产品安全之道
安全测试理论与实践

南京翰海源信息技术有限公司

©2011 Vulnhunt, Inc. All rights reserved.

FlashSky

- 启明攻防实验室经理、美国EEYE高级研究员、美国微软特聘安全测试专家、南京翰海源CEO
- 2003年LSD RPC DCOM；2003年WINDOWS 2003堆保护绕过技术；2004年WINDOWS内核远程溢出技术
- 数百个软件高危级安全漏洞的发现者，大多是微软的核心产品。
- 微软BLUEHAT演讲者，5届XCON演讲者，2届VARA演讲者

©2011 Vulnhunt, Inc. All rights reserved.

主题

- IT产品和系统的安全
  - 信息化下的安全思考
  - 国外对产品安全的认知现状
  - 做负责任的厂家
  - 产品安全之道
- IT产品和系统的安全测试理论
- IT产品和系统的安全测试实践

©2011 Vulnhunt, Inc. All rights reserved.

IT产品和系统的安全挑战

- IT系统发展的趋势
  - 成为人类的脑
    - 信息存储
    - 处理计算
    - 决策依赖
  - 成为人类的意志传输扩展
    - 信息与意志的传递
    - 信息与意志的控制
- 解决IT系统的安全问题成为IT系统发展最大的问题

©2011 Vulnhunt, Inc. All rights reserved.

事后追责安全体系的失效

- 现实生活中低成本的安全依赖于事后追责体系
  - 追责和法律风险大大降低犯罪收益
  - 信任的前提是：相信一旦违反信任，对方会遭受更大损失
- IT系统安全和现实安全的区别
  - 非接触性
  - 证据非物理性
  - 跨域性
  - 损害非及时可知性
- 事前事中防范不低于事后追责作用
- 事中危害及时发现能力是事后追责体系的依赖

©2011 Vulnhunt, Inc. All rights reserved.

让安全成为IT系统基础属性

- 现代IT系统是复合的
  - 自身可控部分的安全
    - 意识与能力
    - 安全开发
    - 安全验证
  - 自身依赖不可控部分的安全
    - 供应链安全保证
    - 未知危害感知能力
  - 整体
    - 纵深的安全防御与监控体系
    - IT教育与培训体系

©2011 Vulnhunt, Inc. All rights reserved.

做负责任的厂家

- 要想占有市场，就要对用户负责；要想对用户负责，必须重视安全
  - 用户数量大了，厂家的责任就越大，一旦出现一个严重的安全漏洞，影响面将会非常之广
  - 竞争对手，黑客都盯着你。
  - 微软：
  - 腾讯、阿里：

©2011 Vulnhunt, Inc. All rights reserved.

国外对产品安全的认知现状

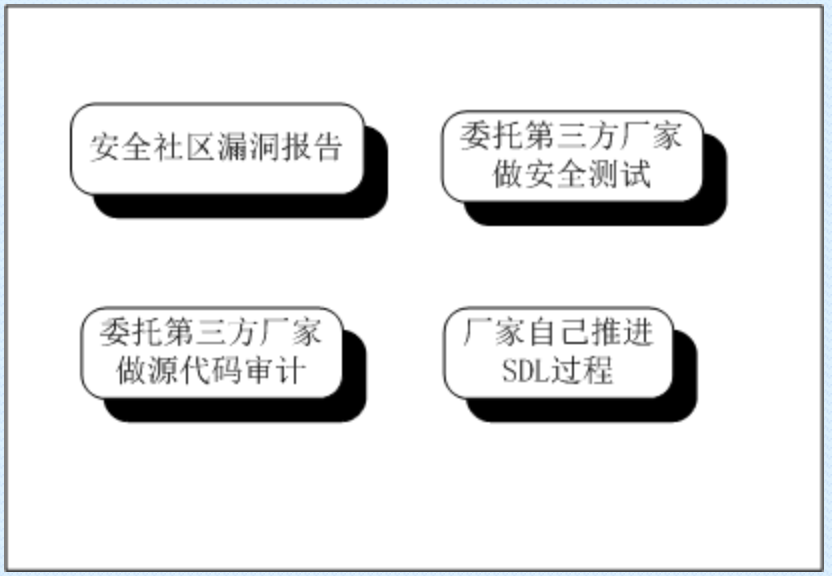
- 微软/adobe全力推进sdl开发过程
- Chrome,Mozillia,Facebook对发现他们产品的安全漏洞报告者予以奖励
  - Chrome $3133.7 $2337 $2000 $1337 $1000 $500
  - Mozillia $500 to $3000
  - Facebook $500++
  - 其他 wordpress, piwik, barracudalabs, Hex-Rays, tarsnap, Drupal
- Pwn2Own

- 发公告感谢漏洞发现者

©2011 Vulnhunt, Inc. All rights reserved.

产品安全之道

- 当前主流方法
  - 安全社区漏洞报告
  - 安全测试（黑盒）
  - 源代码审计（白盒）
  - SDL安全开发过程



- 安全社区漏洞报告/安全测试/源代码审计成本相对较小

©2011 Vulnhunt, Inc. All rights reserved.

主题

- IT产品和系统的安全
- IT产品和系统的安全测试理论
  - 安全测试当前困境与原因
  - 安全问题的各种视角与要素
  - 翰海源的IT 产品与系统的安全测试体系
  - 工具支撑
- IT产品和系统的安全测试实践

©2011 Vulnhunt, Inc. All rights reserved.

