# 苏宁安全生态之眼

苏宁攻防实验室
黄宙

# 个人经历

黄宙 ID:tombook

# 目 录


苏宁安全生态介绍

索伦之眼架构与技术概况

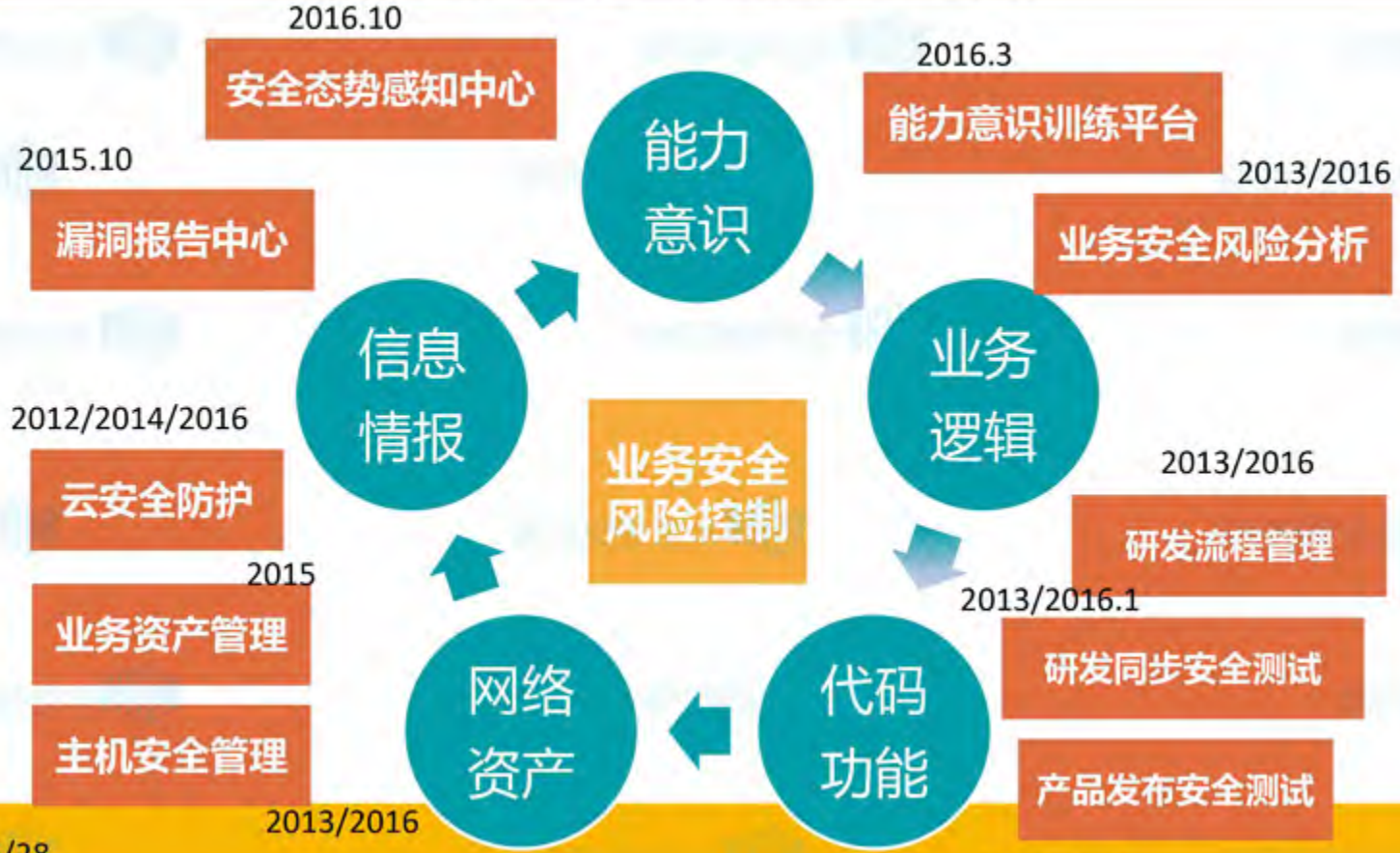
索伦之眼功能与技术实现

索伦之眼建设中的曲折经历

索伦之眼未来规划

# 前次回顾

《电商云安全成长之道》 2015.11 GITC（北京）



# 一、苏宁安全生态介绍

# 项目代号：索伦之眼

# 目 录


苏宁安全生态介绍

索伦之眼架构与技术概况

索伦之眼功能与技术实现

索伦之眼建设中的曲折经历

索伦之眼未来规划

# 理论基础

## 基于日志的挖掘安全未知漏洞的方法和系统

申请号：201510026904.6 申请日：2015-01-19

**摘要：**本发明提供一种基于日志的挖掘安全未知漏洞的方法和系统。该方法包括步骤：S1、网站服务器根据用户请求资源，产生用户访问日志；S2、对所产生的用户访问日志进行访问；S3、判断服务器域名和用户请求资源信息是否属于分析清洗的范围，若是，则对所述服务器域名和用户请求资源信息进行分析清洗；S4、对所述服务器域名和用户请求资源信息进行未知漏洞分析与挖掘。本发明的技术方案可以通过对日志数据正向过滤与安全漏洞攻击特征逆向排除，实现挖掘利用漏洞攻击发现，降低安全漏洞挖掘成本，提高了挖掘未知漏洞效率。

