电商企业的漏洞挖掘大全

Ruby

漏洞盒子

WWW.VULBOX.COM

关于我

- 孙捷 Ruby
- 安氏、华为、Check Point
- Freebuf & 漏洞盒子 合伙人
- 坐不住的人

漏洞盒子
WWW.VULBOX.COM

关于漏洞盒子

身份

桥梁

- 测试人员（白帽子）<=> 企业
- 测试人员（白帽子）<=> 相关机构 <=> 企业

合作

漏洞盒子
WWW.VULBOX.COM

我们想做什么？

白帽子

企业

漏洞盒子
WWW.VULBOX.COM

互联网安全服务平台

安全专家/团队

安全厂商

企业的安全“深井”

漏洞安全需求

- 企业漏洞收集、响应以及危害消除
- 行业安全情报整合
- SOC、SRC 完善企业安全机制
- “江湖”地位

企业业务安全 +

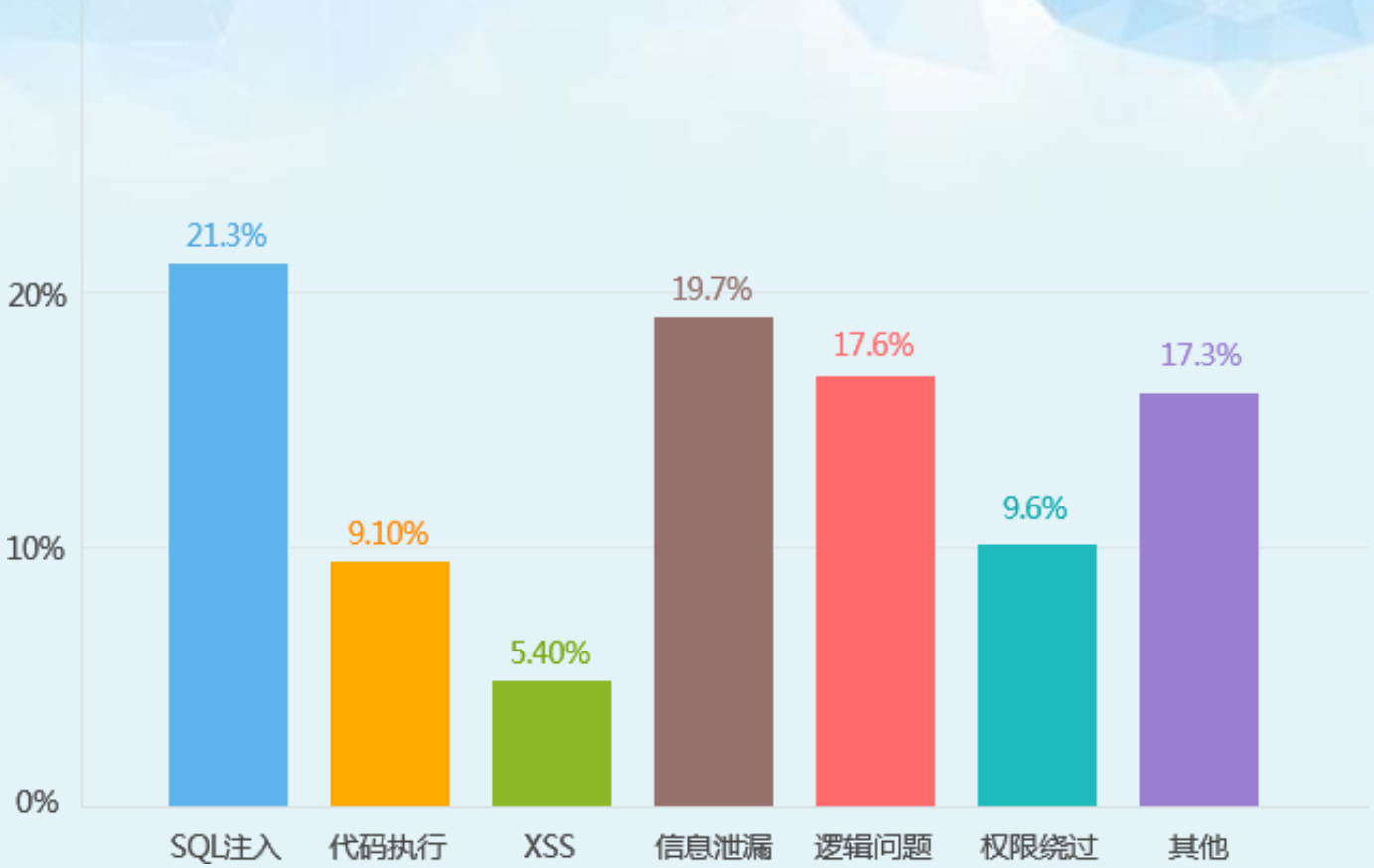
- 安全事件+ 漏洞
- 基础运维+ 漏洞
- 补丁管理+ 漏洞
- 业务审计+ 漏洞
- 人员管理+ 漏洞