安全测试是什么

- 以漏洞挖掘之手段，在系统上线或产品交付前，尽量保证其安全性的系统化行为
  - 覆盖性
  - 完备性
  - 可度量性

- 当前安全测试困境
  - 测试理论很难适用于安全领域
  - 安全测试基础理论薄弱,当前测试方法缺少理论指导，也缺乏技术产品工具

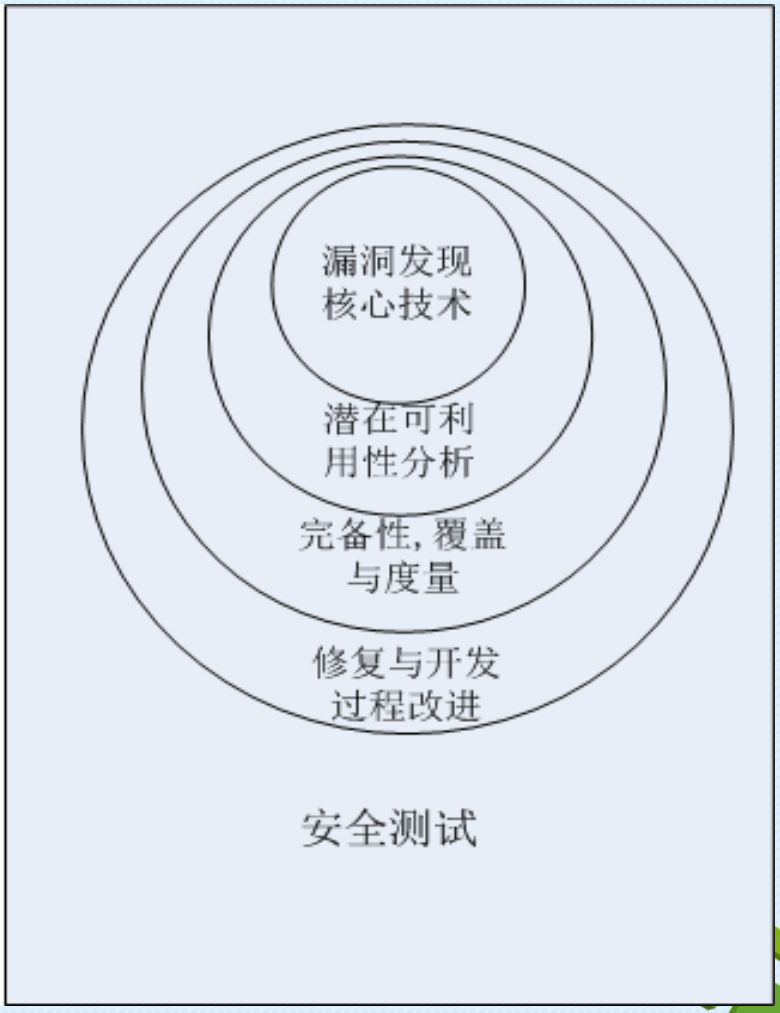
©2011 Vulnhunt, Inc. All rights reserved.

安全测试与测试

- 测试 VS 安全测试
  - 信息泄露，WMF，LNK，SYN FLOOD漏洞是BUG吗？
- 假设条件
  - 测试：导致问题的数据是用户不小心构成的
  - 安全测试：导致问题的数据是攻击者处心积虑构成的
- 思考域
  - 测试：功能本身
  - 安全测试：功能，系统机制，外部环境，应用与数据自身安全风险与安全属性
- 问题发现模式
  - 测试：违反功能定义的输出
  - 安全测试：违反权限，能力与约束

©2011 Vulnhunt, Inc. All rights reserved.

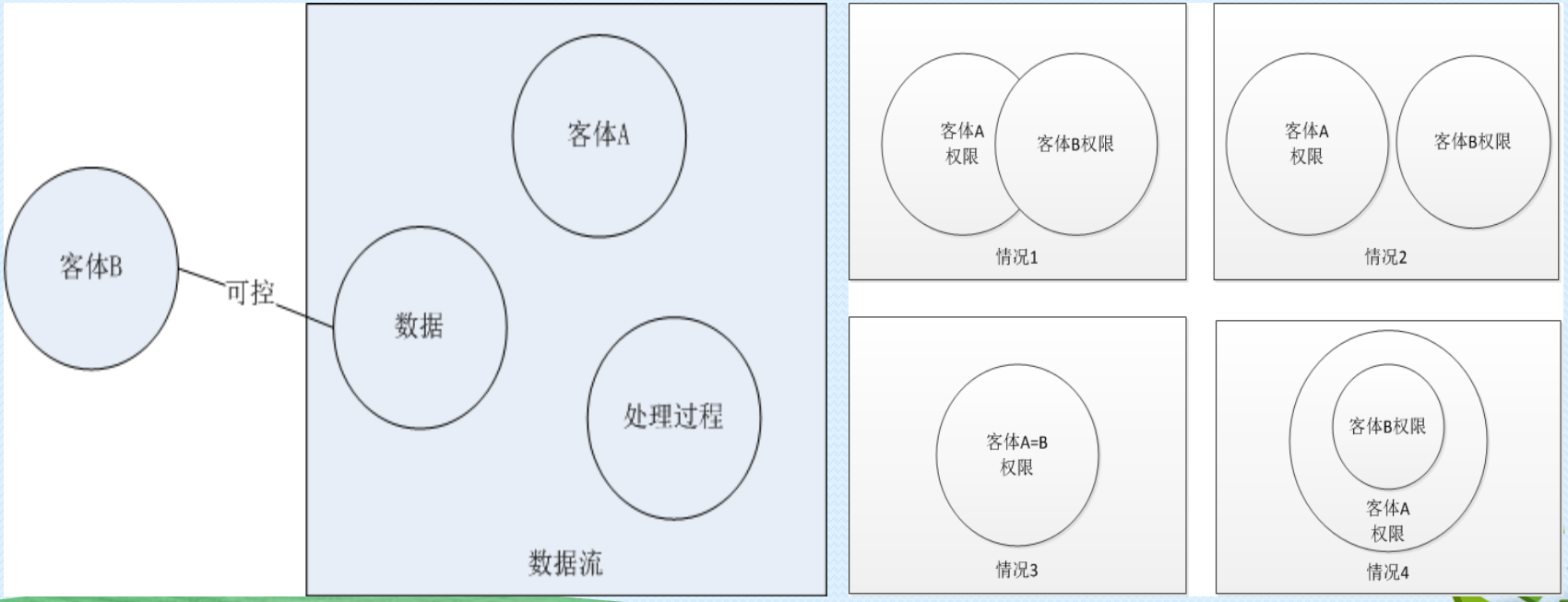
安全测试与漏洞挖掘



©2011 Vulnhunt, Inc. All rights reserved.

