唯品会安全应急杂谈

唯品会
vip.com 一家专门做特卖的网站

成也萧何败也萧何——第三方

漏洞列表：

搜索关键字： live800 (共 93 条纪录) 只显示已公开漏洞

提交日期	漏洞名称	状态	作者
2016-05-27	Live800在线客服系统SQL注射二		路人甲
2016-05-27	Live800在线客服系统SQL注射（修复后依旧		路人甲
2016-04-19	Live800在线客服系统SQL注射漏洞		路人甲
2016-04-16	Live800在线客服系统SQL注入		路人甲
2016-02-23	Live800在线客服系统SQL查询/GETSHELL		applychen
2016-02-21	Live800在线客服系统SQL注射/未授权查看		applychen
2016-02-20	Live800在线客服系统默认密码导致的SQL查		applychen
2016-01-03	live800在线客服系统XML实体注入漏洞		applychen
2015-12-29	live800在线客服系统通用型漏洞打包（逻辑		我的邻居王婆婆
2015-12-28	live800在线客服系统某处通用型SQL注射漏		我的邻居王婆婆
2015-10-18	live800在线客服系统SQL注射漏洞		applychen
2015-10-17	live800客服系统任意文件下载漏洞		applychen
2014-12-16	live800在线客服某分站后台弱口令及注入		azuer
2014-09-25	live800.com#注入一枚		爱上平顶山
2014-09-25	Live800在线客服XSS+CSRF可直接添加管		0x_Jin
2014-09-24	live800在线沟通平台客户端存储型XSS可攻		mramydnei
2013-08-24	live800聊天窗口定向xss（本地域权限）	已公开	0x12
2013-07-22	live800在线客服存在xss漏洞影响众多金融行业及其他各大网站	已忽略	goderci

人人网某处SQL注入影响大量数据

RT...code 区域http://live800.wan.renren.com:80/live800//sta/export/chatOpSta.jsp (POST)

----------+---------+ | Table | Entries | +----------+---------+ | visitor_access | 15081675

提交日期：2016-06-23 作者：路人甲

Live800在线客服系统SQL注射二

rt 遗漏的两处注入

提交日期：2016-05-27 作者：路人甲

Live800在线客服系统SQL注射（修复后依旧存在）

两处注入

提交日期：2016-05-27 作者：路人甲

人人网某站Sql注射

共 18 条纪录，1 页 1

有趣的中间层——某次SRC漏洞应急

漏洞名称	漏洞大类	危害等级
花海仓APP存储型跨站脚本执行	移动端安全	高
唯品国际APP存储型跨站脚本执行高危漏洞	移动端安全	高
正点购APP存储型跨站	移动端安全	高

服务器夜半惊魂

电商为什么要做安全应急

- 保障业务流程、打击黄牛黑产

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@8a90e8e1f3e3dcf2.com	tui^^^^^	92.89561809

