B/S架构软件的安全性测试研究

郑雷雷[1,2],宋丽华[1,2],郭 锐[1,2],张建成[1,2]
(1.山东省计算中心,山东 济南 250014;
2.山东正中计算机网络技术咨询有限公司,山东 济南 250014)

摘 要:网络技术的发展使得以Web2.0为核心的应用越来越广泛,B/S架构软件的安全缺陷和漏洞不断增多,B/S架构的特殊性使得对B/S架构软件的安全性测试方法应不同于传统软件。文中描述了B/S架构软件的特点,对Web软件的安全性测试进行了分类,并详细阐述了测试要点和测试内容。从攻击者的角度,分析了Web软件常见的安全漏洞和测试方法。最后总结了当前研究工作并指出了未来软件安全性测试技术的研究重点与发展方向。

关键词:Web服务;B/S架构;安全性测试;安全漏洞
中图分类号:TP31 **文献标识码**:A **文章编号**:1673-629X(2012)01-0221-04

Research on Security Testing to B/S Structure Software

ZHENG Lei-lei[1,2],SONG Li-hua[1,2],GUO Rui[1,2],ZHANG Jian-cheng[1,2]
(1. Shandong Computer Science Center,Jinan 250014,China
2. Shandong Zhengzhong Computer Network Technology Consulting Co.,Ltd, Jinan 250014,China)

Abstract:Web 2.0 service applications are applied more and more widely based on network technology, the security flaws and vulnerabilities of B/S structure software are growing, the B/S structure software's security testing is different from the traditional software because of its own unique attributes. In this paper, firstly described the attributes of the B/S structure software, classified the content of its security testing, and then, elaborated the main testing points and context. From the perspective of attacker,analyzed the common Web services security vulnerabilities and the test methods. In conclusion,summarized the present study and pointed out future focus and development directions of software security testing technology.

Key words:Web service;B/S structure;security testing;security vulnerability

0 引 言

随着网络的快速发展和应用,信息系统模式的解决方案中以Web为核心的应用也越来越多,当前的信息化建设中,多数用户都开始采用B/S架构的软件。在Browser/Server(B/S)架构下,用户通过Web浏览器(Browser)来处理少量的事务逻辑,主要的工作在Web服务器端(Server)实现。B/S架构软件大大降低了用户端的数据处理量,降低了用户承担的负载,系统维护与升级消耗的工作量和费用大大减轻。

软件测试是保证软件产品质量的重要手段,除了传统的功能和性能测试之外,安全性测试也越来越成为人们关注的重点。软件安全性测试除了明确用户需要做什么之外,更关注于用户不该做什么[1],一个安全的软件需要对数据进行加密、对用户进行相应的授权,保证数据传输过程中或到达目的地后不被非授权的人访问,软件的安全性还表现在软件在受到恶意攻击时仍提供所需功能的能力。因此对软件的安全性测试:一方面是对已有的功能模块进行安全验证;另一方面是发现软件中存在的各种隐患,也就是漏洞[2]。B/S架构软件的结构特点,决定了对B/S架构软件的安全性测试要采用特殊的方法。

收稿日期:2011-06-15;**修回日期**:2011-09-22
基金项目:山东省信息产业专项发展资金项目(2010X0125)
作者简介:郑雷雷(1984-),男,山东潍坊人,硕士研究生,研究方向为计算机软件与理论、信息系统咨询与监理。

1 B/S架构软件的特点

B/S架构(见图1)软件特点如下所示[3]:

(1)用户所在的客户端使用Browser访问服务器,访问结果以网页表单的形式进行展示;

(2)用户的客户端一般只能完成很简单的功能操作,如浏览、查询、输入等,绝大部分数据处理工作都由服务器完成;

(3)服务器采用Cookies保存用户信息,客户端与服务器之间的信息交流通过Internet传送完成[4]。典型的B/S系统是一种三层结构的系统,客户端应用程

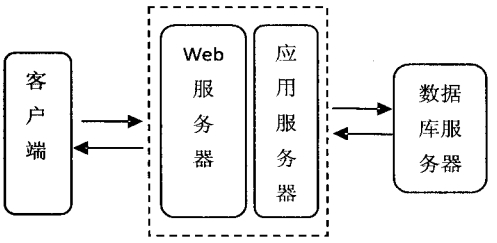

图 1 B/S 架构软件结构

序精简到一个浏览器软件,服务器端 Web 程序的功能模块由 Web 页面构成,客户端使用浏览器和服务器进行数据交换,因为 Web 服务应用直接对外开放,Web 服务的安全性至关重要。

2 B/S 架构软件安全性分类

软件的安全性侧重于两个方面[5]:一方面是应用程序级别的安全性,包括对数据或业务功能的访问,确保操作者只能访问授权的功能和数据;另一方面是系统级别的安全性,包括对系统的登录或远程访问,确保只有具备相应访问权限的用户才能访问应用程序,而且只能通过相应的入口来访问。

