唯品会 vip.com

唯品会安全应急响应中心
VIP Security Response Center

2016唯品会互联网电商安全峰会

电商安全的闭环

电商安全体系建设的血与泪

从企业安全开发生命周期SDL

到熟悉而又充满惊喜的VSRC2.0时代！

唯品会 vip.com | 唯品会安全应急响应中心 VIP Security Response Center

唯品会SDL发展历程

2014年8月 《VIP项目安全上线管理流程V1.0》发布

2014年9月 《产品设计与开发安全红线V1.0》发布

2015年3月 VIP安全评审自助提测系统上线

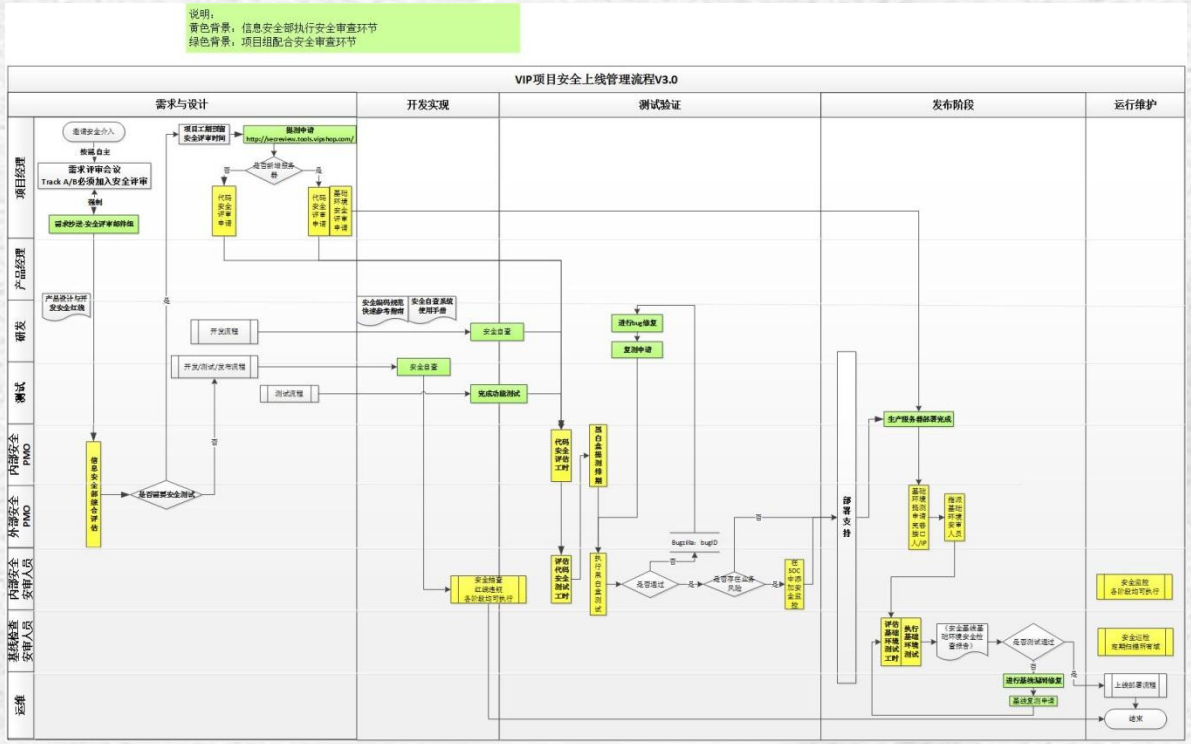
2015年 全年2000+项目通过上线前评审

2016年5月 《web安全测试基线用例》发布

2016年6月 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

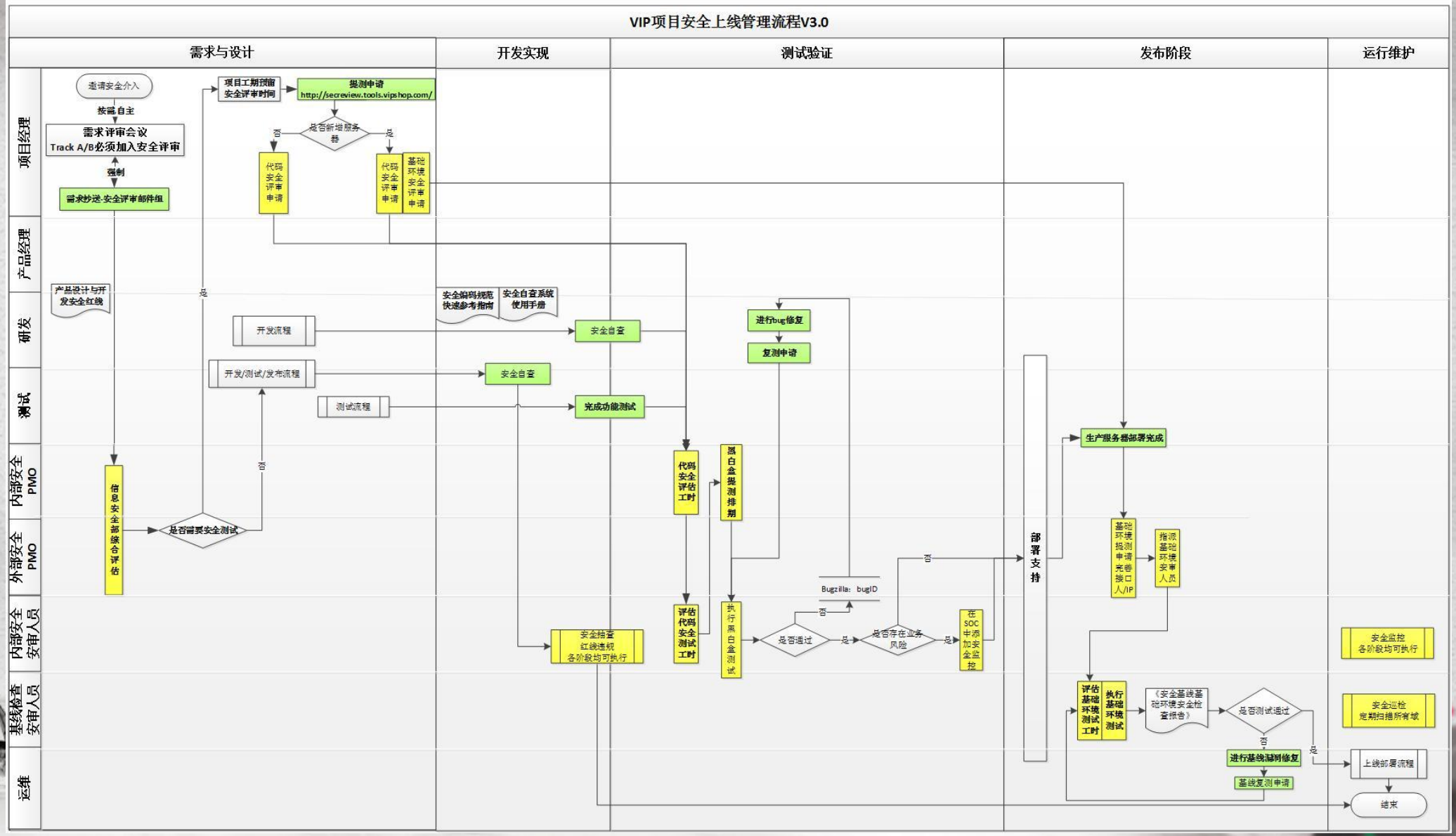


持续改进

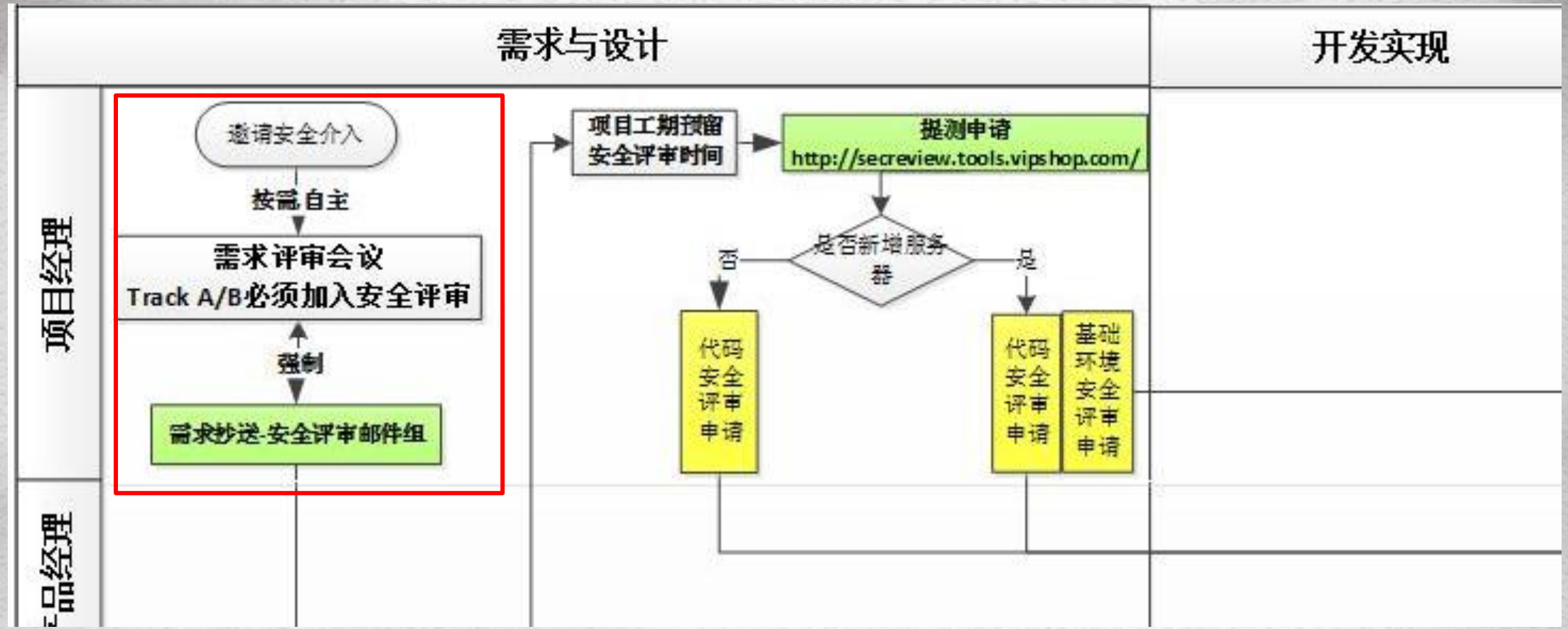
唯品会安全应急响应中心
VIP Security Response Center

