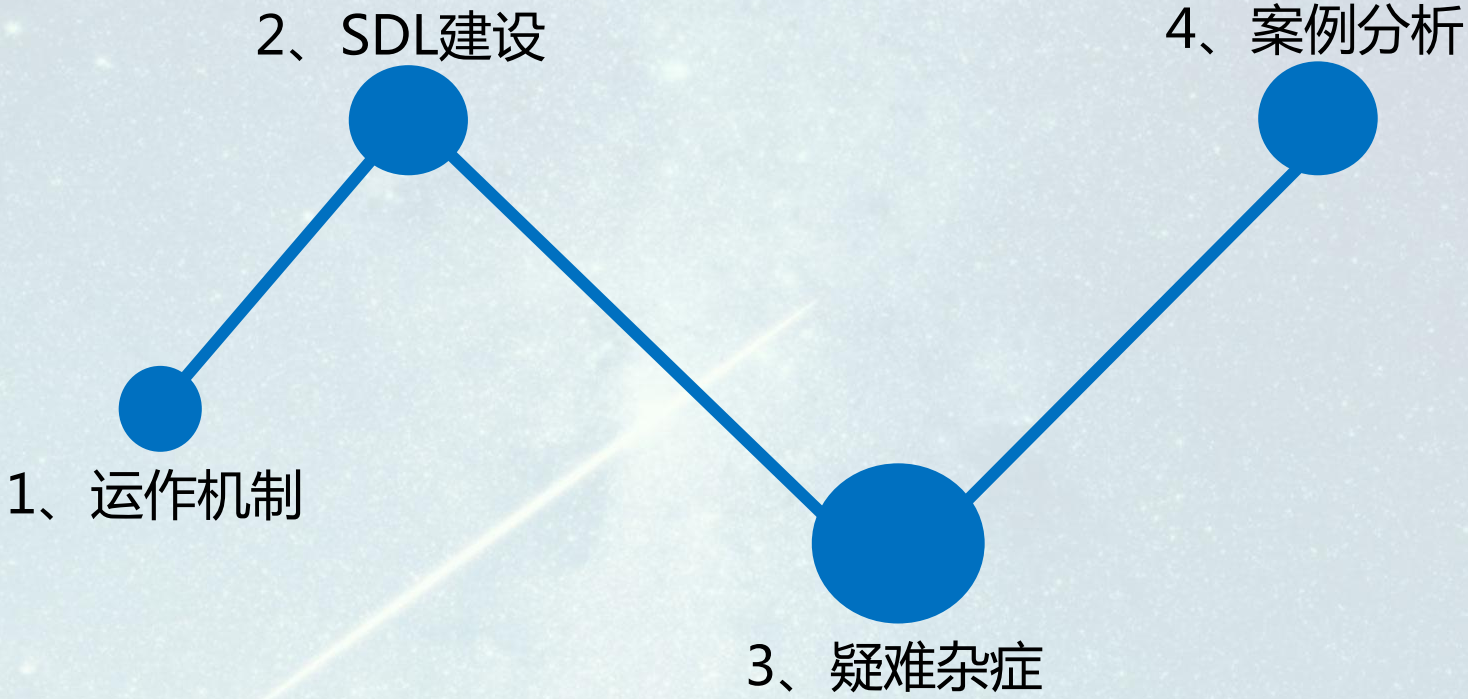
唯品会产品安全技术实践

唯品会安全测试经理、VSRC负责人 方斌

关于我

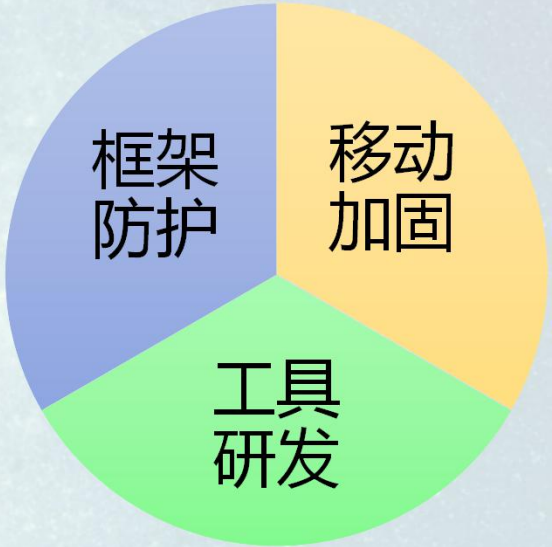

2009
东方财富网
先后从监控、
IT转到安全
2014
入职唯品会，
负责安全测试
唯品会
2015
唯品会
负责内部产
品安全工作
2016
负责VSRC
唯品会