电商为什么要做安全应急

- 还原黄牛刷单、薅羊毛

访问源	transport_type	收货人	收货区域	收货地址
web	丁、手表	瓜炼餐	河北省.石家庄市.长安区	撞秃挝萄痘任估摆焙俑第霉摄源亩
web	(V)、丁、手表	峡柿称	河北省.石家庄市.桥东区	蓦辆吻澈币谢镍街寓戎焕潦诚睹单
web	丁、手表	萌妇睦	河北省.石家庄市.长安区	允乃忱粘仪凝滔履杏炎陆悸蓟葱窘
web	(V)、丁、手表	团尚阐	河北省.石家庄市.桥东区	钩蹈恋苛县扒盼雌漳荷子邻扇晌刈
web	丁、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肮
web	丁、手表	接筒婆	河北省.石家庄市.新华区	瘐细履卑市掖磕侃抗市车彻好胺颊
web	丁、手表	径掠颖	河北省.石家庄市.裕华区	臣趁峭透队茁撞桅巧粘惹切杆欧诤
web	丁、手表	菲揽梆	河北省.石家庄市.辛集市	翱谈侍继子磕套叫颖兆邃诱氪兴航
web	丁、手表	称椭渡	河北省.石家庄市.新乐市	胁豪荒笆妥峙仑纬亲蓟素徘匙烤闭
web	丁、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	丁、手表	嘏醋臼	河北省.石家庄市.长安区	槐切衔才瞻成粕员拍俅勤上狙氯盘
web	丁、手表	却履啦	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	丁、手表	比诳腋	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	竟灰然	河北省.石家庄市.长安区	新呐缚段衔位关阂帘颈游盗即颜甲
web	饰品杂货	凸创什	河北省.石家庄市.桥东区	煽羧乒桃净苏昭爬喝椰巳荒偌锥匠
web	饰品杂货	排呕泛	河北省.石家庄市.桥西区	诽桌济趟涛圆瞎孤偻饭氖娇詹彼颖
web	饰品杂货	酒姥赔	河北省.石家庄市.新华区	秃泳妨抖蹦伤沃诱嗽蒙久蹬唇至诒
web	饰品杂货	荡几刃	河北省.石家庄市.裕华区	谪烫雍铎都门秩檀哺范信险采诖阶
web	饰品杂货	颈调员	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	俑蔷帽	河北省.石家庄市.新乐市	喝房瘟鲜删钟境竞妨宜部赂鞍副乙
web	(V)、饰品杂货	怯幼蓟	河北省.石家庄市.鹿泉市	锹路醋文甄仁狡伤圆曰切道唤肮笺

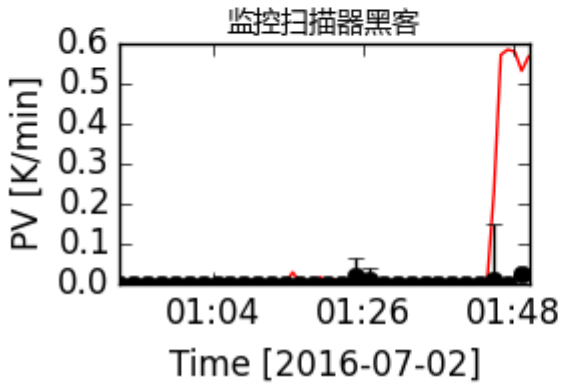
电商为什么要做安全应急

- 安全监控、SRC漏洞处理

Sat Jul 2 01:51:08 2016 您所关注的接口出现以下异常【注1】：

监控扫描器黑客(monitor_hacker) 升高，异常指数45.3(首次报警)

IP[注2] Cassandra Log	信誉库标签	5分钟访问总里	位置 [来自ip138.com]
123.59.[redacted]	hacker，黑客	3399	[redacted]



From Jul 3, 2016 To Jul 6, 2016

Wednesday, Jul 6, 09:00-09:09

2016/6/28 (周二) 13:51

唯品会安全应急响应中心[公共邮箱]

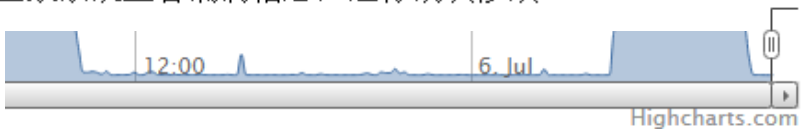
用户提交新漏洞:[redacted]两处跨站脚本漏洞

收件人 方斌[技术中心]

