

深入研发流程的安全建设

乌云 章华鹏

QCon

2016.10.20~22

上海·宝华万豪酒店

全球软件开发大会 2016

[上海站]



购票热线: 010-64738142

会务咨询: qcon@cn.infoq.com

赞助咨询: sponsor@cn.infoq.com

议题提交: speakers@cn.infoq.com

在线咨询(QQ): 1173834688

团·购·享·受·更·多·优·惠

7折

优惠(截至06月21日)
现在报名, 立省2040元/张

关于我

- 独立思考的白帽子黑客，boooooom
- 前百度高级安全工程师
- 乌云，唐朝安全巡航产品负责人

写在前面

- 讨论企业(研发)安全之前需要的思考
 - 企业安全的核心是数据安全
 - 深入研发流程了解数据流，剖析风险(新技术探索)
 - 问题推动安全建设，解决风险

内容概要

- 项目研发的核心五个流程
- 全研发流程中的安全风险
- 深入研发流程的安全建设

核心五个流程



项目需求&安全风险

缺陷编号：**WooYun-2015-105814**

漏洞标题：WiFi网络安全之万能钥匙类产品导致企业用户边界突破可被渗透

相关厂商：**itcast.cn**

漏洞作者：**末笔、**

提交时间：2015-04-04 16:32

公开时间：2015-04-13 16:58

漏洞类型：内部绝密信息泄漏

漏洞概要

关注数(86) [关注](#)

缺陷编号：**WooYun-2015-98435**

漏洞标题：WiFi万能钥匙客户端泄露用户wifi密码 💰

相关厂商：**WiFi万能钥匙**

漏洞作者：**hqdvista**

提交时间：2015-02-26 16:56

公开时间：2015-05-27 18:52

漏洞类型：用户敏感数据泄漏

危害等级：中

自评Rank：10

漏洞状态：厂商已经确认

漏洞来源：<http://www.wooyun.org>，如有疑问或需要帮助请联系 help@wooyun.org

Tags标签：**android安全** **手机软件安全**

分享漏洞： 分享到     0

11人收藏

项目需求&安全风险

- 需求的本质是为了解决问题创造价值
- 需求本身是没有任何安全风险的
- 当前需求的核心风险点在哪？
- 安全需要介入产品的需求评审阶段

需求潜在风险点分析

- 互联网产品的核心是数据安全
- 核心数据是什么？
- 当前需求条件下，核心数据是否安全？

系统设计

- 好的系统设计方案
 - 实现产品需求
 - 规避核心数据的风险

系统设计缺陷一

漏洞概要

关注数(86) [关注](#)

缺陷编号：[WooYun-2015-98435](#)

漏洞标题：WiFi万能钥匙客户端泄露用户wifi密码 💰

相关厂商：[WiFi万能钥匙](#)

漏洞作者：[hqdvista](#)

提交时间：2015-02-26 16:56

公开时间：2015-05-27 18:52

漏洞类型：用户敏感数据泄漏

危害等级：中

自评Rank：10

漏洞状态：厂商已经确认

漏洞来源：<http://www.wooyun.org>，如有疑问或需要帮助请联系 help@wooyun.org

Tags标签：[android安全](#) [手机软件安全](#)

分享漏洞：[分享到](#) [☆](#) [🔗](#) [🐾](#)

缺陷编号：[WooYun-2015-99268](#)

漏洞标题：WIFI万能钥匙密码查询接口算法破解（可无限查询用户AP明文密码） ⚡ 💰💰

相关厂商：[WiFi万能钥匙](#)

漏洞作者：[路人甲](#)