目录



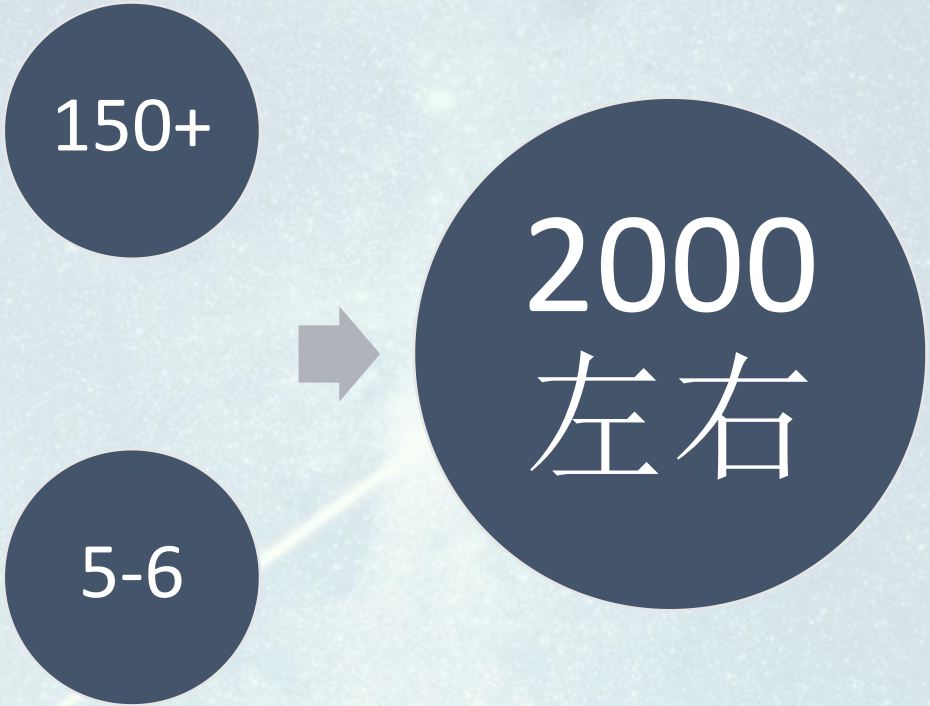
运作机制

运作机制



13名技术支撑人员

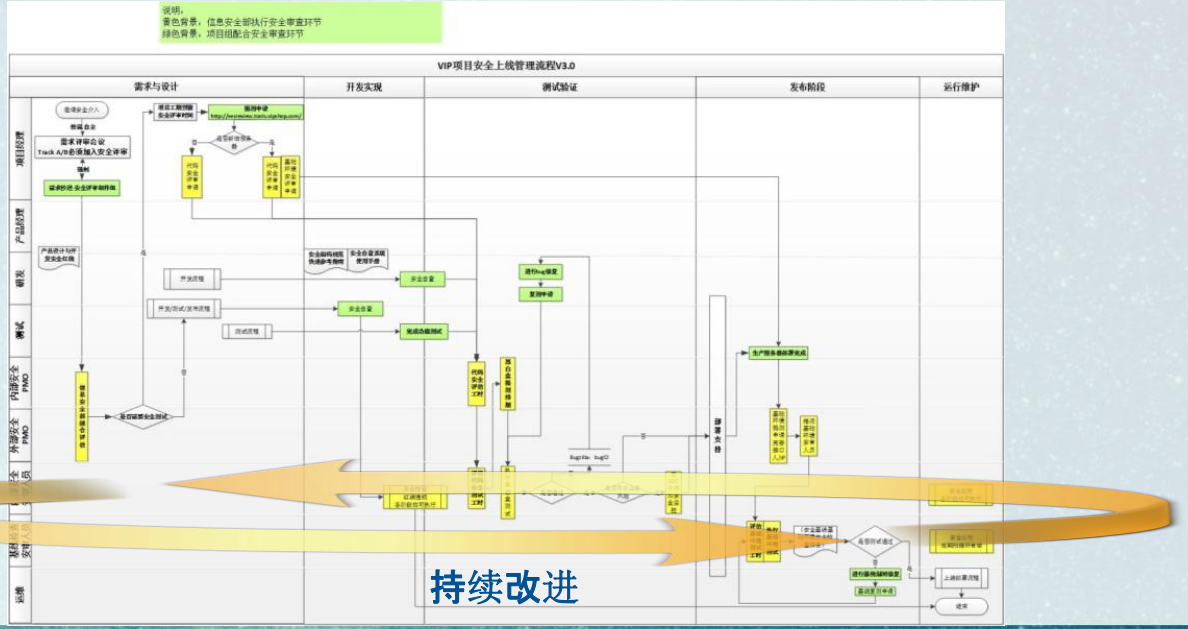
一组数据



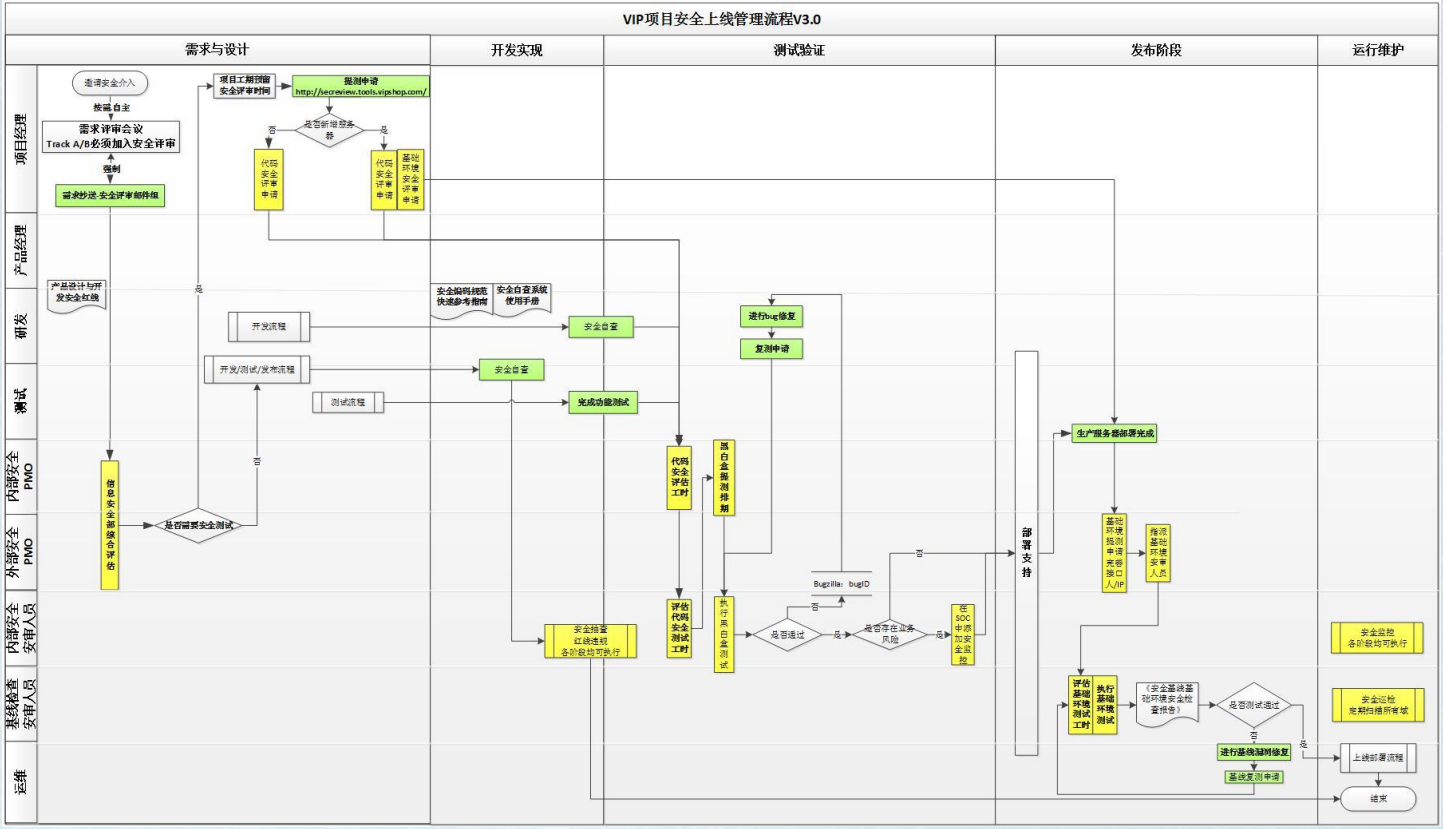
