Geekbang 极客邦科技 InfoQ

QCon 全球软件开发大会【北京站】2016

SDL的深入探究及实践

金山云 – 邱雁杰

Intemational Software Development Conference

关于我

SYClover安全研究团队核心成员

- Web安全研究
- 网络渗透研究

百度高级安全工程师

- 百度安全扫描系统
- 企业安全（应急响应、安全评估等SDL相关）

金山云高级安全工程师

- 安全产品研发
- 企业安全整体建设

大纲

- SDL简介
- 项目生命周期中的安全风险
- SDL如何介入研发流程
- SDL的最佳实践
- Q&A

大纲

- SDL简介
- 项目生命周期中的安全风险
- SDL如何介入研发流程
- SDL的最佳实践
- Q&A

SDL是什么

- SDL即Security Development Lifecycle (SDL)，是微软提出的从安全角度指导软件开发过程的管理模式,是一种专注于软件开发安全保障的流程。

SDL能解决什么问题

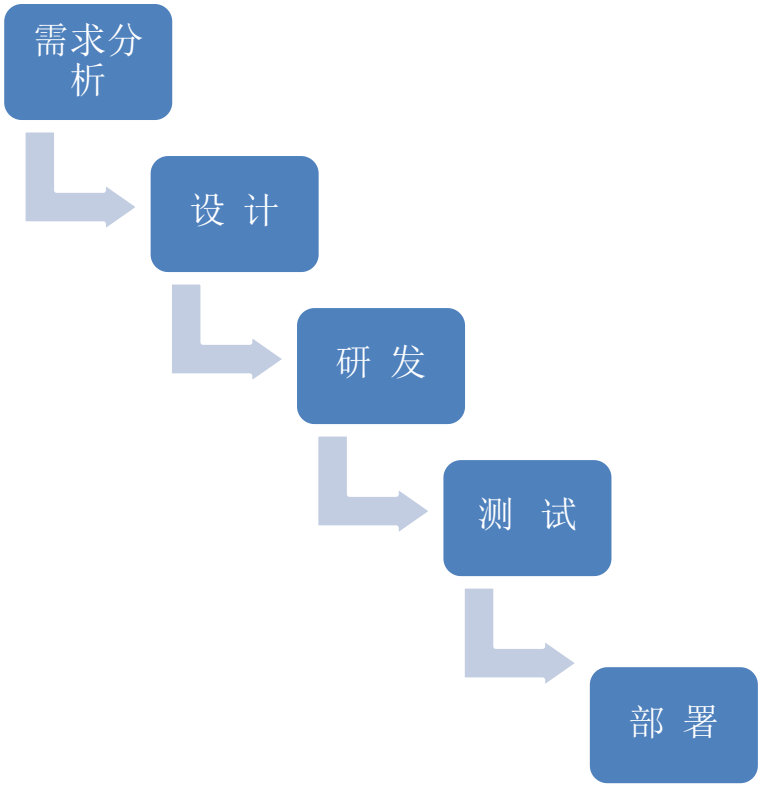
- 是将设计、代码和文档等与安全相关漏洞减到最少，在软件开发的生命周期中尽可能的早地发现解决相关漏洞建立的流程框架;
- 为了实现保证最终的用户安全，在软件开发各阶段中引入针对项目安全和用户隐私问题的解决方案。

