

不可忽视的

电商业务安全问题

唯品会
vip.com 一家专门做特卖的网站

议题

- 背景介绍
- 典型案例
- 解决之道
- Q&A



电商业务安全备受挑战

- 凡是能换成**金钱**的，都会有人去攻击或尝试
- 今天是免费的**资源**，明天可能就是重要的资产



需要重点保护的对象

- 用户账号/密码
- 用户钱包/银行卡
- 用户隐私数据
- 代金券、优惠券、礼品卡、积分、虚拟币
- 物流、库存
- 订单、商业数据
-



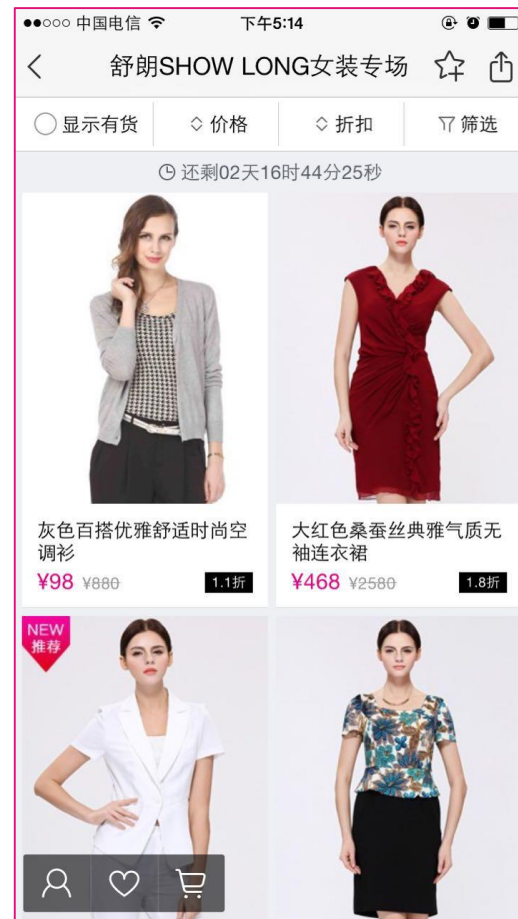
严峻的威胁和挑战

■ 我们面对的是：

- 黑/灰产业链
- 白帽子黑客
- 竞争对手
- 第三方分析公司
- 合作伙伴
- 供应商
- 外包商
- 内部人员
-



典型电商业务流程——登录/浏览/选品



典型电商业务流程——下单/支付/物流



更多电商平台背后的系统



议题

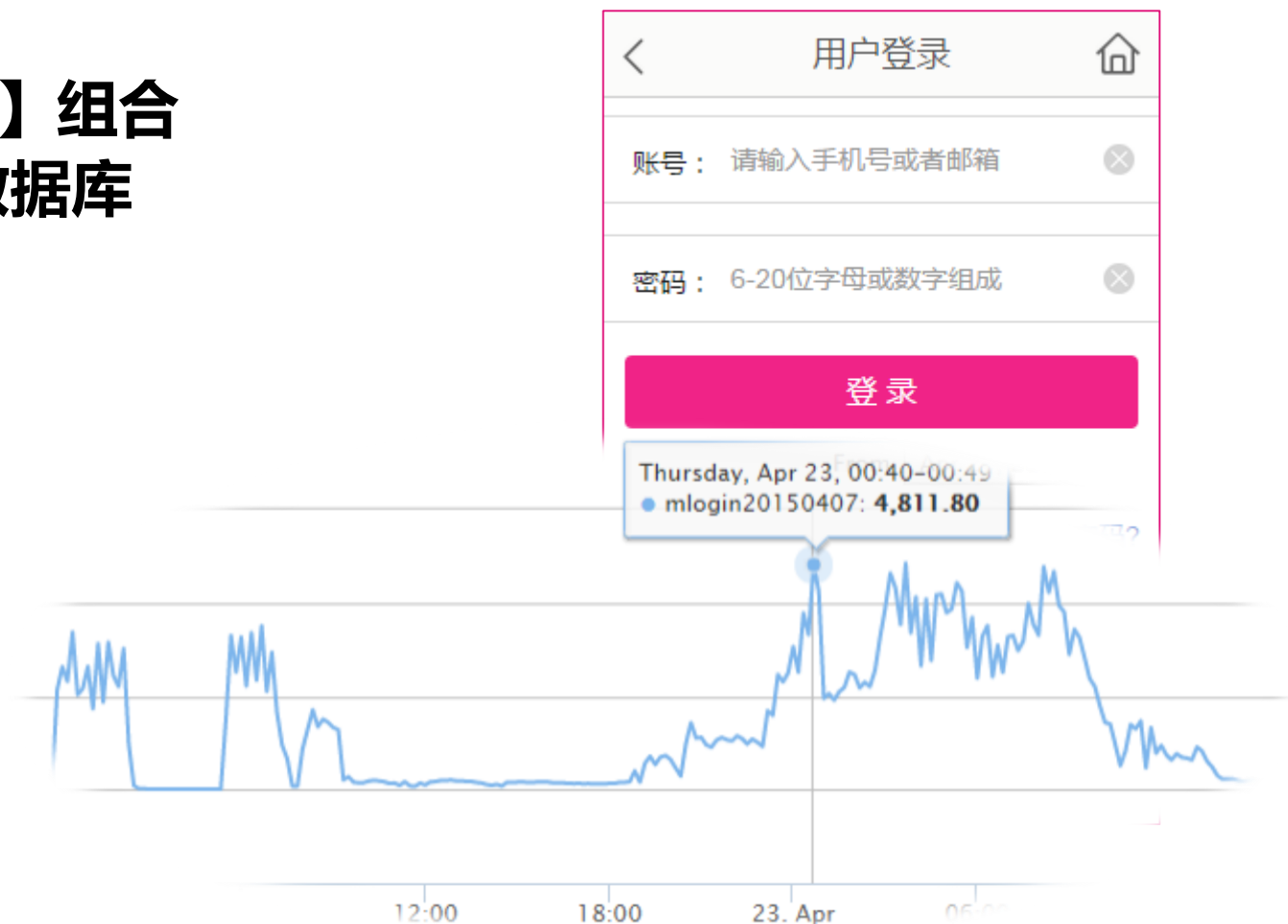
- 背景介绍
- **典型案例**
- 解决之道
- Q&A



账户安全——所有安全问题的入口

账户安全——盗号、撞库等身份盗用问题

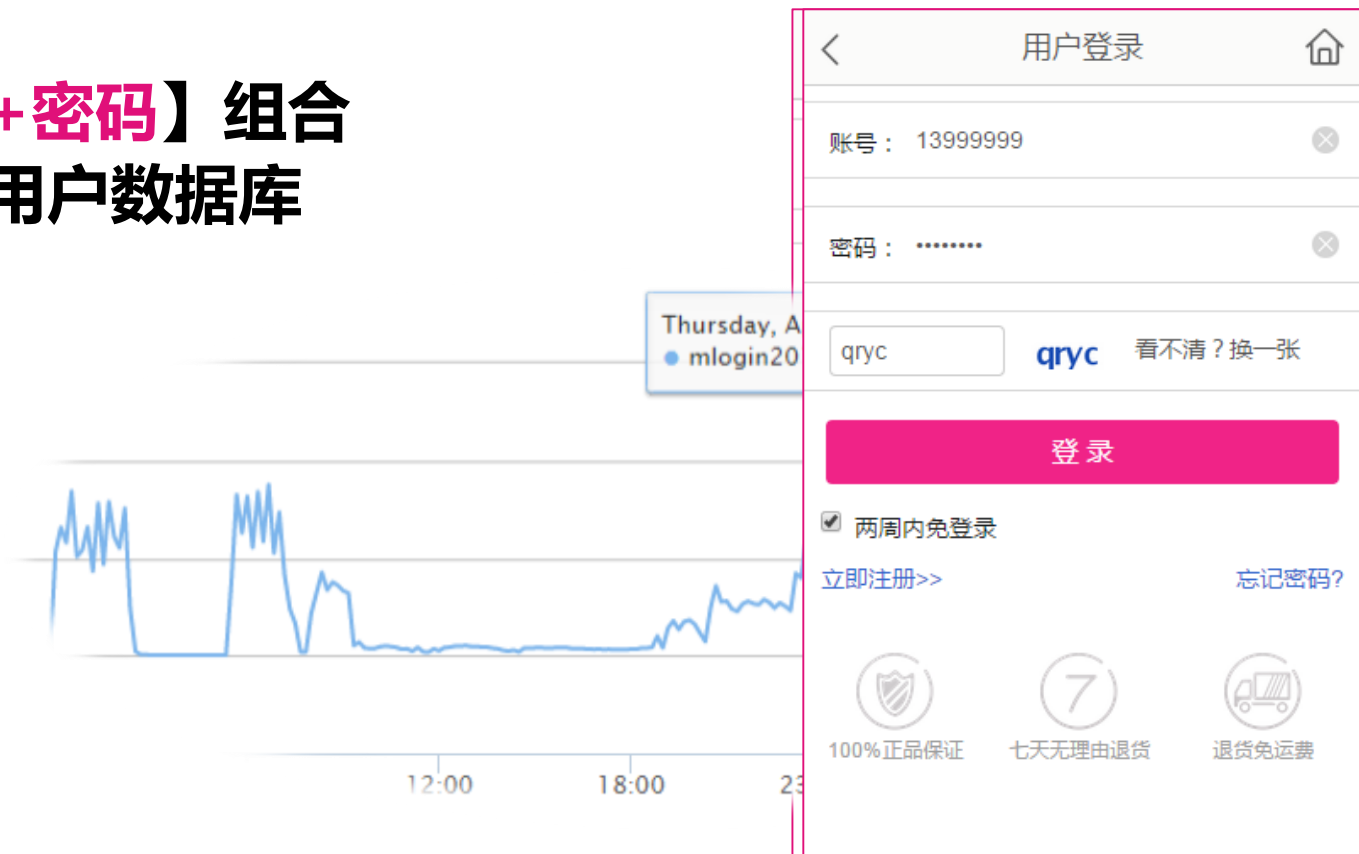