提交时间：2015-03-03 16:59

公开时间：2015-06-04 12:58

漏洞类型：敏感信息泄露

危害等级：高

自评Rank：18

系统设计缺陷一

- 移动端设计缺陷（数据交互弱加密）

系统设计缺陷二

缺陷编号：**WooYun-2016-179969**

漏洞标题：腾讯QQ邮箱开发平台的SSRF可扫描内网

相关厂商：**腾讯**

漏洞作者：**李长歌**

提交时间：2016-03-02 08:59

公开时间：2016-03-02 12:41

漏洞类型：未授权访问/权限绕过

缺陷编号：**WooYun-2012-15881**

漏洞标题：百度网盘极速秒传设计缺陷

相关厂商：**百度**

漏洞作者：**lotus**

提交时间：2012-12-11 16:19

公开时间：2013-01-25 16:19

漏洞类型：设计缺陷/逻辑错误

MD5碰撞问题

系统设计缺陷二

- **SSRF**（可跨网络边界攻击内网）
- 算法缺陷：**MD5 碰撞问题**

系统设计缺陷三

缺陷编号：**WooYun-2015-109734**

漏洞标题：**龙贷某站未授权访问+命令执行导致十几亿资金可随意操作**

相关厂商：**龙贷**

漏洞作者：**杀器王子** ▼

提交时间：2015-04-24 20:43

公开时间：2015-06-08 18:20

漏洞类型：命令执行

缺陷编号：**WooYun-2015-146475**

漏洞标题：**国联证券某站点sql注入到webshell**

相关厂商：**国联证券**

漏洞作者：**路人甲**

提交时间：2015-10-13 16:32

公开时间：2015-12-02 13:48

漏洞类型：SQL注射漏洞

系统设计缺陷三

- 授权问题（敏感系统可任意未授权访问）
- 网站架构设计（站库未分离）

更多关于系统设计缺陷

- 撞库问题
- 任意用户密码重置
- 第三方开源引用及服务的使用（openssl, struts2, redis）
- 心脏滴血、struts2命令执行、redis getshell

系统设计阶段的风险

- 基础：安全规范&执行
 - 尽量避免使用第三方高危应用
 - 内部系统不得对外未授权访问
- 深入：系统设计阶段安全评估介入
 - 围绕核心数据流向的风险挖掘

“研发”出来的漏洞一

缺陷编号：**WooYun-2016-185510**

漏洞标题：**官方APP存在SQL注入（涉及100W+用户信息/100W+订单数据）**

相关厂商：**ai.com**

漏洞作者：**路人甲**

提交时间：2016-03-16 23:03

公开时间：2016-04-30 23:03

漏洞类型：SQL注射漏洞

危害等级：高

当前位置：[WooYun](#) >> [搜索结果](#)

搜索关键字：**sql注入** （共 19584 条纪录） [将未公开漏洞纳入搜索结果](#) **19584条记录**

[北京网元圣唐娱乐科技有限公司存在sql注入](#)

北京网元圣唐娱乐科技有限公司存在**sql注入**...漏洞地址：code 区域<http://cs.gamebar.com/faq.php?id=1> 用sqlmap跑 数
基本都可以跑出来了 ...漏洞地址：code 区域<http://cs.gamebar.com/faq.php?id=1> 用sqlmap跑 数据库：系统库的表：表
过滤

提交日期：2016-03-16 作者：路人甲

“研发”出来的漏洞一

- SQL注入

```
8  mysql_select_db("my_db", $con);  
9  
10 $result = mysql_query("SELECT * FROM Persons where id = " . $_GET['id']);  
11
```

更多“研发”出来的问题

- 代码/命令执行
- 本地/远程文件包含
- 任意文件读取
- XSS 跨站漏洞
- XXE 漏洞
- 任意文件上传导致代码执行

更多“研发”出来的问题

应用程序/应用漏洞： XSS 跨站脚本攻击 CSRF SQL注射漏洞 任意文件遍历/下载 文件上传导致任意代码执行 文件包含 命令执行 应用配置错误
敏感信息泄露 未授权访问/权限绕过 后台弱口令 设计缺陷/逻辑错误 URL跳转

提交日期	漏洞标题	评论 / 关注	作者
2016-03-16	西南医科大学三处注入+四处敏感信息泄露 (包括身份证)	0/0	路人甲
2016-03-16	超星某站存储XSS	0/0	路人甲
2016-03-16	长城汽车某站存在SQL注入漏洞	0/0	路人甲
2016-03-16	雷神科技主站存在SQL注入漏洞 (附脚本)	0/0	路人甲
2016-03-16	车易拍官方APP存在SQL注入 (涉及100W+用户信息/100W+订单数据)	2/8	路人甲
2016-03-16	好未来 (前学而思集团) 旗下某站点系统未授权访问导致命令执行/涉及多个系统	0/1	路人甲
2016-03-16	百视通某站存在SQL注入漏洞	0/0	路人甲
2016-03-16	赶集网某站SQL注入	0/9	路人甲
2016-03-16	11对战平台用户身份信息遍历&用户密码重置	4/10	路人甲
2016-03-16	武汉大学某处SQL注入漏洞	0/0	路人甲
2016-03-16	重庆大学某站存在SQL注入漏洞	0/0	路人甲
2016-03-16	茨城县筑西市公式ホームページ存在SQL注入	0/0	路人甲
2016-03-16	娇妍商城某处存在sql注入一枚	0/0	bigcow
2016-03-16	新輝国際株式会社网站存在SQL注入	0/0	路人甲
2016-03-16	苏宁易购某站SQL注入 (dba权限)	0/0	路人甲
2016-03-16	暨南大学医学院SQL注入漏洞	0/0	路人甲
2016-03-17	某党员管理平台存在漏洞#大量数据泄漏	0/0	狼牙月
2016-03-16	トロッコ列車 嵯峨野観光鉄道网站存在SQL注入	0/0	路人甲
2016-03-17	某省住房保障网一枚SQL注射漏洞	0/0	Pzacke...
2016-03-16	国信证券某站任意文件上传Getshell	2/9	路人甲