上线管理流程 — —降低人为因素

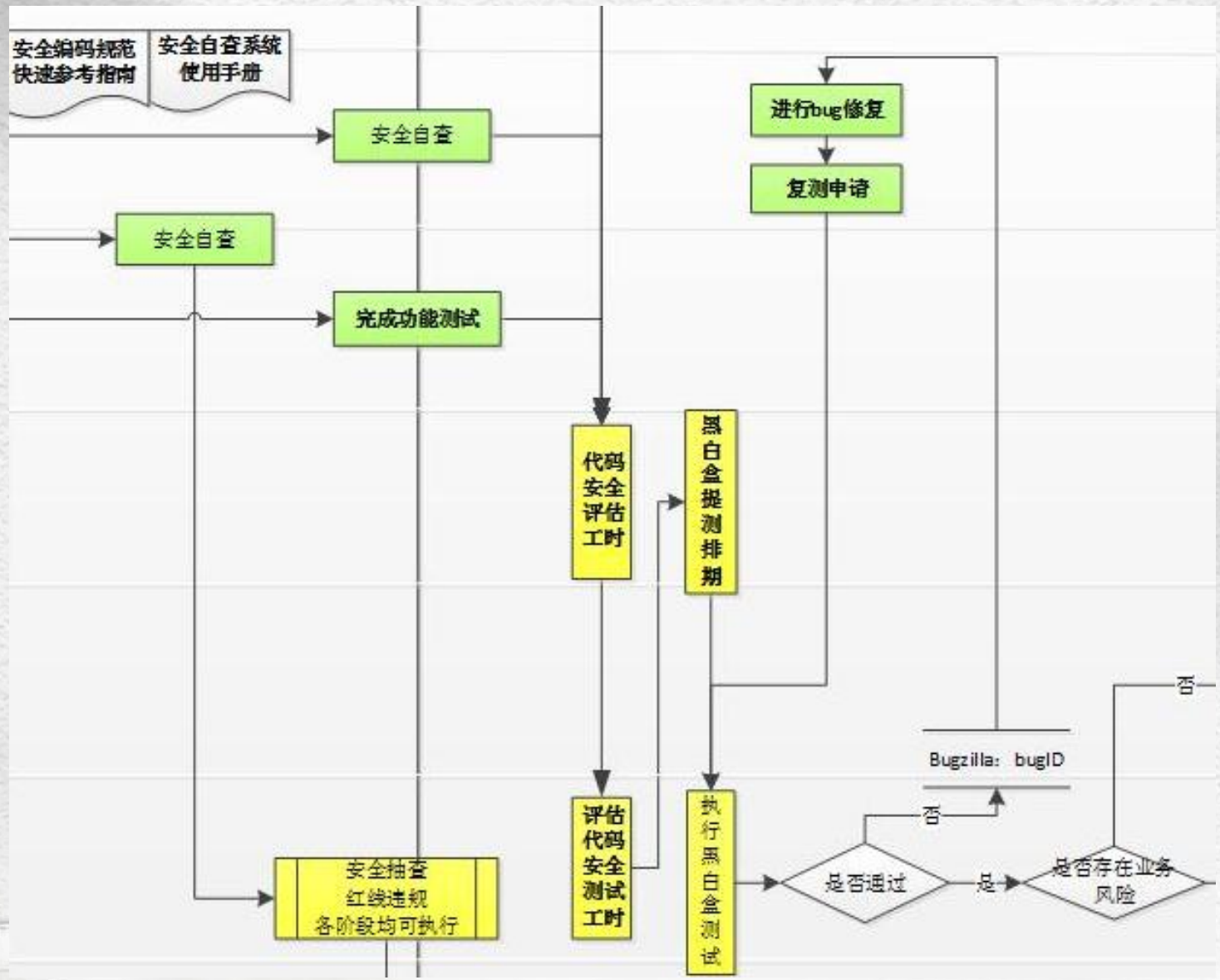
说明：
黄色背景：信息安全部执行安全审查环节
绿色背景：项目组配合安全审查环节



需求阶段尽早干预 降低漏洞发现成本



红线评审未通过 立即中断安全测试



唯品会 vip.com | 唯品会安全应急响应中心 VIP Security Response Center

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、删除或清空的权限。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	禁止在代码中留置后门	
	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	

唯品会 vip.com | 唯品会安全应急响应中心 VIP Security Response Center

提测流程变形记——Excel到平台

安全测试提测准备说明（示例）

提测项目名：某某项目	提测人(接口人)：总接口人	注意：提测准备不足会导致安全评审延期！
请在提交安全测试前进行如下的需求准备（重要性：必备 重要 一般）：		

唯品会安全评审自助提测系统

Search Project

我要提交代码评审

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

提单详情（项目PMO填写）

*项目类型： 市场活动 项目

*项目名称： 非市场活动，必填PLCS中的项目名称

*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： 2016-07-27 系统计划上线时间： 2016-07-27

登记评审

其他管理

已完成 1590

不评审 303

异常上线

BUG跟踪

4-3	测试环境访问地址	业务系统访问方式			同事姓名	

人在塔在 德玛西亚

有策略

