



追踪二进制代码审计系统

(版本：1.0)

技术白皮书



翰海源

南京翰海源信息技术有限公司



目录

1	背景介绍	3
2	软件安全的现状	3
3	目前软件安全测试的困境	4
1.	目前的测试方法	4
a)	静态的代码安全测试	4
b)	动态的安全测试	5
2.	当前的困境	5
4	追踪二进制代码审计系统	5
1.	产品特点	5
2.	软件架构	6
3.	基本原理——动态污染传播方法（Dynamic Taint Propagation）	6
4.	与其他测试方法比较	7
5.	功能特性	7
a)	自动化安全测试	7
b)	“零”样本测试，提高安全测试效率	8
c)	支持超过 30 多种漏洞类型的检测	8
d)	被测试产品提供较少的接口信息	8
e)	多种运行模式	8
f)	高级用户可编写插件，自行扩展检测规则	8
g)	详细的检测报表	9
6.	给您带来的价值	9
5	关于我们	9
6	联系我们	10

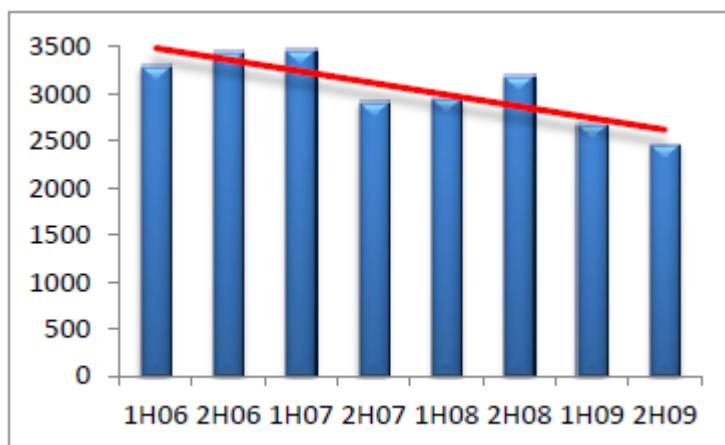
1 背景介绍

信息系统与网络特别是互联网的发展，促进了社会各个领域的发展，也使得人类社会对此产生了极大的依赖。而由于网络通信协议及信息系统软、硬件及其他方面存在的漏洞，也使得信息系统与网络特别脆弱，直接威胁到国家安全、经济建设、社会秩序、公众利益及公民的个人利益。目前，对于漏洞信息的公布已经逐渐商业化，成为国与国之间在现代战争中的秘密武器之一，造成漏洞无法及时得到修复或者根本得不到修复，网络安全形势日趋严峻。

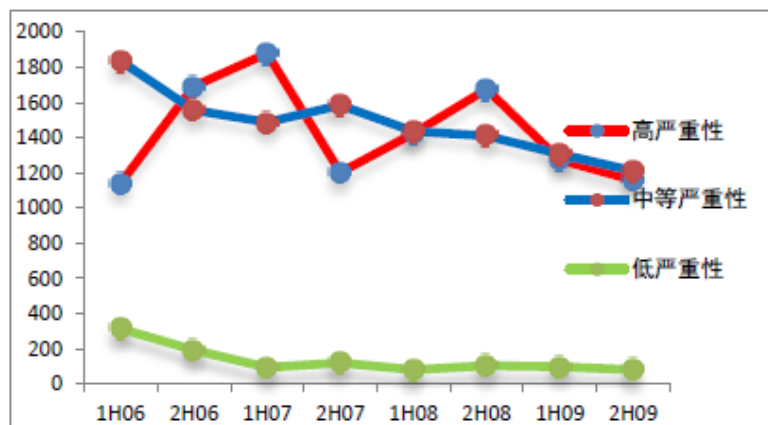
软件安全测试是修复安全威胁，保证软件能够安全使用的最主要的手段，如何进行高效的安全测试成为业界关注的话题。多年的安全测试经验告诉我们，做好软件安全测试的必要条件是：一是充分了解软件安全漏洞，二是拥有高效的软件安全测试技术和高可扩展性的测试工具。