SDL建设

构建SDL——标准化安全开发流程

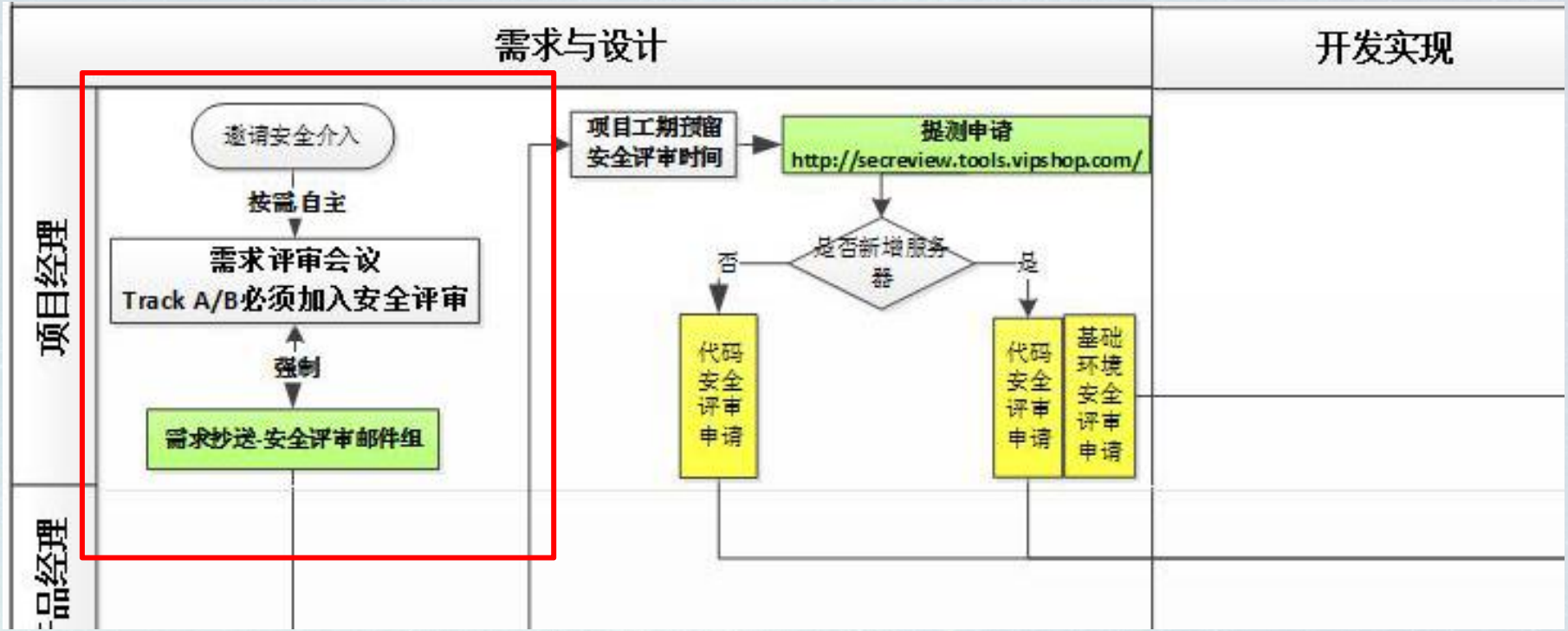
培训 → 需求与设计 → 开发实现 → 验证与发布 → 响应



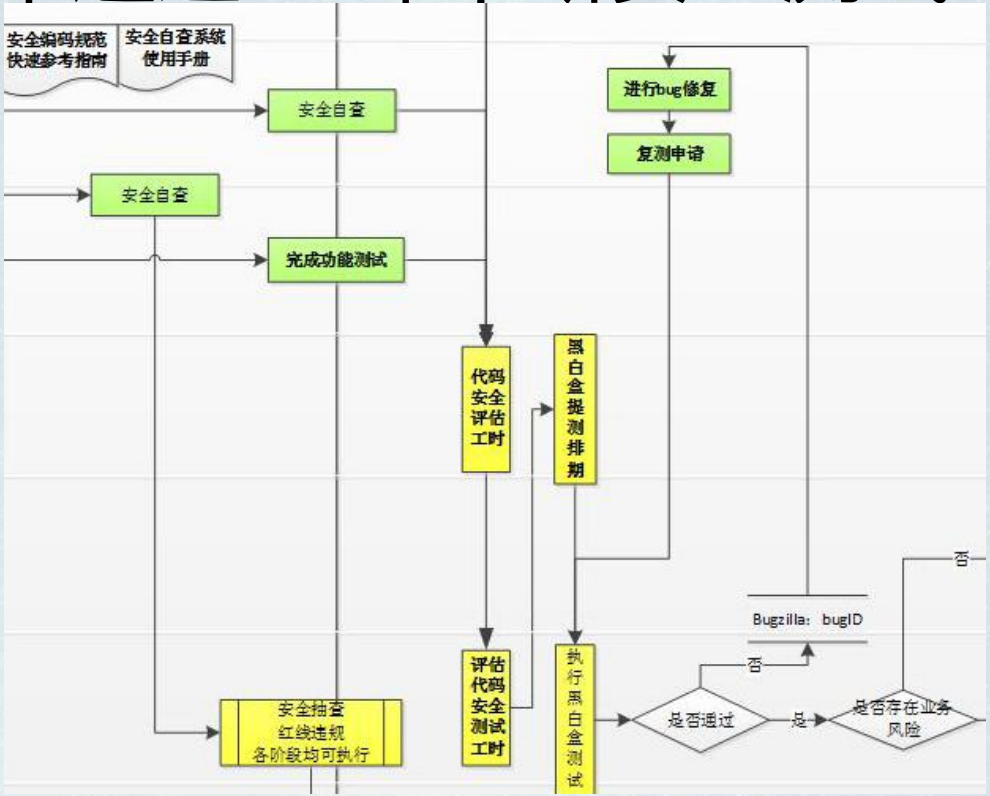