安全交付服务

- 安全漏洞“Turnkey”挖掘服务
- 行业应用层漏洞最佳方案交付服务
- 安全培训（运维级培训+开发级培训）
- 漏洞闭环管理交付

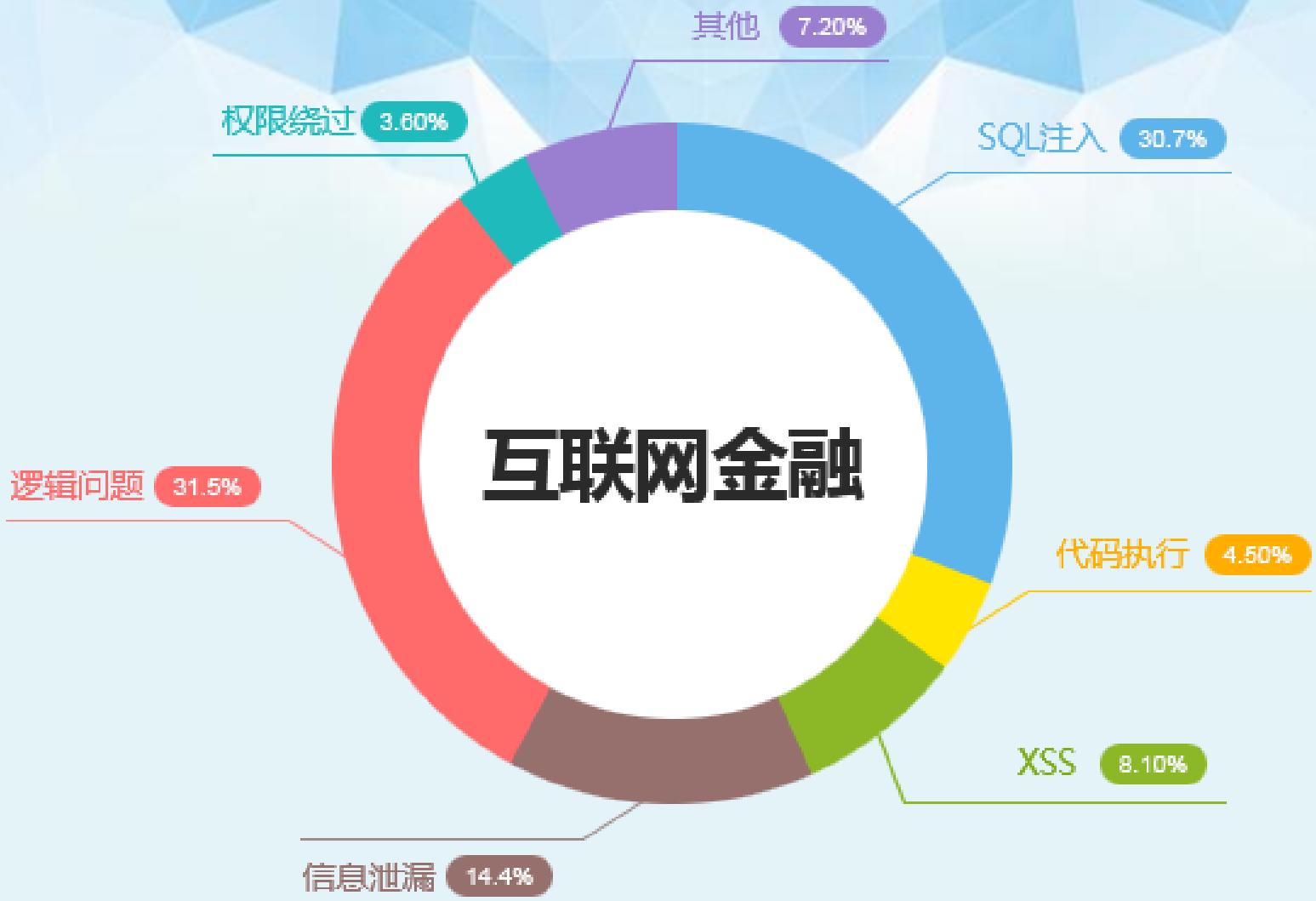
企业关注业务层面安全风险的发现、消除、闭环管理，应用层漏洞的生命周期跟踪

电商平台漏洞类型



漏洞盒子
WWW.VULBOX.COM

安全漏洞向“钱”看



漏洞盒子
WWW.VULBOX.COM

详情可在Freebuf.com下载
《2015金融行业互联网安全报告》

漏洞盒子
WWW.VULBOX.COM

漏洞攻击趋势

- 普通漏洞--->业务逻辑漏洞（支付，金额，用户数据相关的逻辑漏洞）
- Web应用漏洞--->APP漏洞/各类API接口/微信接口漏洞
- 一次性攻击--->APT（高级持续性威胁）攻击

核心：盗取用户数据，获取金钱利益

漏洞盒子
WWW.VULBOX.COM

面临问题

- 技术层面
  - 来自外部的黑客攻击，非授权访问；数据库数据被非法下载，篡改等；
- 管理层面
  - 主要表现为人员的职责、流程有待完善，内部员工的日常操作有待规范；研发运维缺乏安全意识带来的安全隐患等等

漏洞盒子
WWW.VULBOX.COM

案例一：利用逻辑缺陷重置任意用户密码

1. 通过正常步骤获得有效的digiSign状态

- 正常步骤重置自己账号的密码

漏洞盒子
WWW.VULBOX.COM

- 提交时候通过截包工具拦截数据包。可以看到重置密码是有digiSign签名字段验证的

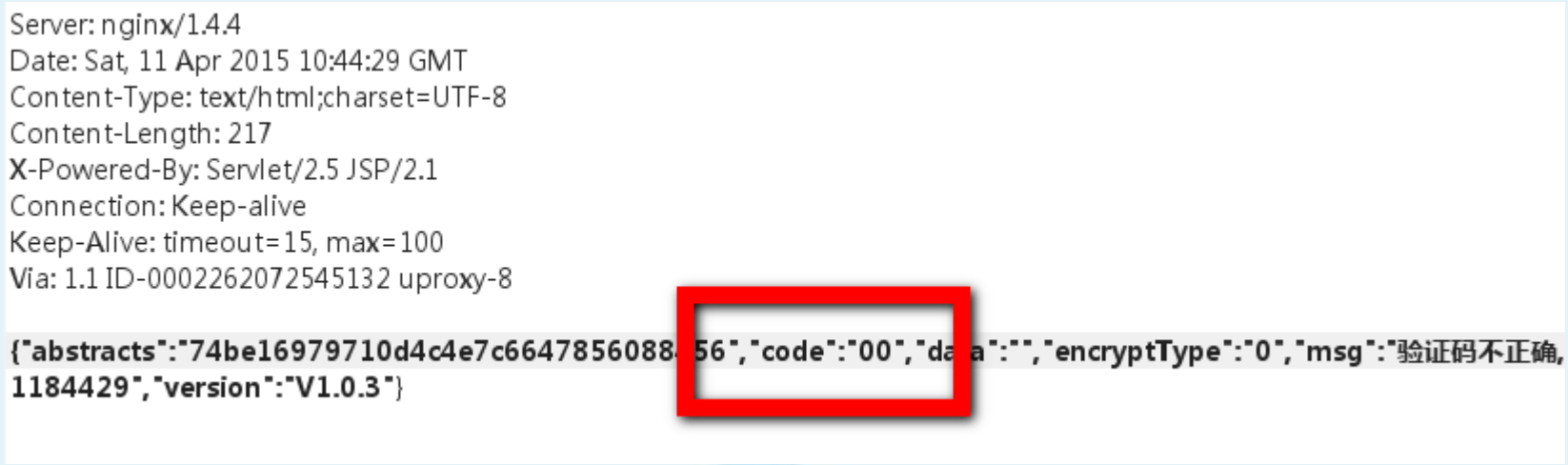
- 保存下digiSign字段，即会话状态。Drop掉数据包，避免会话一次验证失效

漏洞盒子
WWW.VULBOX.COM

2. 绕过手机验证码，进入下一步

找回他人手机的密码，验证码任意输入

- 将服务端返回的数据包code改为成功状态的00，绕过进入下一步



漏洞盒子
WWW.VULBOX.COM

3. 使用digiSign重置他人密码

- 在很多情况下，通过简单改包可以绕过步骤，提交服务器会失败，因为没有有效的会话状态。但是如果服务端校验逻辑出现问题，就会出现：替换第一步的有效digiSign，最终成功重置他人密码

漏洞盒子
WWW.VULBOX.COM

案例二：绕过签名任意修改支付金额

- 购买商品，选择网银在线支付。直接修改金额提交会直接提示参数错误。

  但是在正常请求提交返回包中不经意间泄露了一个叫key的字段

```
CNZZDATA1252940216=1308[redacted]5880408-%7C1415890632; IESESSION=alive;
pgv_pvi=2469454848; pgv_si=s2978352128;
A98B_viewed_goods=pydRcvBUuioaZgXDvwqxVtBDXrQNCqE7cn_I9TndqWYt_GTCKIbDTX9OKXqDTMn
FIEnNDArPnI6iETpZr[redacted]vUqgkBpTjd-shL;
A98B_sdmenu_my_menu=001; A98B_msgnewnum431=0;
A98B_seccode8173bd43=myt5lDr8PqdqMmeSXf[redacted]mdojrdhBrQU_kNmf;
A98B_msgnewnum427=0; A98B_cart_goods_num=1
Connection: keep-alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 71

pay_sn=900469[redacted]799427&payment_code=chinabank&order_type=product_buy
```

