

捍卫电商安全

一个半马胖子的瘦身大法



唯品会安全应急响应中心

VIP Security Response Center

解答疑惑

< Joyrun·悦跑圈

2016年10月 - 本月跑步总里程: 102.80 KM

15 KM

7.5 KM

0 KM



唯品会安全保护对象

- 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
- 物流、库存
- 订单、商业数据
-



shadu1..., 欢迎回来! 请登录

邮箱/手机号/QQ号

请输入登录名

密码

登录

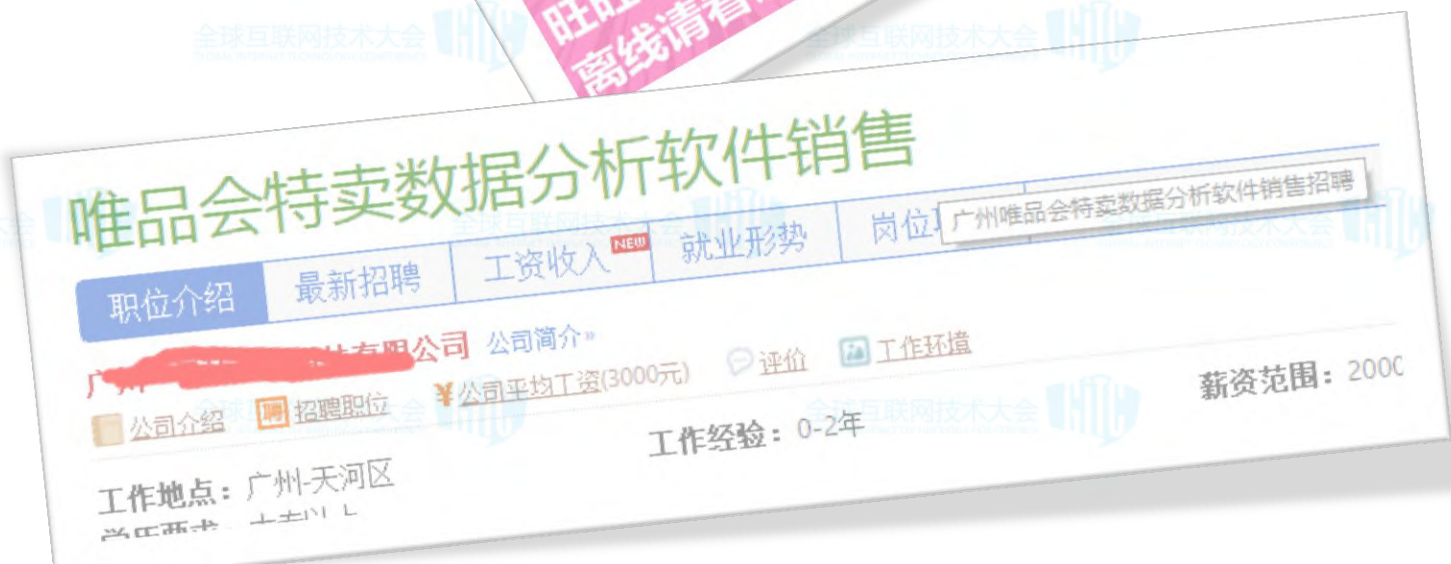
☒ 记住用户名 [忘记密码?](#) [免费注册](#)