宏观安全分析的本质要素

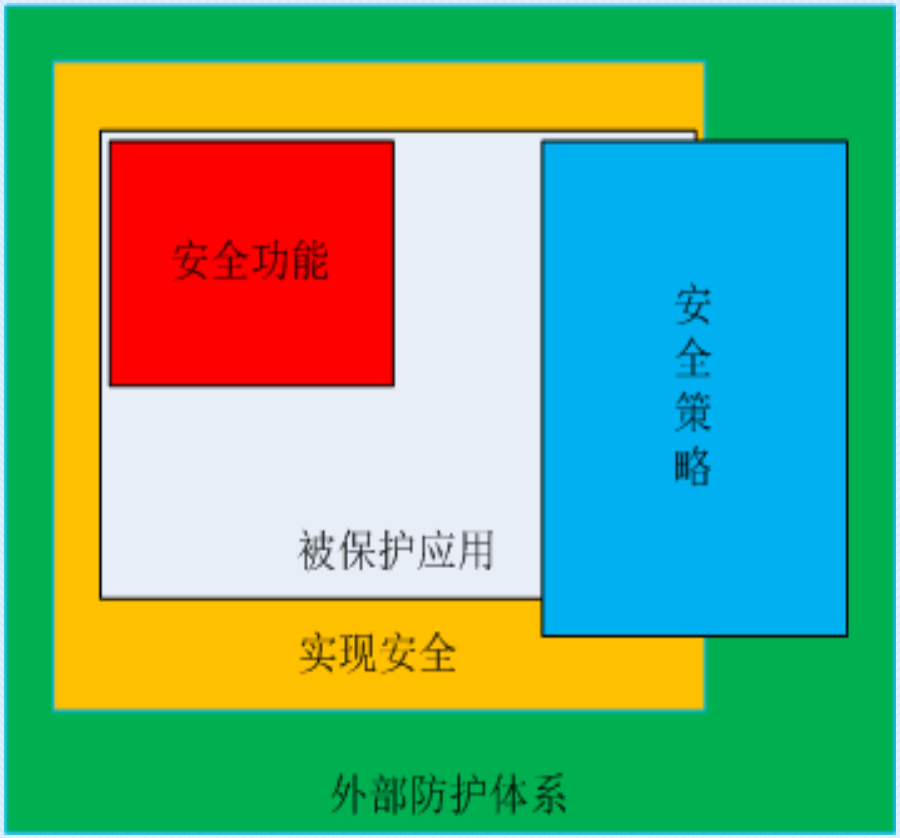
- 宏观
  - 不同权限或能力的对象之间存在着对同一数据流的处理和控制权限
  - 权限的提升



©2011 Vulnhunt, Inc. All rights reserved.

安全语义分析的本质要素

- 安全包括了三个层次
  - 安全功能（特性）
  - 安全策略（部署，配置，全局设计准则）
  - 安全实现

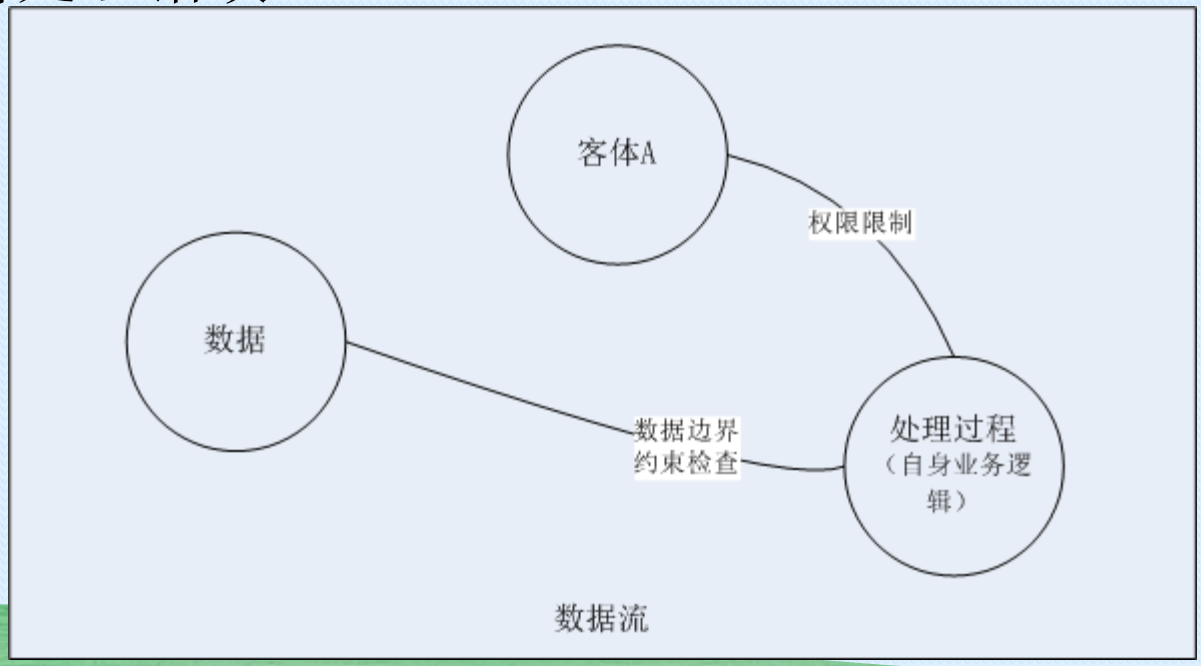


- 安全测试是对以上几个层次的验证和度量
- 外部防护系统是一种补充保护

©2011 Vulnhunt, Inc. All rights reserved.

