代码安全机制与实现技术

测试应用程序的安全性

姚砺

东华大学计算机学院

我测故我在

软件测试是一项非常复杂的、创造性的和需要高度智慧的挑战性任务。

软件测试的现状

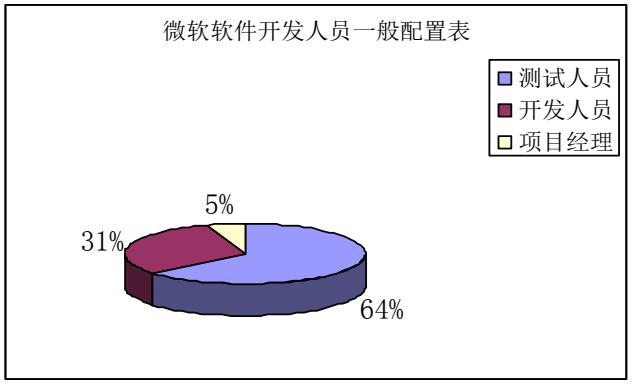
- 软件测试在软件生命周期中占据重要的地位，软件测试慢慢的独立发展成为一个行业，并且在迅猛发展。
- 对美国大量软件项目的观察结果表明，软件项目的成功在很大程度上依赖于软件测试的成功。软件测试在软件企业中担当的角色是“质量管理”，即及时纠错及时更正，为产品推向市场贴上“质量合格”的标签。
- 开发与测试
  - 进攻与防守：好看靠进攻，冠军靠防守

软件测试的现状

- 对国际著名IT企业的统计数据表明，软件测试在整个软件项目中所占的比例为 40% 以上，占整个项目费用的 50% 以上，软件测试人员与开发人员的人数比例接近1:1。
- 国内软件企业在软件测试上的投入一般在 5% 以下，测试人员所占比例很小(软件测试人员与开发人员之比仅为1:8)，经常处于从属地位。中国软件工业要健康发展，必须正视和努力缩小这个差距。

微软的测试

- “很多人都认为微软是一家软件开发公司，而事实上，我们是一家软件测试公司” —比尔盖子
- 在微软内部，软件测试人员与软件开发人员的比率一般为1.5-2.5左右



	Exchange2000	Windows2000
项目经理	25人	约250人
开发人员	140人	约1700人
测试人员	350人	约3200人

软件测试的作用

- 软件质量与软件质量保证
  - 教学考试与教学质量保证
- 软件开发的每个阶段都要测试，测试人员应该参与设计阶段：评审安全性设计
- 传说中的微软测试部门的格言：没有最BT，只有更BT。

软件测试之独孤九剑

- 全程测试，测试先行
- 剑走偏锋 — 不走寻常路
- 完全测试程序是不可能的
- 软件测试是有风险的行为
  - 程序中的大部分错误往往是在一小部分模块中发现的--帕雷托定律
- 设计周密的测试用例
  - 先求开展，后求紧凑，乃可缜密矣----《九阴真经》
- 框起你的测试来
  - 刚中带柔，柔中带刚，如海中波涛，刚柔并济。— 排云掌第五式“云海波涛 ”
- 具有良好的计算机编程基础
- 优秀的安全测试人员格言：给我一个socket，我能破坏任何软件。

一次转身最远能产生多远的距离 —从传统软件测试转向安全性测试

- 如果不付出相当大的努力去消除，每个复杂的软件程序都会有代价高昂的安全漏洞。这些漏洞会造成病毒和蠕虫的横行，也会使得罪犯能够攫取用户的个人财务数据，而这些用户已如惊弓之鸟，并且本来就很不愿意把他们的个人数据放在Internet上。
- 2005年，CardSystems成为数字化攻击的牺牲品，由于对信用卡数据在未加密情况下存储，有4000多万张借记卡和信用卡泄密，4个月后，这家公司倒闭出售。
- 安全性测试：不是验证软件的正确性，而是挖掘软件的漏洞（软件中的“不应该”和“不允许”部分，例如：代码中的缓冲区溢出漏洞，电子秤中的作弊后门等）。--- 越崩溃越快乐！
- RFC2828将漏洞定义为“系统设计、实现或操作和管理中存在的缺陷或弱点，能被利用而违背系统的安全策略”
- 例如：对于一个web输入界面的测试，其上有个字段【银行账号】（正确输入是12个数字），对该字段的测试包括：
  - 正确输入验证：正好12个数字（分该账号存在和不存在两种情况验证）
  - 异常输入验证：（模仿用户的一些无意错误操作）输入不满12个数字，超过12个数字，有非数字字符，空，等等。
  - 安全测试：SQL注入攻击（用web代理来输入，绕过客户端的检验检查）、跨站点脚本输出、整数溢出等。
- 安全测试的出发点：像攻击者一样思考