唯品会主要安全威胁

■ 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
-



关于我

2009

东方财富网

先后从监控、
IT转到安全

入职唯品会，
负责安全测试

唯品会

2014

2015

唯品会

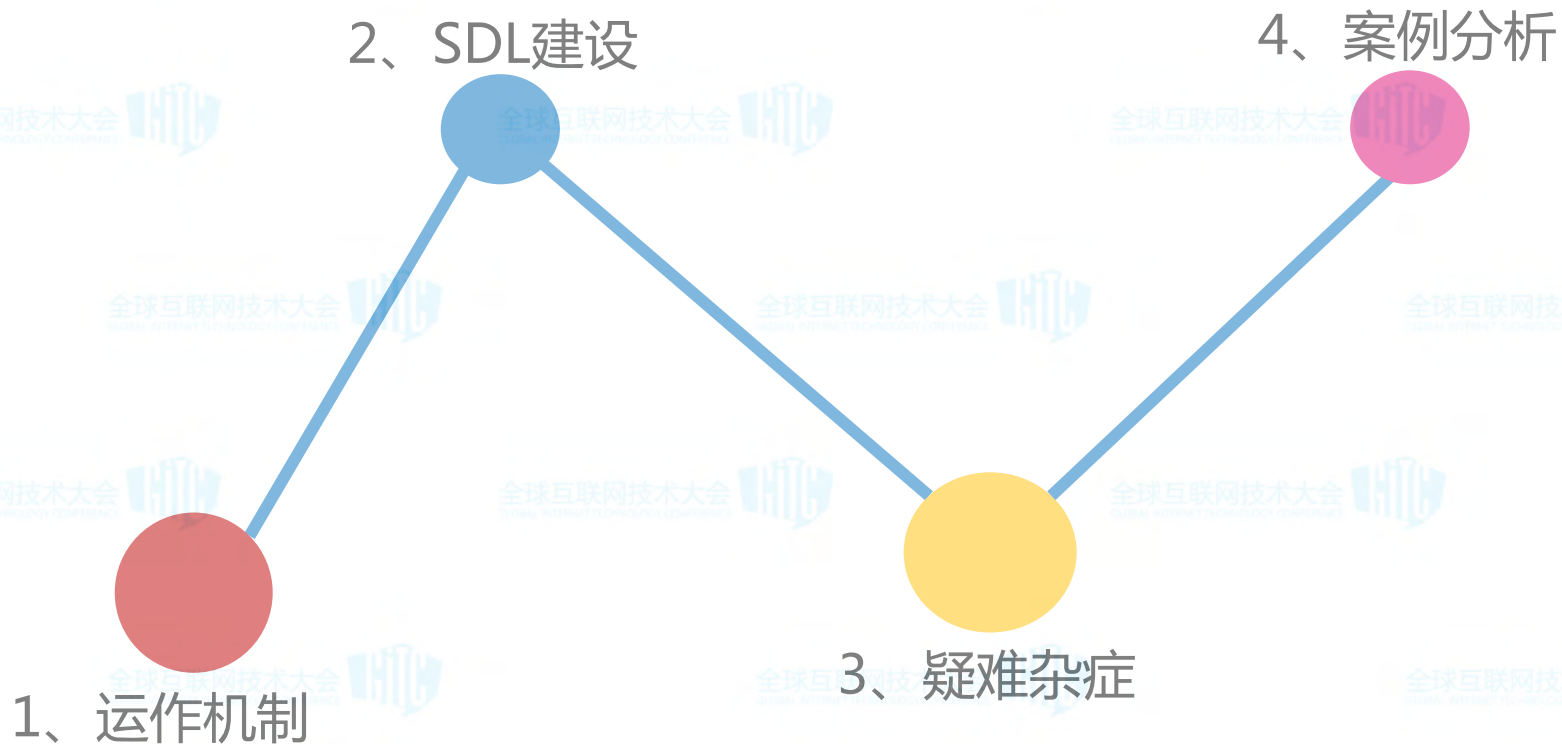
负责内部产
品安全工作

负责VSRC

唯品会

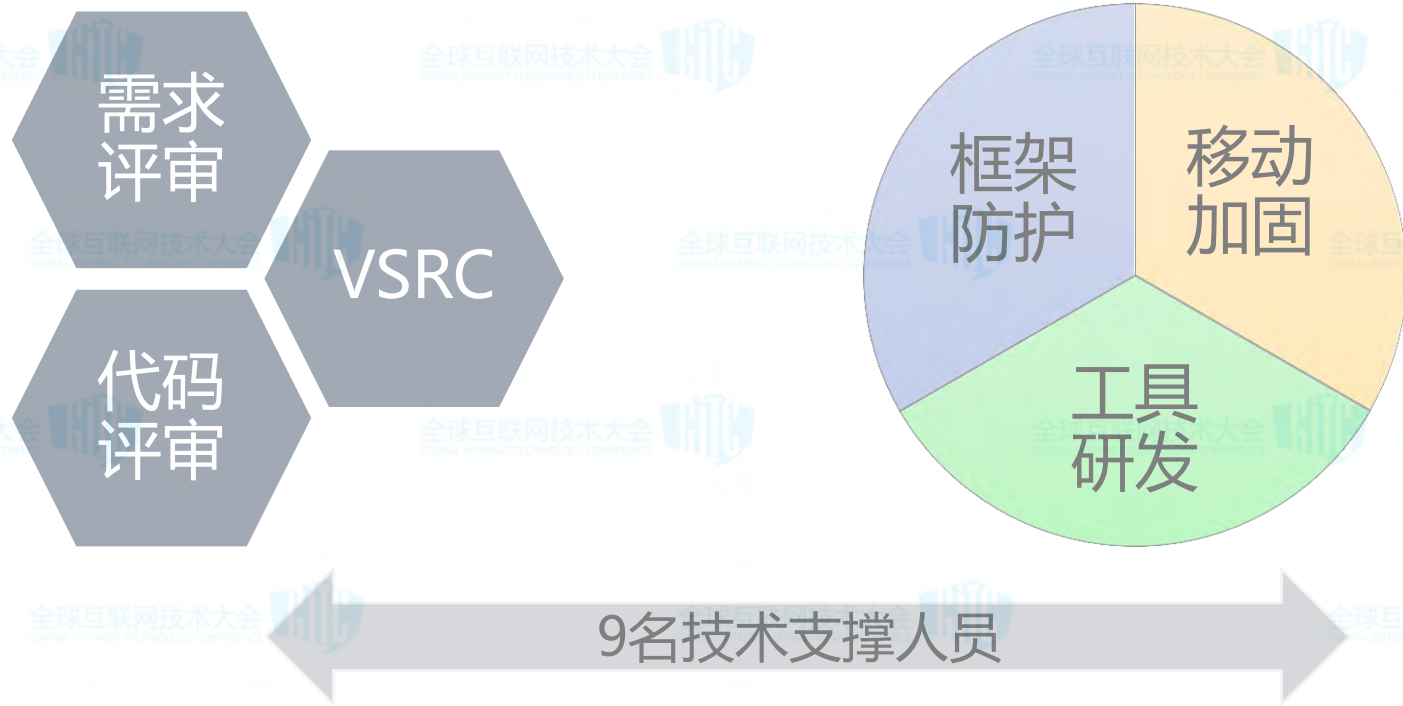
2016

目录



运作机制

运作机制



一组数据

150+

5-6



~2000

SDL建设

唯品会SDL发展历程

《VIP项目安全上线
管理流程V1.0》发布

2014年9月

VIP安全评审自
助提测系统上线

2015年3月

2015年

《web安全测试
基线用例》发布

2016年5月

2016年6月

2014年8月

《产品设计与开发安
全红线V1.0》发布

全年2000+项目
通过上线前评审

自主研发黑盒
扫描系统上线

构建SDL标准化安全开发流程