大纲

- SDL简介
- 项目生命周期中的安全风险
- SDL简介
- SDL的最佳实践
- Q&A

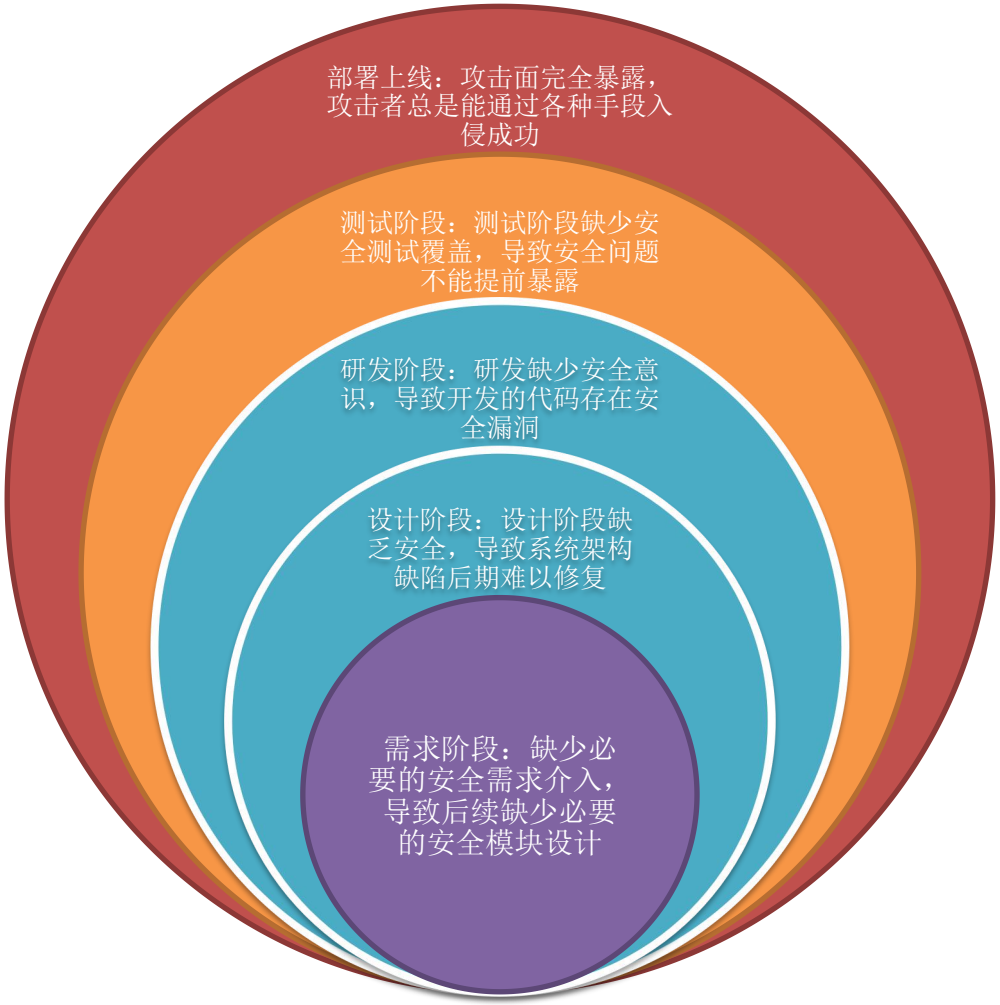
SDL如何介入研发流程

项目研发生命周期：



项目周期中的安全风险

项目研发生命周期中安全风险暴露模型：



项目周期中的安全风险


任意密码重置，导致主站及数十分站getshell RMB
订单遍历，查看全部用户敏感信息
所属项目：互联网漏洞与威胁情报 提交者：匿名者 公开时间：2016-04-17
上营业厅存在漏洞，泄露订单，用户
所属项目：互联网漏洞与威胁情报 提交者：匿名者 公开时间：2016-04-17
存在漏洞导致泄露用户订单号、航班信息、姓名、身份证号码、联系电话等
所属项目：互联网漏洞与威胁情报 提交者：匿名者 公开时间：2016-04-14
（泄漏十多万订单详细信息/五万用户详细信息/包括银行帐号转账情况等）
所属项目：互联网漏洞与威胁情报 提交者：匿名者 公开时间：2016-04-13
某站配置不当导致订单信息泄露
所属项目：互联网漏洞与威胁情报 提交者：xxzapml 公开时间：2016-04-10
大量保险订单信息 RMB
所属项目：漏洞盒子挖洞联盟赛 提交者：匿名者 公开时间：2016-04-01
APP所有功能未做权限验证，可以访问40W用户全部信息，包括手机、地址、订单 RMB
所属项目：漏洞盒子挖洞联盟赛 提交者：匿名者 公开时间：2016-03-28
查看详情