2 软件安全的现状

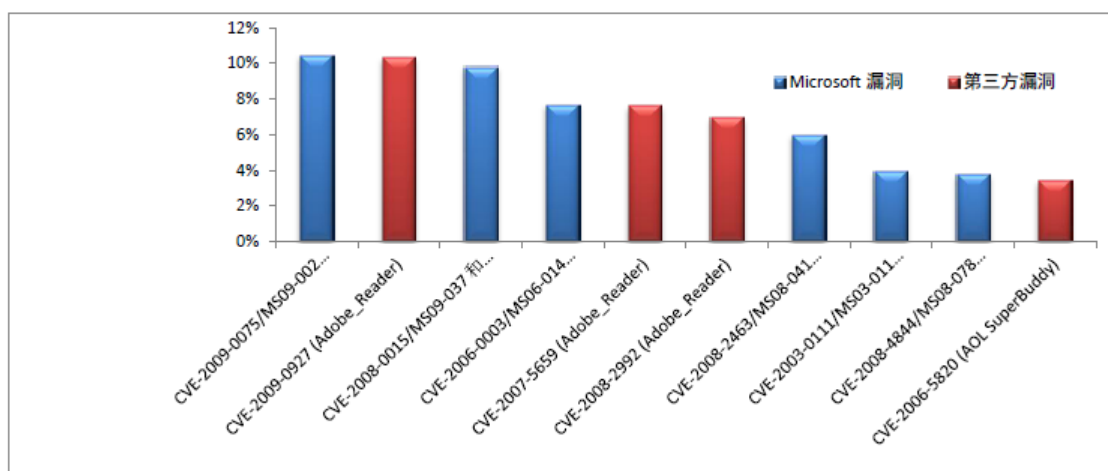
当今软件的安全性问题是越来越严重了，一方面黑客利用软件漏洞引起的安全事件数量越来越呈上升趋势，另一方面软件公司推出的补丁数量也呈上升趋势，尽管有些补丁是为加强软件的功能而推出的，但大部分的补丁却是针对软件漏洞的。



图一 2006 年上半年至 2009 年下半年的行业范围漏洞披露情况（按半年列出）



图二 2006 年上半年至 2009 年下半年的行业范围漏洞披露情况（按严重性列出）



图三 2009 年下半年内 Windows XP 上最常受到攻击的 10 大基于浏览器的漏洞

软件安全漏洞引发黑客攻击，挂马，蠕虫传播等危害，而针对软件漏洞的补丁对提高安全性起的作用又不是很大，看来为了提高软件的安全性和减少漏洞看来只有从软件开发时抓起，而软件开发公司对待软件开发的态上，为了节约成本、迎合用户及投资者以及为了在竞争中占尽先进，一心想着赶在约定的日期之前完成软件开发，只要提供预定的功能即可，软件安全性考虑的不多。按照业界的思维定势，软件安全性以后可以“借助于补丁解决”，但“功能要尽可能地多，因为功能特别是特色功能是卖点”。因此，软件漏洞越来越多也是自然的事了。大小软件公司国内国外基本都是如此。

近年来，微软在引入安全开发生命周期(SDL)之后，被研究人员发现的漏洞和几年前相比，数量已经下降了一半以上。对于某些产品(如 IIS 和 SQL 服务器等)而言，安全性能的改进是非常惊人的，从以前每年暴几十个漏洞利用程序，到 5 年才出现少数漏洞利用程序。而在 SDL 模型中，产品发布前的一个过程就是安全测试。