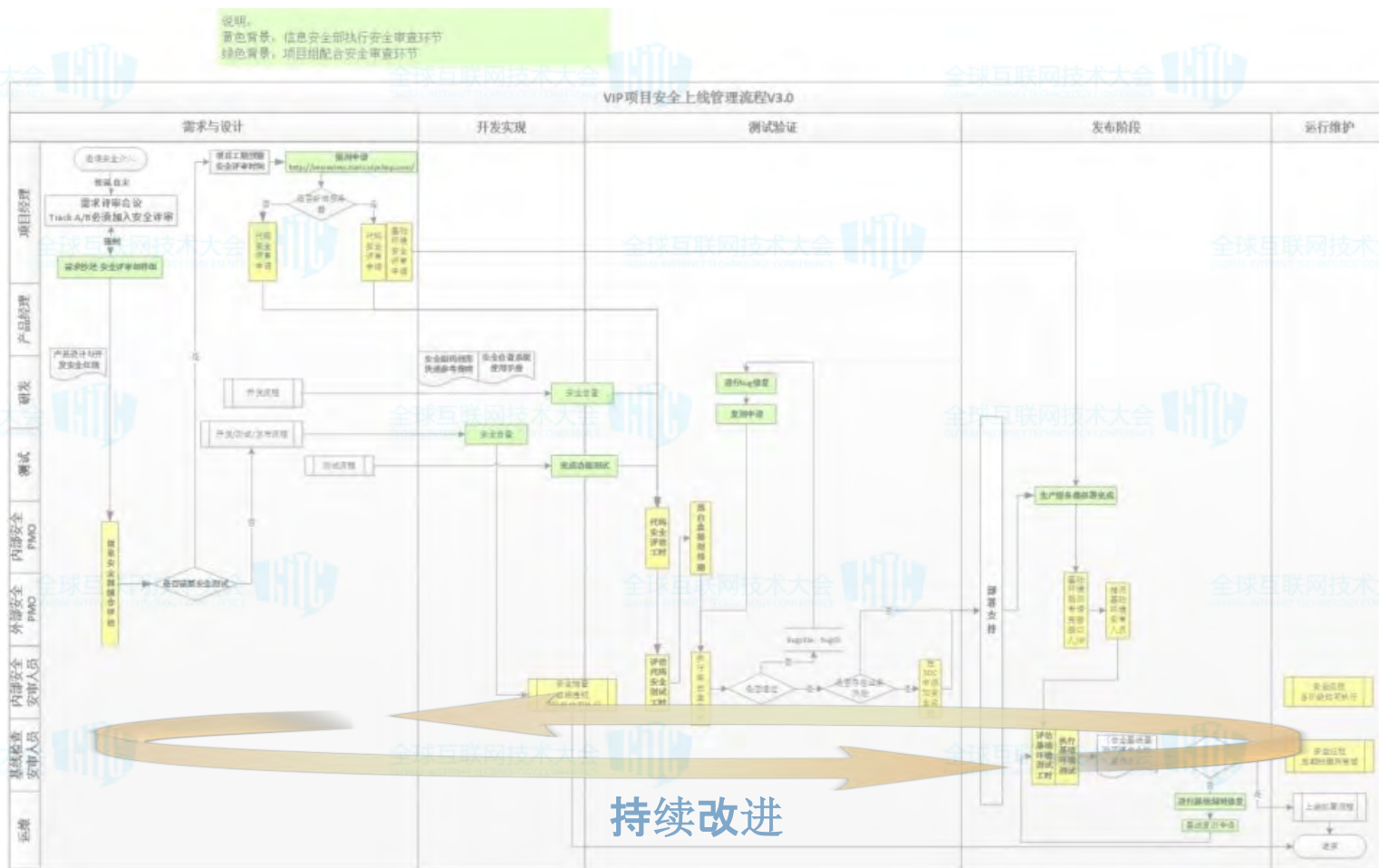
培训

需求与设计

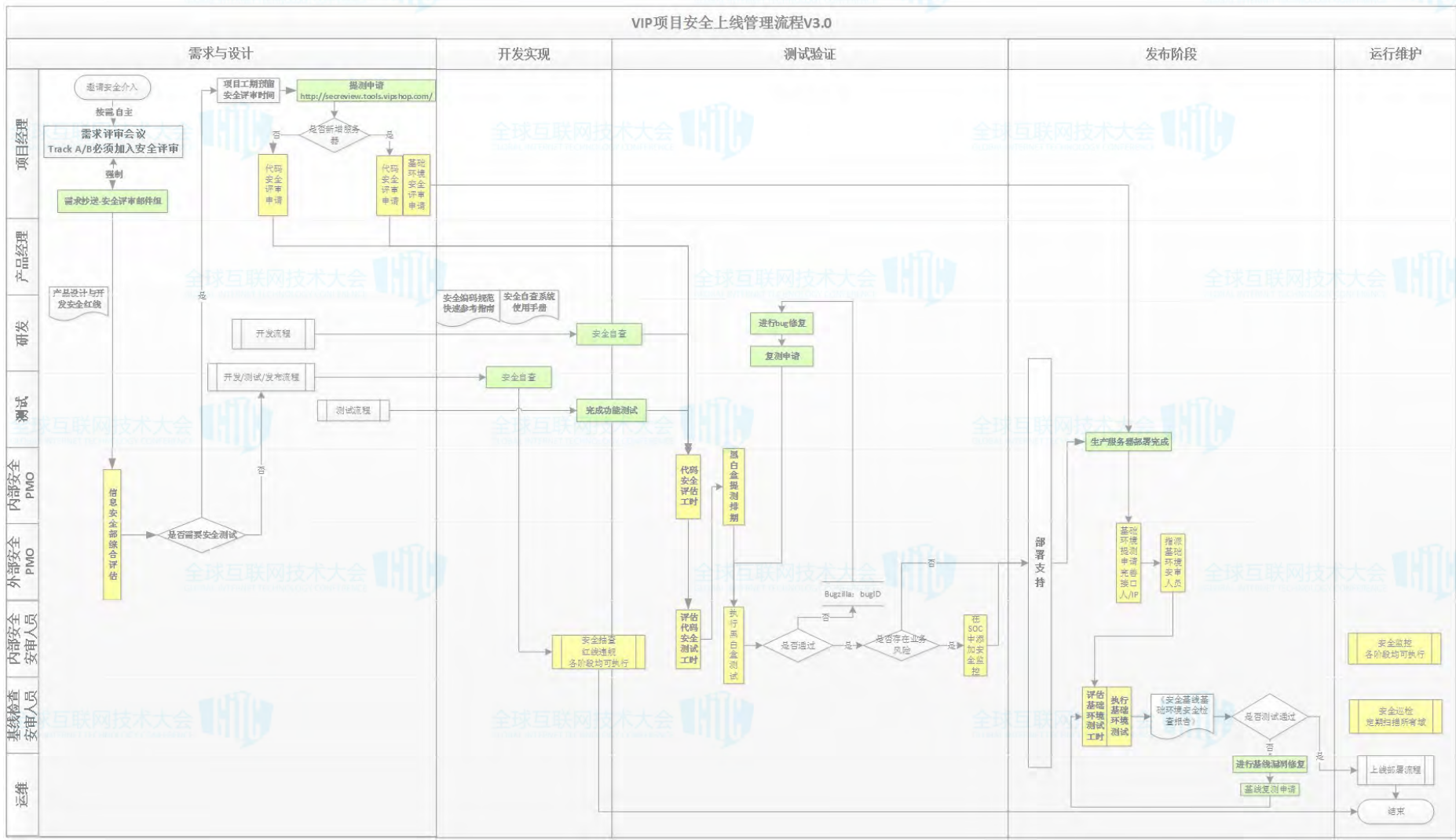
开发实现

验证与发布

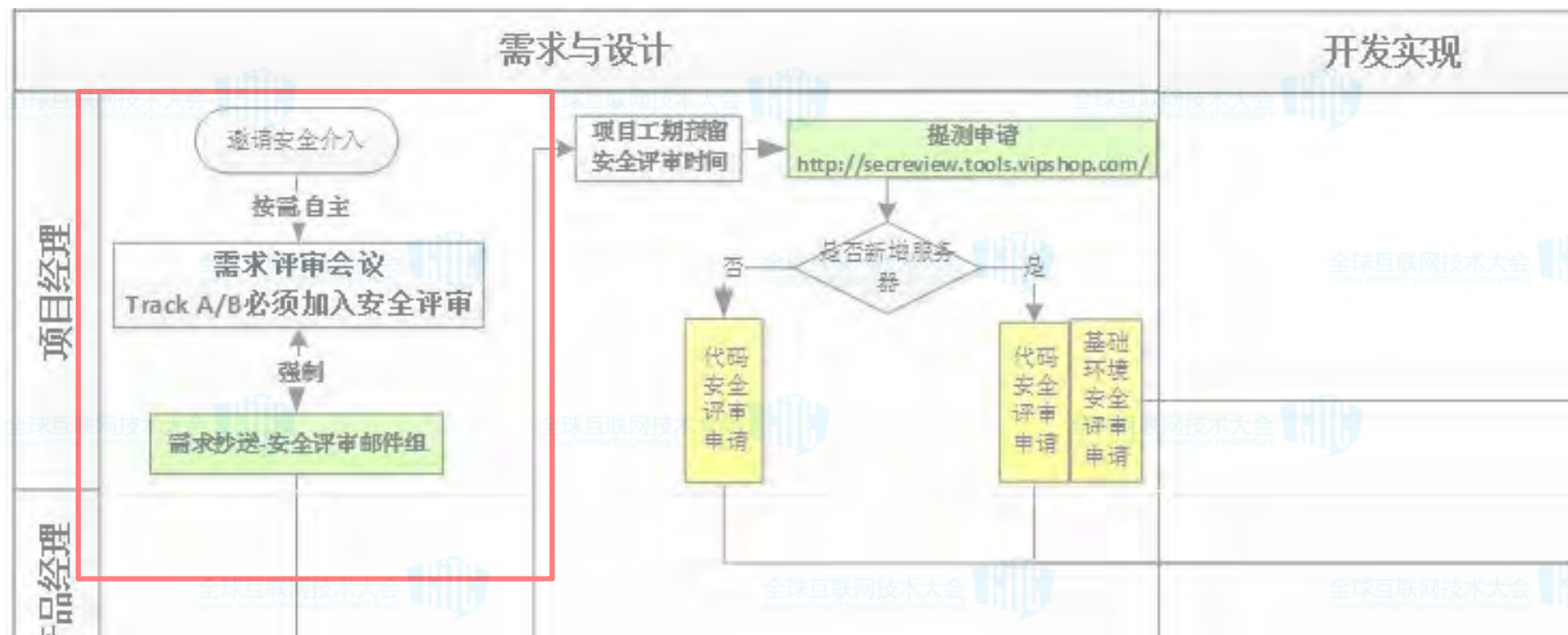
响应



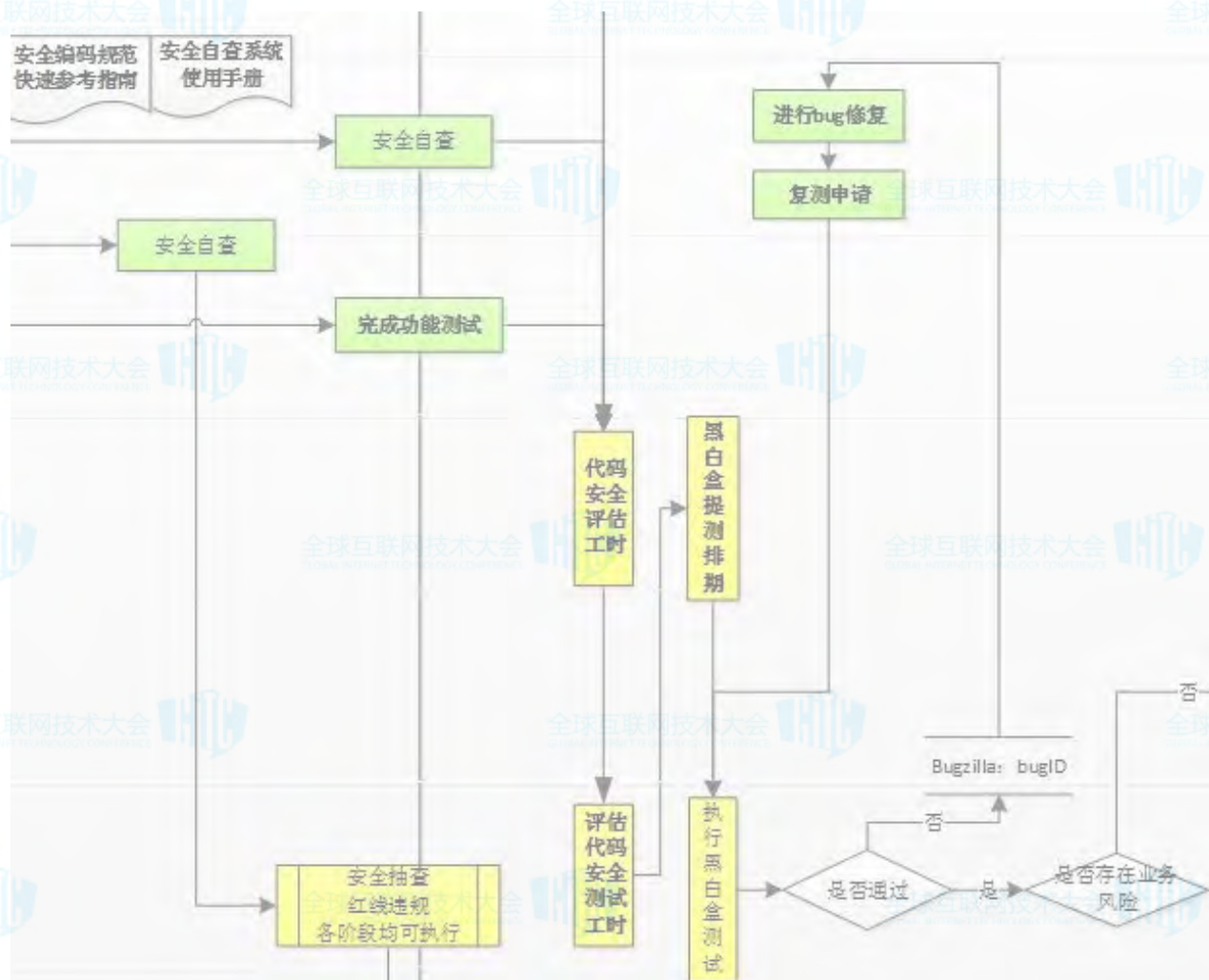
说明：
黄色背景：信息安全部执行安全审查环节
绿色背景：项目组配合安全审查环节



需求阶段尽早干预 降低漏洞发现成本



红线评审未通过 立刻中断安全测试



安全红线 消除低级漏洞

VIP产品设计与开发安全红线 v2.0

编号	类别	概述	细则	备注
L01	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）	
L02		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”）	
L03		登录与注销	有登录功能的系统必须同时有注销功能	
L04		后台页面	后台页面必须对用户身份和访问权限进行检查	
L05	验证码	管理界面	管理后台的登录界面必须设置验证码	
