火龙果•整理
uml.org.cn



# 基于Web应用的威胁建模分析和实现①

刘华群① 张勇斌② 陈秋月③
(①,②北京印刷学院 信息与机电学院 北京 100260; ③北京印刷学院 网络教学中心 北京 100260

[摘 要]为了解决Web应用所面临的各种网络安全问题，本文首先分析了威胁建模的有关原理与过程，然后讨论了适用于Web应用系统的威胁建模步骤，最后以“济宁市农业局信息网”为例进行了详细讨论，并对系统进行威胁评估，结果表明：该系统具有较强的抵抗风险的能力。

[关键词]网络安全 Web应用 威胁建模
中图分类号：TP393.08 文献标识码：A 文章编号:1009-914X(2009)9(b)-0197-02

**前言**

随着Internet的普及，人们对其依赖也越来越强，WWW服务作为现今Internet上使用的最广泛的服务，从某种程度上说：没有Web应用就没有如今强大的Internet发展；但是由于Internet的开放性，及在设计时对于信息的保密和系统的安全考虑不完备，造成现在网络的攻击与破坏事件层出不穷。因此，设计安全可靠的Web站点与保证WWW数据传输中的安全性，就成了WWW服务能够正常提供的重要前提，为此，微软推出了能够对对设计的程序进行潜在性的威胁评估的“威胁建模”，用于确定和处理程序设计的漏洞[1][2][4]。

**1 威胁建模的原理与过程**

威胁建模是一项工程技术，它主要是用来帮助系统设计者确定应用程序方案上下文中的威胁、攻击、漏洞和对策。

由于威胁建模不可能一次识别其所有可能的威胁，而且应用程序需要不断增强其功能并做出调整以适应不断变化的商业需求等诸多原因，因此，威胁建模过程不应当是一次性的过程，而是在应用程序设计的早期阶段启动、贯穿于整个应用程序生命周期的迭代过程。其建模过程如图1所示：

识别资产：识别系统必须进行保护的有价值的资产；

创建体系结构概述：使用简单的图表可以将应用程序的体系结构记录在文档中，包括子系统、信任边界和数据流；

分解应用程序：分解应用程序的体系结构（包括基础网络和主机构造设计），以创建应用程序的安全配置文件。安全配置文件旨在发现应用程序的设计、实现或部署配置中的安全漏洞；

识别威胁：始终记住攻击者的目标、了解应用程序的体系结构和潜在的安全漏洞、识别可能影响应用程序的威胁；

用文档记录威胁：用定义了一组核心属性以捕获每个威胁的常用威胁模板，将每个威胁记录在文档中；

评估威胁：对威胁进行评估，以便对威胁进行优先级排列，并首先致力于解决最明显的威胁。评估过程对威胁的可能性进行评估，以防止发生攻击而带来的损害。

**2 Web应用程序威胁建模的过程分析**

在当今的基于Web应用程序设计当中，对其所可能遭遇的各种威胁建模的主要目的用于：帮助在程序设计中找出应用程序中的漏洞，可以利用已经确定的漏洞来帮助构建程序设计、指导安全测试以及界定其范围。将微软推出的“威胁建模”相关理论应用到Web应用程序[3]，则可以得到如图2所示的5个步骤[3]：

（1）确定安全目标

这是整个Web应用程序威胁建模最重要的步骤，只有明确了“Web应用程序中需要保护的对象，也即是非法攻击者攻击的对象”，才能够有助于我们理解潜在攻击者的目标 并将注意力集中于那些需要密切留意的应用程序区域。而安全目标一般都是代表了“数据及应用程序的保密性、完整性和可用性相关的目标和约束”。其中机密性包括：防止未经授权的信息泄漏；完整性包括：未经授权的信息更改；可用性包括：即使在受到攻击时也可以提供所需的服务。

（2）Web应用程序概述

Web应用程序概述主要包括：介绍应用程序的功能、应用程序的体系结构、物理部署配置以及构成解决方案的技术等方面内容。为了提高整个Web应用程序的可靠性及安全性，需要在应用程序的设计或实现中不断查找潜在的安全漏洞。对于Web应用程序功能的介绍及其使用方法等有