一些攻击模式的范例

- 验证用户输入不会提供机会让攻击者通过已知的SQL注入攻击来操纵后台数据库；
- 验证不存在跨站点执行脚本的可能性；
- 验证在向服务器发送一个它不能正确处理的非法数据包的情况下，服务器不会崩溃；
- 验证用户输入不会导致数据处理溢出；
- 验证程序对错误的处理是恰当的；
- 验证数据在网络传输中或存储时是经过了保护的
- 验证不会出现信息泄露
- 验证访问控制
- 。。。。。

建立安全性测试计划---基于风险的安全测试

- **威胁/风险建模：排定安全测试的优先级。在对应用程序的设计和应用流程加以理解的基础上，可假定潜在的安全风险并对其进行评价。然后，根据易于攻击和攻击的影响严重性，将这些威胁进行分级并依次消除。然后安全测试人员就可以将其注意力集中于那些攻击难度最低而影响最大的领域。**
- **流程：**
  - 信息搜集：需要测试哪个应用程序和应用程序中的哪些模块（组件），对每一个模块（组件）做哪些安全假设，每个组件的哪些安全因素需要测试，预期的结果是什么。
    - 登录页面：（见后）
  - 识别威胁
  - 将与威胁相关的风险进行分级
  - 潜在的破坏程度
  - 再现性和可利用性：探测并利用这个漏洞所做的努力
  - 受影响的用户

登录页面的威胁分析

- 猜测口令：设计时应设计登录试探次数，例如：只许试探三次，然后锁定ip地址。
- 利用password文件系统地猜测口令：加密文件（密码强弱，文件存放是否安全）
- 分析协议和滤出口令：不能明文传输，密码的强弱
- 重放攻击：加时间戳
- 木马监视登录/口令：系统安全，一次性口令
- 盗链：
- SQL注入漏洞
- 异常输入破坏：

安全测试技术之七种武器

- 一个完整的WEB安全性测试可以从以下几个方面入手：
- 1.安全体系测试
  - 网络是否提供了安全的通信
  - 部署拓扑结构是否包括内部的防火墙
  - 部署拓扑结构中是否包括远程应用程序服务器
  - 操作系统是否存在漏洞，例如Unix上的缓冲区溢出漏洞、Windows上的RPC漏洞、缓冲区溢出漏洞、安全机制漏洞等；
- 2. 输入验证
  - 如何验证输入
  - 是否清楚入口点
  - 是否验证Web页输入
  - 是否对传递到组件或Web服务的参数进行验证
  - 是否验证从数据库中检索的数据
  - 是否依赖客户端的验证
  - 应用程序是否易受SQL注入攻击
  - 应用程序是否易受XSS攻击
  - 如何处理输入

- 3. 身份验证和授权
  - 是否区分公共访问和受限访问
  - 如何验证调用者身份
  - 如何验证数据库的身份
  - 如何向最终用户授权
- 4. 敏感数据
  - 是否存储机密信息
  - 如何存储敏感数据
  - 是否在网络中传递敏感数据
- 5. 加密
  - 为何使用特定的算法
  - 如何确保加密密钥的安全性
- 6. 参数操作
  - 是否验证所有的输入参数
  - 是否在参数过程中传递敏感数据
  - 是否为了安全问题而使用HTTP头数据
- 7. 审核和日志记录
  - 是否明确了要审核的活动
  - 是否考虑如何流动原始调用这身份

应用服务器的安全性测试技术

- 一、应用服务器的安全性测试内容

  基于应用服务器的安全性测试内容主要包括：验证隐私系统是否受到保护、数据是否加密，检测系统是否有安全保密的漏洞，检验系统及其所在的网络是否能够承受各种类型的恶意攻击。对于Web 服务器而言，具体测试内容还有测试用户登录与注册、是否有超时限制、服务器脚本语言、日志文件、目录安全、SSL 安全传输测试等。

- 二、应用服务器的安全性测试方法与技术

（一）全面搜集与应用服务器安全相关的各种信息，分析其可能出现的安全隐患应用服务器被使用的企业单位基本信息、管理中薄弱环节、应用服务器配置信息、系统可访问的主机IP 地址及对应的主机名、服务器所在网络的拓朴结构等，这些信息可能成为被利用的安全隐患，有的可能在互联网上搜索得到，要对其进行分析和安全隐患检查。