L06		有效期	验证码必须设置有效期（有效时间和错误次数）	
L07		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	
L08	会话安全	会话超时	会话token/session必须设有超时机制	
L09		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	
L10	Cookie	HTTP Only	cookie参数中Session Id等认证相关的字段必须设置HTTP Only	
L11	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	
L12		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）	
L13		目录权限	存储上传文件的目录必须禁止脚本执行权限	
L14	传输安全	参数提交	禁止通过HTTP GET方式提交不安全算法 ^[1] 处理过的用户密码	
L15		明文传输	禁止在未加密的HTTP协议中明文传输用户登录密码、支付密码、银行卡卡号、有效期、持卡人姓名、身份证号码、CVV等交易敏感数据。会员系统、支付系统还应在此基础上进一步增强安全措施 ^[2] 。	
L16		支付安全	禁止在支付密码的传输过程中使用不安全算法 ^[1]	
L17	存储安全	敏感数据存储	禁止数据库、日志文件中明文存储用户支付密码、银行卡卡号、有效期、持卡人姓名、身份证号码等交易敏感数据。禁止存储信用卡CVV信息。禁止使用不安全算法 ^[1] 存储用户身份校验凭据，如：密码。会员系统、支付系统还应在此基础上进一步增强安全措施 ^[2] 。	
L18	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	
L19		日志清除	除审计用户外，其他人员不应具备日志修改、删除或清空的权利。必须记录清空日志的行为	
L20		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	
L21	其它	后门	禁止在代码中置留后门	
	备注[1]	不安全算法	明文、标准MD5算法、Base64编码、私有算法等。	
	备注[2]	增强安全措施	参考等级保护、PCI-DSS、ADSS等法规和标准并严格执行安全编码规范	