**申请人：** 苏宁云商集团股份有限公司

**地址：** 210042 江苏省南京市玄武区苏宁大道1号15楼

**发明(设计)人：** 黄宙

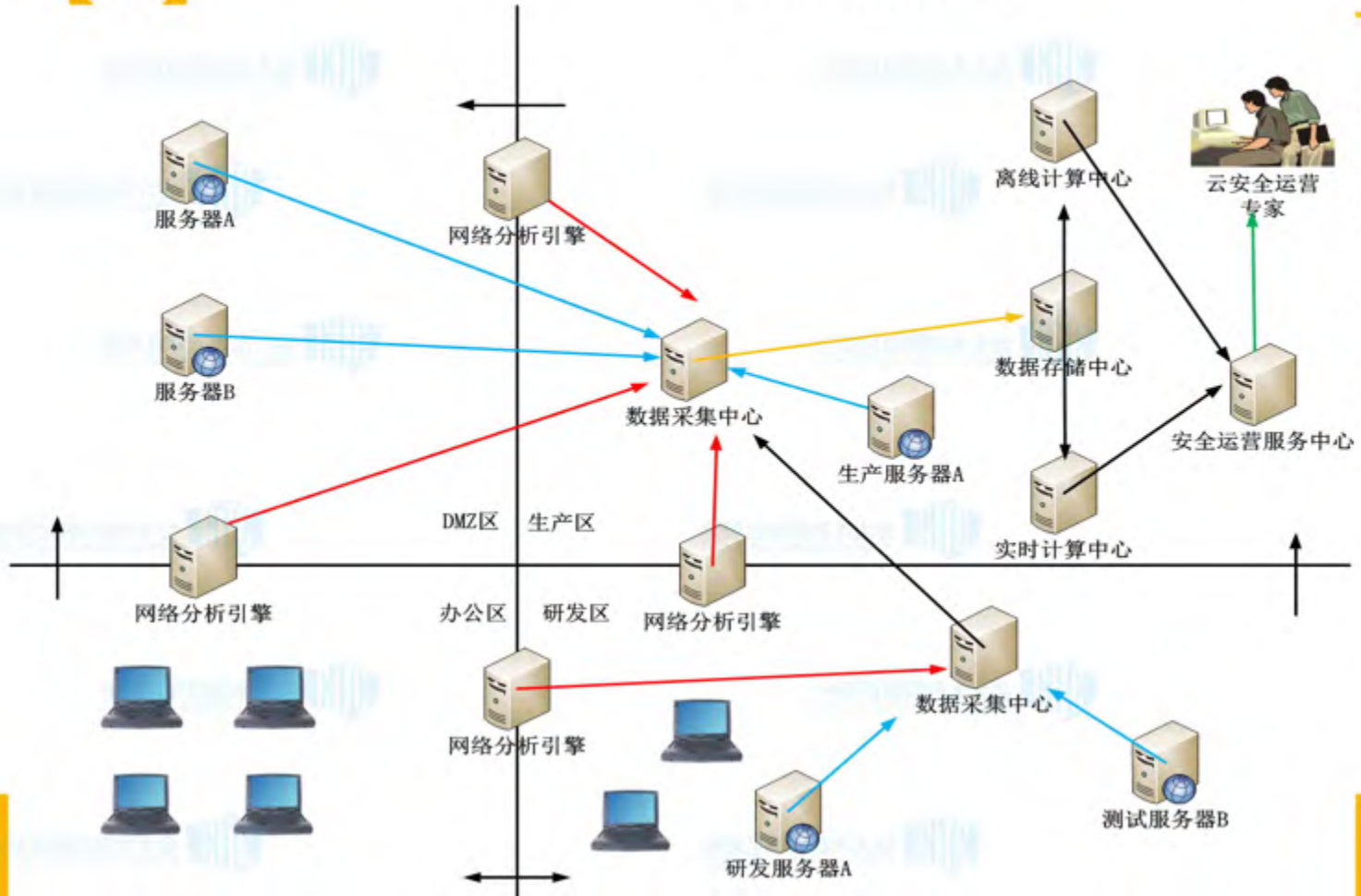
**主分类号：** H04L29/06(2006.01)I

**分类号：** H04L29/06(2006.01)I H04L12/26(2006.01)I

# 平台架构

- Spark
- Spark Streaming
- Hbase
- Flume
- Kafka
- Mysql
- Nginx
- Redis
- Sqoop
- … …

# 适应场景路线




开放云服务

私有云服务