含整体的安全管控策略、安全目标，针对重要业务的安全策略；

有组织

含角色和职责分工、协作；

有标准

含设计标准/规范、部署标准/规范，以及适合公司环境的产品/工具/组件等标准；

有流程

将上述策略、标准/规范嵌入到流程中；

能落实

策略、标准/规范得到贯彻实施，如代码审计、安全测试、安全部署等，通过技术、工具或审计等手段辅助落地。

漏洞管理——通过流程闭环解决

评审了怎么还有漏洞

手工测试，难免遗漏

业务发展迅速

每周有近百个需求需要评审

安全评审要前置

降低漏洞发现和修复成本

无奈的第三方

业务发展迅速的同时也需要第三方来支撑

人工绕过上线流程

开发团队内部宣导与意识不足

开发技术水平不一

每周都有开发入职，新入职的开发安全意识比薄弱

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

唯品会 vip.com | 唯品会安全应急响应中心
VIP Security Response Center

sec.vip.com

1

VSRC2.0 主站风格不错！

——太棒了！ 现在我们都知道它能做什么了！

VSRC2.0 礼品商城很棒！

—— 是的！ 然而这只是升级的一部分！

… 之后呢？

—— 聆听大家内心最真实的想法！

VSRC2.0功能简介

2

自动化流程
自动化分配漏洞进行修复

漏洞去重
新增漏洞域功能

sec.vip.com

报表分析
此次改版新增智能化报表分析平台

数据统计
优化数据统计平台

2015年8月VSRC上线运营 → 2016年2月17日微信公众号 → 2016年5月10日VSRC2.0升级上线 → 2016年第二季度T-Safe团队

VSRC2.0升级一览

3

VSRC2.0未来规划

4

壹·增加 现金奖励

贰·加强 技术交流

叁·共建 SRC 联盟

唯品会 vip.com 唯品会安全应急响应中心 VIP Security Response Center

谢谢欣赏

唯品会安全应急响应中心