助于有针对性地确定威胁可能发生的地点；为了说明Web应用程序的物理部署特性和应用程序及其子系统的组成和结构，可以采用体系结构图表的表达方式，从而可以将威胁目标进一步确定于某一特定区域；识别用于实现解决方案的特定技术则可以在此过程后期关于特定技术的威胁。

（3）分解应用程序

本部分的主要功能是：了解Web应用程序的结构来确定信任边界、数据流、 数据入口点和数据出口点。确定信任边界主要是用于注明在Web程序设计过程中需要特别关注的区域，而且必须能够确保相应的安全措施可以将所有入口点保护在特定的信任边界内，并确保容器入口点可以充分验证通过信任边界的所有数据的有效性；确定数据流是指从入口到出口，跟踪应用程序的数据输入输出。这样做可以了更全面的找出威胁所在。入口点和出口点都是应用程序遭攻击的地方，都是在进行威胁建模时需要重点考虑的地方。对应用程序结构了解的越多， 我们就越容易发现威胁和漏洞。

（4）确定威胁

本部分主要是：确定可能影响应用程序和危及安全目标的威胁和攻

图 1 威胁建模过程

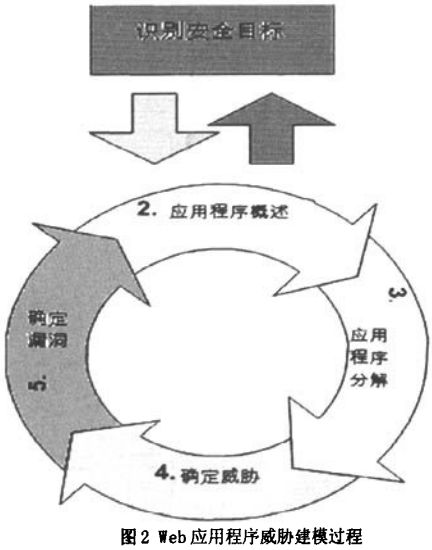



图2 Web应用程序威胁建模过程

①北京印刷学院 2008青年基金项目，项目编号为：09000108009；北京印刷学院 党建课题，项目编号为：0250108005。

万方数据

火龙果•整理
uml.org.cn



击。确定威胁主要有两种方法，一是利用基于目标的STRIDE方法来识别威胁。考虑多种威胁种类（例如电子欺骗术、篡改和拒绝服务），使用威胁和对策的STRIDE模型来对有关应用程序的体系结构和设计的每个方面提出质疑。在该方法中，我们考虑的是攻击者的目标；另外一种方法是使用分类威胁列表。利用这种方法，先按照网络、主机和应用程序进行分类的常见威胁用列表形式表示出来，然后将前面已在经应用程序体系结构及其之前识别出的所有漏洞剔除，由此得到适用于本系统的威胁类型。

（5）确定漏洞

其主要任务是检查应用程序的各层以确定与系统有关的弱点，以加强对于最常出现漏洞的关注。

**3. 威胁建模在Web应用系统的应用实现**

“济宁市农业信息化网”是济宁市农业局在通过济宁地区的“电话、电脑、电话”三电合一信息服务网络系统，为公众和单位内部提供高效的“政务信息公开、公共服务及公众参与”服务。将前面的Web应用的威胁建模理论应用到“济宁市农业局信息网”的实现过程，得到了如图3所示的总体框架：

* 接入层：各级用户使用 Web 浏览器（包括公众、管理人员、工作人员、业务系统办理人员）、PDA等来访问济宁市农业局门户网站。

* 门户层：济宁市农业局通过门户网站进行信息发布、网上信息采集、行政许可公布的应用。

* 业务逻辑层：主要是各种业务应用，包括行政许可、网上办公等，所有的业务应用都是建立在应用支撑层基础上，并通过门户进行承载。

图3 济宁市农业信息网

* 应用支撑层提供：内外应用的电子政务应用所需的公共技术支撑。应用组件包括工作流引擎、统一消息、用户和权限管理、数据访问、内容管理、搜索引擎和通用报表等公共应用组件。