3 目前软件安全测试的困境

1. 目前的测试方法

目前主要安全测试方法主要有基于源代码静态的代码安全测试和基于 Fuzzing 技术的动态安全测试。

a) 静态的代码安全测试

主要是通过对软件系统的源代码进行安全扫描，根据程序中数据流、控制流、语义等信息与其特有软件安全规则库进行匹配，从中找出代码中潜在的安全漏洞。静态的源代码安全测试是非常有用的方法，它可以在编码阶段找出所有可能存在安全风险代码，这样开发人员可以在早期解决潜在的安全问题。而正因为如此，静态代码测试比较适用于早期的代码开发阶段，而不是测试阶段。同时，由于关系到开发部门，测试部门，管理部门等多个部门的工作，在实际的贯彻实施工作上有一定的难度。

b) 动态的安全测试

动态的测试也是常用的安全测试方法。使用自动化工具或者人工的方法模拟黑客的输入，对应用系统进行攻击性测试，从中找出运行时刻所存在的安全漏洞。这种是测试的特点就是真实有效，一般找出来的问题都是正确的，也是较为严重的。但渗透测试一个致命的缺点就是，但由于模拟的测试数据只能到达有限的测试点，覆盖率很低。根据美国权威机构统计，渗透测试的覆盖率只能达到 20%-30%，漏报率比较高。

2. 当前的困境

在当前基于源代码的安全测试中，呈现出来的困境是

- a) 误报率太高
- b) 动态数据流不完整，无法验证其报的结果

在当前动态的基于 fuzzing 的安全测试中，呈现出来的困境是

- a) 测试的深度较浅，漏报率太高
- b) 测试的覆盖率没有办法度量

4 追踪二进制代码审计系统

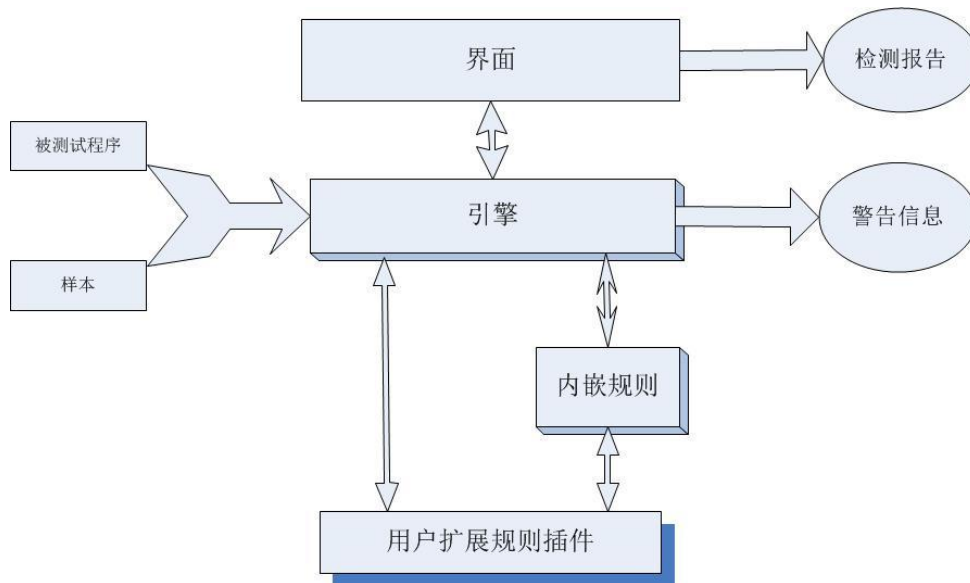
追踪二进制代码审计系统（以下称“追踪”）是一套针对编译好的二进制代码进行代码安全测试的系统，采用的是灰盒动态二进制测试方法，一种全新的安全测试方法，能够自动化发现软件中存在的安全漏洞。所以不需要软件的源代码就可以做安全测试。

1. 产品特点

“追踪”利用动态污染传播方法的特点，全自动化的进行污点源的标记，污染的传播，以及安全检测。测试过程可以不需要测试人员输入任何带攻击性的测试数据，就可以进行安全测试了，“追踪”会根据功能测试自动地找出软件中所有可能因外部输入数据而造成的安全问题，并根据漏洞类别清晰地报告出来。追踪代码审计的主要特点有：