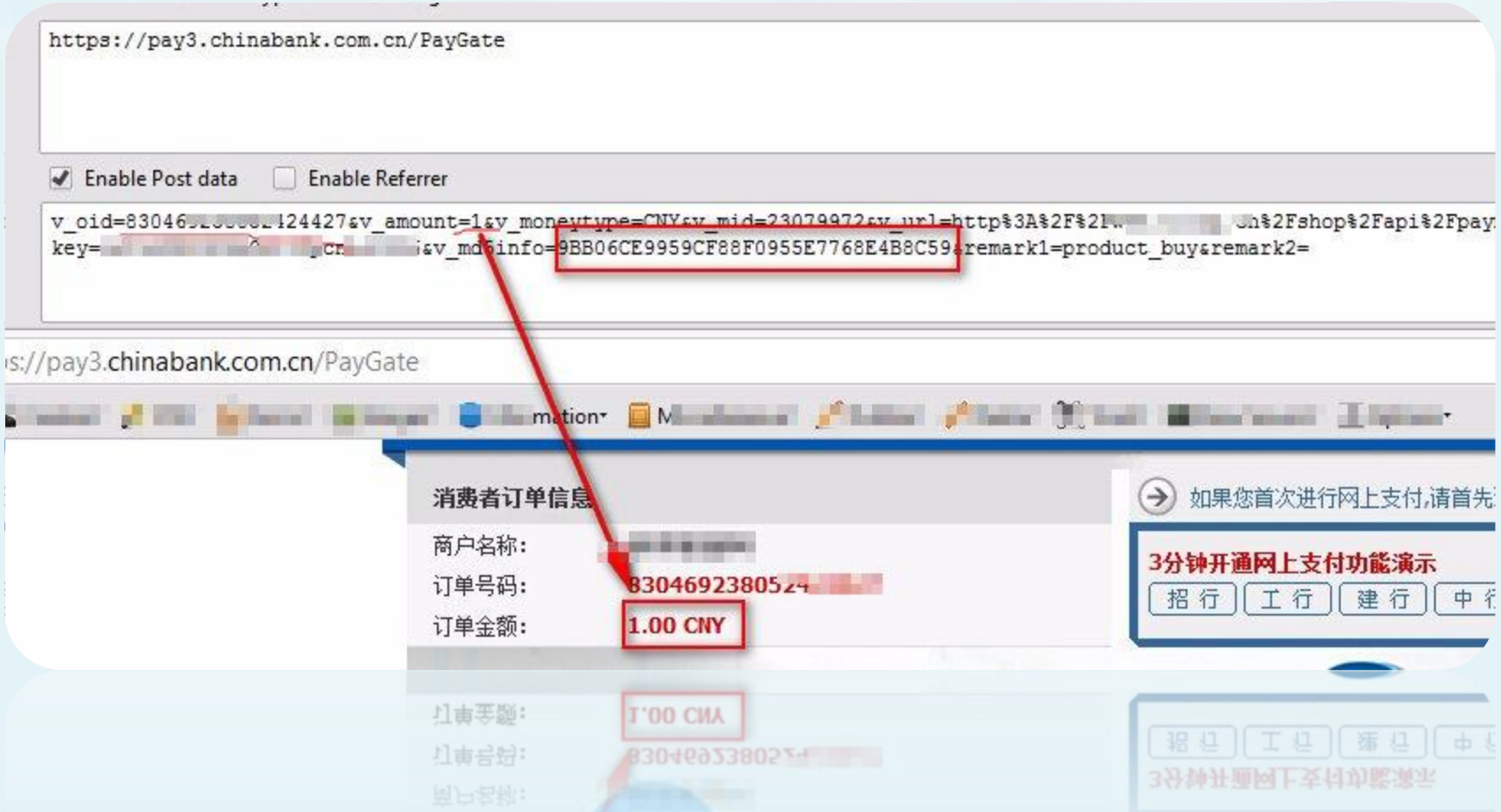
```
Content-Length: 769

<html><head></head><body><form method="post" name="E_FORM
action="https://pay3.chinabank.com.cn/PayGate"><input type='hidden'
value='900469[redacted]9427' /><input type='hidden' name='v_amou
type='hidden' name='v_moneytype' value='CNY' /><input type='hidde
value='23079972' /><input type='hidden' name='v_url'
value='http://www.allzp.cn/shop/api/payment/chinabank/return_url.php
name='key' value='[redacted]006' /><input type='hidden' na
value='4A6530A781122A091BEE650F51E924F9' /><input type='hidde
value='product_buy' /><input type='hidden' name='remark2' value='' /
type="text/javascript">document.E_FORM.submit();</script></body
```

漏洞盒子
WWW.VULBOX.COM

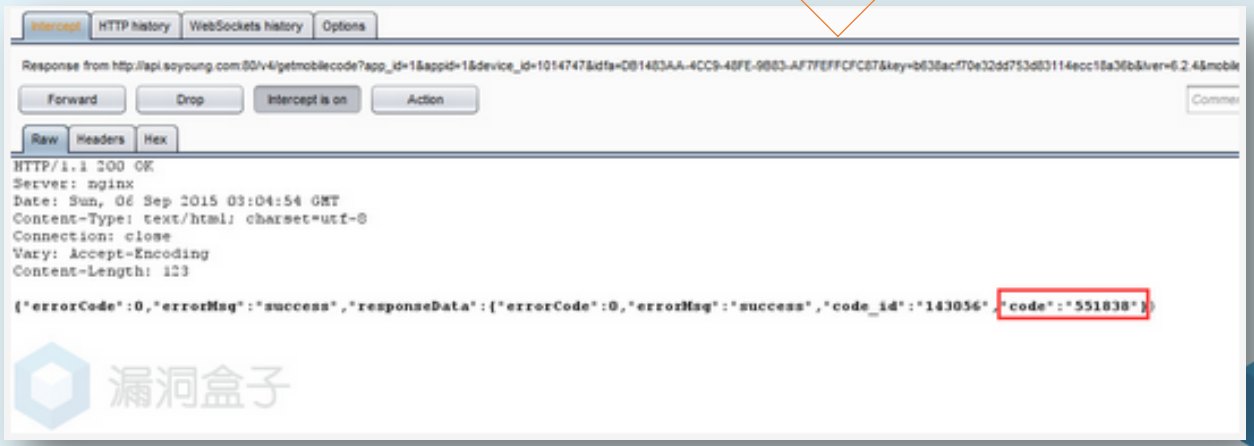
- 经人工分析发现：key就是对请求参数进行md5的salt

  将订单中的v_amount,v_moneytype,v_oid,v_mid,v_url参数的value值拼成一个无间隔的字符串,使用key作为salt即生成任意伪造数据签名