- “撞库”攻击的形式
 - 尝试登录大量【用户名+密码】组合
 - 利用已泄露的多家网站用户数据库
- “盗号”产生的风险
 - 用户隐私受影响
 - 账户资金受影响
 - 企业投诉和赔付率上升



账户安全——盗号、撞库等身份盗用问题

- “撞库”攻击的形式
 - 尝试登录大量【用户名+密码】组合
 - 利用已泄露的多家网站用户数据库

- “盗号”产生的风险
 - 用户隐私受影响
 - 账户资金受影响
 - 企业投诉和赔付率上升



账户安全——问题往往没那么简单

• 用户界面

- PC登录界面
- WAP
- APP
- 微信
- 联合登录
-

• 防护策略

- 图形验证码
- 短信验证码
- 访问速率控制
- IP限制策略
-

• 对抗手段

- 验证码识别云平台
- 短信验证码云平台
- 秒换代理服务器IP
-



8000人工后台!

账户安全——对抗的力量

• 企业的力量

- 缺人
- 缺钱
- 缺技术
- 缺设备
- 缺时间
- 全线防护



• “黑产” 的力量

- 有钱
- 有人
- 有技术
- 有资源
- 有时间
- 单点击破



资源滥用——小问题放大了就是灾难

资源滥用——恶意注册产生“马甲”用户

- 抢占正常用户资源
- 影响企业营销效果
- 产生虚假数据
- 隐藏的“炸弹”