1. 无需特殊的攻击性测试数据，让 QA 开发人员都可以做安全测试。解决测试缺乏安全知识，攻击知识的难题。
2. 由于直接跟踪外部输入数据，所以能够很真实、有效地找出系统中最严重，最关键的安全问题。
3. 可发现当前市面上的安全测试软件不能发现的二进制的潜在漏洞，内嵌上百个检测规则。
4. 可定位到该漏洞在什么地方产生的，能快速修复该漏洞；而且依托系统提供的信息，可快速构造出测试样本来验证该漏洞。
5. 支持强大的插件，可根据用户需求自定义标记污染源的规则和检测规则。

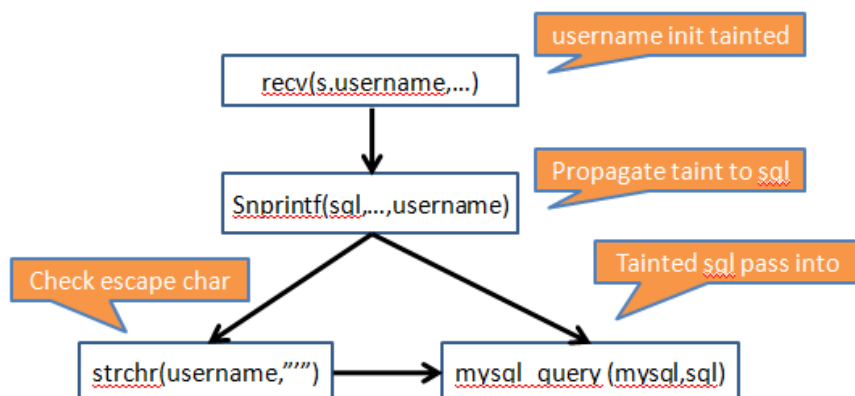
2. 软件架构



图四

3. 基本原理——动态污染传播方法（Dynamic Taint Propagation）

动态污染传播方法，主要通过跟踪外部输入的数据在程序中的传播过程，和最终执行的情况来分析是否存在安全漏洞和存在什么类别的漏洞。如下图五，它不需要任何特殊的攻击性的测试数据，它假定由外部输入的数据都是不可信的、污染的数据，为数据打上污染的标记，在程序中传播的过程中，如果经过了严格的，可以依赖的安全验证的话，就认为它不再是污染的，去掉污染标记，否则污染标记在整个传播过程都会被继承下来。一旦有污染标的数据被送到执行代码中执行的时候，就判断这里可能存在一个安全漏洞。



图五：污染数据的传播过程图



4. 与其他测试方法比较

“追踪”采用的是灰盒动态二进制测试方法，一种全新的安全测试方法。

二进制安全测试方法

静态的二进制安全测试

数据流，控制流，语义等信息与其特有软件安全规则库进行匹配

问题：动态过程追踪困难,中间语言转换困难

动态的 FUZZ 渗透测试

使用自动化工具或者人工的方法模拟黑客的输入

问题：覆盖率只能达到 20%-30%。漏报率比较高

	灰盒动态测试	动态测试	静态测试
		Fuzz 测试	白盒测试
软件源代码?	不需要	不需要	必须提供
二进制代码?	支持	支持	不支持
速度?	特快	慢	快
大量畸形样本?	不需要	需要	不需要
覆盖率?	与样本相关, 可以记录覆盖	与样本相关, 无法记录覆盖	可以记录覆盖情况
快速定位异常数据点?	可以	不可以	可以
动态数据跟踪?	完全	不可以	部分
测试深度?	深	浅	中
分析测试结果难易度?	简单	困难	简单
漏报率?	相对小	相对大	相对中
误报率?	相对小	基本无	大量
样本生成难易度?	相对简单	畸形测试数据就是样本	基本不可能