* 数据层：用来存放业务系统运行的数据，以及网站的信息等。

* 基础层：基础设备层是整个系统正常运行保障。对于全市农业信息网的系统和网络资源的管理和监控可以通过相应的管理软件实现，作为安全管理平台、网络和系统管理平台的解决方案。

* 安全平台：本项目需要实施统一的安全管理机制，建议采用成熟的中间件产品；安全平台纵贯了本系统的各个层次。

* 管理保障：主要包括规划、组织、项目、资金、技术、建设、运行维护管理等方面，是电子政务建设和运行的重要保障。

设计上述的总体系统结构是基于如下的考虑：

（1）根据济宁市农业局的要求，我们最终将“使用本系统人员的身份验证、授权用户的权限内容及其在整个系统中的通信安全”作为本系统设计中需要特别关注的安全问题。

（2）在包括操作系统、数据库等软件基础架构平台之上，再构建的一层专门为支撑应用开发的“应用支撑平台”的软件平台，为济宁市农业局信息化的各种应用提供一个可靠、高效、安全、易用、可扩展的集成环境、运行环境和支持环境。系统实施时根据应用系统的需要，基于应用支撑平台开发相应的公共组件和应用组件，通过灵活的组件布局，满足应用开发或系统整合的需要。主要包括：用户管理、单点登陆、内容管理、通用交互、网站统计、统一权限、全文检索、动态表单、繁简转换、日常管理等组成。

（3）为了让所设计的系统能够运行正常，根据Web应用系统威胁建模的有关理论，在本系统的设计中，采用了多项技术措施。

其一就是“安全认证及权限管理”，主要用于实现：分级管理、用户管理（包括用户组织结构定义、临时性机构管理、角色职位管理）、用户组和用户管理、角色管理、身份认证（支持基于PKI的身份认证，在信息的管理中可嵌入信息防篡改，提供无缝接合）

其二就是“信息完整性与安全性保障”，主要采用了：数据加密（对于不同的数据，采用不同的加密政策，对于敏感数据，为防止数据库管理员查看数据和其他的意外情况发生，所有保存到数据库的关键数据经过128位的RSA算法或者其他高级加密算法进行加密，保证数据在保存点的安全性；日志管理（对系统中所有用户的重要操作进行记录，明确地记录操作人、操作时间、使用应用名称、操作所在机器名称和IP地址等内容，进一步增强了系统的安全性。所有的日志一般人员只能浏览，不能修改。

其三就是网络安全通道传输。由于本系统是基于浏览器的应用系统，用户的所有操作都是基于WEB来运行的。因而，通过HTTPS（HTTP OVER SSL）通道传输，HTTPS可为在网络上传输的日常信息交互加密，初步保证数据通道的安全性；而且每次会话所使用的加密密钥都是随机产生的。这样，攻击者就不可能从网络上的数据流中得到任何有用的信息。

其四就是系统运行管理。系统的安全除了一系列的安全技术外，更重要的是有好的安全管理制度来协调各种技术，充分发挥各种技术的作用。主要包括：制定各项访问控制措施，包括对网络、主机、数据库等的访问；禁止在系统中使用未经批准的应用程序，禁止在系统上加载无关软件，严禁擅自修改系统的有关参数等。

（4）风险评估

将适用于Web应用威胁建模技术应用到上述系统中，大大提高了系统的安全性能。根据公式：风险=可能性×潜在的损害，得出的风险粒度远低于未使用威胁建模技术的其他系统的风险粒度。

**4. 结语**

本次基于Web应用威胁建模的分析与实现设计，将威胁建模方法学应用到Web应用程序后，可以基于对应用程序漏洞的充分理解，而对现存的威胁进行识别和评估。同时通过此信息，可以从代表最强大风险的威胁开始，按照逻辑顺序使用相应的对策来解决现存的威胁。

显然，在当今的网络环境中，有效而全面的威胁建模方案不是一种意见，而是现在程序设计中必不可少的。网络中Web应用面临的威胁和风险数不胜数，而且不仅源自边界外，还包括有意或意外的内部威胁。推理严谨的威胁建模解决方案要考虑所有威胁，并要求对这些威胁有着透彻的理解，同时还要了解Web应用程序的架构以及可能危害该Web应用系统上驻留数据的潜在威胁与活动的特点。有效而又准确的模型建立，可以减少Web应用程序设计的成本和开发期限。