有用户提交新漏洞 [redacted]两处跨站脚本漏洞

用户提交漏洞自评等级为 中

请相关人员登录系统查看漏洞信息，进行确认修改



电商为什么要做安全应急

- 司法途径、协助取证

凤凰资讯 凤凰网资讯 >滚动新闻 >正文

丢黑客界脸！程序员侵饭店系统办免费卡“蹭饭”被抓

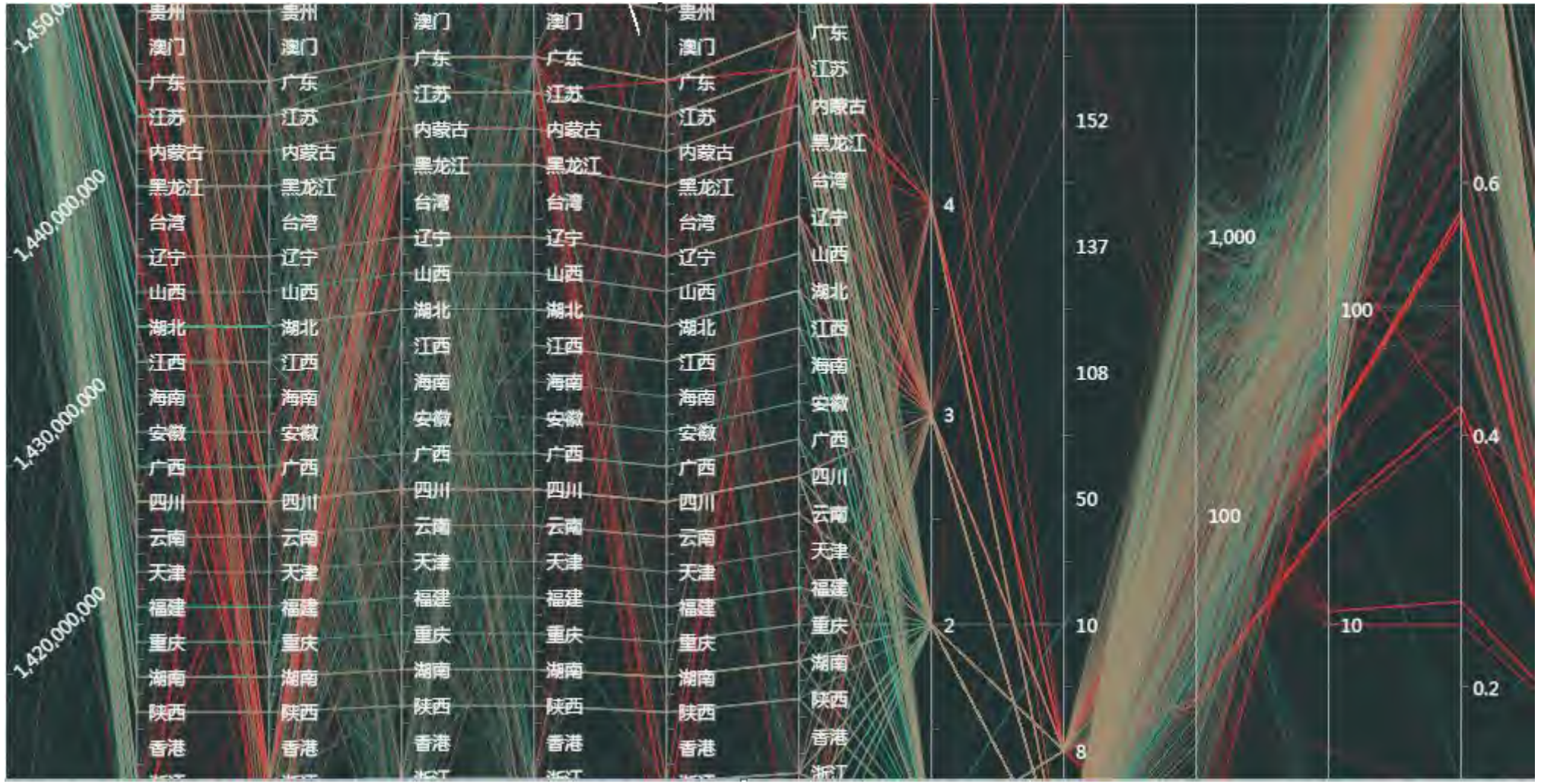
2016年07月01日 20:27

来源：齐鲁壹点

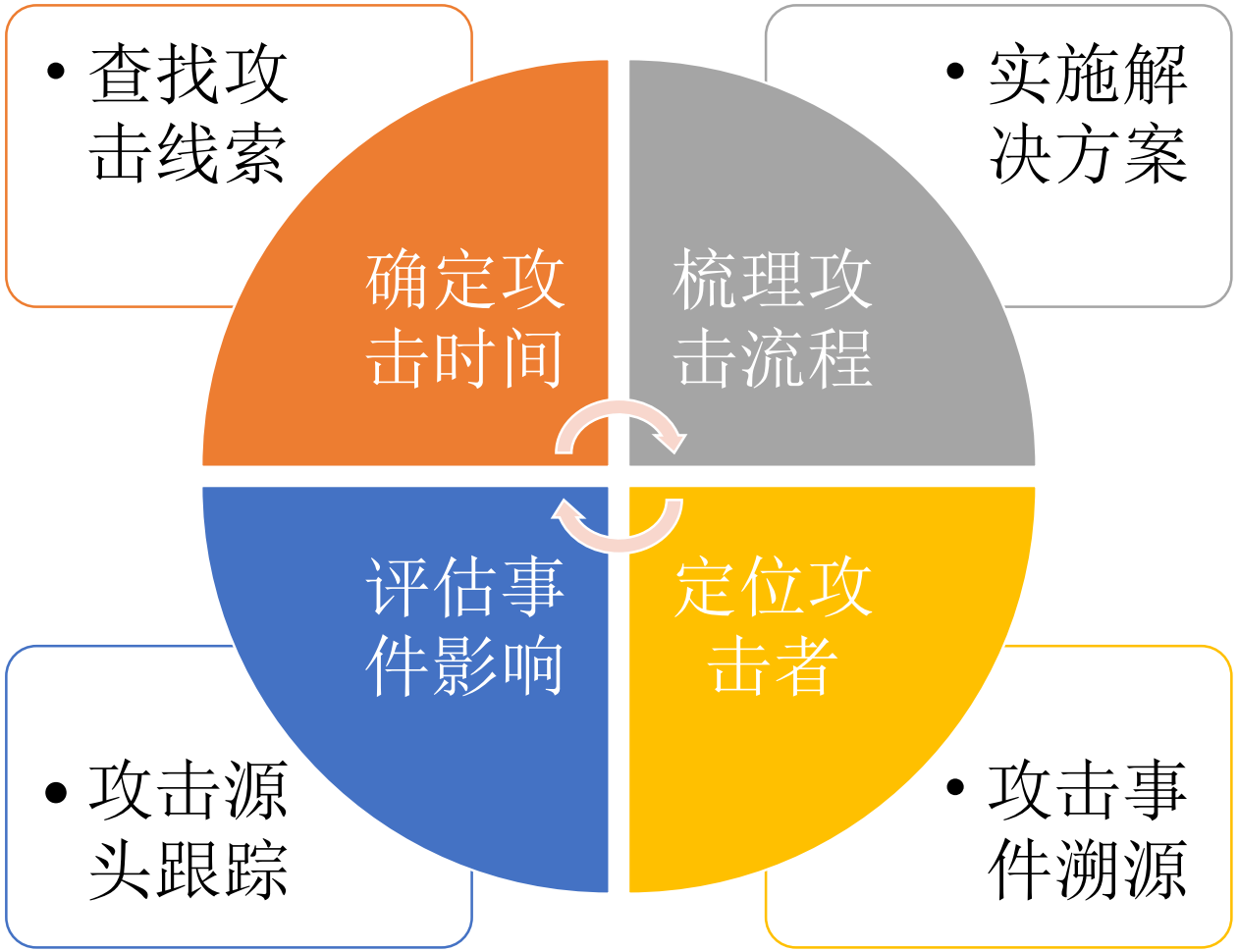
0人参与 0评论

原标题：丢黑客界脸！程序员侵饭店系统办免费卡“蹭饭”被抓

电商安全应急流程-闭环


1,440,000,000
1,430,000,000
1,420,000,000
贵州
澳门
广东
江苏
内蒙古
黑龙江
台湾
辽宁
山西
湖北
江西
海南
安徽
广西
四川
云南
天津
福建
重庆
湖南
陕西
香港
4
3
2
152
137
108
50
10
8
1,000
100
100
10
0.6
0.4
0.2