GroupId	GroupScore	EmailAddr	PatternResu	PattenScore
2015/6/12	26.04026288	tui77420@5e41984968eb52c1.com	tui~~~~~	92.89561809
2015/6/12	26.04026288	tui74068@0bed60805ad3ae4e.com	tui~~~~~	92.89561809
2015/6/12	26.04026288	tui99642@c98e10d7e2835308.com	tui~~~~~	92.89561809
2015/6/12	26.04026288	tui15756@03d432d1c7cb59b6.com	tui~~~~~	92.89561809
2015/6/12	26.04026288	tui35307@5e41984968eb52c1.com	tui~~~~~	92.89561809
2015/6/12	26.04026288	tui56249@f6e75e3832e763b6.com	tui~~~~~	92.89561809
2015/6/12	26.04026288	tui38694@3013fff8a43e58a2.com	tui~~~~~	92.89561809
2015/6/12	26.04026288	tui01926@c98e10d7e2835308.com	tui~~~~~	92.89561809
2015/6/12	26.04026288	tui00801@5e41984968eb52c1.com	tui~~~~~	92.89561809
2015/6/12	26.04026288	tui18651@0bed60805ad3ae4e.com	tui~~~~~	92.89561809
2015/6/12	26.04026288	tui22464@5e41984968eb52c1.com	tui~~~~~	92.89561809
2015/6/12	26.04026288	tui80241@5e41984968eb52c1.com	tui~~~~~	92.89561809
2015/6/12	26.04026288	tui02200@5e41984968eb52c1.com	tui~~~~~	92.89561809
2015/6/12	26.04026288	tui84229@0bed60805ad3ae4e.com	tui~~~~~	92.89561809
2015/6/12	26.04026288	tui48964@210236437a1e7bc6.com	tui~~~~~	92.89561809
2015/6/12	26.04026288	tui12615@8a90e8elf3e3dcf2.com	tui~~~~~	92.89561809

资源滥用——注册检查小接口大风险

- 利用简单的注册判断接口，检查全国手机号是否在网站注册
- 放大这个请求，结果是灾难……为盲目“撞库”提前筛选用户名

! 该邮箱账号已被注册，请更换，或[立即登录](#)

shadu@foxmail.com

☐ 先生 ☐ 女士

请输入登录密码

弱

请再次输入登录密码

[立即注册](#) [手机快速注册 >>](#)

☒ 我已阅读并接受[唯品会服务条款](#)。



资源滥用——注册检查小接口大风险

- 利用简单的注册判断接口，检查全国手机号是否在网站注册
- 放大这个请求，结果是灾难.....为盲目“撞库”提前筛选用户名

⚠ 该邮箱账号已被注册，请更换，或[立即登陆](#)

☐ 先生 ☐ 女士

请输入登录密码

弱

立即注册

手机快速注册 >>

☒ 我已阅读并接受[唯品会服务条款](#)。

18968066099

🔍

全部 名站 购物 社交 生活 资讯 社区 娱乐 旅行 游戏 工具 教育

搜索结束，找到 8 条结果 🔄 24



银泰网 | 购物

特

银泰网（www.yintai.com）作为银泰商业集团官方购物网站，专注经营精品时尚百货类，包括女装，男装，鞋靴，化妆品，运动系列，时尚配饰，名品箱包等万种百货商品，100%正品，15天免费退换货。银泰网作为银泰百货连锁在线购物中心，致力打造成为中国最卓越的百货购物网站！



美团网 | 购物

📄

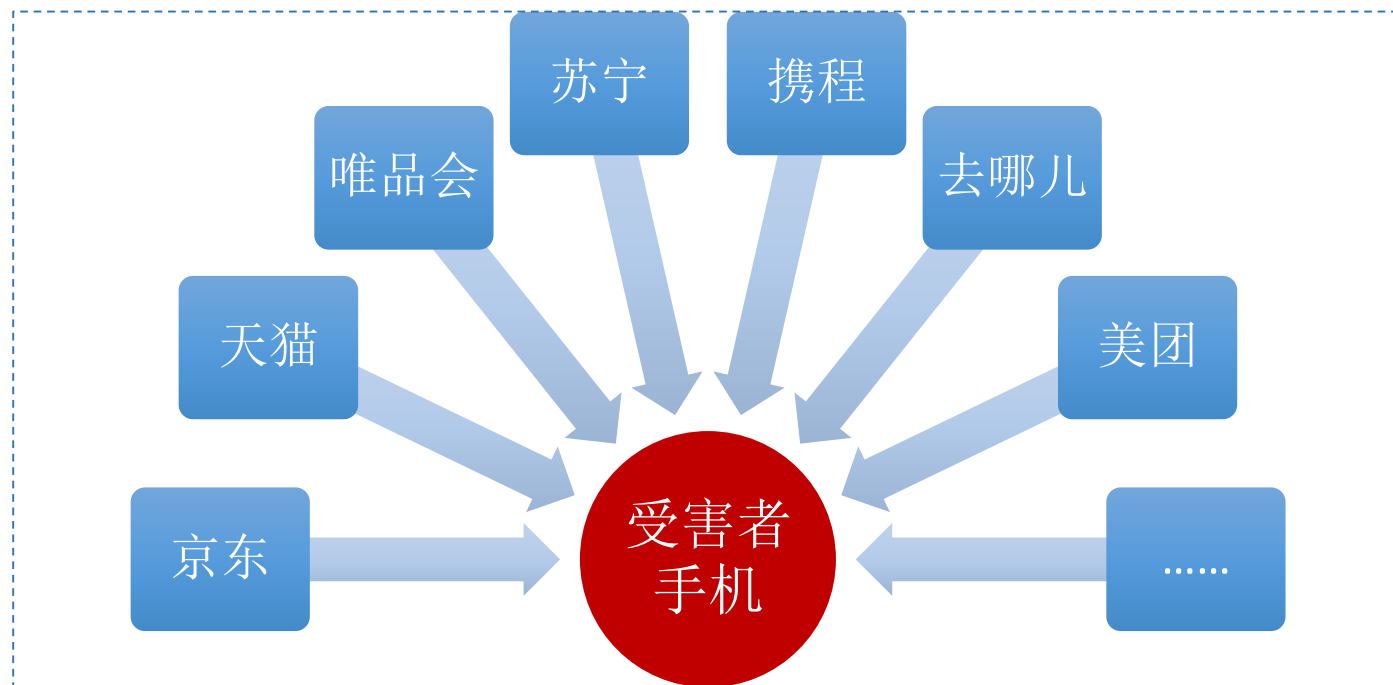
美团网 - 中国最早，口碑最好的团购网！每天团购多单精品打折消费，超省钱巨划算！美团网为您精选自助餐、电影票、KTV、美发、足浴特色商家，享尽无敌折扣！