应用服务器的安全性测试技术

（二）应用服务器的漏洞探测和扫描

1、利用搜索引擎搜索已公布的漏洞。可利用Google 等工具搜索资源，研究系统漏洞。可访问CVE（公共漏洞和暴露）数据库，查找漏洞。Packet Storm 组织是由一些致力于提供必要信息以安全化全球网络的安全专业人士组成的非盈利组织，在其网站上可以找到许多安全信息，如Windows 中缓冲区溢出漏洞、Unix主机中远程过程调用（RPC）的安全隐患、FTP漏洞，Sendmail邮件服务软件的漏洞等。

2、利用扫描工具进行漏洞探测。服务器漏洞扫描的工具很多，基于Linux的扫描工具有Namp、Netcat、Nessus。基于Windows的端口扫描器有NeWT 等。还有很多扫描工具，如：著名的COPS、Tiger、Fluxay5（流光）、X-scan、N-Stealth、Metasploit Framework（http://metasploit.com:55555/）等。其中，很多工具可以在网上免费下载。可以利用上述工具探测系统漏洞，查看系统是否打了补丁。

应用服务器的安全性测试技术

（三）模拟攻击测试

采用拒绝服务、缓冲区溢出攻击、密码破解攻击等方法进行测试。

1、Web 服务器利用测试。针对Windows IIS5.0 Web 服务器中的目录遍历漏洞（CVE-2001-0333），可采用如下方法测试。若主机IP 为：67.168.100.102，则在IE 的地址栏中输入：

http://67.168.100.102/scripts/..%255c..//winnt/system32/cmd.exe?c+dir

若在浏览器中看到目录C:\inetpub\scripts 中的内容，则说明存在漏洞。

2、拒绝服务攻击测试。Land 攻击：判断网络数据包的源地址和目标地址是否相同。

Ping Of Death 攻击：判断数据包的大小是否大于65535 个字节。如果操作系统接收到长度大于65535 字节的数据包时，就会造成内存溢出、系统崩溃等后果。

Teardrop 攻击：对接收到的分片数据包进行分析，计算数据包的片偏移量(Offset)是否有误。某些操作系统收到含有重叠偏移的伪造分片数据包时将会出现系统崩溃、重启等现象。

SYN Flood 攻击：从随机的或欺骗来的IP 地址产生大量的SYN数据包，导致合法请求被拒绝。

SMBDie 攻击：利用SMB（服务器消息块）中代号为CVE-CAN-2002-0274 的缓冲区溢出漏洞攻击，可能导致Windows 计算机死亡蓝屏。

应用服务器的安全性测试技术

3、E-mail 炸弹攻击测试。邮件炸弹不仅能造成收件人信箱爆满而无法再接收其他的邮件，而且还会加重网络的流量负荷，甚至会导致整个邮件系统瘫痪。常见的邮件炸弹软件有KaBoom!、Avalanche 等。

4、密码破解和特权提升测试。采用穷举法、漏洞利用和字典法等方法破解系统用户密码，常用工具有：L0phtcrack 、Crackerjack、John the Ripper 等，在试着破解前用pwdump5来获取密码的哈希，可参考网站：http://www.openwall.com

SQL Server 弱口令测试：用scansql.exe 工具测试SQL Server 数据库应用系统是否有默认用户SA 及弱口令。

击键记录测试：采用击键记录工具（如keylog5.exe）进行测试。检查能否记录管理员的用户名和口令。

登录测试：对用户名和匹配的密码进行校验，以阻止非法用户登录。可测试输入的密码是否对大小写敏感、是否有长度和条件限制、最多可以尝试多少次登录等情况。

测试时可以将上述多种方法混合使用，进行暴力攻击测试。

应用服务器的安全性测试技术

（四）使用计算机病毒及木马测试系统的防护能力

最典型的计算机病毒和木马有“木马代理”、“网游大盗”、“艾妮”、“熊猫烧香”、“QQ 木马”、“灰鸽子”等。有的木马能绕过天网等大多数防火墙的拦截。可以利用这些典型病毒和木马测试应用服务器系统的防护能力，验证服务器检测到病毒时的应急能力。许多病毒和木马在网上很容易下载到。可以使用网页木马生成器方便地生成木马。也可以利用操作系统的Shell 编程技术和Socket 编程技术尝试编写新的攻击程序，用于系统安全性测试。

（五）数字取证测试

利用系统中的日志、审计、Cookies、历史记录等功能，验证应用服务器遭到攻击后是否留下痕迹，便于取证。