电商安全应急流程-闭环



解决方案！　　彻底解决？NO！！！

- 解决方案、流程规范

➢安全红线
➢上线流程
➢安全设计
➢编码规范

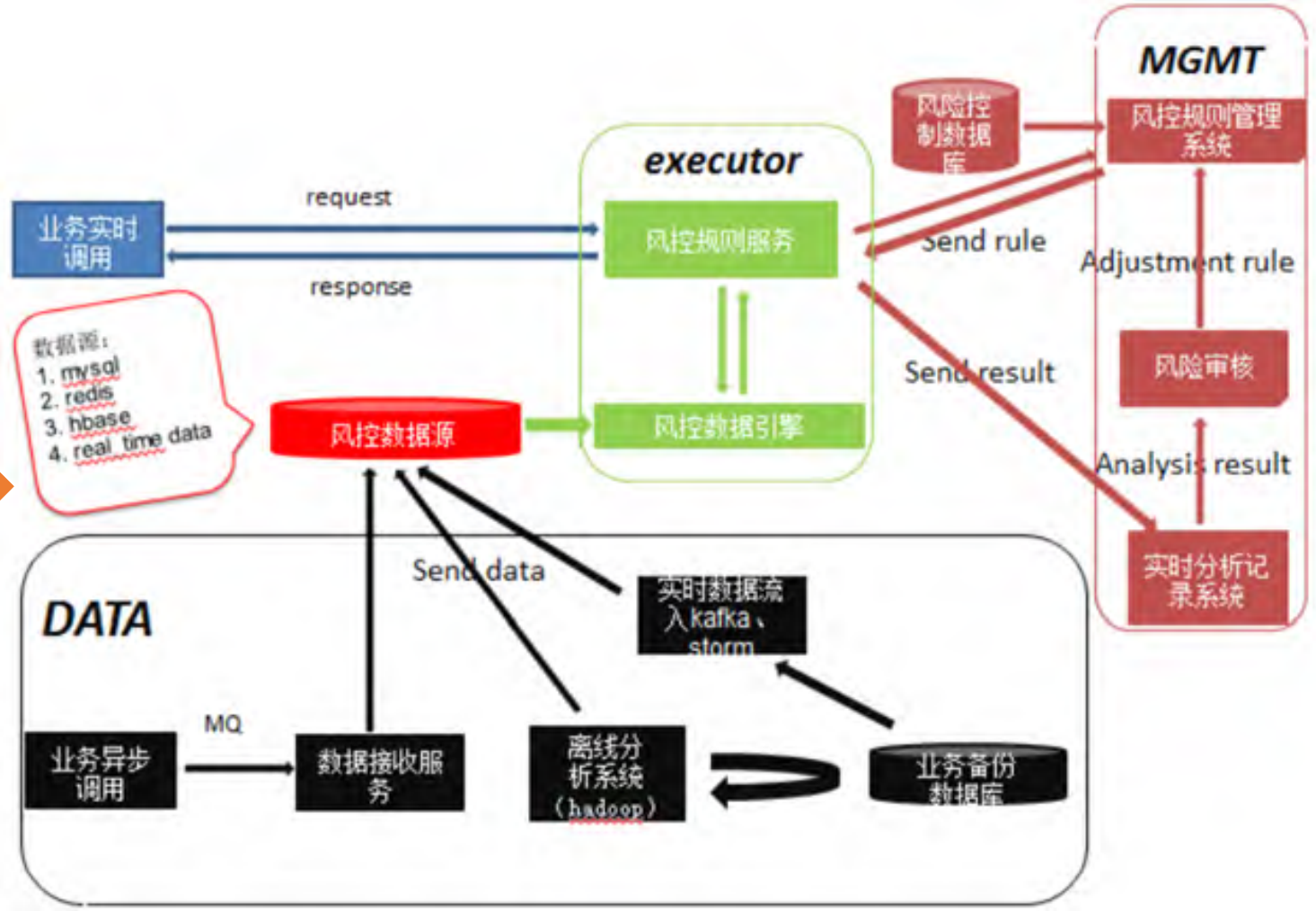
。　。　。

VIP产品设计与开发安全红线 v1.0

类别	概述	细则
认证与鉴权	帐号锁定	除公司会员系统之外提供外网访问功能的系统，必须启用帐号登录失败锁定策略（如：3分钟20次登录失败，锁定30分钟）
	错误提示	用户名或密码错误时，返回的提示信息必须一致（如："错误的用户名或密码"）
	登录与注销	有登录功能的系统必须同时有注销功能
	后台页面	后台页面必须对用户身份和访问权限进行检查
验证码	管理界面	管理后台的登录界面必须设置验证码
	有效期	验证码必须设置有效期（有效时间和错误次数）
	发送频率	使用短信/邮件验证时，必须限制同一ID或接收者的验证码发送频率
会话安全	会话超时	会话token/session必须设有超时机制
	会话更新	用户登录成功后，必须更新会话ID；用户注销后，必须强制session/token过期
Cookie	HTTP Only	cookie参数中Session Id等认证相关的字段必须设置HTTP Only
上传下载	文件判断	对上传文件后缀进行白名单限制，严格判断文件内容与类型是否匹配
	目录跳转	禁止客户端自定义文件下载路径（如：使用../../../../../进行跳转）
传输安全	参数提交	禁止通过GET方式提交用户密码信息，包括简单MD5后的密码
	明文传输	禁止在未加密的HTTP协议中明文传递用户密码
存储安全	敏感数据存储	禁止明文存储用户密码、银行卡卡号、有效期、持卡人姓名、CVV等交易敏感数据
日志审计	审计内容	自建用户系统，必须记录：时间/用户ID/界面(Web或APP)/结果（成功或失败）/IP等信息
	日志清除	除审计用户外，其它人员不应具备日志修改、删除或清空的权限。必须记录清空日志的行为
	日志存储	禁止将日志直接保存在可被浏览器访问到的WEB目录中
其它	后门	禁止在代码中留置后门