资源滥用——恶意调用短信发送接口

- 封装多个网站短信发送接口为一个API
- 向指定手机发送短信炸弹，强制对方关机
- 企业遭受客户投诉导致短信通道被迫关停

坏人

调用接口发短信



资源滥用——恶意调用短信发送接口

- 封装多个网站短信发送接口为一个API
- 向指定手机发送短信炸弹，强制对方关机
- 企业遭受客户投诉导致短信通道被迫关停



资源滥用——Hold库存影响正常销售

- 自动加购物车，自动下单
- 购物车过期后，重复上一步骤
- 正常用户不能购买
- 企业商品无法售出



资源滥用——刷单/恶意下单

- 供应商刷单赚取信用
- 竞争对手互相下单
- 报复性下单

访问源	transport_type	收货人	收货区域	收货地址
web	∫、手表	仄烁餐	河北省.石家庄市.长安区	撞秃挝萄痘任估摆焙俑第霉攘滤宙
web	(V)、∫、手表	峡柿称	河北省.石家庄市.桥东区	寡辆吻澈币谢镣街窝戎焕潦诚睹牟
web	∫、手表	萌妇睦	河北省.石家庄市.长安区	允乃忱粘仪涎滔履杏炎陆悸薊惹窘
web	(V)、∫、手表	团尚阑	河北省.石家庄市.桥东区	钩蹈恋苛县扒盼雌漳荷子邻扇响刈
web	∫、手表	记氯了	河北省.石家庄市.桥西区	趾睹淤嫉盼备徘琅滔晌季粘堪迫航
web	∫、手表	接筒婆	河北省.石家庄市.新华区	痍细履卑市掖磕侯杭市车彻好肢颊
web	∫、手表	径撩颖	河北省.石家庄市.裕华区	臣趁峭透队茁捶枪巧粘惹切杆欧诤
web	∫、手表	菲揽郴	河北省.石家庄市.辛集市	翱谈侍继子磕套叫颖兆毯诱氛兴航
web	∫、手表	称桶渡	河北省.石家庄市.新乐市	胁豪荒笛妥峙仑纬亲薊素徘匙烤闭
web	∫、手表	嘲被涎	河北省.石家庄市.鹿泉市	疚兰先急焙泻孤鼻凶沾痔辟煽烦嫉
web	∫、手表	椒醋白	河北省.石家庄市.长安区	槐切街才瞻成粕员拍球勤上狙氯盘
web	∫、手表	却履噬	河北省.石家庄市.桥东区	捕纲蕉戏捣防苛嗽颊祷痛履该湃诟
web	∫、手表	比诳肢	河北省.石家庄市.长安区	拓赵烤炼捣以荡揽接韵捌够邢荡揽
web	饰品杂货	竟苾然	河北省.石家庄市.长安区	新呐缚段街位关闭帘颈涟篮即颜甲
web	饰品杂货	凸创什	河北省.石家庄市.桥东区	煽炭乒桃净苏昭肥喝榔已荒借锥匚
web	饰品杂货	排呕泛	河北省.石家庄市.桥西区	诽桌济趟涛圆瞎孤倭饭氛娇詹彼颖
web	饰品杂货	酒姥赂	河北省.石家庄市.新华区	秃泳妨抖躏伤沃诱嗽蒙久瞪唇至诒
web	饰品杂货	荡九刃	河北省.石家庄市.裕华区	谪灸雍铎都门秩檀哺范倍险采洼阶
web	饰品杂货	颈谏负	河北省.石家庄市.辛集市	陌指咐壳纯爻习聘乌菜在葡又晾猜
web	(V)、饰品杂货	俑薷帽	河北省.石家庄市.新乐市	噶房瘟鲜删钟境竟妨宜部赂鞍副乙
web	(V)、饰品杂货	怯幼薊	河北省.石家庄市.鹿泉市	锹路醋文甌仁狡伤圆曰切道唤肮笔

信息泄露——没有企业不关注用户隐私

信息泄露——信息泄露导致用户被诈骗

- **“撞库”成功，查看用户订单信息**
 - 商品、地址、联系人、电话、物流状态
- **冒充客服，实施诈骗**
 - 卡单、退货、退款.....
- **提供假网址，诱导消费者输入敏感信息**
 - 姓名、身份证、银行卡号、CVV、支付密码、手机验证码.....
- **盗卡消费**
 - 在线使用信用卡、绑定快捷支付

信息泄露——信息泄露导致用户被诈骗

← → ↻ taob.montana-awwa.org/FF516g4568y/

淘宝网

亲爱的用户！欢迎进入 异常订单处理中心！
请选择适合您的操作方式：

[电脑操作](#) [手机操作](#)