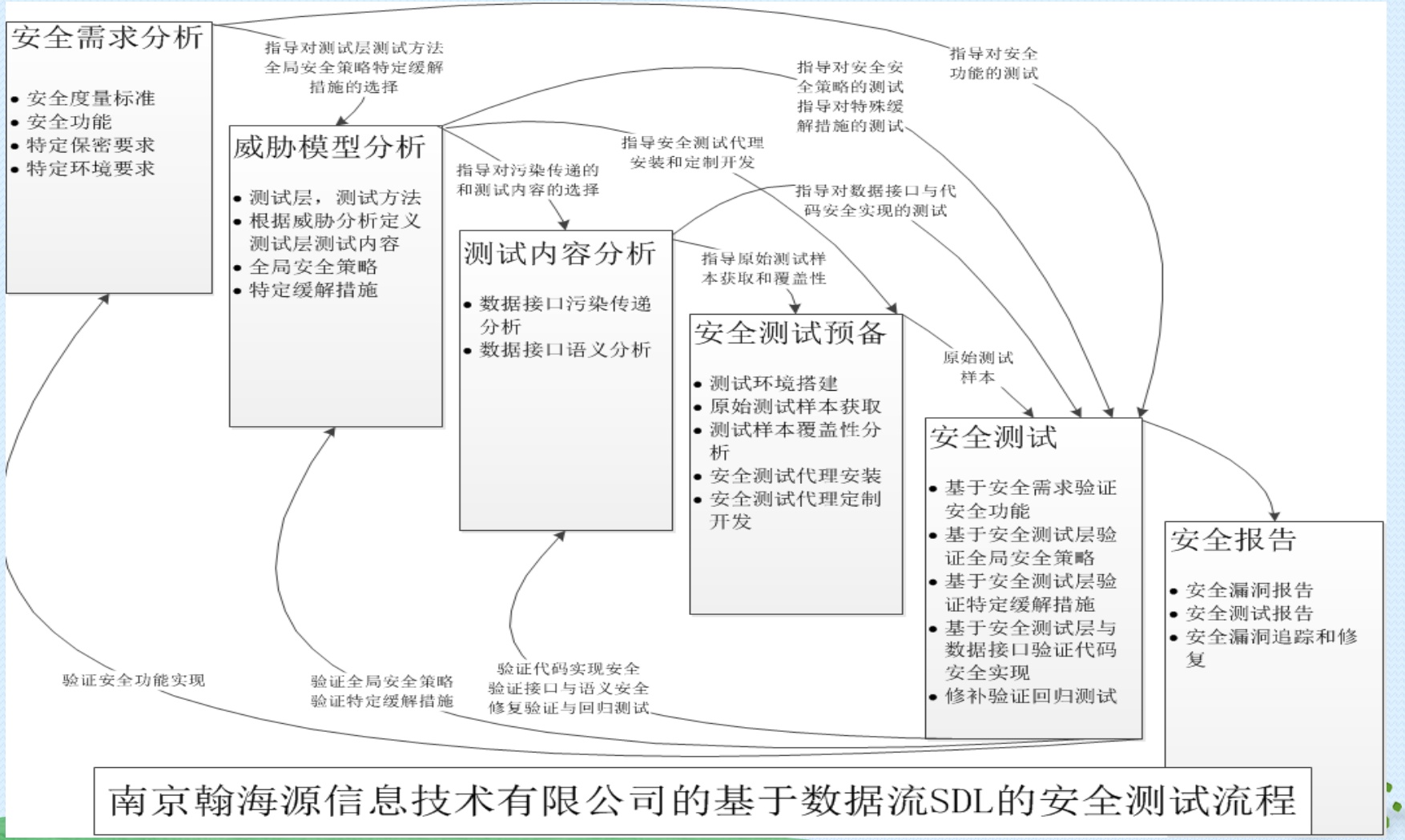
安全微观分析的本质要素

- 把程序看作数据流+数据处理+权限对象
  - 对数据流上的数据边界缺乏检查
  - 对客体权限本身缺乏限制
  - 逻辑处理错误



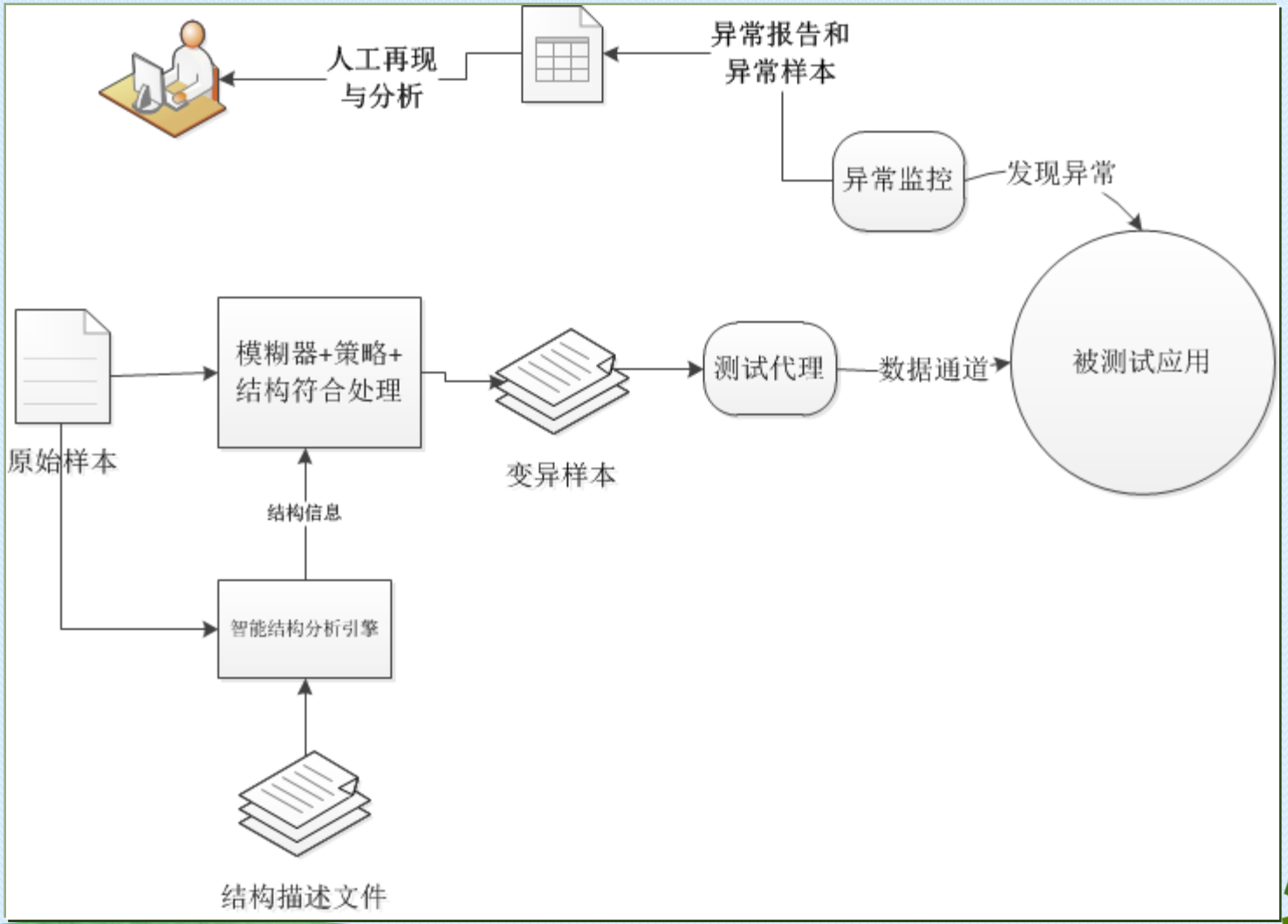
©2011 Vulnhunt, Inc. All rights reserved.