5. 功能特性

a) 自动化安全测试

给一个普通样本，出安全漏洞报告，全自动化。



b) “零”样本测试，提高安全测试效率

较少的样本发现潜在安全问题。
方便快捷得到检测报告。

c) 支持超过 30 多种漏洞类型的检测

- ▣ 命令注入(Command Injection)
- ▣ 跨站脚本(Cross-Site Scripting)
- ▣ 格式化串(Format String)
- ▣ 缓冲区溢出(Buffer Overflow)
- ▣ 整型溢出(Integer Overflow)
- ▣ 整数符号扩展(Signed Integer Extern)
- ▣ 双重释放内存(Double Free)
- ▣ 释放内存后再使用(Use After Free)
- ▣ 数组索引越界(Array Index Overflow)
- ▣ Directory Traversal
- ▣ Sql Injection
- ▣ 等等……

d) 被测试产品提供较少的接口信息

无需被测试软件提供源代码，只需要提供执行程序的二进制执行文件环境和一些简单的接口信息，就可以在“追踪”的系统上进行灰盒测试。在测试过程中，“追踪”引擎跟踪程序执行的每一条指令，并对其的执行进行规则检查，通过指令规则和插件规则，进行自动处理污染传播。对于产品的源代码级别相当于黑盒测试，而相对于被执行的指令级别是白盒测试。

e) 多种运行模式

多种污染源模式，对于文件、网络、流文件等有不同的模式，针对性地处理样本，以提高运行的效率。

文件模式：记录来自文件的数据，并检测其传播过程。

网络模式：记录来自网络的数据，并检测其传播过程。

流文件模式：记录来自流文件的数据，并检测其传播过程。

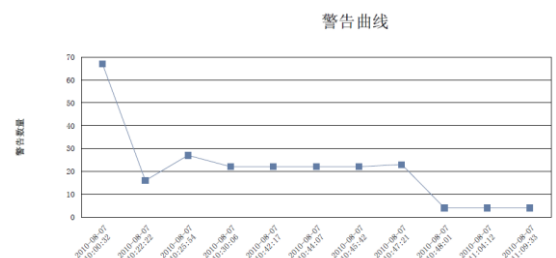
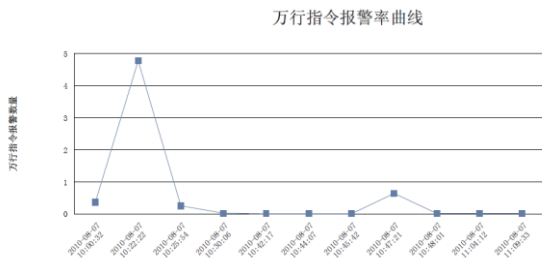
指令模式：记录指令执行流程，检测执行数据。

f) 高级用户可编写插件，自行扩展检测规则

引擎会提供接口，安装时已提供一个常用的规则插件。会有专门的插件编写手册。



g) 详细的检测报表



6. 给您带来的价值

1. 降低对安全测试人员的要求
2. 提高代码质量，增加在客户心中的形象
3. 减少安全测试的时间
4. 减少修复漏洞的成本
5. 规避安全事件带来的危害

5 关于我们

中国首家专注于软件安全测试的专业公司，十多年的软件安全领域研究经验，依托全球知名的 Code Audit Labs(代码审计实验室)，默默地在为各大软/硬件产商提供安全测试外包服务，为软件的代码质量做出自己的贡献。安全测试是个高门槛，高技术含量的工作，一般的企业很少有自己的安全测试团队。那么，我们翰海源就是您的安全测试团队。



翰海源 追踪二进制代码审计系统 V1.0

目前翰海源的产品包括：

- a) 追踪二进制代码审计系统
- b) 起航黑盒测试系统

目前翰海源的安全服务包括：

- a) 软件安全测试服务
- b) 硬件安全测试服务
- c) SDL 培训
- d) 安全过程改进服务

目前，我们的客户已经遍布世界各地，包括：中国大陆，中国台湾，美国，英国，西班牙，澳大利亚，新加坡，德国，以色列，巴西，印度等。行业覆盖：金融、电信、服务业、政府等。

我们的愿景：专注于安全测试，为信息安全提供基石；希望能成为您的安全测试团队。

翰海源—您身边的安全测试专家。

6 联系我们

南京翰海源信息技术有限公司

地址：南京市鼓楼区管家桥华荣大厦 2211 室

邮编：210005

电话/传真：025-84430521

软件测试外包或者购买我们的产品，请联系

sales@vulnhunt.com

www.vulnhunt.com