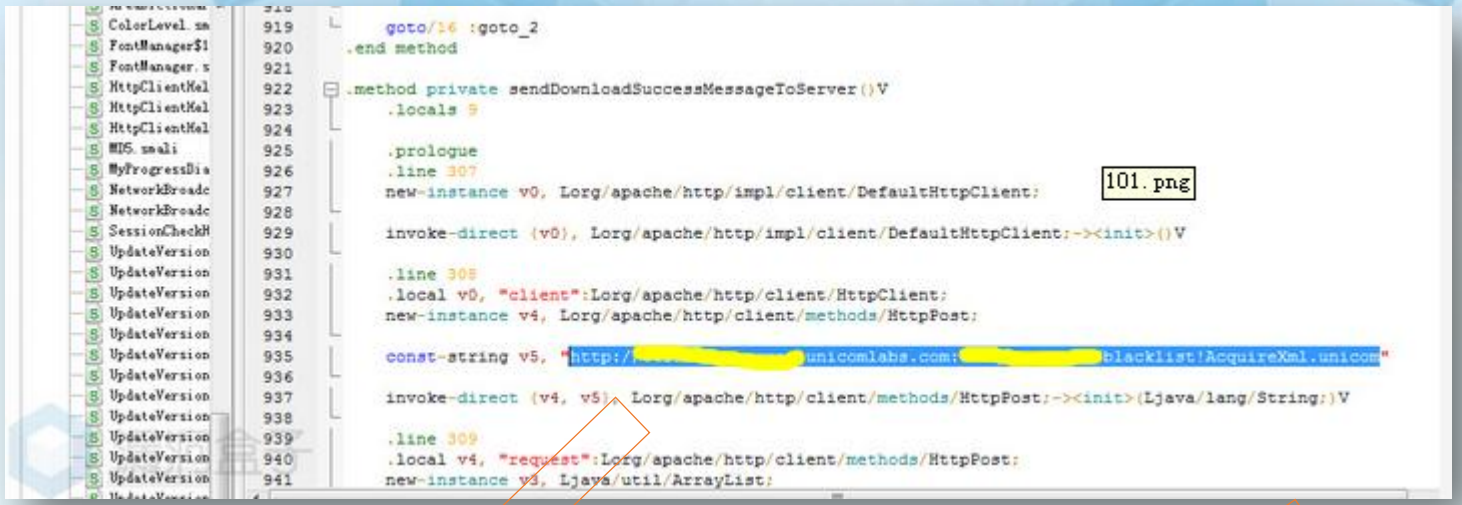
漏洞盒子
WWW.VULBOX.COM

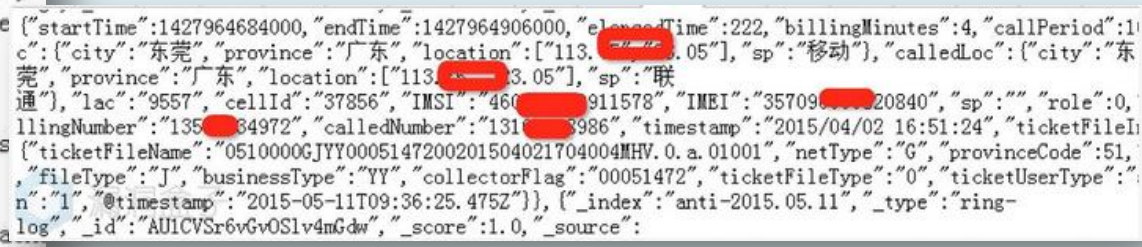
案例三：APP明文传输、无校验、越权、SQL注入



漏洞盒子
WWW.VULBOX.COM

案例四：运营商APK程序可逆20亿通话信息





漏洞盒子
WWW.VULBOX.COM

传统安全问题

框架安全问题
- 表达式语言注入（Struts,Spring任意代码执行）

常规安全问题
- 各类系统的SQL，HQL注入漏洞
- 逻辑漏洞（越权修改信息，任意密码重置，订单遍历，支付金额篡改）
- 登录绕过（弱密码组合，万能密码，逻辑判断失误，脆弱的验证码）

运维安全问题
- MongoDB未授权访问
- JBoss jmx-console各种Invoker war包部署
- Websphere/ WebLogic/ WebLogic/ Tomcat弱密码，后台部署war包
- Oracle数据库各类Web组件利用
- Resin任意文件读取
- WEB-INF/web.xml可读取导致源码及敏感信息泄露

Web2.0 互联网安全问题

XML类型安全问题
- XXE外部实体攻击
- XML注入
- XPATH，XQUERY注入
- XML DoS拒绝服务攻击
- SSRF服务端请求伪造

REST类型安全问题
- 过度依赖SSL通信
- SESSION和认证管理缺陷
- 依赖HTTP基础认证

Web认证及授权安全问题
- OAuth授权实现不当
- HASH长度扩展攻击
- CBC比特反转攻击
- 基于SAML的外部实体攻击

漏洞盒子
WWW.VULBOX.COM

安全服务生态的建立

	生态服务者
基础网络安全	Check Point SOFTWARE TECHNOLOGIES LTD. We Secure the Internet. · SANGFOR 深信服科技 · paloalto networks. · RSA The Security Division of EMC · ZTE中兴 · BlueCoat · IBM · ArcSight · JUNIPER NETWORKS · symantec. · CISCO · FORTINET
应用安全	RSA The Security Division of EMC · w3af · TREND MICRO · symantec. · EXPLOIT DATABASE · IMPERVA
主动防御	paloalto networks. · SOURCEfire · Check Point SOFTWARE TECHNOLOGIES LTD. We Secure the Internet. · ixia · FireEye · Bit9
数据分析	同盾科技 Fraudmetrix.cn · 透视宝 Cloudwise · 听云 TINGYUN · FIREMON · riverbed Think fast.
云安全	云智慧 Cloudwise · 阿里云 aliyun.com · 腾讯云 · upyun · 美团云 Meituan Open Services
国家合作	CNVD 国家信息安全漏洞共享平台 · CN-CERT/CC 国家互联网应急中心 · 公安三所 · CNNVD 国家信息安全漏洞库 · 国家信息技术安全研究中心 · 上海市网络与信息安全应急管理事务中心
企业解决方案	IBM · 神州数码 Digital China · Ruijie 锐捷 Networks · teambition · GitCafé