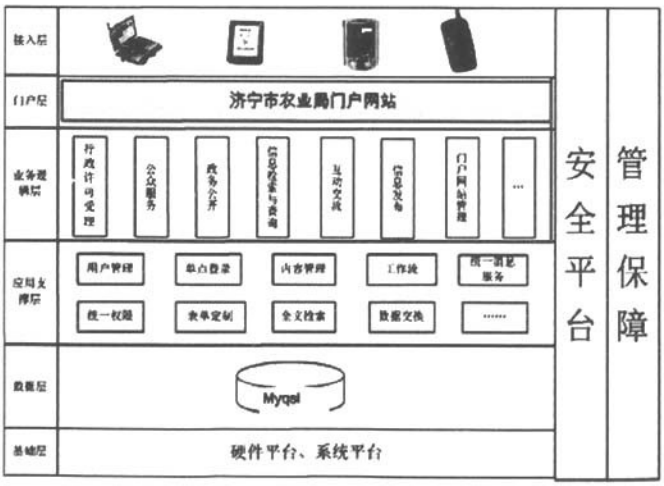
**参考文献**

[1] Steve Kalman著[美].冯大辉，姚湘忆译. Web安全实践(第一版)[M]. 北京：人民邮电出版社，2003。

[2] Joel Scamray,，Mike Shema著[美]. 田芳，陈红等译Web 应用黑客大曝光(第一版)[M]. 北京：清华大学出版社，2003。

[3] J.D. Meier, Alex Mackman, Blaine Wastell. 如何：在设计时为Web 应用程序创建威胁模型[EB/OL]. http://www.microsoft.com/china/MSDN/library/Security/default.mspx?mfr=true，

[4] 威胁建模 [EB/OL]. http://www.microsoft.com/china/technet/security/guidance/secmod76.mspx，





万方数据

火龙果•整理
uml.org.cn

# 基于Web应用的威胁建模分析和实现

作者： 刘华群， 张勇斌， 陈秋月
作者单位： 刘华群,张勇斌(北京印刷学院,信息与机电学院,北京,100260)， 陈秋月(北京印刷学院,网络教学中心,北京,100260)

刊名： 中国科技博览
英文刊名： CHINA SCIENCE AND TECHNOLOGY REVIEW
年，卷(期)： 2009，""(22)
被引用次数： 0次

## 参考文献(4条)

1. Steve Kalman. 冯大辉. 姚湘忆 Web安全实践 2003

2. Joel Scamray. [美]Mike Shema. 田芳. 陈红 Web应用黑客大曝光 2003

3. J D Meier. Alex Mackman. Blaine Wastell 如何:在设计时为Web应用程序创建威胁模型

4. 威胁建模

## 相似文献(10条)

1. 学位论文 曾宇胸 Web应用安全与风险评估研究 2009

随着Internet的高速发展，基于Web和数据库架构的应用系统已经逐渐成为主流，广泛应用于企业内部和外部的业务系统中，电子政务、电子商务以及各种基于Web应用的新业务模式也不断成熟。与此同时，由于Web应用所固有的易攻击性也使Web应用安全问题日益严重，已经成为网络安全的主要问题之一。因此对Web应用安全和它风险评估的研究具有重要的理论意义和实用价值。<br>

本文对常见Web应用安全漏洞进行了详细分析，深入地研究了Web应用攻击的常见方法与防范措施。同时对Web应用风险评估进行了有益的探索，提出了一个实用的风险评估模型。本文实现了一个Web应用安全扫描系统。该系统能够对一些常见的漏洞进行扫描，并自动生成扫描报告；系统还具有代理拦截功能，以辅助手工测试。本文还利用该系统对实际Web站点进行了安全测试实验和分析。从实验结果看，该系统对Web应用安全的分析有较好的辅助作用，具有一定的实用价值。

2. 期刊论文 孙庆华 浅谈Web应用防火墙和传统网络防火墙共同构建图书馆网络安全 -内江科技2010,31(4)

本文针对Web应用防火墙及其特点,结合图书馆网络管理和应用的实际,将Web应用防火墙和传统网络防火墙相结合应用于目前图书馆的网络安全管理.