公有云服务

混合云服务

# 目 录


苏宁安全生态介绍

索伦之眼架构与技术概况

索伦之眼功能与技术实现

索伦之眼建设中的曲折经历

索伦之眼未来规划

# 苏宁安全生态“十戒”

# 网络安全——网络之戒

攻击预警

攻击 | 规则库

规则自动发送 勾选后产生的规则会自动的发送给waf平台

发送

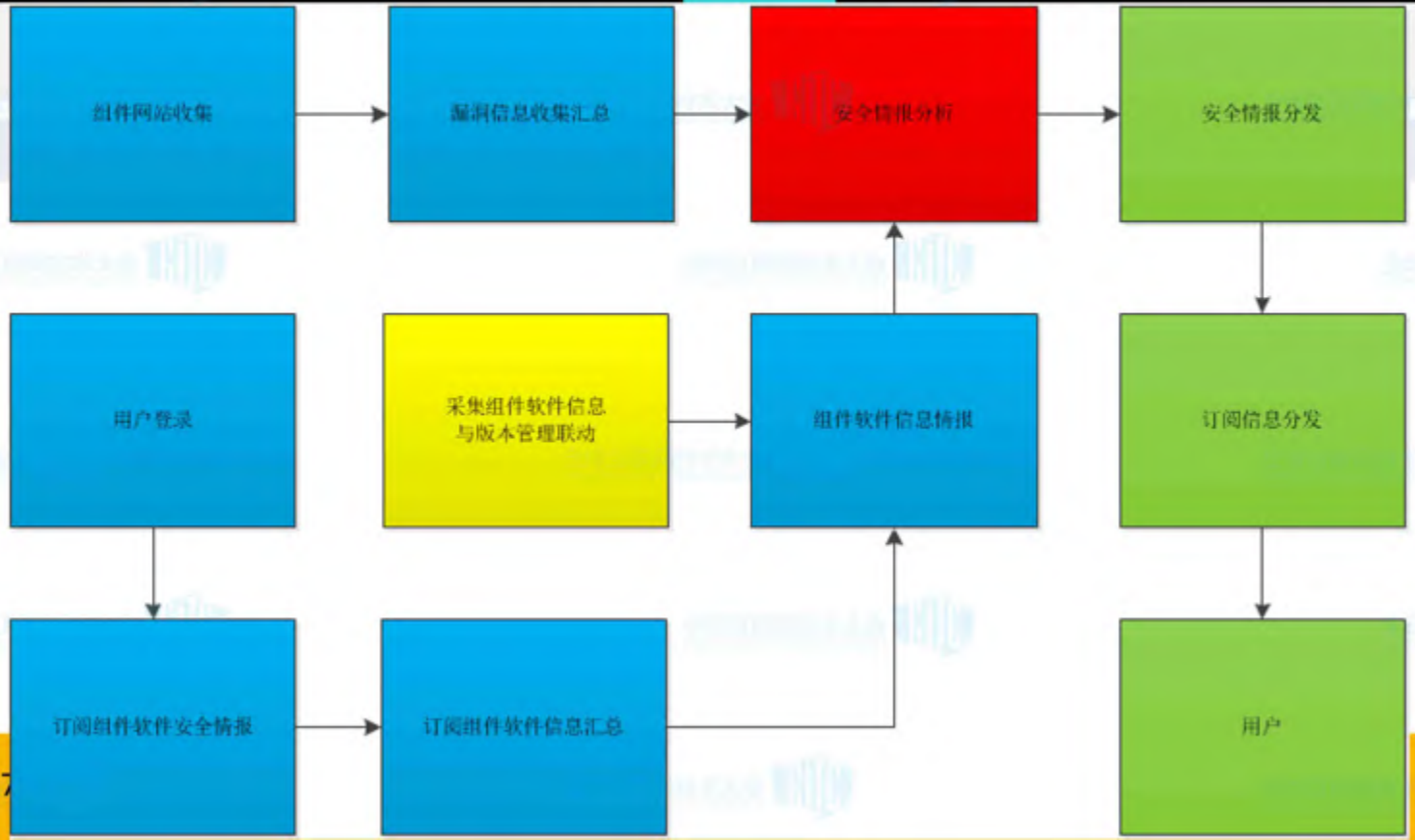
| | 规则序号 | 拦截IP | 拦截时段 | 域名 | 发送状态 |
|---|---|---|---|---|---|
| ☐ | 1 | 112.80.230.69 | 9:00 -21:00 | 58.221.78.105 | 未发送 |