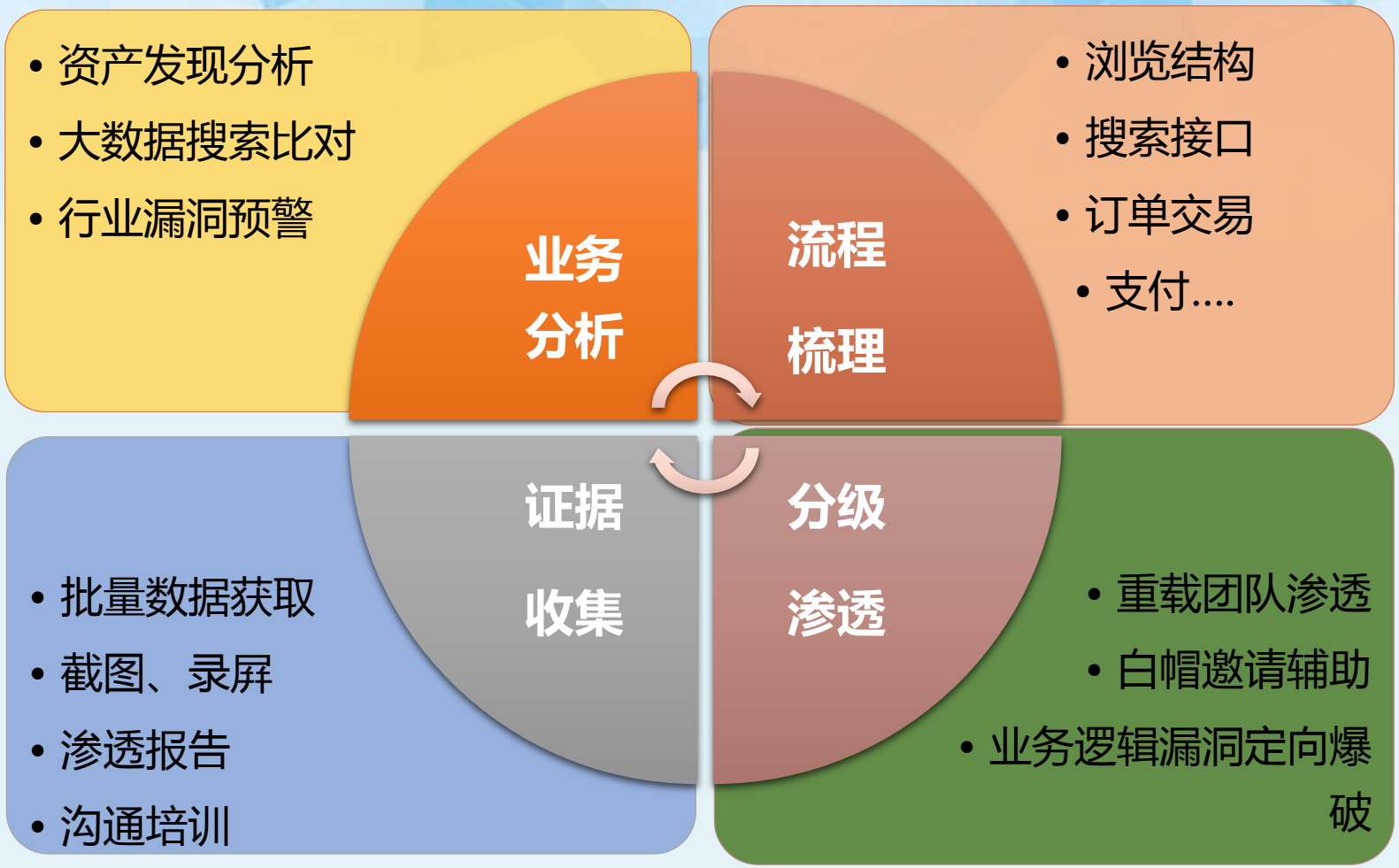
漏洞盒子 WWW.VULBOX.COM

“深井+江湖”意识

- 受利益驱使，金融、电商行业被更多黑客“盯上”，厂商越早地主动客观对待安全问题，才能避免更多的损失；
- 建议企业更多地关心业务逻辑层面安全问题，APP/API/微信接口问题；
- 有人的地方就有江湖，有江湖就有漏洞。人永远是安全威胁中最薄弱的环节；
- 网站安全，内外兼修：解决网站本身安全漏洞，防止黑客攻击；加强内部研发运维人员安全意识与知识。