说明：
黄色背景：信息安全部执行安全审查环节
绿色背景：项目组配合安全审查环节



需求阶段尽早干预 降低漏洞发现成本



红线评审未通过 立即中断安全测试

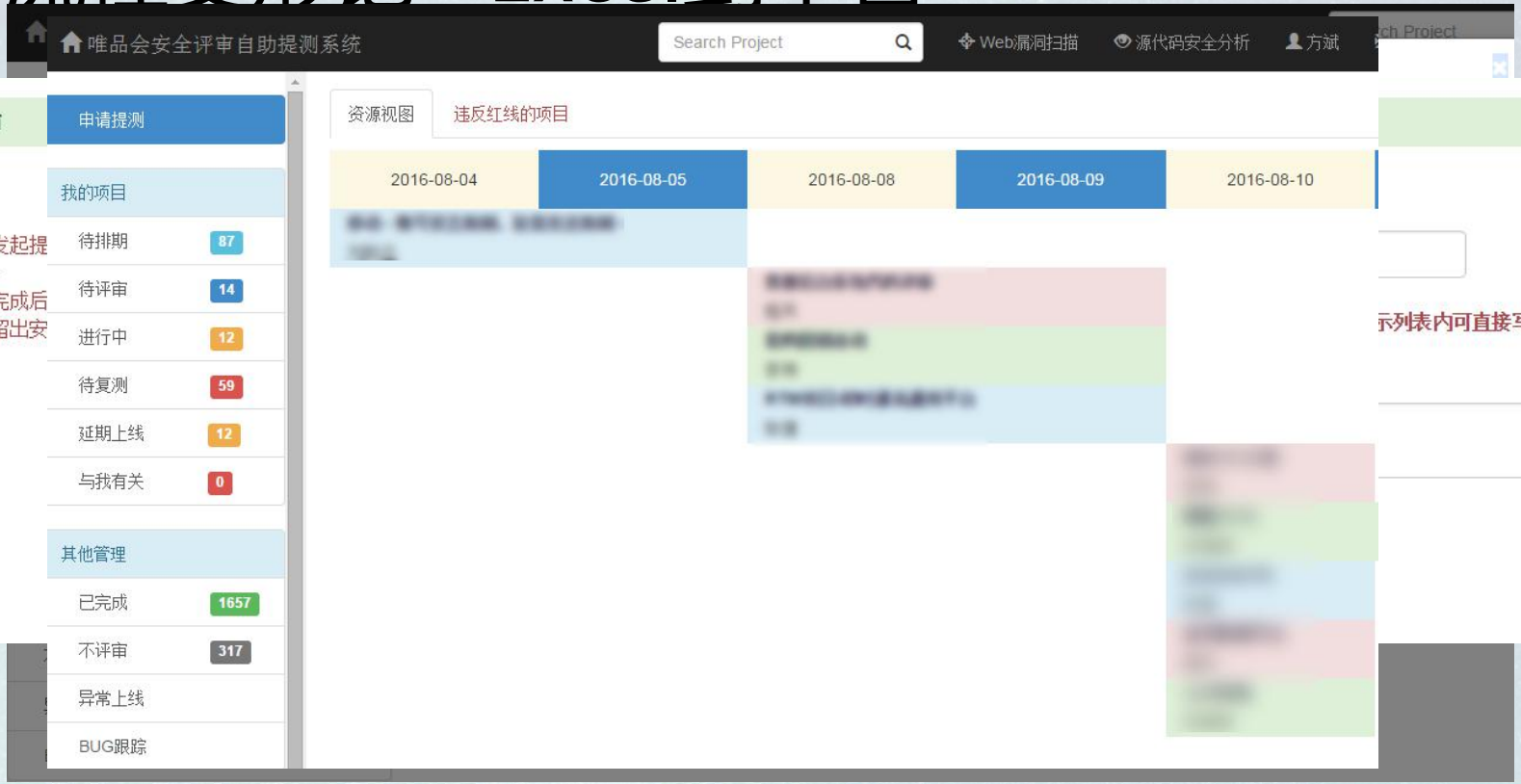


安全红线　消除低级漏洞