| 序号 | 检测区域 | 规则总数 | 命中数 | 未命中数 |
|---|---|---|---|---|
| 1 | engine-10.101.250.175 | 9 | 0 | 9 |

# 应用安全——应用之戒

主机安全 | 网络安全 | 移动安全 | 业务安全 | 应用安全 | 攻击溯源 | 主机管理 | 系统管理

弱口令



主机安全 网络安全 移动安全 业务安全 应用安全 攻击溯源 主机管理 系统管理

场景列表 > 0001

请输入URI关键字过滤

| 规则ID | 域名 | URL | 规则 | 状态 | 规则属性 | 准确性 | 附加规 |
|---|---|---|---|---|---|---|---|
| 7001000164 | my.suning.com | /wap/addrInput0.do | 参数名:addrNum, 参数类型:A... | 停用 | 正常 异常 | 精确 模糊 | 编辑 |
| 7001000165 | my.suning.com | /ajax/getCommonHorizontalMenu.do | 参数名:_t,参数类型:A,最大长度... | 停用 | 正常 异常 | 精确 模糊 | 编辑 |
| 7001000166 | my.suning.com | /ajax/getCommonVerticalMenu.do | 参数名:_t,参数类型:A,最大长度... | 停用 | 正常 异常 | 精确 模糊 | 编辑 |
| 7001000167 | my.suning.com | /wap/addrInput0.do | 参数名:addrNum, | 停用 | 正常 异常 | 精确 模糊 | 编辑 |

948 /popupLoginSuccess 2017-06-08

查询参数: service=https://aq.s...

异常报告: [redacted]异常，正常概率:0.000000

引用: http://m.suning.com/product/0000000000/123129118.html

# 移动安全——移动之戒

HelloWorld

版本号：1.0
大小：0.27
包名：com.app.helloworld141
检测时间：2017-06-07 17:23:58.0

漏洞检测(374)

| 高危漏洞 | 中危漏洞 | 低危漏洞 |
| --- | --- | --- |
| 次数 1 | 次数 1 | 次数 0 |

| 漏洞详情 | 风险等级 | 修复建议 | 操作 |
| --- | --- | --- | --- |
| 应用没有被安全加固，攻击者可以利用重打包等手段修改程序的原始逻辑和内容，并上传仿冒app到第三方应用市场，欺骗用户。 | 高危 | 使用苏宁安全加固方案的防反编译功能，防止应用被反编译。 | 收起 |
| 漏洞位置：<br>1. 应用没有做安全加固，存在安全风险。 | | | |
| Android 2.1以上的系统可为App提供应用程序数据的备份 | | N/A | |