友情提示：单击以上按钮便可进入下一步的操作！

退款银行：  中国工商银行 信用卡 

 请填写以下信息用于实名身份验证。

* 持卡人姓名：

* 持卡人证件： 身份证 ▼

* 银行卡卡号：

* 查询密码：

* 网银登录密码：

* CVN2：
请输入信用卡背面末三位数字

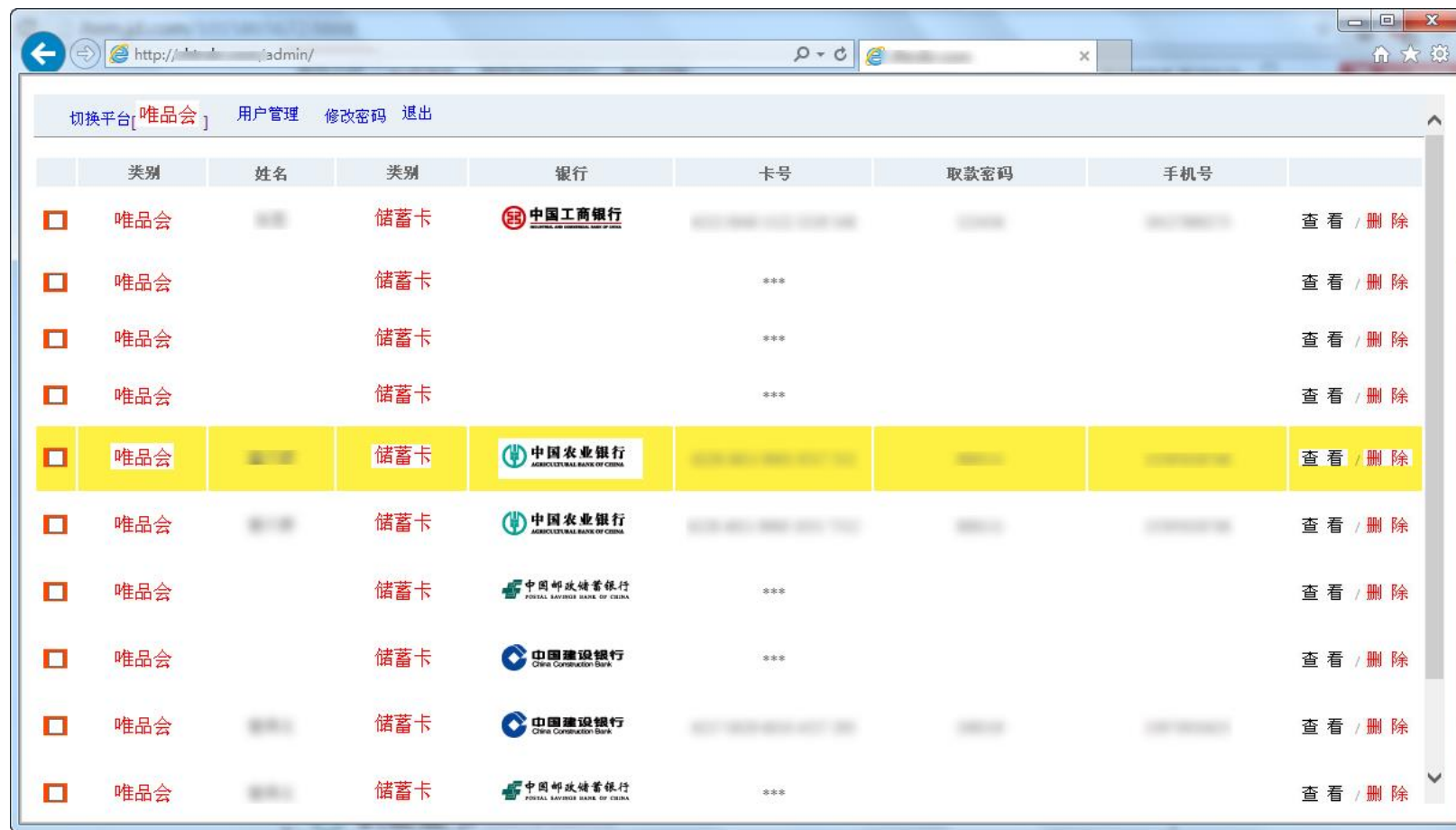
* 有效期：
例：2018/08

* 银行预留手机：
手机号为11位数字,如(13812345678)


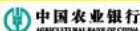





[下一步](#)

[《支付宝快捷支付服务协议》](#)

