网络优先数字出版时间:2014-7-22
网络优先数字出版地址:http://www.cnki.net/kcms/doi/10.13657/j.cnki.gxkxyxb.20140722.004.html
广西科学院学报 2014,30(3):211~216
Journal of Guangxi Academy of Sciences Vol.30,No.3 August 2014

集约化信息安全测评平台设计*

Design of An Integrated Information Safety Evaluation Platform

杨雪君
YANG Xue-jun

(广西壮族自治区电子信息产品监督检验所,广西南宁 530031)
(Guangxi Institute of Electron Production Supervision and Inspection, Nanning, Guangxi, 530031, China)

摘要:【目的】探讨如何为各类信息系统安全性保障测试提供综合性支撑服务。【方法】综合应用网络主机检测、数据库检测、Web应用漏洞检测等关键技术,通过协同集成方法,设计一个集约化信息安全测评平台。【结果】该平台集网络攻防演练和演示、管理安全测试、数据安全测试、外部安全测试及网站系统内容测试、产品与系统测评、信息安全应急响应为一体,可以在信息系统功能、性能、安全等方面为政府各部门及社会各界提供测试和评估服务。【结论】实际应用表明,该平台能够满足信息系统安全测评的关键需求,能够提供一体化信息安全测评功能。

关键词:信息安全评测 漏洞管理 漏洞扫描
中图分类号:TP309 **文献标识码**:A **文章编号**:1002-7378(2014)03-0211-06

Abstract:【Objective】To provide comprehensive support services for safety testing of information systems.【Methods】An integrated information safety evaluation platform has been designed by integrating multiple key detection technologies covering network host, database and Web application loophole etc.【Results】This platform integrates network attack and defense, demonstration, management safety testing, data safety testing, external safety testing and web content system testing, product and system testing, and information safety emergency response. It also can provide testing and evaluation services to the departments of government and community for the function, performance, safety, and other aspects of their information systems.【Conclusion】The actual application of the platform meets the key demand of information system safety evaluation and provides the integrative evaluation of information safety.

Key words: information safety evaluation, vulnerability management, vulnerability scanning

【研究意义】随着社会信息安全问题的日益突出,相关部门对信息安全问题关注程度日益提高,给信息安全测评服务带来了良好的市场收益。建立集信息安全等级保护测评、信息安全分级保护测评、信息安全风险评估、计算机信息系统安全测评功能一体化的信息安全测评体系为目的的信息安全测评平台非常必要。【前人研究进展】国内已有不少单位开展信息安全测评平台相关的研究开发工作,取得一些成果[1~3],但是总体而言已建立的信息安全测评体系功能尚不够全面。文献[2]研发了一个信息安全工程综合实验与服务平台,提供信息安全保障体

收稿日期:2014-04-10
修回日期:2014-06-10
作者简介:杨雪君(1971-),女,高级工程师,主要从事电子与信息技术、信息安全研究。
*广西壮族自治区科学技术厅"计算机网络信息系统测评实验室"项目(桂科条字[2008]5号),"广西壮族自治区信息安全测评平台"项目(桂科条字[2010]12号)资助。