1 共1页


攻击来源
城市
3235 Beijing
2118 Guangzhou
1930 Hangzhou
1559 Meizhou
1430 Nanjing
1387 Chengdu
1227 Shanghai
1009 Shenzhen
攻击类型
# 攻击类型
32177 CC_Attack
95 XSS_Attack
57 CommExec_Attack
9 FileIn_Attack
4 SQL_Attack
实时攻击列表
攻击时间 攻击者IP 攻击者所在地 被攻击应用IP 攻击类型 攻击端口
00:02:02.353 42.94.66.56 Lanzhou, China dt.suning.com CC_Attack 80
00:02:02.561 112.225.011.122 Qingdao, China passport.suning.com CC_Attack 80
00:02:01.31 140.237.98.68 Yong'an, China reg.suning.com CC_Attack 80
00:02:00.991 122.238.216.240 Wenzhou, China reg.suning.com CC_Attack 80
00:02:00.555 113.250.191.15 Chongqing, China aq.suning.com CC_Attack 80
00:02:00.145 224.285.69.167 Wuhan, China reg.suning.com CC_Attack 80
00:01:59.785 119.0.0.24 Jagdagi, China cart.suning.com CC_Attack 80
00:01:59.471 10.52.145.89 Changsha, China reg.suning.com CC_Attack 80