62155个真实漏洞

共 62155 条纪录, 3108 页 [1](#) [2](#) [3](#) [4](#) [5](#)

研发代码风险

- 基础：安全编码规范
- 自动化审计：运行&编译时高危函数风险检查
 - 数据库相关操作：sql 注入
 - 执行系统命令&eval() 检查
 - 文件上传move_uploaded_file()等
- 使用统一封装的安全方法
 - 好的开发框架

系统(安全)测试

- 安全建设的核心是问题推动！！！！
- 测试阶段本身就是针对之前阶段的一个安全检查
 - 黑盒安全测试
 - 白盒代码审计

黑盒安全测试

- 人工渗透测试
 - 众测
- 自动化测试(☆)
 - 盲测(动态spider+通用漏洞检测)
 - 透明测试(基于业务全流量的风险探测)

黑盒安全测试的未来

- 全业务逻辑(数据流)遍历
- 业务逻辑解析（让机器读懂业务）
- 基于业务逻辑的智能安全测试(唐朝安全巡航引擎)
- 像黑客一样思考

全业务逻辑遍历

- 主动的业务逻辑抓取遍历
- 被动的业务流量解析

业务逻辑解析

- 通过一个HTTP(s)请求包去理解业务
- `http://order.ny.cn/storeOrderDetail.htm?orderNo=15030801994800`

order.ny.cn/storeOrderDetail.htm?orderNo=15030801994800

卖家订单管理 > 订单详情

当前订单状态：买家申请退款成功

退款详情

订单号：15030801994800 下单时间：2015-03-08 23:19:35

买家信息	物流信息
昵称： lushaohuan	收货人： 卢少欢
真实姓名： lushaohuan	收货地址： 广东省肇庆市

智能安全测试

- 机器读懂这个HTTP请求是一个订单访问操作
- 订单访问会出现什么风险？
- 越权？SQL注入？

运维上线风险一

缺陷编号：**WooYun-2015-93382**

漏洞标题：**新浪**某处svn信息泄露到getshell到漫游内网，导致微博用户信息泄露(老曹竟然关注xxx)

相关厂商：**新浪**

漏洞作者：**booooooom** ▼

提交时间：2015-01-22 16:31

公开时间：2015-03-08 16:32

漏洞类型：敏感信息泄露

危害等级：高

自评Rank：20

运维上线风险一

- 上线流程不规范，敏感文件未删除
 - /.svn/
 - /.git/
 - xx.bak
 - xx.zip

运维上线风险二

缺陷编号：WooYun-2015-92151

漏洞标题：腾讯某服务配置不当导致包括数据库文件、密码hash等任意文件可下载

相关厂商：腾讯

漏洞作者：booooooom

提交时间：2015-01-16 08:53

公开时间：2015-03-02 08:54

漏洞类型：系统/服务运维配置不当

危害等级：高

自评Rank：20

详细说明：

code 区域

```
[root@localhost ~]# curl 176.243.8003/etc/passwd

root:x:0:0:root:/root:/usr/local/bash_4.1/bin/bash

bin:x:1:1:bin:/bin:/sbin/nologin

daemon:x:2:2:daemon:/sbin:/sbin/nologin

adm:x:3:4:adm:/var/adm:/sbin/nologin

lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin

sync:x:5:0:sync:/sbin:/bin/sync

shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown

halt:x:7:0:halt:/sbin:/sbin/halt

mail:x:8:12:mail:/var/spool/mail:/sbin/nologin

uucp:x:10:14:uucp:/var/spool/uucp:/sbin/nologin
```


运维上线风险二

- webserver 配置风险
- 各种服务配置：高危服务对外（ssh, mysql...）

运维风险控制

- 基础规范
 - 系统&服务配置规范
 - 自动化上线流程
- 全网资产管理（确定潜在风险目标）
- 合规性检测
 - 外网IP端口扫描
 - 服务配置弱点扫描

谢谢大家