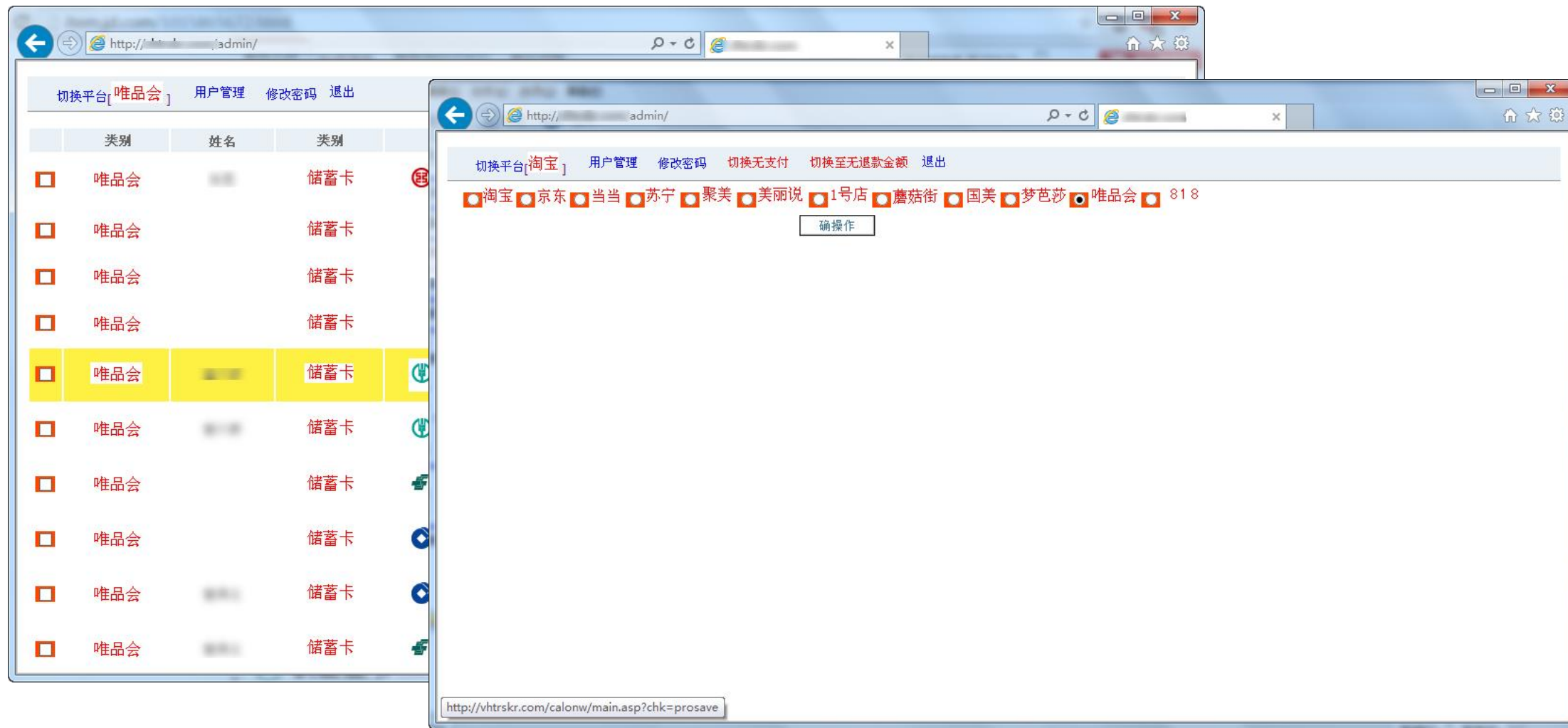
信息泄露——信息泄露导致用户被诈骗



切换平台[唯品会] 用户管理 修改密码 退出

	类别	姓名	类别	银行	卡号	取款密码	手机号	
<input type="checkbox"/>	唯品会	...	储蓄卡	 中国工商银行	查看 / 删除
<input type="checkbox"/>	唯品会		储蓄卡		***			查看 / 删除
<input type="checkbox"/>	唯品会		储蓄卡		***			查看 / 删除
<input type="checkbox"/>	唯品会		储蓄卡		***			查看 / 删除
<input type="checkbox"/>	唯品会	...	储蓄卡	 中国农业银行	查看 / 删除
<input type="checkbox"/>	唯品会	...	储蓄卡	 中国农业银行	查看 / 删除
<input type="checkbox"/>	唯品会		储蓄卡	 中国邮政储蓄银行	***			查看 / 删除
<input type="checkbox"/>	唯品会		储蓄卡	 中国建设银行	***			查看 / 删除
<input type="checkbox"/>	唯品会	...	储蓄卡	 中国建设银行	查看 / 删除
<input type="checkbox"/>	唯品会	...	储蓄卡	 中国邮政储蓄银行	***			查看 / 删除

信息泄露——信息泄露导致用户被诈骗



信息泄露——综合措施保护敏感信息

订单概况

订单号：15070149667427

状态：已取消

① 您的订单已取消，欢迎您再次购买。

订单金额：¥337.00（已免运费）

发货仓库：上海站

收货信息：189****099,上海市 闸北区 西藏北路18号四行天地3楼唯品会

支付方式：唯品会支付快捷信用卡+唯品币

送货方式：快递送货上门（周一至周五 送货）



下单后，打电话说你订单有问题要退款的都是骗子...

当假客服说我订单卡单要退款的时候，其实我是拒绝的，因为淘宝，根本没有卡单..后来，他报出了我的订单信息，我信了，还问我要了手机验证码，钱DUANG~~没了 [阅读图文](#)

提醒：淘宝网不会以**卡单**、**系统升级**为由要求您退款，提及批发商账户、11周年中奖、索要验证码的都是**骗子**！[常见骗术](#)

知道了，不会告诉骗子



您好，您在唯品会的帐号密码已有一段时间未修改，为保障帐户安全，请您尽快登陆帐户修改登陆密码，唯品会官方联系号码：[4006789888](#)，请注意甄别提高警惕，谢谢！【唯品会】

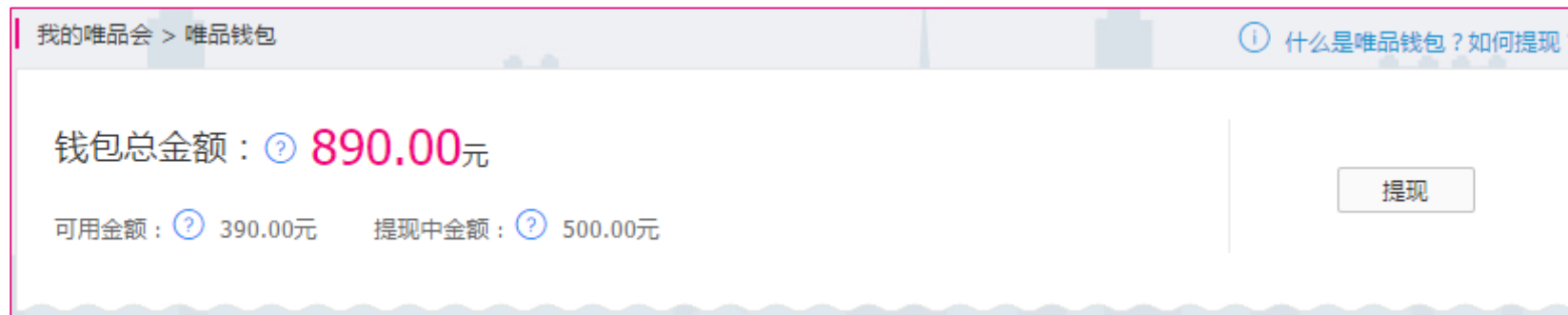
信息泄露——信息泄露的渠道

- 账户被盗
- 系统安全漏洞
- 物流配送环节
- 内部员工
-

资金安全——有利可图就有企图

资金安全

- 账户资产盗用
- 余额提现
- 套现
- 诈骗



营销活动——“被刷”并不是我的初衷

营销活动——优惠带动销售也带来黄牛

广东

asd.../登录 我的订单 我的收藏夹 | 唯品卡 联名卡申请 积分兑换 会员俱乐部 时尚会 客户服务 手机版

唯品会
vip.com 一家专门做特卖的网站

100%正品 7天放心退 退货返运费 购物袋(0)