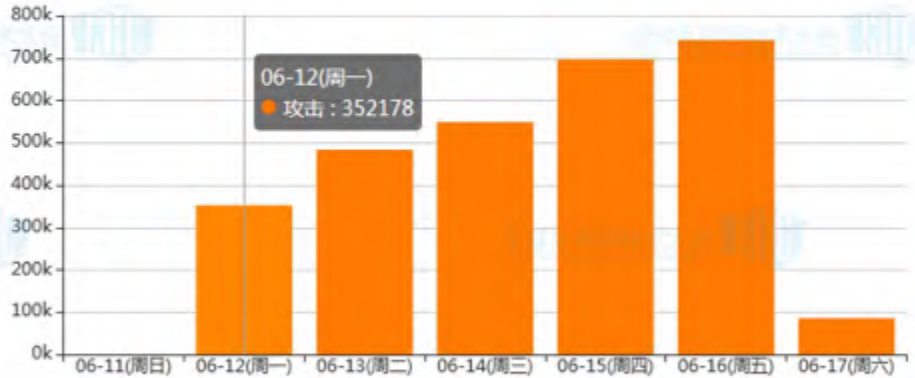
# 主机安全——主机之戒



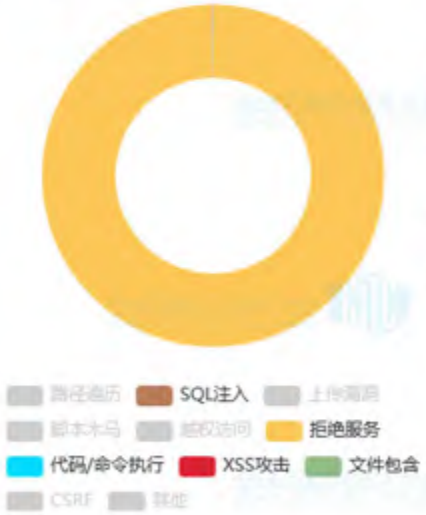
主机监测
任务管理
升级管理

攻击

最近7日应用攻击趋势




最近7日应用攻击类型统计

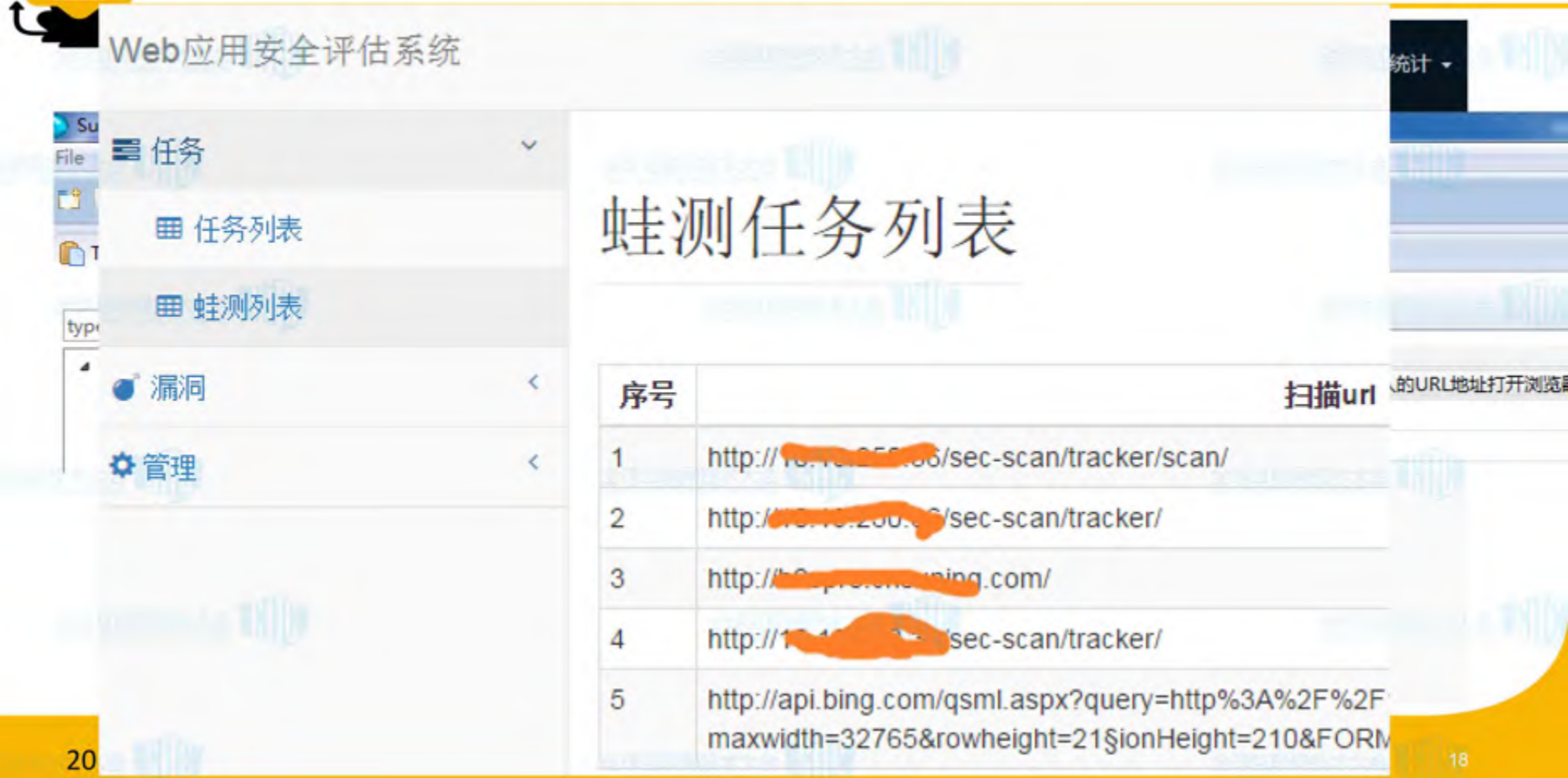



任务
看
看
看
起

类型: 全部(2909612) 其他(0) 木马脚本(0) SQL注入(629) 代码/命令执行(541) 上传漏洞(0) 路径遍历(0) 拒绝服务(2906105) 越权访问(0)
XSS攻击(869) CSRF(0) 文件包含(1468)

2017/6/28

# 研发安全——研发之戒


Web应用安全评估系统
任务
任务列表
蛙测列表
漏洞
管理
蛙测任务列表
序号
扫描url
1
2
3
4
5
http://api.bing.com/qsml.aspx?query=http%3A%2F%2F
maxwidth=32765&rowheight=21§ionHeight=210&FORM

# 安全情报——情报之戒


未知安全分析平台
主机安全
网络安全
移动安全
业务安全
应用安全
攻击溯源
异常访问行为
未知攻击预警
钓鱼网站检测
业务规则管理
首页
钓鱼网站检测
检测功能
待检测内容:
www.taobao.com
提交
清空
检测历史
提交时间
被测域名
安全级别
网站是否备案
访问
2017-06-17 10:38:25
www.taobao.com
未知
2017-06-09 15:01:16
www.suning.com
安全