3. 学位论文 傅灵丽 面向Web应用的认证安全问题及解决方案研究 2007

随着网络技术的快速发展，Web应用由于其使用方便已成为网上应用的主流。而身份认证是Web应用的第一条防线，其安全程度直接影响Web应用程序的健壮程度。目前的很多黑客攻击手段，如钓鱼攻击、SQL注入攻击等各种网络攻击方式都是由身份认证开始的。因此，身份认证安全研究必将会成为网络安全技术研究的新重点。

本文从目前流行的针对Web应用的身份认证的多种漏洞攻击出发，提出了程序级和应用级两层解决方案。程序级解决方案主要面向系统的开发人员，主要采用数据过滤、输出处理、Session管理、缓存清除等技术，这些技术方案均采用跨平台的JAVA作为编程语言，具有一定的普遍性；应用级解决方案提出了目前一些比较常用的、安全的认证机制，如：数字证书、一次性口令、双因子认证、生物识别技术等。其中重点介绍了“一次性口令”+“数字证书”的双因子认证机制。

本文程序级解决措施经过实验证明，具有一定的可行性、实用性，并且其实现方式简单、有效，可以从根本上杜绝针对这些漏洞的认证攻击。此外本文提出的“一次性口令”+“数字证书”的双因子认证机制值得安全系数较高的Web应用程序借鉴。

4. 期刊论文 张洪扬. 唐学文. Zhang Hongyang. Tang Xuewen 用ModSecurity增强Web应用安全 -网络安全技术与应用 2007,""(5)

本文着重介绍当前Web应用中常见的几种入侵攻击形式,以及在Apache服务器上实现Web应用入侵检测和防御,从而扶到网络级防火墙无法实现Web应用级安全防护,减轻IDS压力,增强Web应用的安全防护能力.

5. 学位论文 郑理华 WEB应用安全测试评估系统的研究与实现 2005

随着WEB应用的普及，黑客利用WEB应用漏洞发动的攻击越来越多，造成了巨大的危害。WEB应用的安全问题已经成为网络应用的主要问题之一，目前的检测系统还不够完善，其存在一些问题如只能够探测已知漏洞、扫描不够全面、漏洞检测存在一定的盲目性。科学地、高效地、准确地测试评估WEB应用的安全性十分必要，是所有WEB应用系统所面临的重要课题。因此，对WEB应用安全测试评估技术展开全面的研究具有重要的理论意义和实用价值。

本文在充分研究安全漏洞检测原理及关键技术的基础上，提出了一种基于数据采集的WEB应用安全测试评估模型。安全测试评估模型中的基于数据采集的WEB应用遍历模型能够自动、完整、全面地遍历WEB整个应用，同时提取到WEB应用协议数据，这些协议数据能够帮助理解整个WEB应用，同时有助于发现WEB应用的未知漏洞。基于数据采集的WEB应用安全测试模型有机地将白盒测试元素溶入到黑盒测试当中，能够较好地提高漏洞探查的针对性和准确性、提高测试评估的效能，能够较为行之有效地模拟黑客攻击。提出了一个全新的漏洞规则库优化机制——反馈机制，及其相应的反馈动态优化算法。通过反馈机制能够更好地优化漏洞规则库，使漏洞规则库更好地反映现实漏洞的变化规律；研究了OCTAVE风险评估方法，并应用于WEB应用系统安全的风险评估；最后详细地设计和实现了WEB应用安全测试评估原型系统，该系统能够扫描探测多种类型的WEB应用系统漏洞，特别是与具体WEB应用相关的漏洞；能够给出较为完整详细的WEB应用安全漏洞检测评估报告。

6. 学位论文 崔海波 基于ASP.NET架构Web应用的安全性研究及应用 2009

基于互联网的Web应用发展迅速，尤其是随着微软加入了开源的大军后，基于ASP.NET架构的Web应用发展更是如雨后春笋般迅速。但Web应用程序的安全性却一直被人们忽略，或者通常被当作网络安全问题。应用程序架构师和开发人员将安全性看作事后处理的任务，或在时间允许的情况下(通常是在解决性能问题之后)才考虑安全性要求。面对一系列的安全性事件，Web应用程序的安全性是应该被提到议事日程上来了。<br>