B/S 架构下客户端软件主要是 Web 页面,那么 B/S 架构软件的安全性可分为:数据或功能访问控制安全和页面访问控制安全。

2.1 数据或功能访问控制安全

数据或功能访问安全性可保证在预期的安全性情况下,不同授权的用户只能访问特定的功能,或者只能访问有限的数据。例如,普通用户可进行输入数据、创建新账户等操作而不能随意删除数据或账户,只有管理员才能删除数据或账户。

2.2 页面访问控制安全

页面访问控制安全性主要有:

(1)页面登录。B/S 架构软件必须测试登录用户名和密码的有效性、输入大小写的敏感性、用户登录是否有次数限制;而且要测试是否可以不登陆而直接浏览某个页面、IP 地址登录是否有限制等;

(2)超时限制。如果用户登陆系统后在一定时间内没有进行任何页面操作,应进行超时判断,强制用户重新登陆后才能正常使用系统。

(3)日志文件。日志文件是保证 Web 应用系统安全性的重要的工具。B/S 架构软件需要测试日志文件记录信息的完整性、各类操作的可追踪性。在服务器后台,还要检测服务器的日志记录是否正常进行。

(4)SSL。为保证信息在 Internet 上传输的安全性,B/S 架构软件会采用 SSL 技术。如果使用了 SSL,测试人员需要测试加密的正确性、检测信息的完整性,确定是否有相应的替代页面。当用户进入或离开安全站点的时候,是否有相应的提示信息。

(5)脚本安全性。服务器端的各类数据处理脚本常常成为安全漏洞而被黑客所利用。找出当前站点使用了哪些脚本语言,并研究该语言的缺陷,而且应该确定没有经过授权,相关人员就不能在服务器端保存和编辑相关脚本。

3 安全性测试技术手段

Web 应用软件的安全性测试可总结为:为确保数据访问安全而进行的安全功能测试和为保证页面访问安全而进行的安全漏洞测试两个方面。安全功能测试基于软件的安全功能需求说明,测试软件的安全功能实现是否与安全需求一致;安全漏洞测试则站在攻击者的角度,以发现软件的安全漏洞为目的[6]。

3.1 安全功能测试

Web 服务主要的安全功能需求包括身份认证、消息机密性、不可否认性、完整性、授权、可用性、访问控制、审计跟踪、安全管理、隐私保护等。安全功能测试主要针对上述安全内容的具体实现进行功能性测试验证[7,8]。

功能验证就是对软件需求中确定的有关安全模块的功能进行测试验证。开发者一般会在软件设计和开发过程中增加一些必要的安全防护措施,如权限管理模块、数据加密模块、传输加密模块等。安全功能验证可以采用与一般程序功能测试相似的方法,如黑盒测试、白盒测试或灰盒测试等方法来进行。

Web 服务常见安全功能实现标准见表 1。

表 1 Web 服务常见安全功能实现标准

功能安全需求	功能安全实现标准
身份认证	SAML, Kerberos, WS-Federation, WS-Security, OpenLiberty Project
隐私保护	WS-Privacy, P3P
完整性	WS-Security, XML-Signature
审计跟踪	NIST SP 800-92
访问控制	XACML, JAAS, XrML
不可否认性	WS-Security, XML-Signature
消息机密性	SSL/ TLS/ HTTPS, WS - Security, XKMS, XML-Encryption

3.2 安全漏洞测试

安全漏洞测试就是识别软件的安全漏洞。漏洞指的是存在于一个系统内的弱点或缺陷,漏洞被利用可

能造成软件受到攻击,使软件进入不安全的状态[9,10]。

B/S 应用程序攻击包括[11]:对程序本身的拒绝服务攻击、改变网页内容以及窃取用户信息等。常见的 B/S 应用安全漏洞有:已知弱点和错误配置、隐藏字段、后门和调试漏洞、跨站点脚本编写、参数篡改、更改 Cookies、缓冲区溢出、直接访问浏览等。

3.2.1　参数篡改

WSDL 文件(Web 服务描述文件)保存了 Web 服务提供的方法、调用这些方法需要的参数个数以及需要的参数类型等重要信息。参数篡改是指:首先对 WSDL 文件进行扫描,寻找 Web 服务调用可接受的参数类型,故意发送 Web 服务不期望的数据类型,对 Web 服务进行攻击。

3.2.2　XML 解析器攻击

XML 消息可以对递归实体进行扩展。基于这一特征,攻击者通过恶意构造包含大量递归嵌套元素的消息,例如构造嵌套 100000 层的消息,用来耗尽服务器资源或者使 XML 解析器崩溃,达到拒绝服务攻击的目的。