# 能力安全与管理安全

服务统计

渗透安全工程师 全部 年份 2017 统计类型 按季度 选项 第一季度

完成质量

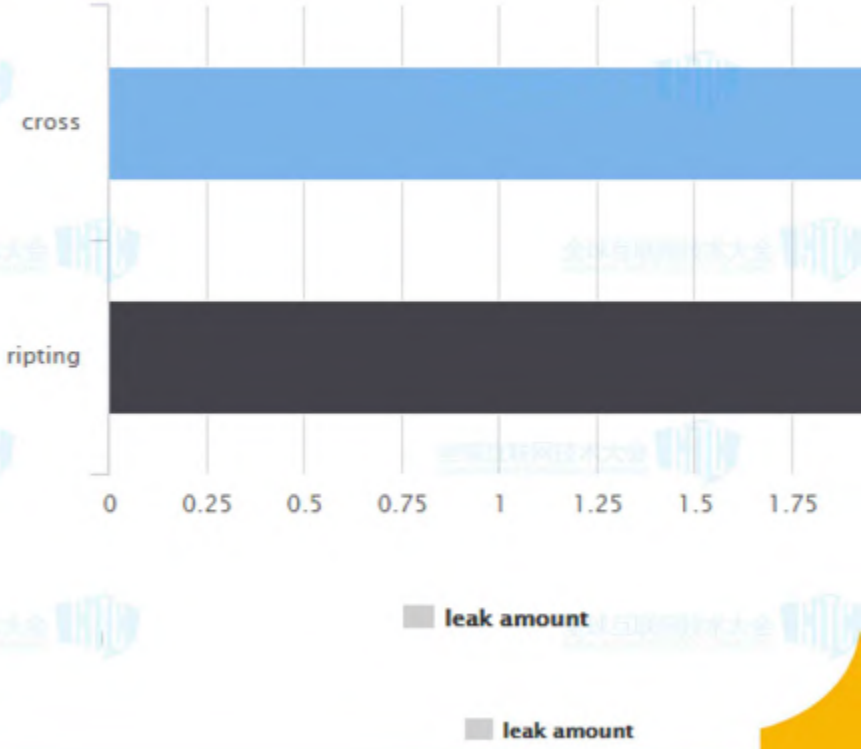

用户评估


| 序号 | 系统名称 | 开始时间 | 完成时间 | 超期情况 | 评分 | 评语 |
|---|---|---|---|---|---|---|
| 1 | 决策分析平台 | 2017-03-01 00:00:00 | 2017-03-11 00:00:00 | 正常 | 5 | |
| 2 | [redacted]红包系统 | 2017-01-07 00:00:00 | 2017-01-09 00:00:00 | 正常 | 5 | 好 |
| 3 | snfs | 2017-02-15 00:00:00 | 2017-02-18 00:00:00 | 正常 | 5 | |