综合的安全测试方法论



©2011 Vulnhunt, Inc. All rights reserved.

翰海源起航-智能FUZZ



©2011 Vulnhunt, Inc. All rights reserved.

翰海源追踪-数据流污染

READFILE（F1， BUF1，
0X100）
……
Malloc(buf2,0x20)
Malloc(buf3,0x100)
……
Memcopy(Buf3,buf1,0x100)
……
A=*(int *)(buf3+4)
……
If(A<=0x200)
{
……
Strncpy(buf2,buf3+8,A)
……

某应用程序

虚拟机（获得所有指令与环境信息）

发现污染源， 如
READFILE
RECV
……
定位污染源BUF1， 知道目标源大小0x100

追踪目标内存大小
BUF2大小0x20
BUF3大小0x100

污染传递追踪
BUF3被污染
A被污染

条件限定分析
A取值范围0到0x200

漏洞检查模式触发
检查条件：
BUF2大小为0x100
A取值分为为0到0x200， 超出限定范围
报警

可疑点报告和技术细节

人工分析与再现

©2011 Vulnhunt, Inc. All rights reserved.

主题

- IT产品和系统的安全
- IT产品和系统的安全测试理论
- IT产品和系统的安全测试实践

©2011 Vulnhunt, Inc. All rights reserved.

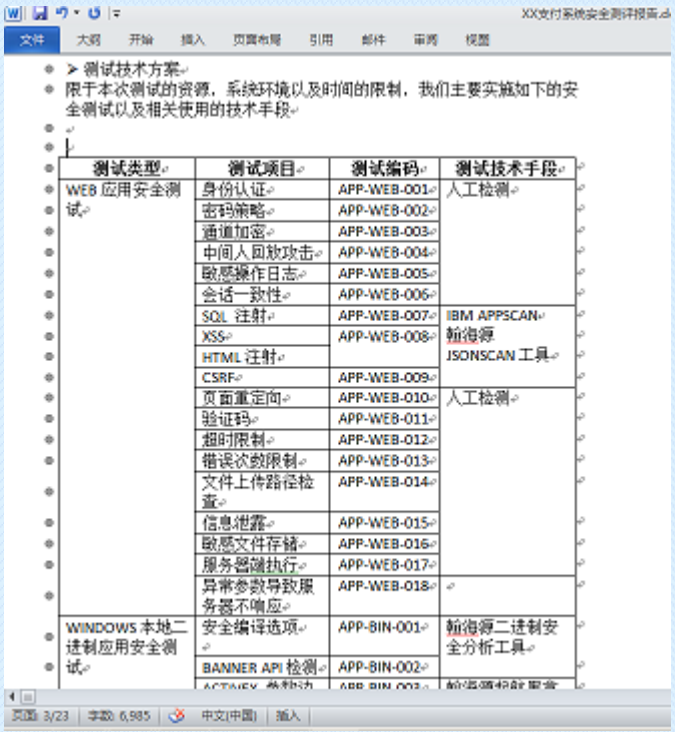
翰海源安全测试实施概况

- 自成立不到两年里，先后完成了超过30个软件安全测试项目（二进制级别）
- 涵盖客户的产品有浏览器，IM，游戏，证券软件，杀毒软件，网银软件等国内外非常著名的软件。这些软件多则覆盖几亿用户，少则也覆盖数千万用户。
- 每个项目都获得用户好评

©2011 Vulnhunt, Inc. All rights reserved.