漏洞盒子
WWW.VULBOX.COM

互联网安全需求矩阵



漏洞盒子
WWW.VULBOX.COM

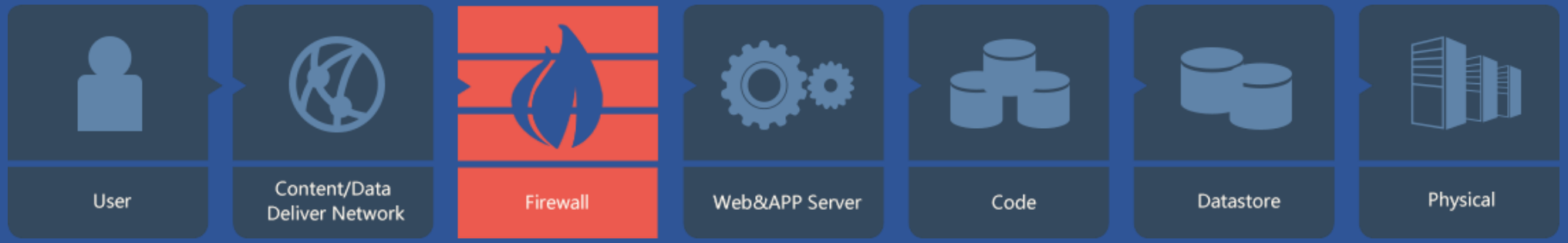
一些建议

解决方案与培训

网藤
互联网安全SaaS云服务

漏洞盒子
企业级安全测试平台

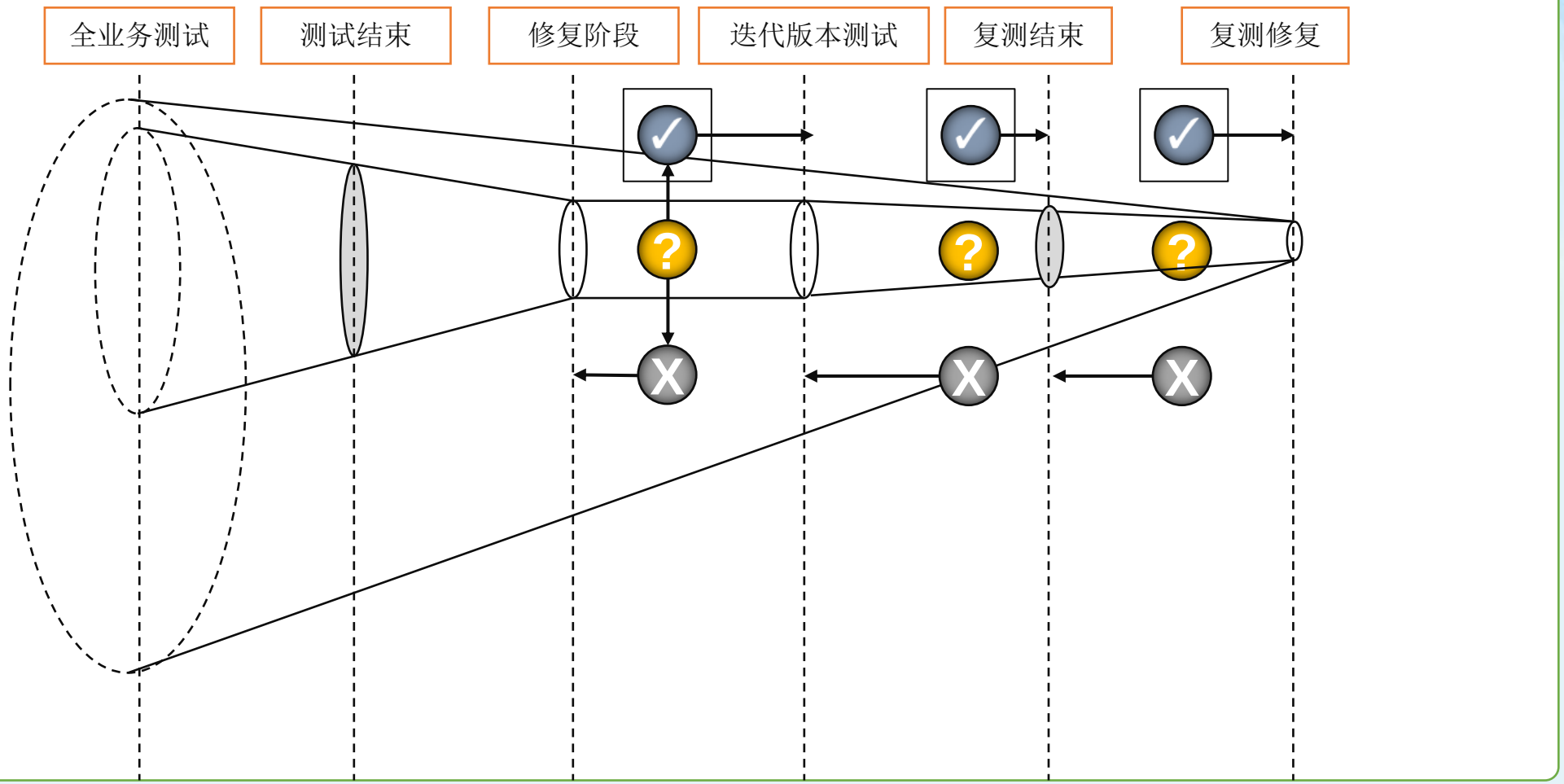
覆盖业务流
安全测试链



贯穿安全漏洞测试 全生命周期

漏洞挖掘 → 漏洞管理 → 版本迭代 → 渗透演练

迭代闭环



首轮测试

迭代测试干预

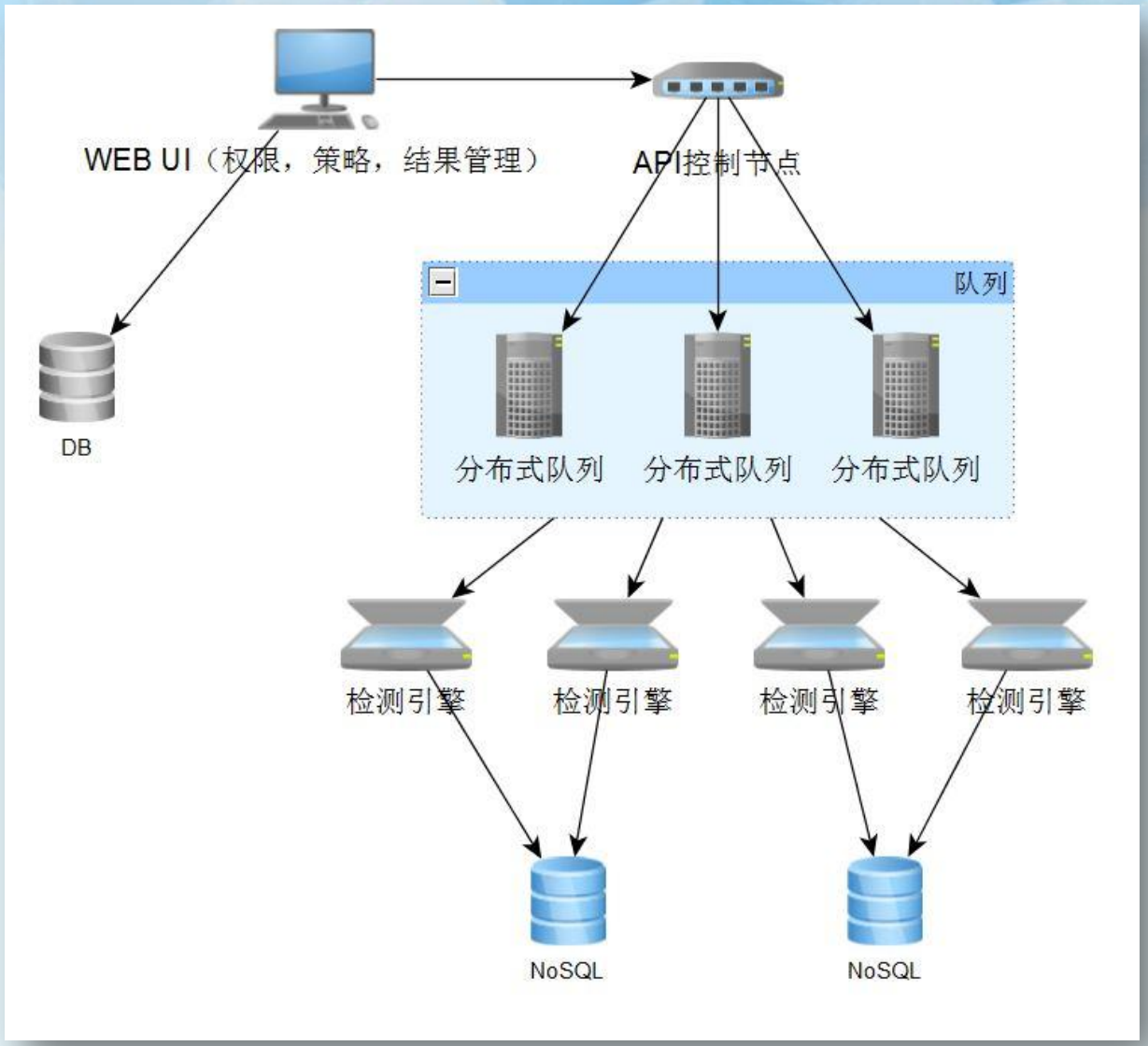
漏洞生命周期管理测试

漏洞盒子安全测试收敛模型

网藤SaaS云服务

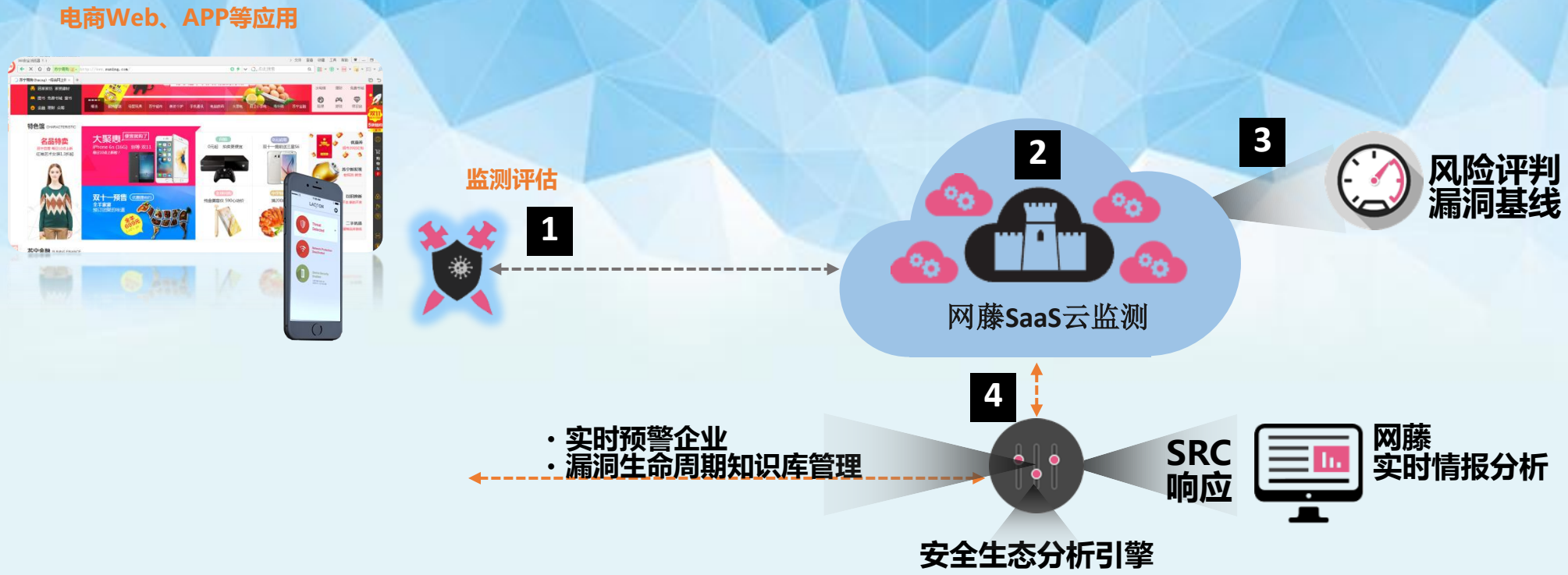
漏洞盒子 | 网藤

技术架构



- 云端？
- 智能？
- 交付？