高危排行

全站任务


我的任务



# 安全生态与功能模块

1. 实现企业安全生态闭环
2. 适应业务安全需要的能力

# 目 录


苏宁安全生态介绍

索伦之眼架构与技术概况

索伦之眼功能与技术实现

索伦之眼建设中的曲折经历

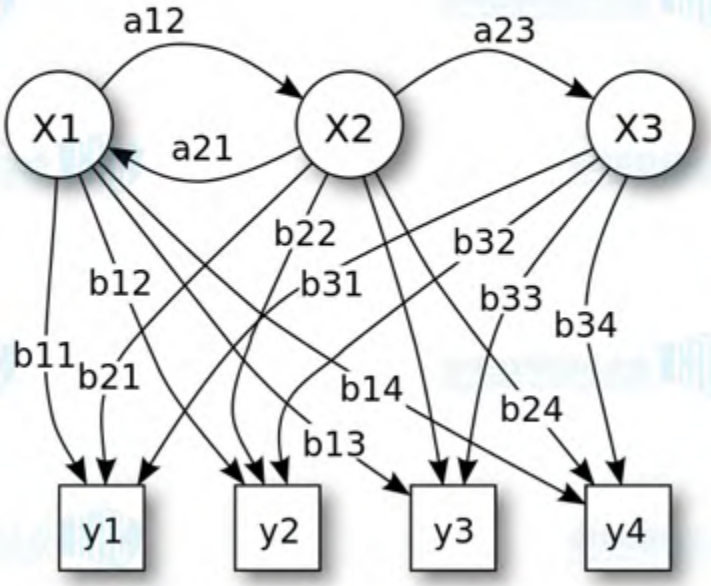
索伦之眼未来规划

# 到底谁做URL跳转

- Apache VS 负载均衡
  - Apache，rewrite_module ，设置重写URL跳转
  - 负载均衡，设置解析URL跳转

# 安全经验与算法（HMM）

隐马尔可夫模型
Hidden Markov Model




**说了很多，往往一句话解决问题。**

**XX，你说的方法，有点像XX模型？**

# 规则训练与修改

URL: order.suning.com /mobile/v1/onlineOrder/queryOrd

属性 1

参数名称： catalogId 类型: 纯数字 最小长度: 5 最大长度: 5

属性 2

参数名称： catalogId 类型: 纯数字 最小长度: 1 最大长度: 1

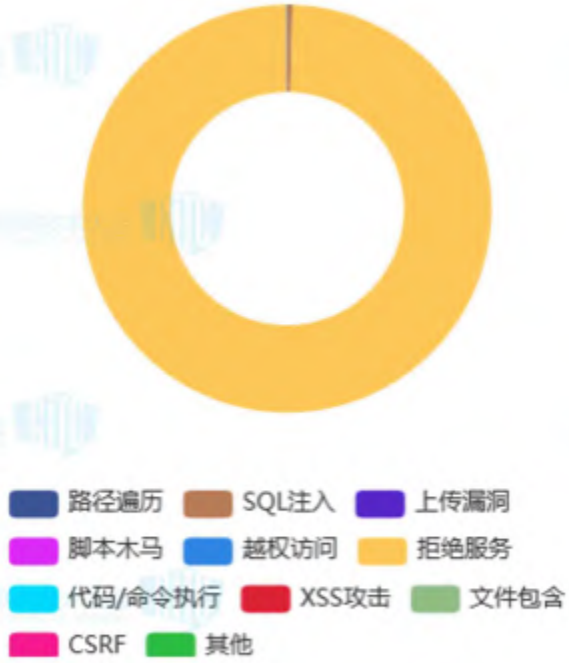
属性 3

参数名称： catalogId 类型: 纯小写字母 最小长度: 3 最大长度: 3

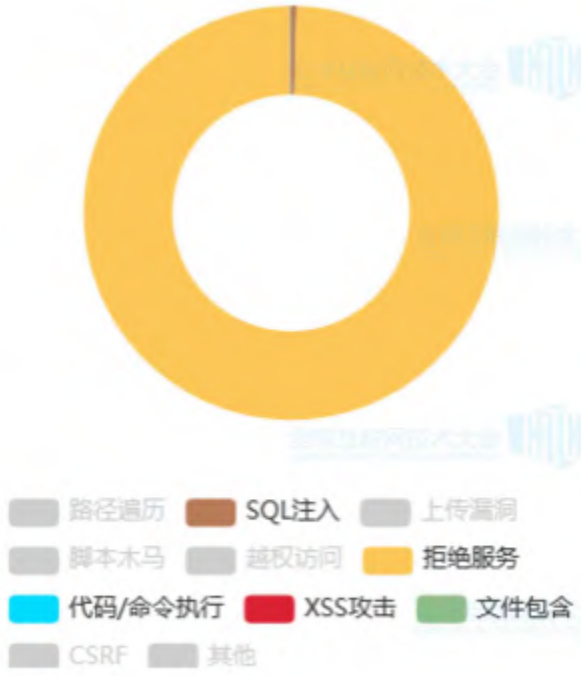
+ 增加属性

# 到底有多少种攻击

最近7日应用攻击类型统计




最近7日应用攻击类型统计



# 目 录


苏宁安全生态介绍

索伦之眼架构与技术概况

索伦之眼功能与技术实现

索伦之眼建设中的曲折经历

索伦之眼未来规划

# 五、索伦之眼未来规划


主机安全
网络安全
移动安全
业务安全
应用安全
攻击溯源
主机管理
系统管理
攻击预警
攻击
规则库
规则自动发送
规则序号
拦截IP
拦截时段
域名
1
112.80.230.69
9:00 -21:00

# 感谢聆听！

# Q&A


联系方式：

tombook@gmail.com