XXX支付网关安全测评

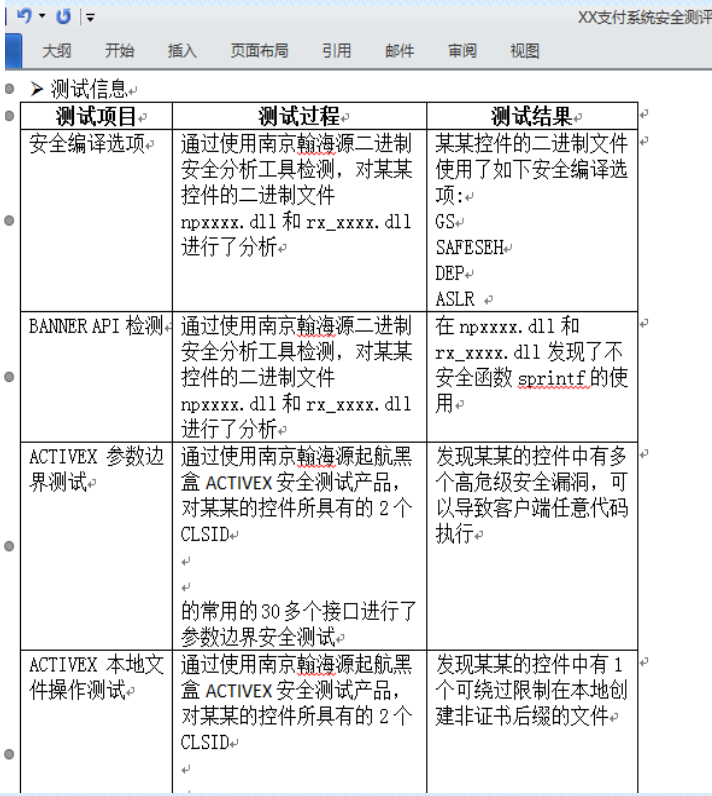
- 背景



➢ 测试技术方案

限于本次测试的资源，系统环境以及时间的限制，我们主要实施如下的安全测试以及相关使用的技术手段

测试类型	测试项目	测试编码	测试技术手段
WEB 应用安全测试	身份认证	APP-WEB-001	人工检测
	密码策略	APP-WEB-002	
	通道加密	APP-WEB-003	
	中间人回放攻击	APP-WEB-004	
	敏感操作日志	APP-WEB-005	
	会话一致性	APP-WEB-006	
	SQL 注射	APP-WEB-007	IBM APPSCAN
	XSS	APP-WEB-008	翰海源
	HTML 注射		JSONSCAN 工具
	CSRF	APP-WEB-009	
	页面重定向	APP-WEB-010	人工检测
	验证码	APP-WEB-011	
	超时限制	APP-WEB-012	
	错误次数限制	APP-WEB-013	
	文件上传路径检查	APP-WEB-014	
	信息泄露	APP-WEB-015	
	敏感文件存储	APP-WEB-016	
	服务器端执行	APP-WEB-017	
	异常参数导致服务器不响应	APP-WEB-018	
WINDOWS 本地二进制应用安全测试	安全编译选项	APP-BIN-001	翰海源二进制安全分析工具
	BANNER API 检测	APP-BIN-002	



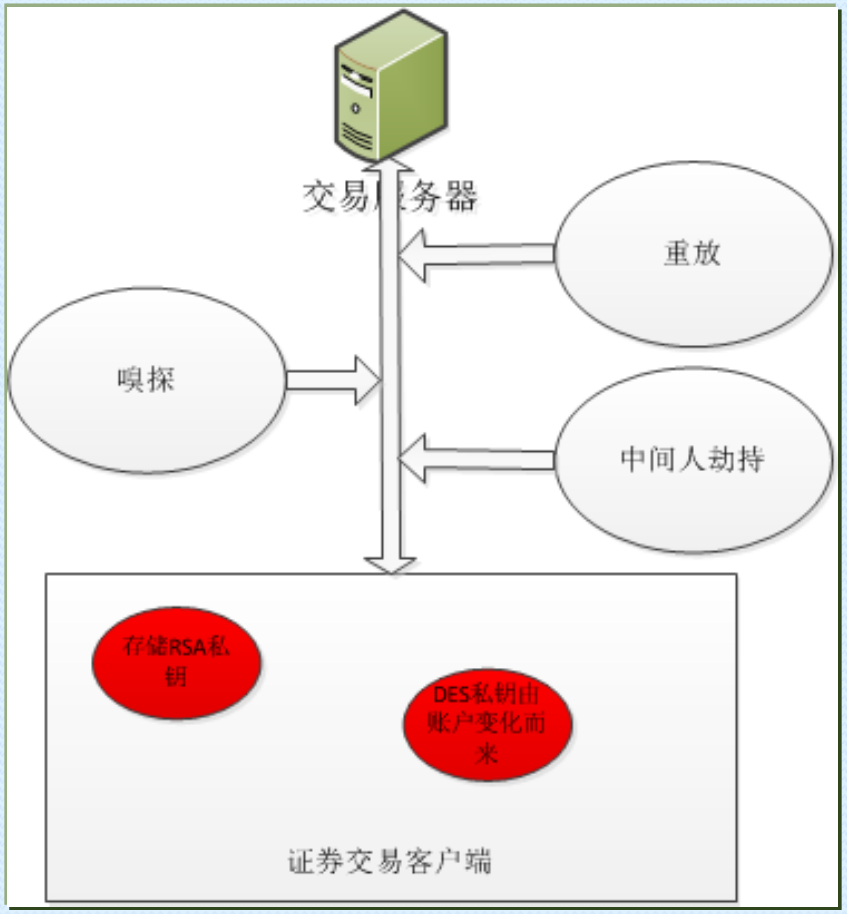
➢ 测试信息

测试项目	测试过程	测试结果
安全编译选项	通过使用南京翰海源二进制安全分析工具检测，对某某控件的二进制文件 npxxxx.dll 和 rx_xxxx.dll 进行了分析	某某控件的二进制文件使用了如下安全编译选项: GS SAFESEH DEP ASLR
BANNER API 检测	通过使用南京翰海源二进制安全分析工具检测，对某某控件的二进制文件 npxxxx.dll 和 rx_xxxx.dll 进行了分析	在 npxxxx.dll 和 rx_xxxx.dll 发现了不安全函数 sprintf 的使用
ACTIVEX 参数边界测试	通过使用南京翰海源起航黑盒 ACTIVEX 安全测试产品，对某某的控件所具有的 2 个 CLSID 的常用的 30 多个接口进行了参数边界安全测试	发现某某的控件中有多个高危级安全漏洞，可以导致客户端任意代码执行
ACTIVEX 本地文件操作测试	通过使用南京翰海源起航黑盒 ACTIVEX 安全测试产品，对某某的控件所具有的 2 个 CLSID	发现某某的控件中有 1 个可绕过限制在本地创建非证书后缀的文件

南京 翰海源

©2011 Vulnhunt, Inc. All rights reserved.

