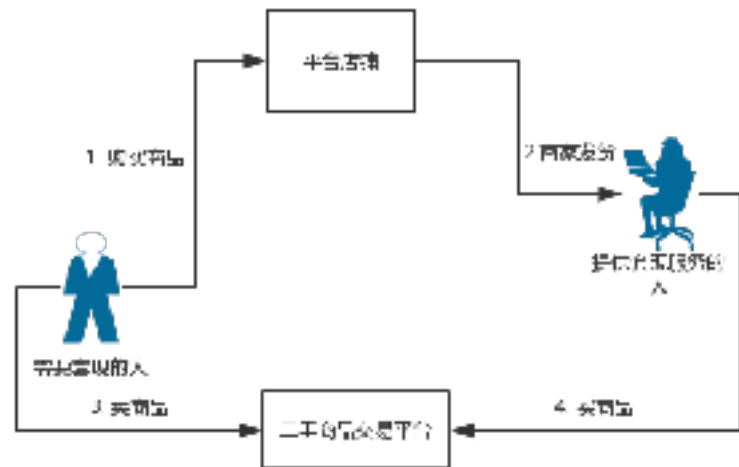
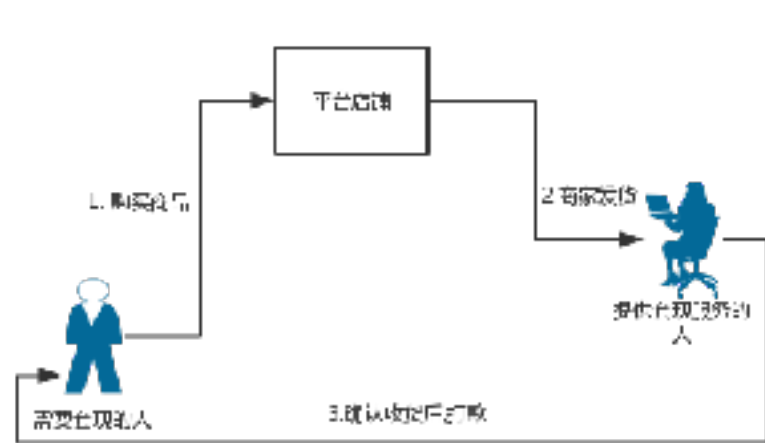
@全体成员 大量收信用住，不怕死的酒店来了，我们拍死他，速度砸单子过来

高级版套现方式



```
14:08:50
最少750起套现
ro 14:09:08
那手续费多少?
14:09:36
30个点
ro 14:10:14
也是这么贵啊
ro 14:10:31
为啥白付钱的都这么贵啊
14:10:34
恩，唐廷衡一直都是这个点位
14:10:41
成本高啊
ro 14:10:59
为啥?
ro 14:11:05
是真的发货还是假的?
14:11:43
真实发货
14:15:47
就是回网上转转手机的
14:15:58
比如之前套现回的转手魅族，手机
14:16:12
现在只套现回新机，那中套现的手机
14:20:18
还有一批中套现之流都是收新机，在收新机
```

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



关注QCon微信公众号
获得更多干货!

Thanks!

INTERNATIONAL SOFTWARE DEVELOPMENT CONFERENCE

Geekbang > InfoQ