提测流程变形记 Excel到平台

安全测试提测准备说明（示例）

唯品会安全评审自动提测系统

申请提测

资源视图

违反红线的项目

选择提测类型

我要提交代码评审

提单详情（项目PMO填写）

说明：

- 1、建议需求阶段发起提单登记，安全评审尽早介入，为安全需求评审做准备
- 2、请在功能测试完成后，启动代码评审
- 3、建议项目组预留出安全评审的项目排期，及早沟通及早安排

*项目类型：☐ 市场活动 ☐ 项目

*项目名称：

*PMO接口人

*开发接口人

*测试接口人

*如不在提示列表内可直接写英文名

简要描述：

简要描述项目类型，新网站？Android 或 IOS APP？旧网站新上线功能？市场活动？

功能测试完成时间：

系统计划上线时间：

登记评审

不评审

303

异常上线

BUG跟踪

4-1

业务逻辑全部可操作

需保证整体业务环境可操作，不存在基本的功能BUG，避免功能无法测试

同事姓名

4-2

提测系统间的依赖关系

提测要依赖其他域的部署或其他特殊条件，需集成测试环境

同事姓名

4-3

测试环境访问地址

业务系统访问方式

同事姓名

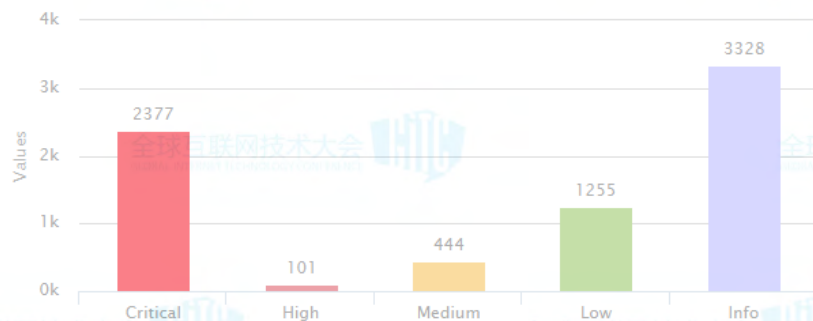
黑白盒助力解决安全漏洞

Web Vulnerability Scanner

首页 任务管理 报表管理 引擎管理 系统管理

Home

Vulnerabilities by Severity



Top 10 Vulnerabilities(High)

跨站点脚本	2335
异常错误消息	168
目录列表	109
缺少跨框架脚本木保护	35

VIP - 静态代码分析平台

Search

- 主页
- 新建任务
- 任务列表
- 漏洞知识
- 安全中心
- 注销退出

VIP SCA

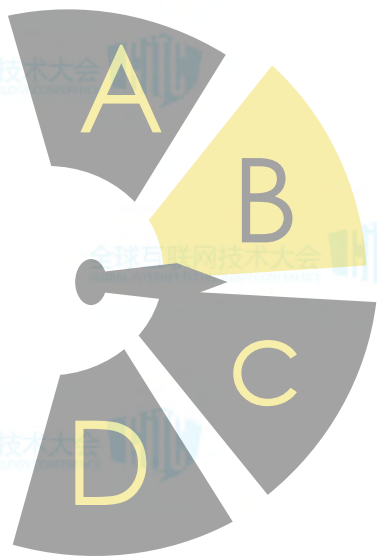
Home

Vip Source Code Analyzer.

2015 © Vip Source Code Analyzer.