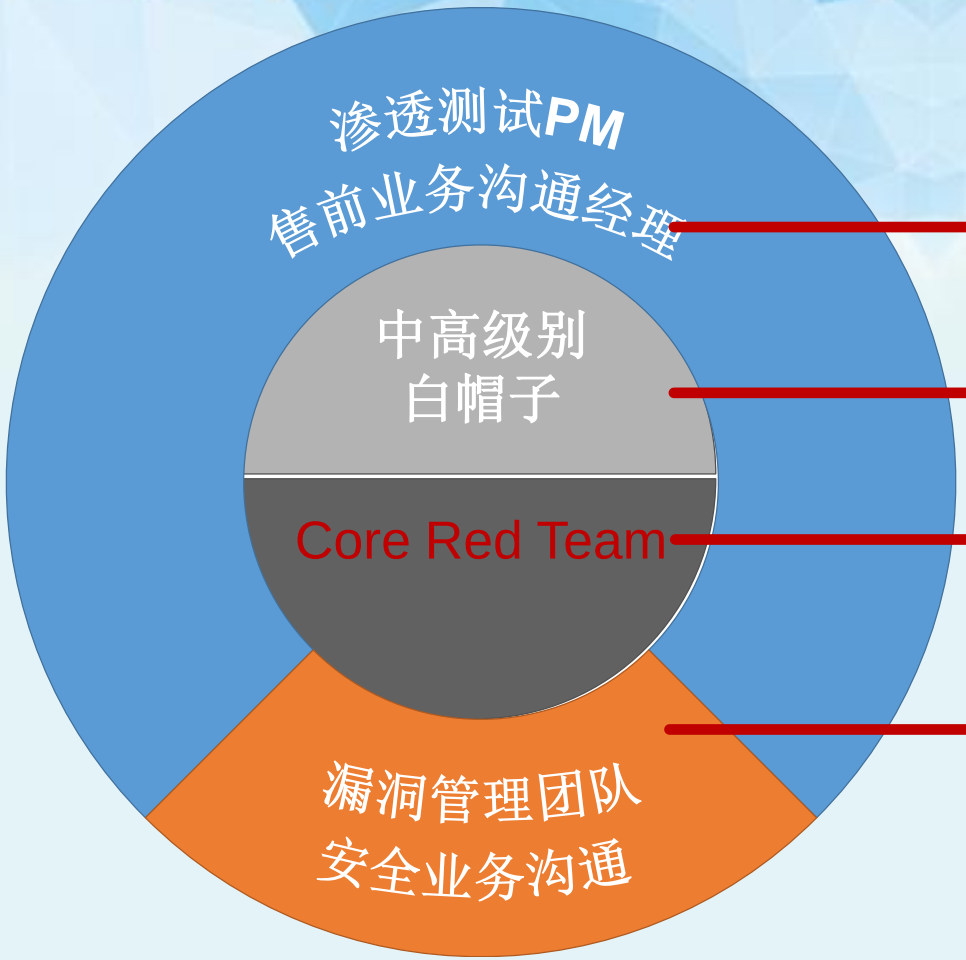
漏洞盒子 | 网藤
漏洞盒子
WWW.VULBOX.COM



网藤原理介绍

1. Docker容器，一键部署
2. 国内外多云商多节点部署，使用最优路径监测（阿里云、腾讯云、亚马逊）
3. 站点安全上下文环境自动筛选规则
4. 全网大数据关联分析，Github Hacking，Pastebin Hacking模块

漏洞盒子
WWW.VULBOX.COM



- 所有渗透实现项目管理，PM管控、反馈、总结
- 技术型销售团队，SE+Sales必须理解、沟通需求

- 平台核心白帽子，项目申请通过率20%
- 白帽背景审核，平台ID实名制

- 平台精英专家，项目申请通过率小于20%
- 精英化测试，特种部队打法
- 远程视频审核、保持线下联系

- 强调漏洞生命周期管理
- 测试前期安全业务梳理清晰
- 成为企业与白帽子的“桥梁”