本文就ASP.NET Web应用程序安全性及在实际中的应用进行了详细的探讨。研究了基于ASP.NET架构的应用程序的安全性基本原理以及它所面临的威胁。结合作者所参与的“企业门户网站信息平台建设”，对ASP.NETA安全行进行分析，并在此基础上，提出了可行的解决方案。研究工作主要涉及以下方面：<br>

1、本文对ASP.NET安全技术作了详细阐述，分析了“企业门户网站信息平台建设”项目的安全问题，提出了解决跨站脚本攻击、HTTP响应拆分攻击及SQL注入攻击的方法；<br>

2、实现了基于角色的Forms身份认证与USBKey认证结合的统一身份认证系统，并且在项目中成功实施。在此基础上实现了“企业门户网站信息平台建设

火龙果•整理
uml.org.cn

”并完成了安全性改造。<br>
3、提出了存储敏感数据的方法，实现了使用带有salt的哈希值对敏感数据加密的算法。

7.期刊论文 张琳.袁捷.李欣.张冬晨.Zhang Lin.Yuan Jie.Li Xin.Zhang Dongchen Web应用的安全防护 -电信工程技术与标准化2010,23(2)

对于Web应用来说,安全防护的作用在整个系统中正变得越来越重要,本文对Web应用层面所面临的威胁进行了分析,进一步对各种防护手段进行了研究.

8.学位论文 马金伟 基于WEB技术的信息网络安全报警系统设计与实现 2006

基于Web的应用系统，在Internet/Intranet技术推广以来，得到了迅速发展。无论是企业、机构的内部计算机应用系统，还是在互联网上的网上应用服务系统，基于Web的计算机应用系统都发挥着越来越重要的作用，逐渐成为计算机应用系统的主流模型。微软的.NET框架为开发Web应用系统提供了全新的平台。

信息网络安全报警系统是公安机关在社会主义市场经济条件和信息网络安全形势下，维护信息网络安全、打击违法犯罪，提高公安机关网上发现、报警能力的重要举措。其核心是利用信息化手段建立畅通的报警渠道、建立网络报警的网上受理、网上报批、网上批复、网上批转、网上反馈等，实现对网络违法犯罪的快速响应，要实现这些功能，就要利用先进而且实用性强的.NET技术。

本文对.NET开发平台进行了论述，并详细描述了运用该技术对信息网络安全报警系统进行的设计和实现。

9.会议论文 付灵丽.金志刚.李娟 Web应用中的认证攻击及解决方案研究 2007

目前,认证问题是Web应用中最值得关注的安全问题之一,它是保护Web安全的第一道门槛。本文从基于Web应用的认证漏洞攻击出发,提出程序级和应用级的解决方案,通过对输入、输出等方面进行有效性处理,从根本上杜绝了应用程序的安全漏洞,加强了Web应用的认证机制。

10.学位论文 吴海翔 Web应用安全分析器的研究与实现 2007

Internet已经成为人类所构建的最丰富多彩的虚拟世界。在世界各地，用户的数目正在飞速增长，而Web作为Internet上最主要的服务，已经成为万众瞩目的焦点和Internet的象征。随着Web服务的快速发展，其安全性问题日益受到人们的关注。Web应用程序作为Web系统中最重要的部分，保障它的安全是重中之重。本文概要介绍了Web应用及其相关技术，网络安全的概念和体系，分析了保障Web应用系统安全的方法，并针对Web应用所面l临的安全问题，设计并实现了Web应用安全分析器。分析器从爬行遍历网页开始，收集Web应用中可能出现安全问题的各种关键点，然后利用扫描器调用不同的安全漏洞测试插件对Web应用可能的问题点进行检测，最后生成详细的报告，揭示安全漏洞并给出解决方案。文章中详细说明了设计和实现此分析器所涉及的各项技术，并给出了具体的设计实现过程；文章最后对分析器进行了总结，提出了进一步研究改进的方向和内容。

本文链接：http://d.wanfangdata.com.cn/Periodical_zgbzkjbl200922178.aspx

下载时间：2010年11月4日