3.2.3　注入式攻击

SOAP(简单对象访问协议)是一种轻量的、简单的、基于 XML 的协议,它被设计成在 Web 上交换结构化的和固化的信息。SOAP 消息携带了 Web 服务调用需要的参数,而这些参数极有可能是 SQL 查询语句或者 XPATH 查询语句的一部分。注入式攻击者构造相关的查询语句或者认证语句用来绕过数据库认证,从而执行非法查询操作、恶意篡改数据或者非法执行系统命令等[12,13]。

例如下面的 XPATH 语句用来在数据库中查询操作者的用户名和密码:

user[name= 'nare' and pass= 'misback']

攻击者通过插入字段'or 1= 1 or'' ',构造新语句,导致系统返回所有的用户信息:

user[name= 'nare' or 1=1or'' and pass= 'misback']

常用的特殊参数集见表 2。

表 2　常用的特殊参数集

对象	元字符
Perl	$ % #/00
HTML	<>
SQL	-;' " '
OS	./%00 * |''
Web 服务器	../%00
C 和 C++	%00

3.2.4　Cookies 测试

Cookies 是指 Web 服务器为了辨别用户身份、进行 Session 跟踪而储存在用户本地终端上的数据(通常经过加密)。当用户访问某些页面时,Web 服务器通过 Cookies 存储用户的相关信息和用户进行的操作序列。Cookies 最典型的应用是判定注册用户是否已经登陆网站,如果 B/S 架构软件使用了 Cookies,而且服务器在 Cookies 中保存了用户的注册信息,那么应确认该 Cookies 能够正常运行而且对用户的注册信息进行了加密处理。Cookies 测试可用 IE Cookies View 或 Cookies Manager 进行。

3.2.5　跨站脚本攻击

跨站脚本攻击(也称为 XSS)指利用网站漏洞从用户那里恶意盗取信息。用户在浏览网站、使用即时通讯软件或者在阅读电子邮件时,通常会点击其中的链接。攻击者通过在链接中插入恶意代码,就能够盗取用户信息。对于跨站脚本攻击进行防范主要有两方面:验证所有输入数据,有效检测攻击;对所有输出数据进行适当的编码,以防止任何已成功注入的脚本在浏览器端运行。

4　安全性测试工具

安全性测试工具以自动化或半自动化的方式验证系统安全功能运行是否正确、安全机制是否有效和查找潜在的安全漏洞,可有效提高测试效率,降低软件安全风险[14]。Web 应用安全测试工具在测试中有的作为客户端使用,向目标服务器发出请求,有的则是作为代理服务器,接收目标客户端的请求。按照文中的测试关注点列举了两类安全测试工具:一类关注于 Web 功能安全,对 Web 服务的安全功能进行测试,另一类关注于 Web 应用漏洞检测,扫描常见 Web 服务安全漏洞。

Web 服务扫描器专用于测试 Web 服务的安全功能并识别 Web 服务的安全漏洞。典型功能有扫描 WSDL 文件,列举 Web 服务提供的方法,生成各种输入参数操纵方法调用,测试 XML 消息加密、XML 消息签名、签名验证等安全功能,WS-Security 安全规范一致性测试。Web 服务扫描器包括 Parasoft 公司的 SOATest、Vordel 公司的 SOAPbox、Optimyz 公司的 WebServiceTester 等;开源的有 Foundstone WSDigger 和 Pushtotest TestMaker 等。

Web 应用漏洞扫描器模拟 Web 客户端,执行特权 URL 扫描,脆弱 CGI 扫描等。典型地记录 HTTP 交互,并在后续交互中注入恶意负载,观察响应数据。Web 应用漏洞扫描器可有效发现跨站脚本、SQL 注入、目录遍历、Cookie 中毒等安全漏洞。常用的 Web 应用漏洞

扫描器包括 SPI Dynamics 公司的 WebInspect、Watchfire 公司的 AppScan 等;开源的有 OWASP WebScarab、Nikto 等。

5 结束语

Web 服务应用日益广泛,存在的安全性问题也日益突出,如何对 Web 服务应用进行安全性测试以确保 Web 应用安全运行,成为当前工作的重点内容。文中系统分析了 B/S 架构软件安全性测试的特点、内容、方法与工具,将 Web 应用软件的安全性测试进行了分类,并对每种分类提出了相应的安全漏洞和测试方法。文中只关注于已经开发完成的 Web 软件,真正的安全性测试应该是软件全生命周期的测试,而且对软件开发相关的文档也应进行检查,发现设计、开发阶段可能存在的漏洞。

软件安全是信息安全体系的重要组成部分,未来软件安全性测试会越来越关注于安全功能建模与测试技术的研究、基于风险的安全测试、利用威胁模型指导安全测试过程等。随着 Web 应用服务相关漏洞的不断发布,安全性测试工具的不断更新,漏洞挖掘技术和安全性测试方法将不断改进,软件的安全性也就更能得到保证。

参考文献:

[1] Potter B, McGraw G. Software security testing[J]. IEEE Security and Privacy, 2004, 2(5):81-85.