项目周期中的安全风险


搜索框存在多处XSS漏洞
所属项目：互联网漏洞与威胁情报 提交者：K4ST 公开时间：2016-02-17
查看详情
言网存在xss漏洞可伪造cookies进入后台
所属项目：互联网漏洞与威胁情报 提交者：匿名者 公开时间：2016-02-10
查看详情
上传未限制导致xss
查看详情
专家指出，这次针对新浪微博的攻击事件在短时间内突然爆发，是源于新浪微博的某些页面存在XSS跨站攻击漏洞。针对社交网站的XSS漏洞曾经多次发生，国外的Facebook、Twitter，国内的人人网、开心网都曾遭遇类似攻击。专家建议一般网民谨
所属项目：互联网漏洞与威胁情报 提交者：匿名者 公开时间：2016-01-31
查看详情
xss漏洞
所属项目：互联网漏洞与威胁情报 提交者：匿名者 公开时间：2016-01-29
查看详情
型XSS
所属项目：互联网漏洞与威胁情报 提交者：匿名者 公开时间：2016-01-28
查看详情
网络文化管理系统存在SQL注入漏洞（影响全省各市网吧监管系统）

项目周期中的安全风险

ipMyAdmin配置不当导致越权访问涉及多个库

所属项目：互联网漏洞与威胁情报　提交者：匿名者　公开时间：2016-04-20

招生系统配置不当导致4000名考生信息可被查看修改

所属项目：互联网漏洞与威胁情报　提交者：匿名者　公开时间：2016-04-14

天河学院服务器配置不当导致服务器沦陷

所属项目：互联网漏洞与威胁情报　提交者：红颜小妖　公开时间：2016-04-13

站配置不当导致订单信息泄露

所属项目：互联网漏洞与威胁情报　提交者：xxzapml　公开时间：2016-04-10

站点配置不当导致服务器沦陷

所属项目：互联网漏洞与威胁情报　提交者：F1uYu4n　公开时间：2016-04-10

站点配置不当可直接进入后台

所属项目：互联网漏洞与威胁情报　提交者：裤衩　公开时间：2016-04-10

站配置不当可至全站源代码信息泄露

所属项目：互联网漏洞与威胁情报　提交者：时空蚂蚁　公开时间：2016-04-08

据采集与监控系统配置不当导致信息泄露

所属项目：互联网漏洞与威胁情报　提交者：裤衩　公开时间：2016-04-08

项目周期中的安全风险

[redacted]处弱口令漏洞，泄漏敏感信息，并可对内部员工流量抓包 RMB

所属项目：互联网漏洞与威胁情报　提交者：F1uYu4n　公开时间：2016-04-20

查看详情

[redacted]的CEO亲密接触的

非洲农业不发达，必须要有金坷垃 日本资源太缺乏，种地要有金坷...github手抖一下 每次手抖都有新发现 这次，我发现了一个光头吴克（误），他说他今年六岁，全家都很喜欢超威蓝猫 https://github.com/liuzhiwang/Test/blob/625a17b8e7dace22b18b10de76497bb3ae5ff285/omega-rds1/target/classes/common_config.properties 乌云审核帮忙打个码 code 区域 #邮箱用户名和密码，用于发送邮件 smtp.username = omega@nongfadai.com smtp.password = CoolTeam2)!% smtp.sender.displayName = Omeg...