XXX证券软件安全测试

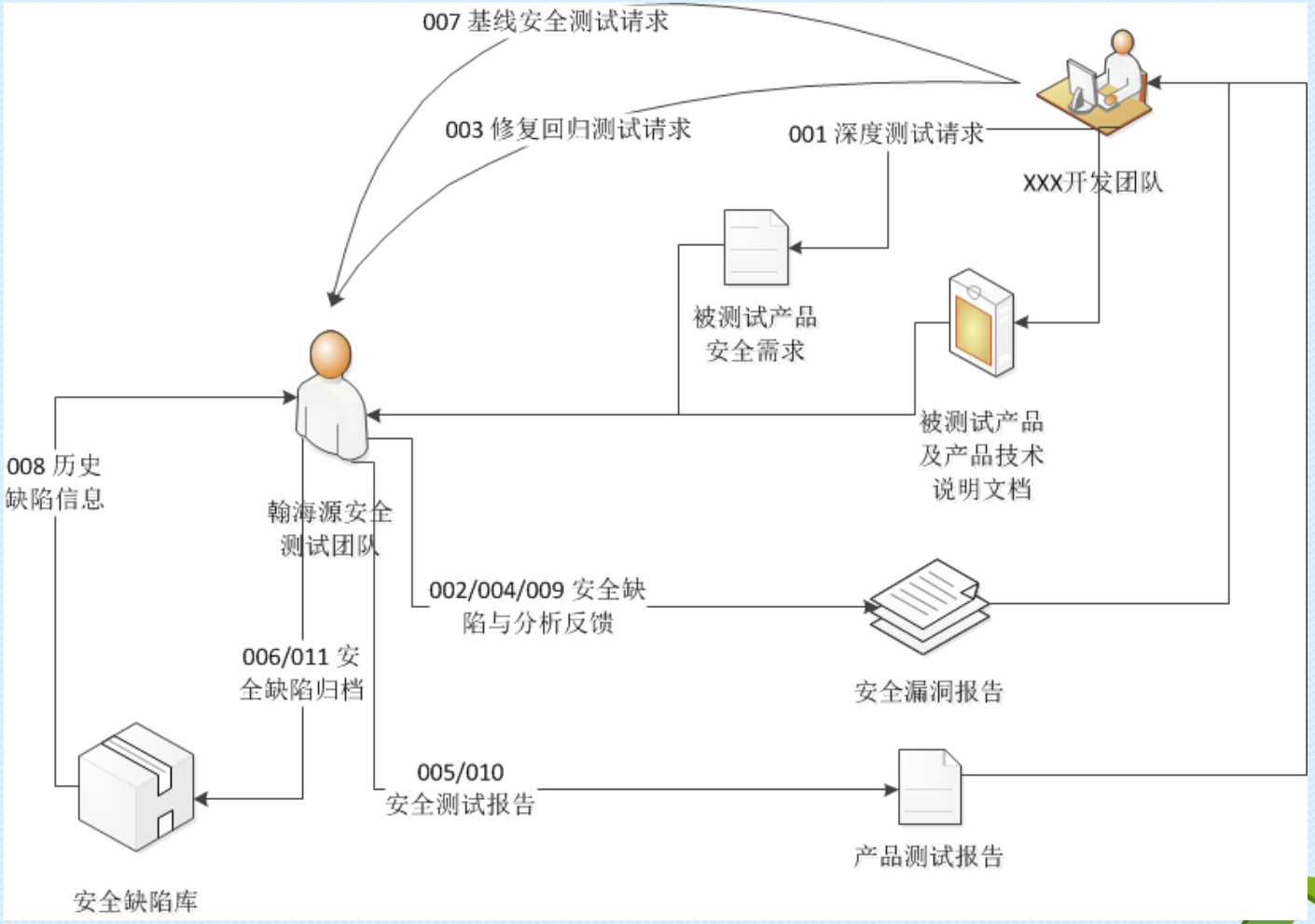


南京 翰海源

©2011 Vulnhunt, Inc. All rights reserved.