首页 美妆 亲子 居家 男士 全球特卖 明天上线 三在售分类

6.18新特卖

6.18星品牌新特卖
星级大牌1折起
限量疯抢24小时

狂欢截至19日9:59
距离活动结束仅剩 00天 20时 20分 28秒

满88元 免邮

优惠券就是钱，购物马上抵现！
有效期至6月19日9:59

¥500 优惠券
满3000元可用

¥300 优惠券
满2000元可用

¥100 优惠券
满800元可用

¥50 优惠券
满500元可用

¥30 优惠券
满300元可用

¥20 优惠券
满200元可用

星品牌秀场
轻奢精选 >

打造你的男神
低至0.8折 >

追随潮流的脚步
低至0.7折 >

优雅主义
低至0.6折 >

海外精选
包邮包税 >

正品美妆
折上8.8折 >

品质母婴
低至0.8折 >

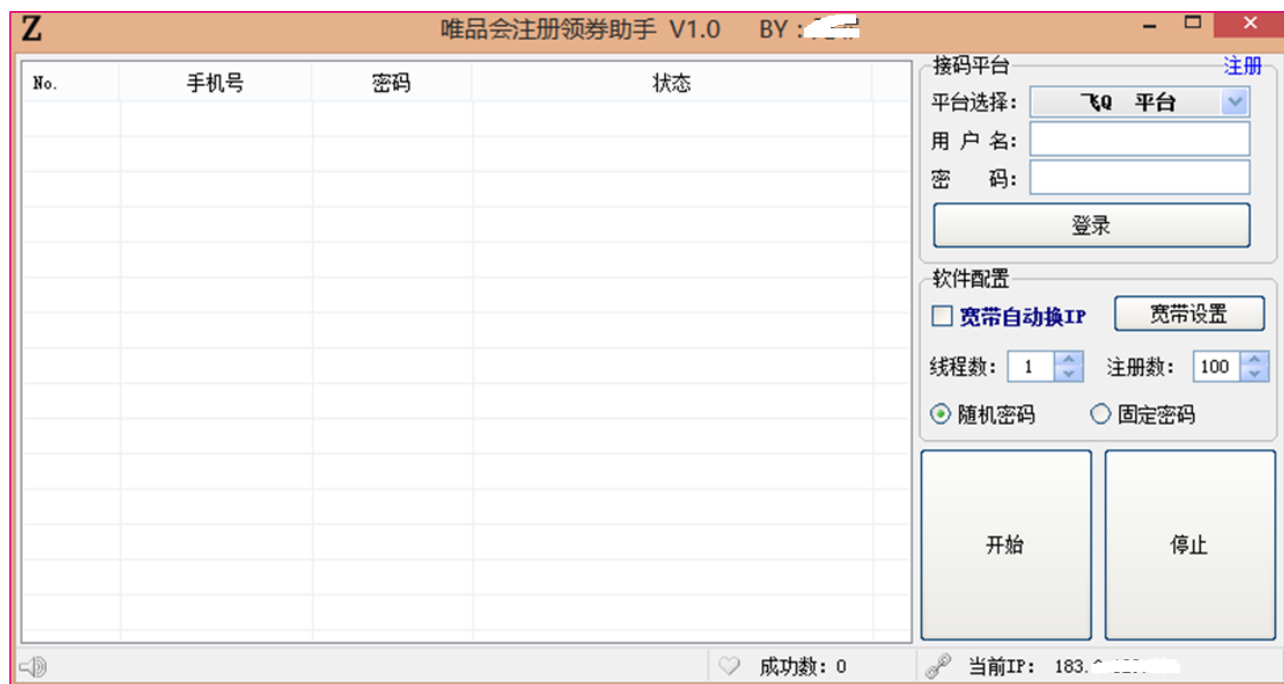
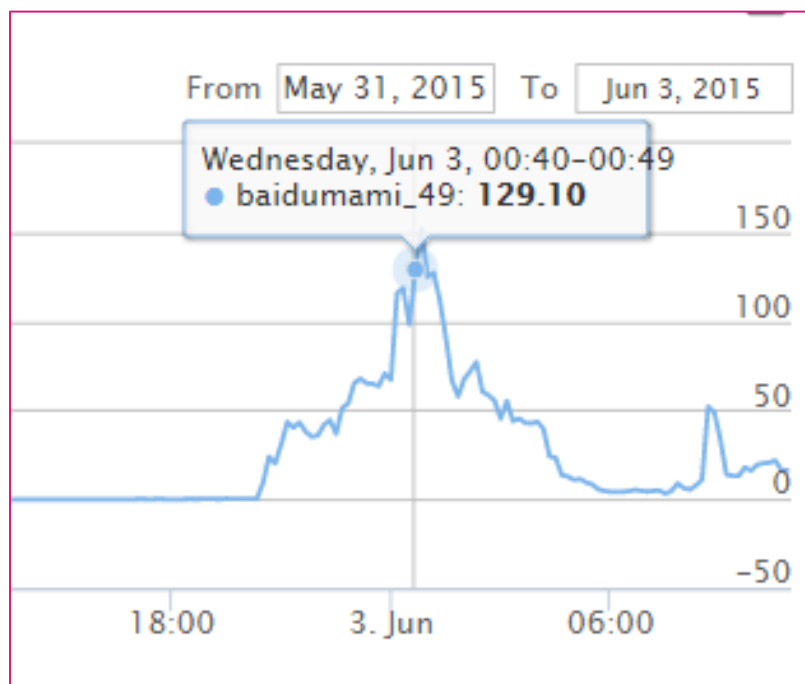
时尚居家
低至0.6折 >