提交日期：2016-04-14　作者：路人甲

[redacted]安卓客户端源码泄露（2016年1月的版本）

已知最新版为3月的，但这个也不老 欢迎哔哩哔哩的大基佬...神奇的github code 区域https://github.com/summerrc/bilibili 果断打包下载啊。 由于在别的电脑上没java和其他，这里我就不演示了。 ...神奇的github code 区域https://github.com/summerrc/bilibili 果断打包下载啊。 由于在别的电脑上没java和其他，这里我就不演示了。 ...把泄露代码的人带到小黑屋，叫比利肛了。

提交日期：2016-04-08　作者：路人甲

[redacted]维不当泄露内部邮箱一枚

rt...https://github.com/Wanghaoran/hyatt_food/blob/7d3ac99c494d975fd1efa28a61c1a143fb64257a/application/controllers/welcome.php code 区域$content = file_get_contents($this->config->base_url() . 'static/mail/email.html'); $this->load->library('sendemail'); $this -> sendemail -> setServer("smtp.exmail.qq.com", "yuexiangjia.hyatt@uniquead.cn", "cxwj9876", 465, true); //设置smtp...

提交日期：2016-04-07　作者：路人甲

[redacted]点弱口令，导致合同泄露

所属项目：互联网漏洞与威胁情报　提交者：匿名者　公开时间：2016-04-17

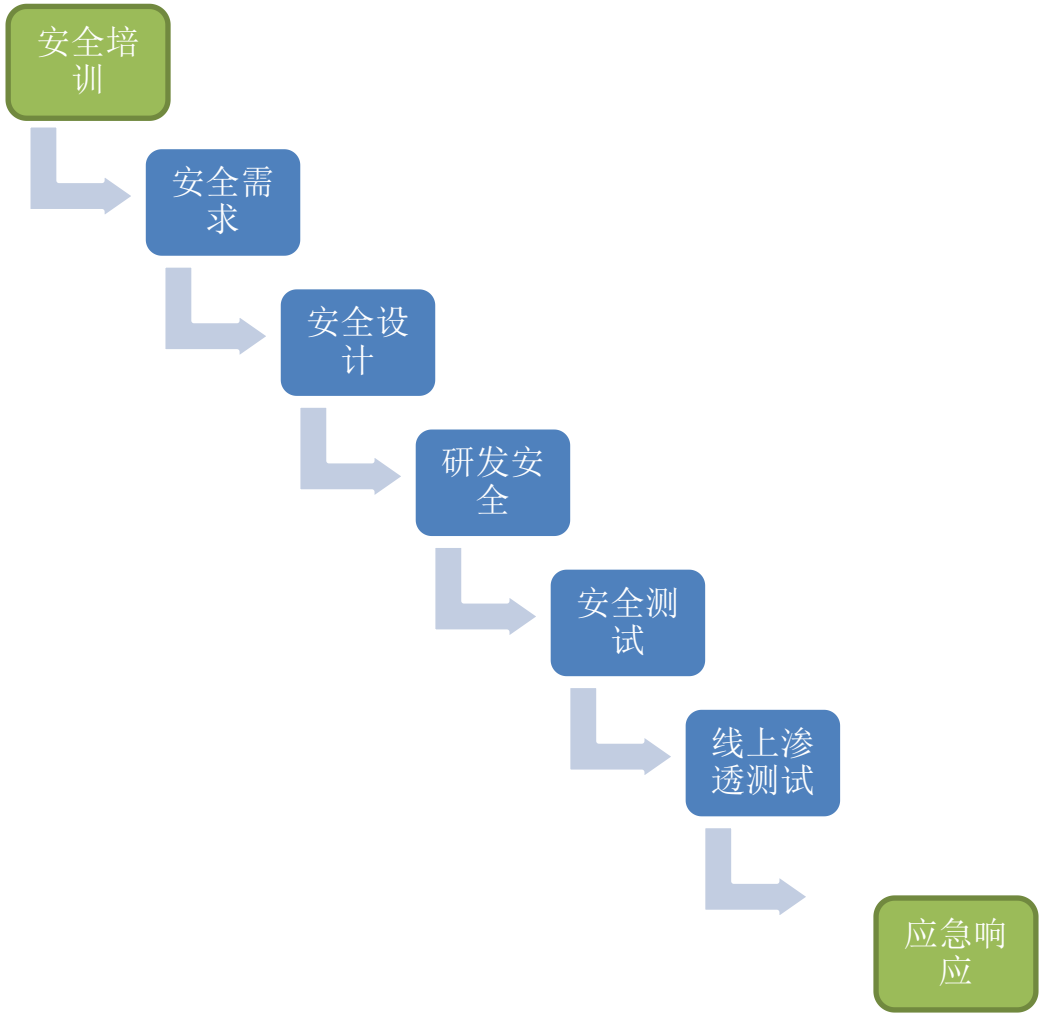
查看详情

大纲

- SDL简介
- 项目生命周期中的安全风险
- SDL如何介入研发流程
- SDL的最佳实践
- Q&A

SDL如何介入研发流程

SDL的工作流程：



大纲

- SDL简介
- 项目生命周期中的安全风险
- SDL简介
- SDL的最佳实践
- Q&A

SDL的最佳实践

安全培训

- 实践方案：
  - 代码安全管理
  - 研发人员信息安全管理
  - 安全编码规范推行
  - 服务器配置安全规范培训