疑难杂症

理想很丰满 现实很骨感

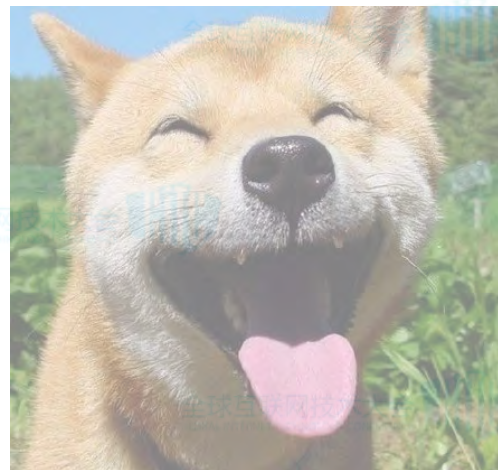


业务发展迅速

开发技术水平不一

人工绕过上线流程

评审了怎么还有漏洞



- 缺少专业的安全人员
- 实施及维护成本高

安全建设要不要上SDL？

6、安全体系的不断完善

日积月累

5、医务团队和保健体系

事前防御为主

4、医务团队及医疗体系

事后多、事前少

1、自行买药

开发解决已知问题

2、求助医生

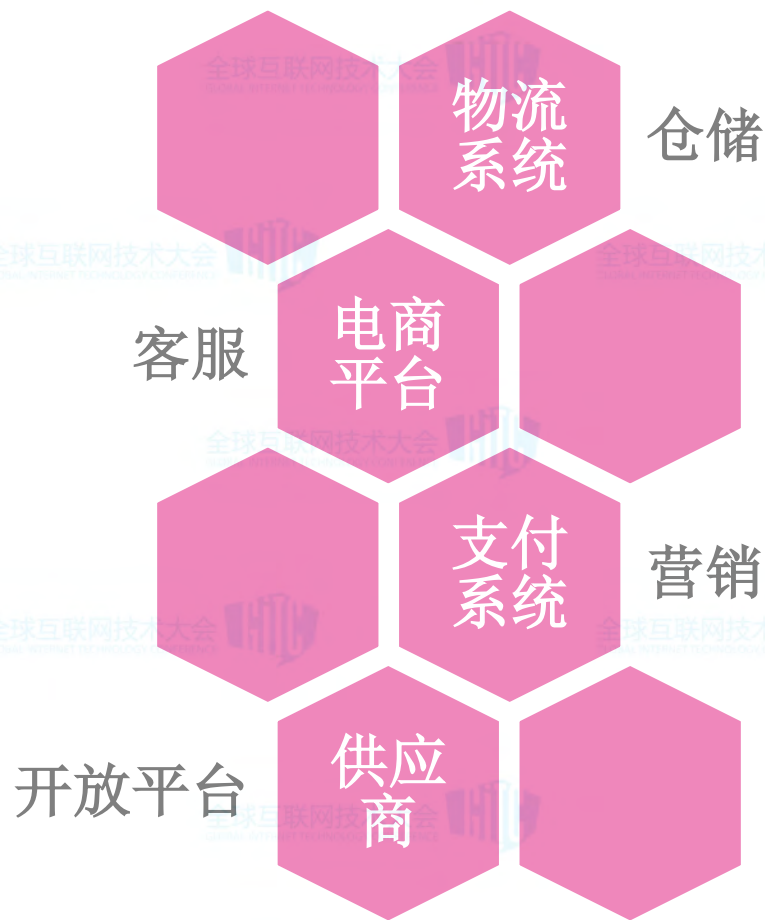
安服、众测

3、私人医生

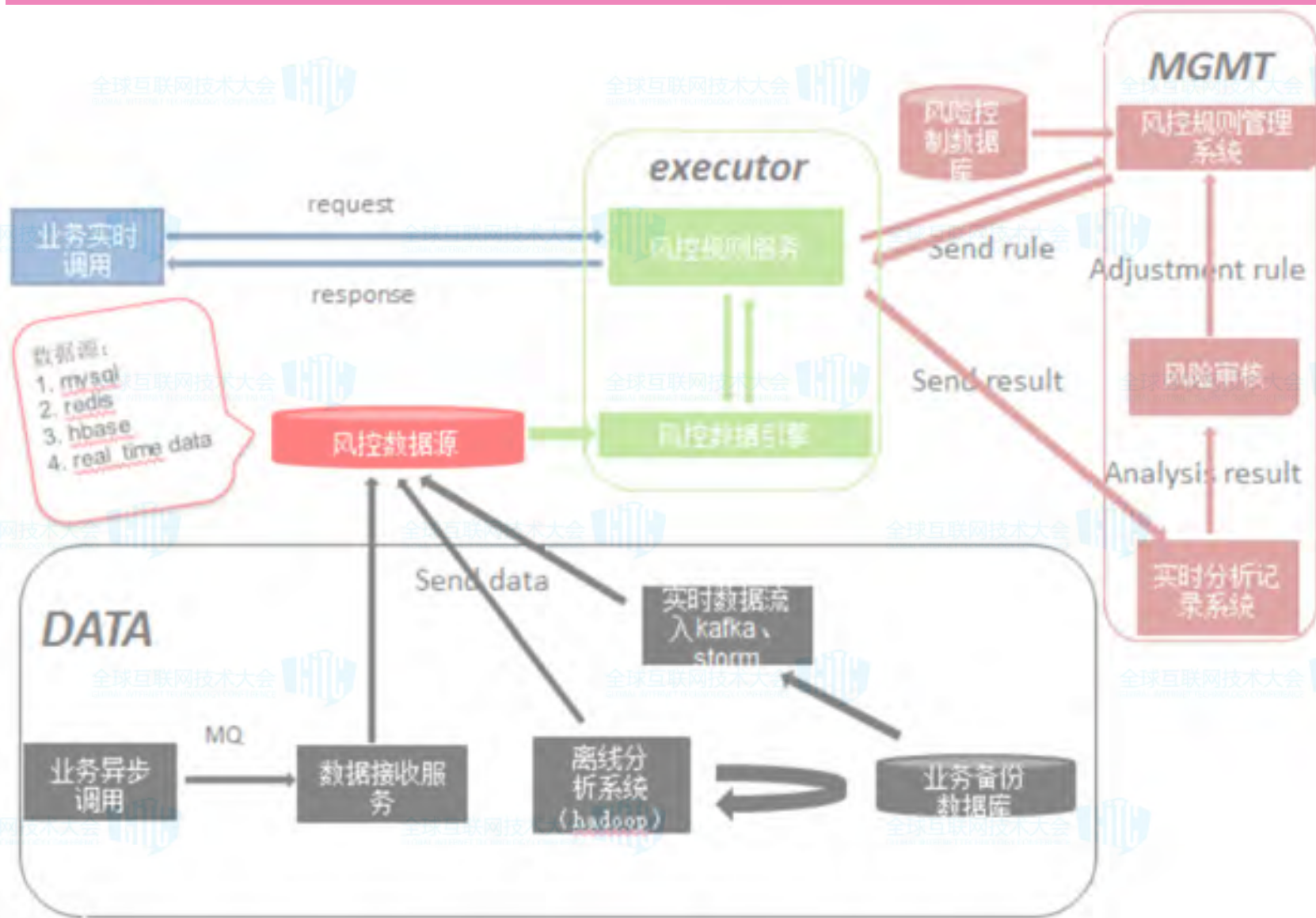
救火阶段



更多电商平台背后的系统



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

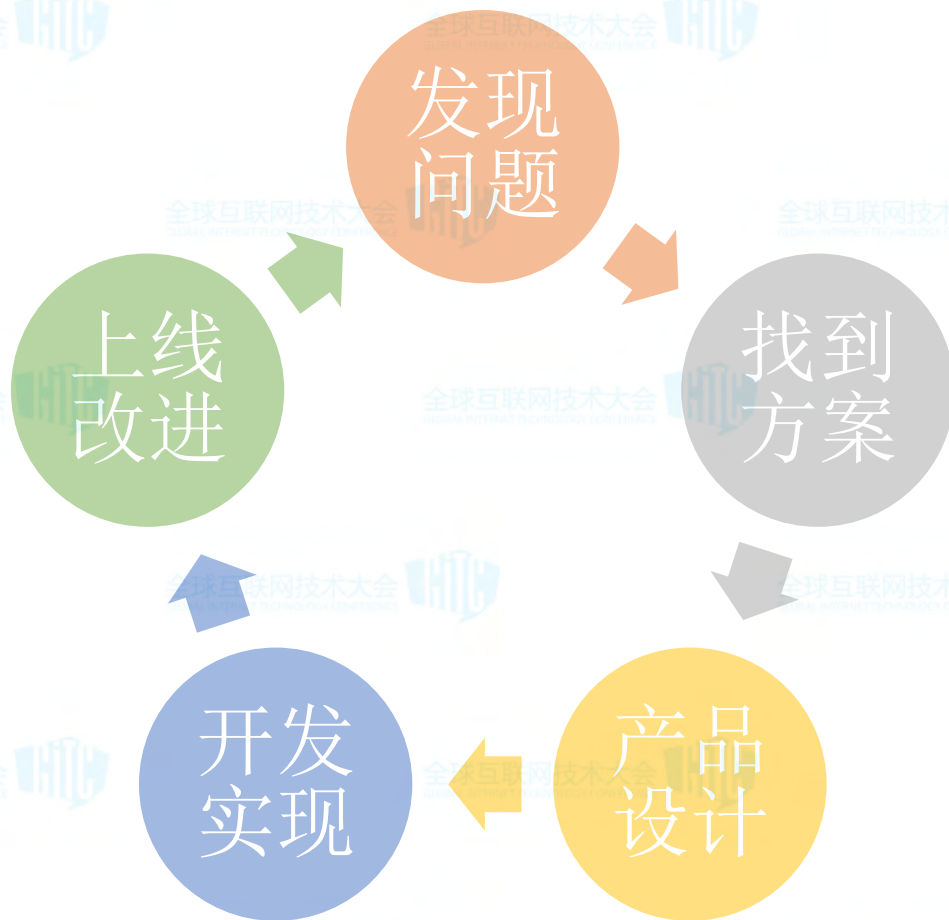
30%

过去一周拦截率

30%

总拦截率

优化产品改进的流程