[2] 颜 炯,王 戟,陈火旺. 基于模型的软件测试综述[J]. 计算机科学,2004, 31(2):184-187.

[3] 李志峥,杨社堂. 基于 B/S 结构下的软件系统测试研究[J]. 科技情报开发与经济,2006,16(7):232-234.

[4] 甘志华,季 超. 基于 B /S 结构的一种网络安全性解决方案[J]. 河南大学学报(自然科学版),2005,35(4):98-100.

[5] de Vries S. Software Testing for Security[J]. Network Security,2007(5):11-15.

[6] 贫 红,徐宝文,袁胜忠. 对应用软件进行安全测试的对手模式及其应用[J]. 计算机科学,2006,3(9):266-267.

[7] Kearney P. Message Level Security for Web Services [J]. Information Security Technical Report,2005(10):41-50.

[8] 周绍君,徐中伟. 面向安全需求的测试用例自动生成技术研究[J]. 计算机工程与应用,2009,45(28):75-78.

[9] 鲁伊莎,曾庆凯. 软件脆弱性分类方法研究[J]. 计算机应用,2008,28(9):2245-2248.

[10] 王 亮,黄 松. 基于软件测试的安全性缺陷分类法研究[J]. 电子质量,2009(10):19-20.

[11] 秦 锋,李 乔. Web 服务测试的一种实现[J]. 计算机技术与发展,2007,17(8):239-242.

[12] 郭瑞杰,宫云战,杨朝红. 软件安全性测试技术研究[C]//第三届全国软件测试会议与移动计算、栅格、智能化高级论坛论文集. 出版地不详:出版者不详,2009:102-105.

[13] 戴 伟,陈永艳. 基于物理隔离环境下的 Web Service 访问研究[J]. 计算机技术与发展,2010,20(4):167-170.

[14] 施寅生,邓世伟,谷天阳. 软件安全性测试方法研究[J]. 微计算机信息,2008,24(1-3):56-58.

(上接第 220 页)

动才能检测冲突的 CFD,提出了单个 CFD 和 CFDs 检测算法,利用片段统计信息、CFD 模式及分配检测处理到多个结点来减少数据移动数量和响应时间。基于依赖保持,描述了垂直划分关系中可以局部检测的 CFDs。对于垂直划分数据,研究了局部检测垂直片段 CFDs 冲突精炼方法。在此研究的是纯水平或垂直划分数据上 CFD 检测算法,如何检测同时具有水平和垂直划分数据中 CFD 冲突将作为接下来的研究工作。

参考文献:

[1] Fan W, Geerts F, Jia X, et al. Conditional functional dependencies for capturing data inconsistencies[J]. TODS, 2008, 33(2):444-491.

[2] 封明玉,赵 政,张 钢. 分布式环境下数据冲突及其解决方案[J]. 计算机应用研究,2002(2):72-74.

[3] Dahav B, Etzion O. Distributed enforcement of integrity constraints[J]. Distributed and Parallel Databases, 2003, 3(3): 227-249.

[4] Golab L, Karloff H, Korn F, et al. On generating near-optimal tableaux for conditional functional dependencies[C]//VLDB. [s. l.]:[s. n.], 2008.

[5] Cong G, Fan W, Geerts F, et al. Improving data quality: consistency and accuracy[C]//VLDB. [s. l.]:[s. n.], 2007.

[6] Fan W, Ma S, Hu Y, et al. Propagating functional dependencies with conditions[C]//VLDB. [s. l.]:[s. n.], 2008.

[7] Agrawal S, Deb S, Naidu K V M, et al. Efficient detection of distributed constraint violations[C]//ICDE. [s. l.]:[s. n.], 2007.

[8] 李爱群,乔 晗,王汝传,等. 基于分布式混合数据挖掘的电信客户流失分析[J]. 计算机技术与发展,2010,20(10):43-46.

[9] 胡文波,徐造林. 分布式存储方案的设计与研究[J]. 计算机技术与发展,2010,20(4):65-68.

[10] 金 杉,徐 佳,闪 烁. 分布式流媒体分发系统的设计与实现[J]. 计算机技术与发展,2010,20(11):84-88.

[11] 童亚拉. 分布式编译的方法和系统研究[J]. 计算机技术与发展,2010,20(5):79-82.

[12] 李 想,吴国新,郭 晶. 基于分布式倒排索引和 VSM 算法的 P2P 复杂搜索[J]. 计算机技术与发展,2009,19(4):25-27.