漏洞盒子
WWW.VULBOX.COM

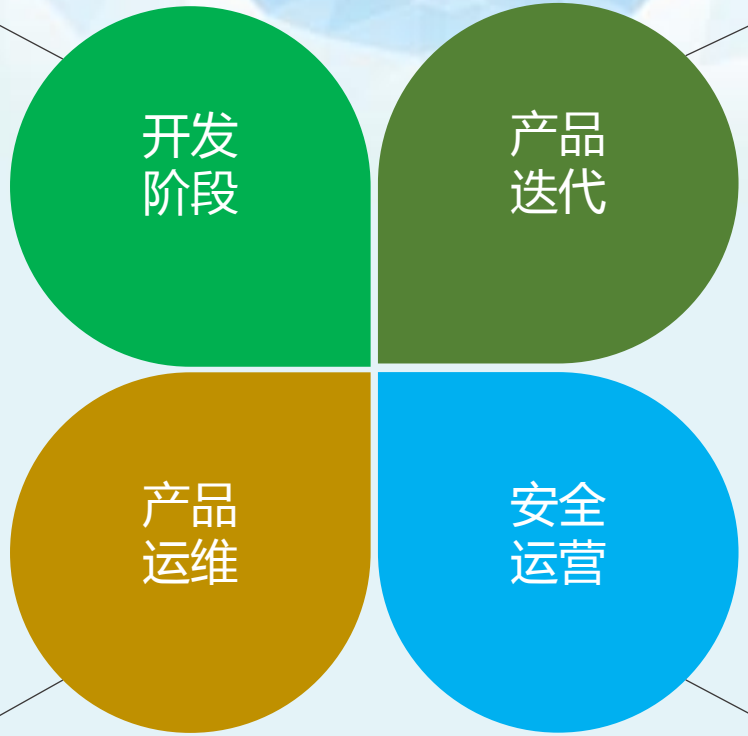
“重测”与“轻测”的结合

漏洞盒子|安全测试

- 专家级互联网安全测试
- 深度漏洞及漏洞链分析
- 架构层面安全修复

漏洞盒子|安全测试

- 分析业务变化及威胁分析
- 发布前安全测试
- 漏洞修复与处理



- 实时安全云端监控
- 应急响应，迅速解决线上问题
- 企业级APT渗透演练

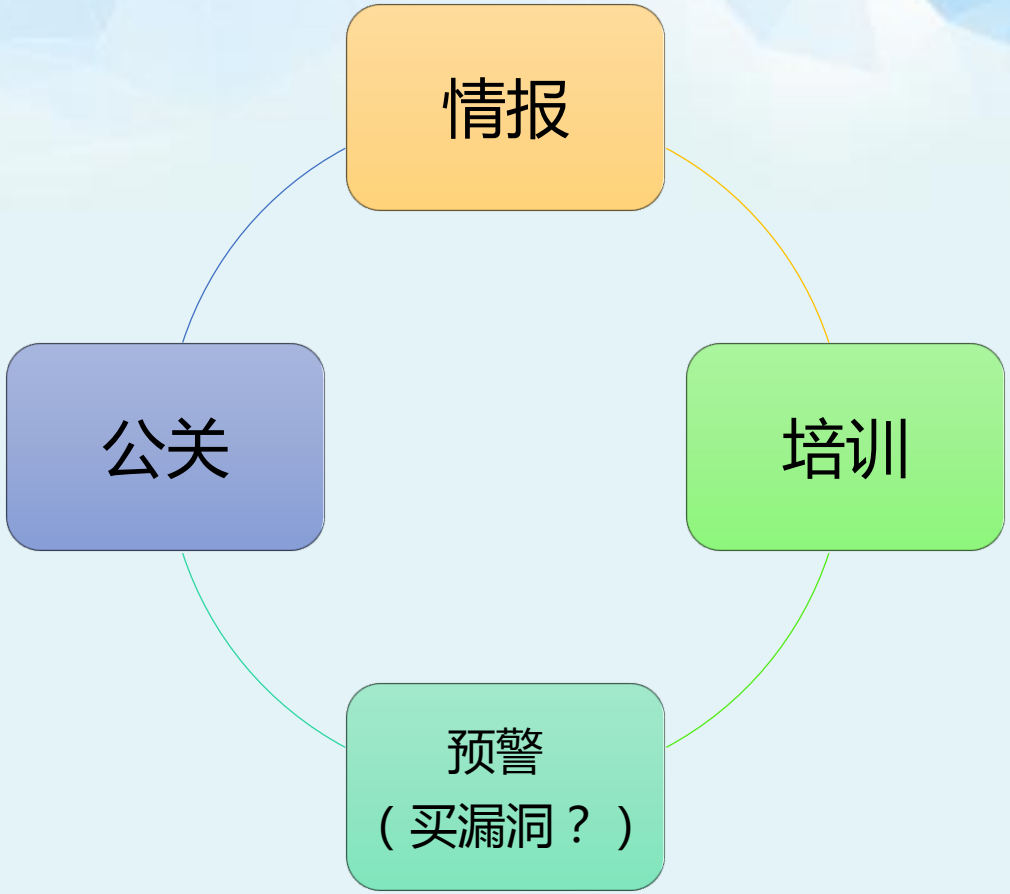
漏洞盒子 | 网藤

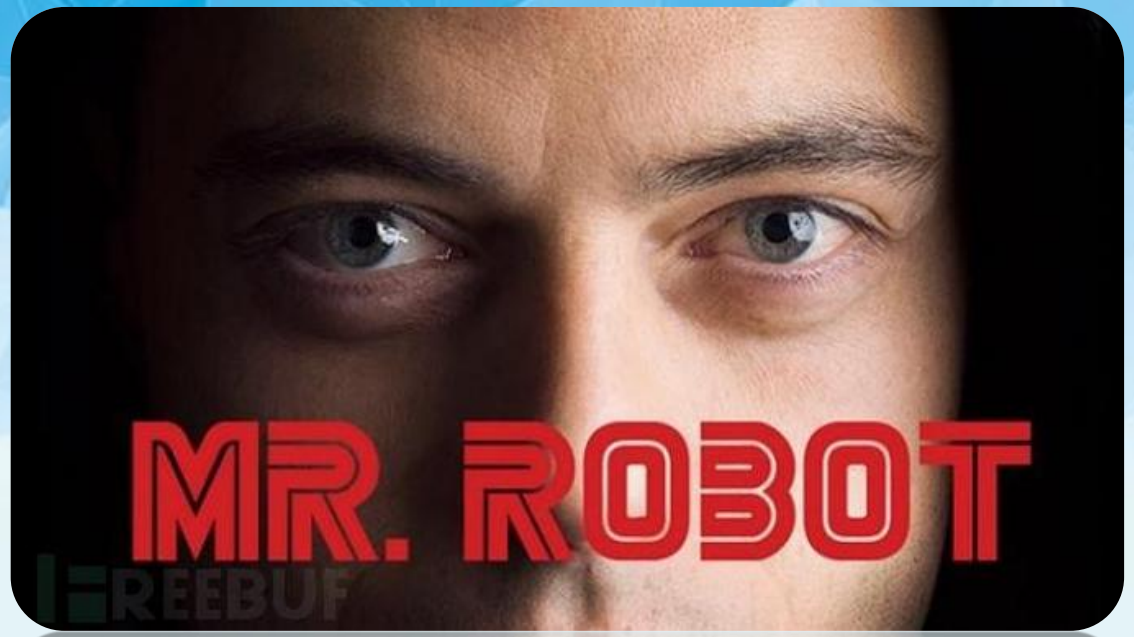
- 安全情报获取
- 互联网漏洞预警
- 安全事件响应与公关

漏洞盒子 | 情报中心

漏洞盒子
WWW.VULBOX.COM

通关了么？





漏洞盒子
WWW.VULBOX.COM

电商安全模型

- 电商业务流程梳理&归类
- 业务上线规划
- 电商业务信息安全合规性需求定义

- 建立SRC漏洞响应体系
- 企业漏洞库管理
- 安全意识培训
- 融合第三方平台安全情报、预警机制

- 私有渗透测试+众测模式
- 企业已有漏洞周期性复测
- 云监测实时预警

- 电商风险模型（交易风险、数据风险...）
- 定义风险加固框架（基础网络安全、应用安全）

- 风险模型落地（行业漏洞、风险测试PoC）
- 面向开发、运维的安全设计向导
- 面向管理的安全设计评审

- 电商代码安全框架
- 白盒安全测试、安全迭代评审
- 安全代码归档及版本控制（业务支配 IT的快捷交付）

漏洞盒子
WWW.VULBOX.COM

改变与变革

收集

索引

关联

响应

漏洞盒子
WWW.VULBOX.COM


问道
电商安全
第二届华为IT网络安全沙龙
中国·深圳 2015.10.30