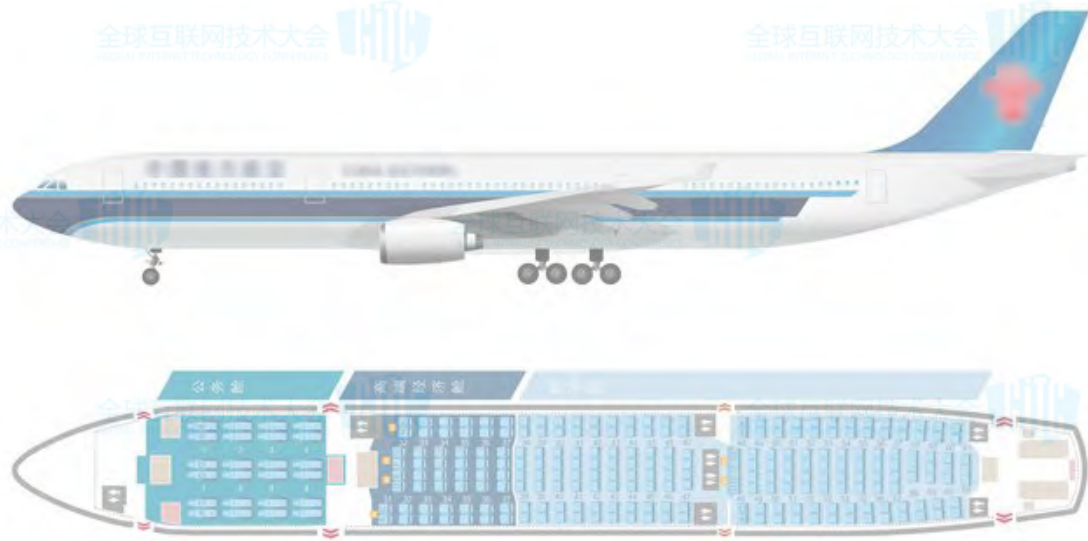
案例分析

服务器夜半惊魂



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



方法都知道 落地很艰难

领导不支持 一切都免谈
除了靠自己 还得靠伙伴

VSRC未来规划



未来

现金奖励机制

加强技术分享

共建SRC联盟

- ✓ 增加威胁情报收集工作
- ✓ 增强运营激励机制
- ✓ 优化礼品走现金流程
- ✓ 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
- ✓ 同成长
- ✓ 共进步
- ✓ 齐发展

Q&A

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



微信号：VIP_SRC

官方网站：<http://sec.vip.com>

微信公众号：唯品会安全应急响应中心

漏洞接收邮箱：sec@vipshop.com

专业
我们致力于保护用户信息安全
我们积极营造更加安全的
线上电商购物平台

唯品会安全应急响应中心