XXX安全系列产品安全测试

- 背景
- 需求

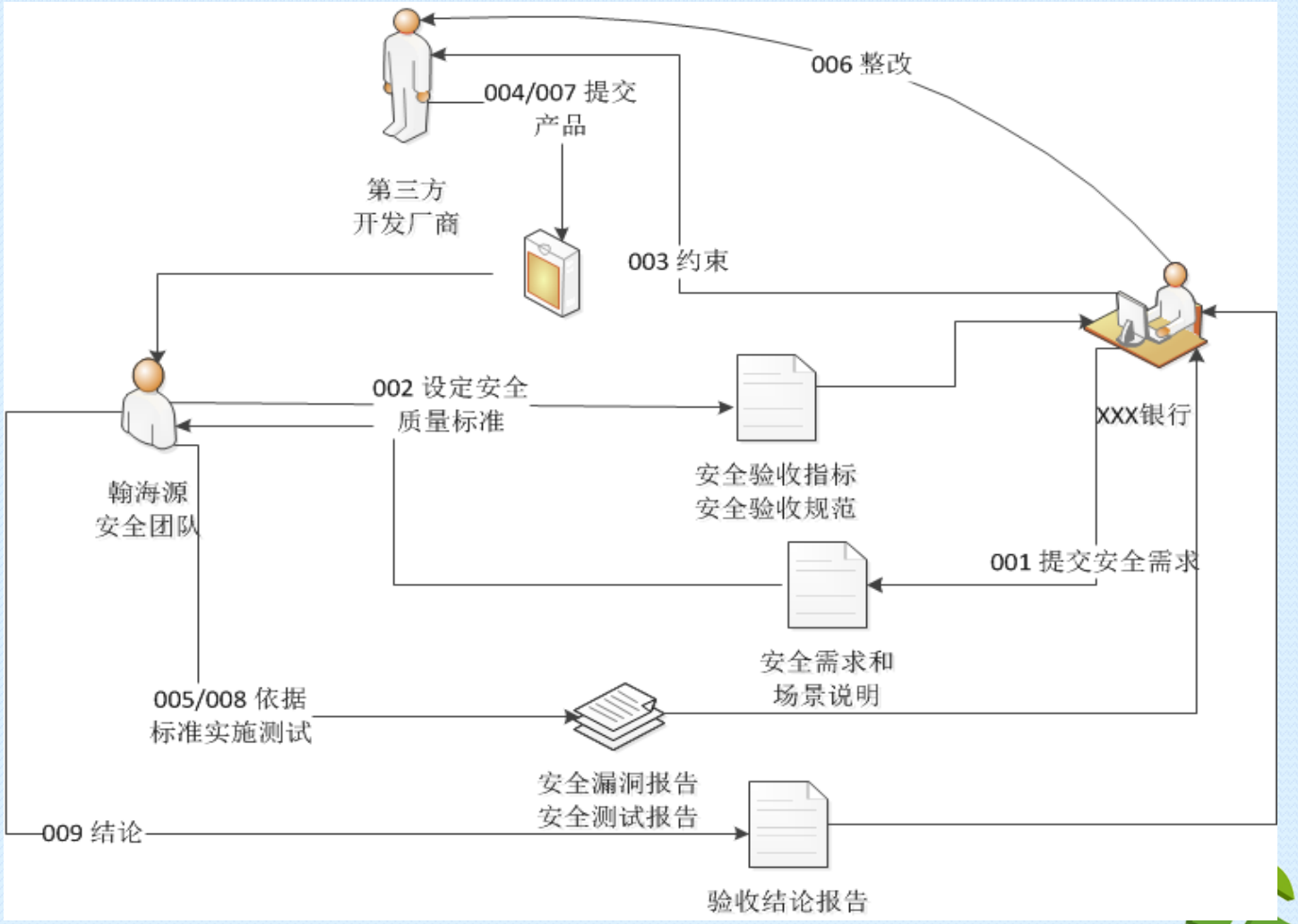


南京 翰海源

©2011 Vulnhunt, Inc. All rights reserved.

XXX银行第三方组件安全验收

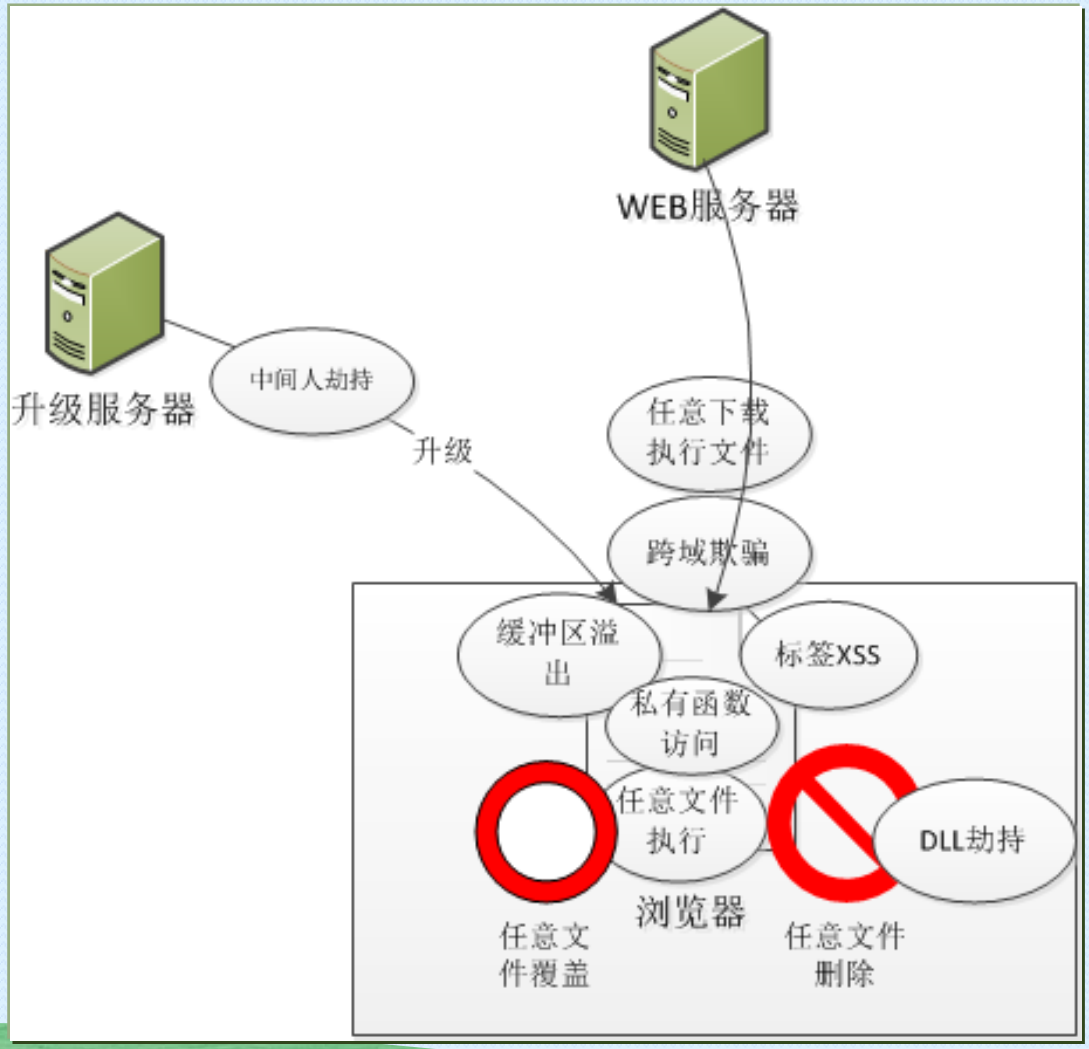
- 背景
- 需求



南京 翰海源

©2011 Vulnhunt, Inc. All rights reserved.

多家浏览器安全测试



南京 翰海源

©2011 Vulnhunt, Inc. All rights reserved.

让安全成为IT系统基础属性！

©2011 Vulnhunt, Inc. All rights reserved.

交流讨论

欢迎联系我们

www.vulnhunt.com

Xing_fang@vulnhunt.com

南京 翰海源

©2011 Vulnhunt, Inc. All rights reserved.