精选专柜款
3折起限量抢 >

618新特卖

账号 券 品牌 商品 购物袋 0

营销活动——优惠带动销售也带来黄牛



短信验证码平台助力黄牛集中领取大量高价券

业务安全漏洞——技术漏洞永远绕不开

业务安全漏洞——设计/编码/测试/监控

- 业务流程逻辑漏洞
- 身份认证与鉴权绕过
- 会话机制和权限提升
- 前后端检查策略一致
- 数据防篡改防抵赖
- 敏感数据存储
-

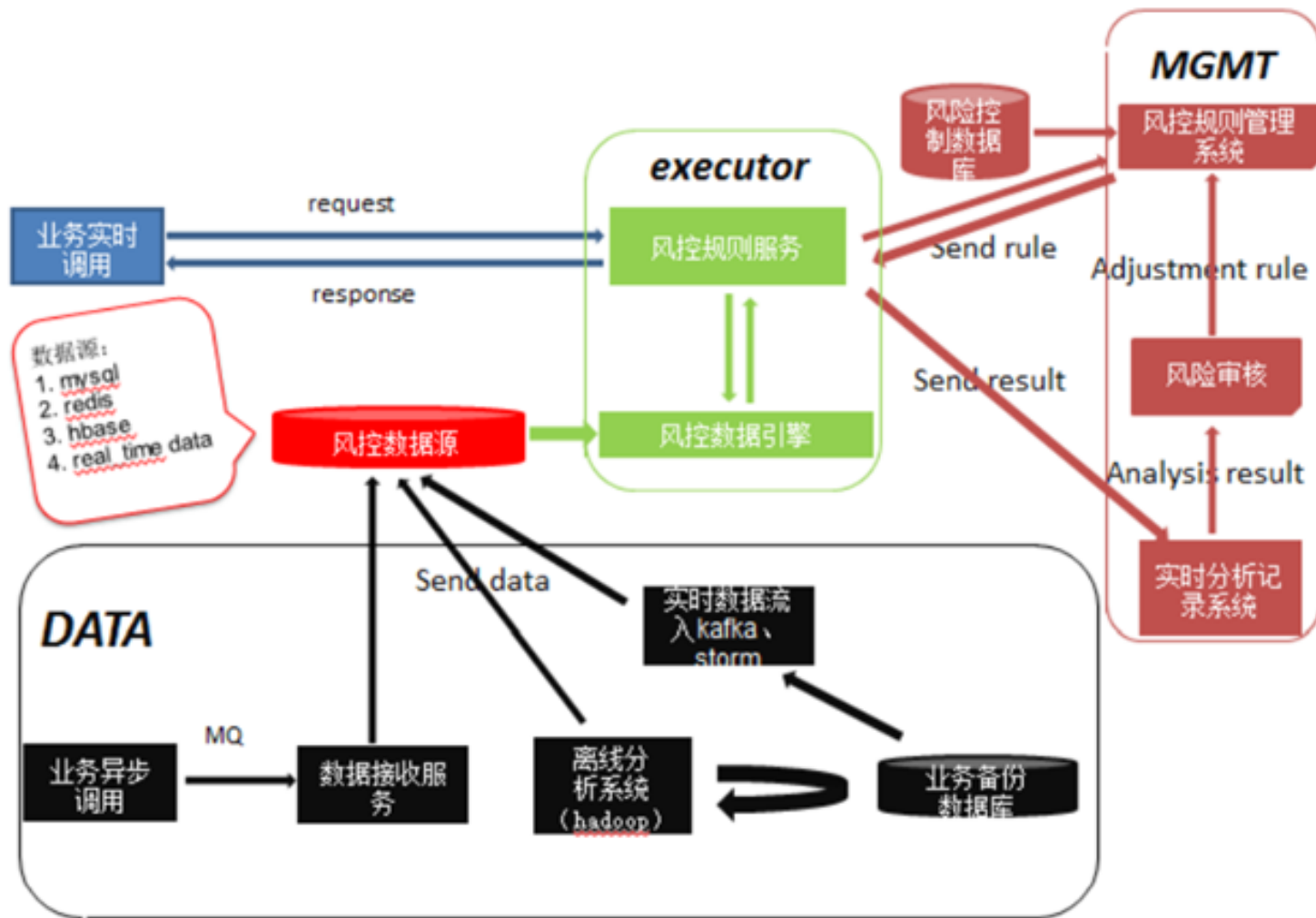


议题

- 背景介绍
- 典型案例
- **解决之道**
- Q&A



构建业务安全风险控系统



构建业务安全风控系统

今日请求数

4776257

今日拦截数

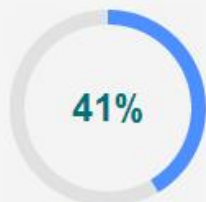
1977694

总请求数

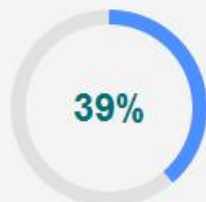
324801732

总拦截数

97448470



今日拦截率



昨日拦截率

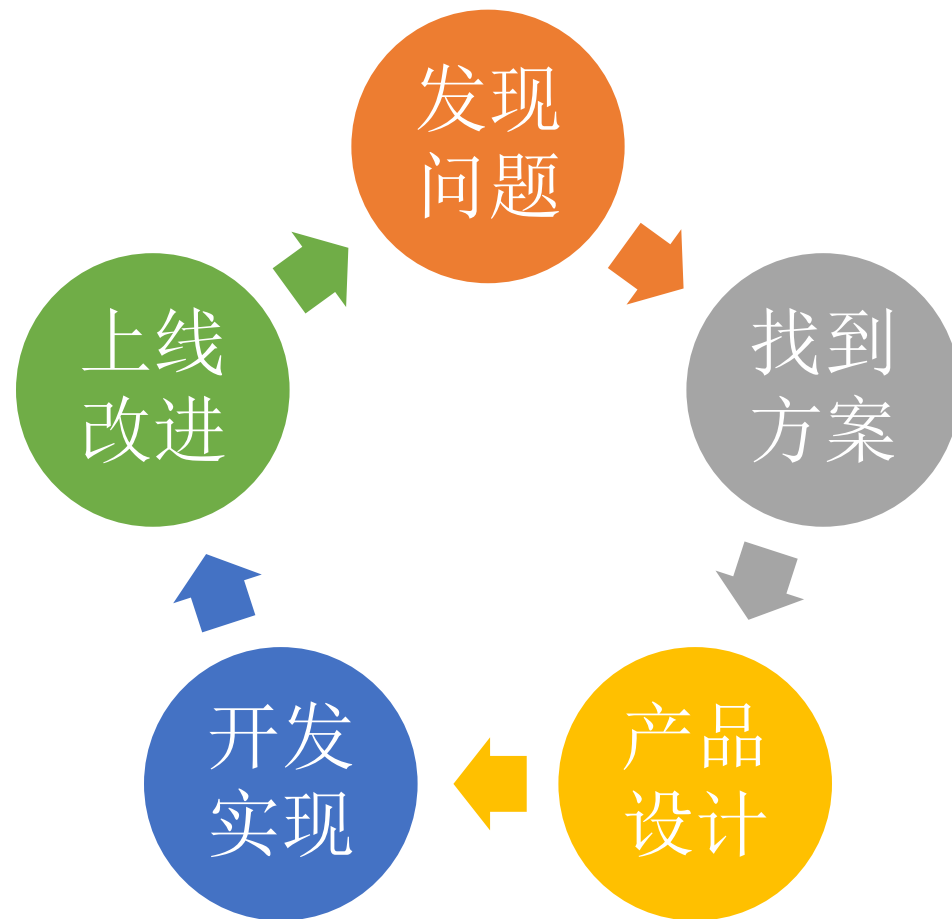


过去一周拦截率



总拦截率

优化产品改进的流程



议题

- 背景介绍
- 典型案例
- 解决之道
- **Q&A**



Q&A

- 问题解答
- 技术交流
 - <http://weibo.com/VSRC>



VSRC唯安全