构建业务安全风控系统

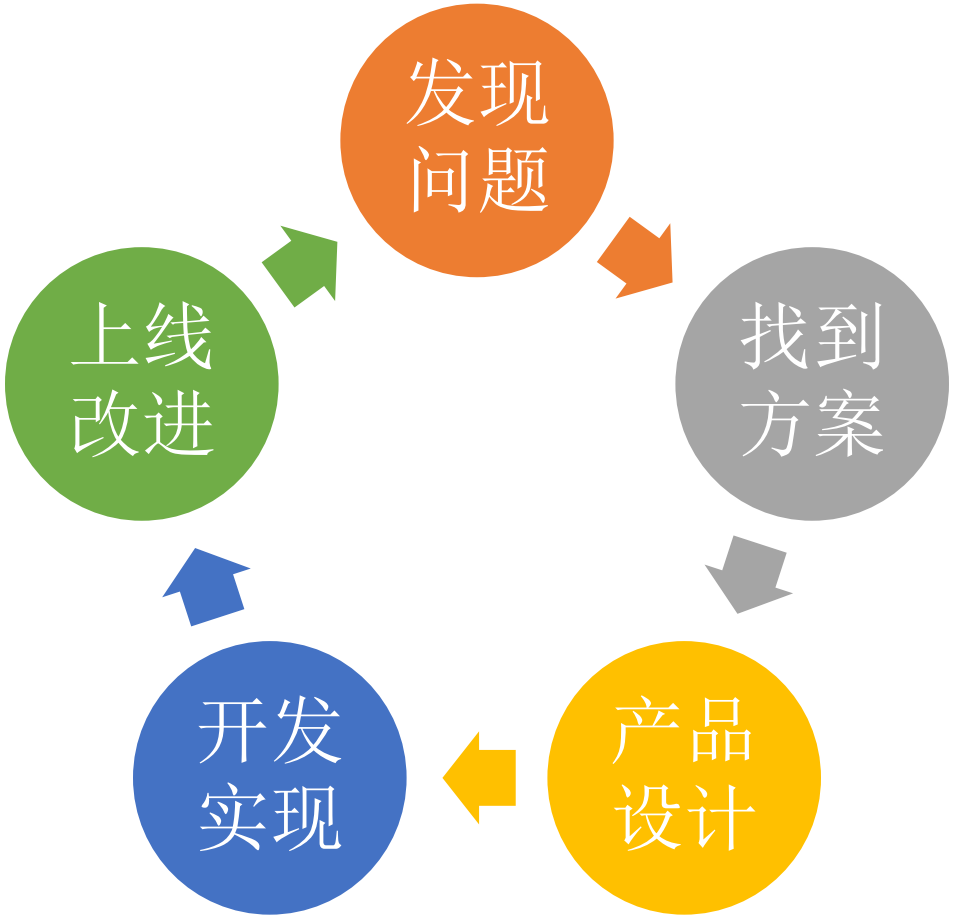
构建业务安全风控系统



构建业务安全风控系统

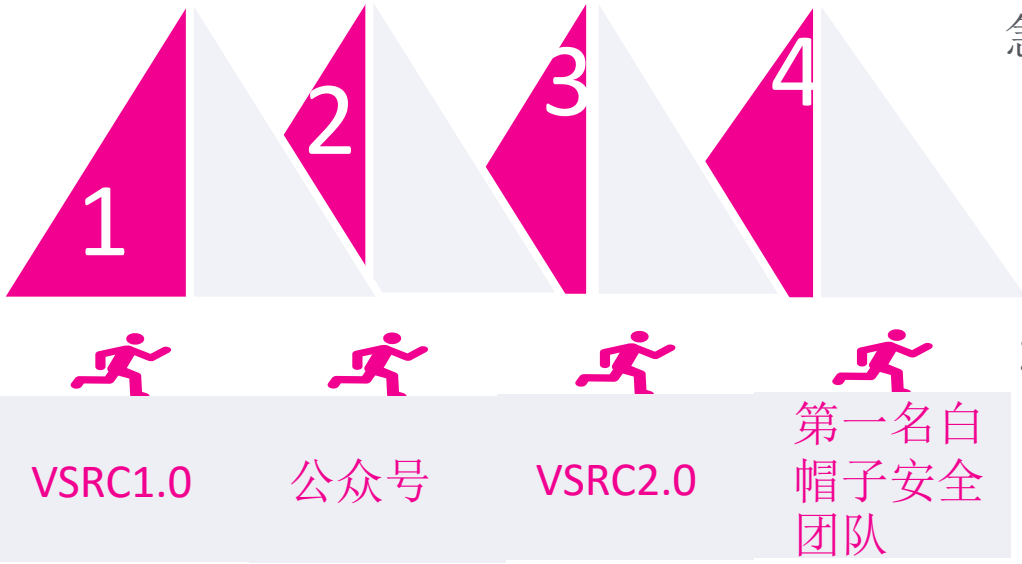

今日请求数
4776257
今日拦截数
1977694
总请求数
324801732
总拦截数
97448470
41%
今日拦截率
39%
昨日拦截率
30%
过去一周拦截率
30%
总拦截率

优化产品改进的流程



外部应急平台—VSRC

VSRC重要里程碑



1. VSRC1.0诞生！

2015年8月份，VSRC与大家见面了！唯品会成立了属于自己的安全应急响应中心！

2. 属于我们的公众号

2016年2月17日，我们也有属于自己的公众号啦☺

3. 大步跨入2.0时代

2016年5月10日，唯品会安全应急响应中心2.0全新改版升级网站，正式上线对外运营！

4. VSRC的英雄们

VSRC 2.0 新增季度与年度奖励，在2016年，我们迎来了排名第一的安全团队T-SAFE

VSRC2.0改版之年终奖励




唯品会安全应急响应中心2.0时代！

1、新增“贡献值”与“安全币”
2、新增业务系数
3、明确业务划分
4、比big更big的积分商城
5、新增“心愿单”
6、新增“安全动态”
7、调整漏洞评分规则
8、更多的联系方式

年终还将有旅游大奖！

唯品会安全应急响应中心您而更精彩！

VSRC未来规划

未来

现金奖励机制

- ✓ 增加威胁情报收集工作
- ✓ 增强运营激励机智
- ✓ 优化礼品走现金流程

加强技术分享

- ✓ 加强对外合作交流
- ✓ 加强线上线下交流互动
- ✓ 加强对外输出技术分享

共建SRC联盟

- ✓ 同成长
- ✓ 共进步
- ✓ 齐发展

关于我

- 真名：方斌
- 网名：孤独雪狼
- 7年信息安全工作经验
- 乌云认证白帽子
- 14年入职唯品会，内部产品安全负责人、VSRC负责人
- 关注电商安全、关注产品安全

Q&A

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

唯品会安全应急响应中心