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	

提测流程变形记 Excel到平台



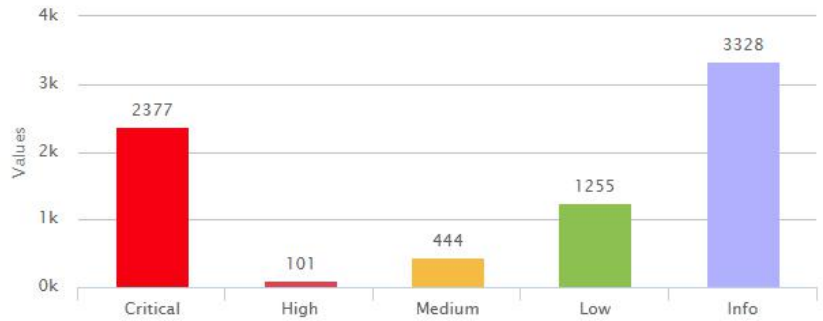
黑白盒助力解决安全漏洞

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

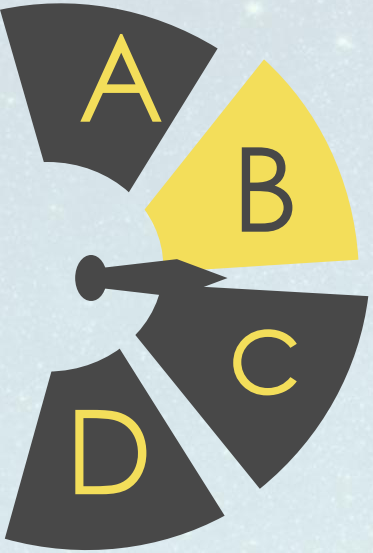
Home

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

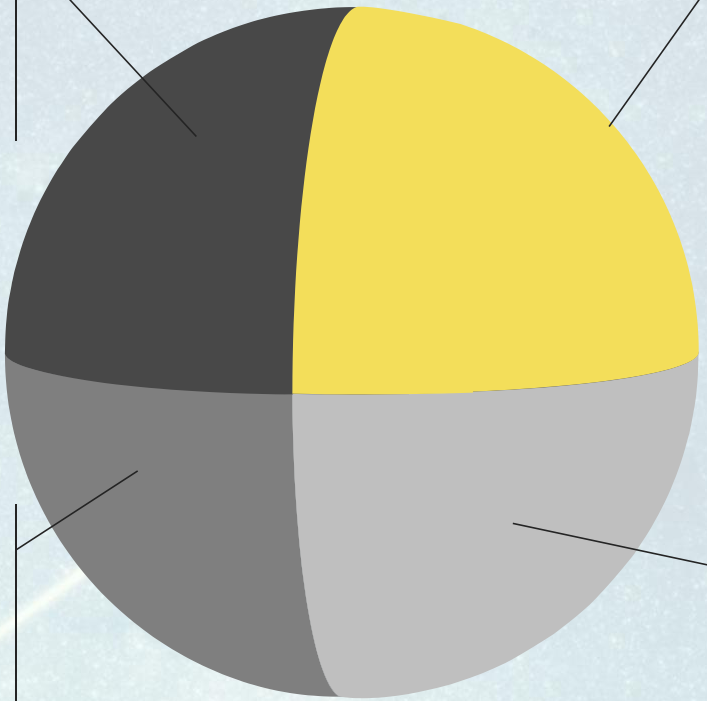
人工绕过上线流程

评审了怎么还有漏洞

案例分析

需求为什么不给过

这是老板的需求



安全不能阻碍业务的发展呀

怎么才能让我的需求通过

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


THANKS
Q&A