SDL的最佳实践

安全培训

- 解决的问题：
  - 建立项目人员信息安全意识
  - 安全编码规范实施，提升研发同学的编码安全性
  - 安全规范实施文档，解决了运维同学部署的安全知识欠缺问题。

安全需求、设计

- 实践方案：
  - 认证安全设计解决方案
  - 权限安全设计解决方案
  - 关键操作安全设计方案：
    - 支付操作
    - 密码重置操作

SDL的最佳实践

安全设计

- 解决的问题：
  - 统一解决方案，解决一处漏，处处漏问题
  - 解决了前期架构缺陷，导致后期修复成本过大，无限延期问题
  - 专业化的安全设计，规避常见的逻辑缺陷

SDL的最佳实践

研发安全

- 实践方案：
  - 梳理语言及框架的安全缺陷
    - 语言特性引起的问题
    - 框架缺陷
  - 统一的安全封装代码库
  - 静态代码分析工具
    - 自研代码分析工具
    - 商业产品的使用

SDL的最佳实践

研发安全

- 解决问题：
  - 自动化的代码安全转换，提升研发安全质量
  - 安全的代码库，保证模块防护的正确性
  - 研发过程中的代码安全检查，避免上线后才发现问题

SDL的最佳实践

安全测试

- 实践方案
  - 黑盒安全扫描系统进行检测
    - 安全自动化扫描平台
    - 浏览器扩展
  - 白盒代码安全审计
    - 《高级PHP应用程序漏洞审核技术》

SDL的最佳实践

安全测试

- 解决问题
  - 上线前的全面体检
    - 覆盖应用层的安全问题
    - 针对基础环境的基本梳理测试

SDL的最佳实践

线上安全评估

- 实践方案：
  - 安全评估面
    - 基础环境的安全评估
    - 应用层的安全评估
    - 信息管理层面的安全评估
  - 安全评估CheckList的推出

SDL的最佳实践

线上安全评估

- 解决问题
  - 完全模拟黑客，提前发现黑客可能的攻击路径，并进行防御

SDL的最佳实践

应急响应

- 实践方案：
  - 安全资产梳理及情报收集机制
  - 安全产品部署
    - WAF
    - 自动化扫描
    - 入侵检测系统

SDL的最佳实践

应急响应

- 解决问题：
  - 第一时间感知漏洞，并进行防御实施，规避漏洞给业务带来的影响
  - 能够第一时间针对受影响的资产进行安全防御。

Q & A

Geekbang 极客邦科技 InfoQ

THANKS!