系架构的展现。文献[3]探讨一致性测试模型的信息安全等级测评系统的设计方案,该方案用强描述性规范化语言把权威的标准条款定义为测评标准库,再通过高层描述语言的通用转换平台转化为测试任务,然后由分布式的测评管理平台调度测评执行平台进行测评。文献[4]采用面向对象的知识分析方法,构建等级测评知识库体系,给出基于知识库的等级测评自动评价系统的基本规则,以及一种等级测评自动评价过程,该过程能够结合业务流程与渗透测试情况进行关联分析和自动处理,进而得到单个测评项的关联分析结果和安全控制测评结果。文献[5]研究了一个信息系统安全等级测评工具,从等级测评流程出发提出拓扑展示和测评知识表达方法,并给出测评工具的系统原型描述。文献[6]结合等级测评、风险评估和专家系统的相关技术,提出一种将故障树和专家系统技术用于等级测评结果的综合分析模型,利用故障树对知识进行展示和分析,从而紧密地将等级保护要求和用户安全需求联系在一起。文献[7]中基于业务的信息安全等级保护风险评估方法,通过对组织业务进行分析,根据组织的业务识别出重要的资产,提出一种基于业务的信息资产识别和评估方法,为等级保护的定级、测评和整改等工作提供参考依据。文献[8,9]结合信息安全等级保护的相关政策以及制度要求,对Web应用安全体系建设进行了探讨和分析。文献[10]针对具体的应用场景,根据国家信息系统安全等级保护体系关键技术要求,研究了基于等级保护的领域性数据中心信息系统安全体系设计方案。总体而言,上述工作的信息安全测评体系的功能较为单一,有些只有信息安全等级保护测评体系,有些只有信息安全分级保护测评体系。**【本研究切入点】**从安全漏洞的整个生命周期着手,在不同周期阶段采取不同的措施,提供一套有效的漏洞管理工作流程。**【拟解决的关键问题】**从网络主机、数据库及Web应用弱点检测多个层次,采用漏洞追踪、安全测试管理、数据安全测试、外部安全测试、网站系统内容测试、信息安全应急响应等多维技术集成方法,研究和实现了一个集约化信息安全测评平台。该平台的投入使用,有助于建设信息安全等级保护测评、信息安全分级保护测评、信息安全风险评估、政府信息安全检查、信息安全检测、计算机信息系统测评为一体的信息安全测评体系,为更充分地满足我国信息安全领域的测评需求,为政府机关、企事业单位、科研院校提供有效的信息安全技术支撑服务。

1 集约化信息安全测评平台的架构

由图1可知,平台的底层是由网络传感器、主机传感器、Web应用传感器、数据库传感器等组成的集成化传感器层。网络传感器组件为硬件产品,主要收集网络中的数据包并对其进行分析统计。主机传感器、服务器传感器、Web应用传感器、数据库传感器安装于被检查的对象系统上,分别开展检测和监管,例如,主机传感器对主机的日志、网络操作、文件操作、重要资源使用等进行操作;服务器传感器实现对服务器本地策略、CPU使用情况、内存使用情况、共享情况等进行监控;数据库传感器对数据库操作行为进行监管,对违规行为进行阻断。最终将所有监控数据以统一格式汇总到上层测评中心,对数据进行关联分析汇总。平台支持多级分布式管理模式,可形成集中统一管理、实时分散处理的高效监管机制。

整个平台主要包括3个子系统,各子系统都相对独立,通过协同管理模块将各子系统集中由控制中心进行统一管理、统一策略配置和报表处理。这些子系统采用网络主机、数据库、WEB应用弱点检测和渗透性测试等多种关键技术相融合开展信息安全测评。通过网络主机漏洞扫描系统的集成应用,可对网络内指定的UNIX、Linux、Windows等主机、网络设备、网络协议进行漏洞扫描,通过WEB应用漏洞扫描系统的集成应用,对网络中的目标应用系统进行SQL注入、跨站脚本、登录口令破解、跨站点请求伪造、网页木马、XPath注入、表单绕过等应用层漏洞扫描。通过据库漏洞扫描系统的集成应用,可对数据库的漏洞进行扫描,能对网络环境中的ORACLE、MySQL、SQL Server等数据库进行授权扫描或非授权扫描。平台根据用户特定需求生成相应的信息安全测评报告,并提供修复漏洞的方法。在集成应用以上多种关键技术的基础上,我们还研究开发了自动化测试接口程序,自动导出测试数据及测试报表,来提高测试平台的自动化程度。

1.1 网络主机漏洞扫描子系统主要提供的功能

1.1.1 资产管理

通过"地址簿"机制实现资产属性的输入和维护,并且按照资产重要性权值进行资产重要性分类。资产管理和用户组织结构或者网络拓扑结构紧密结合。通过资产管理,方便掌握风险分布情况、定位风险和高效实施风险降低或规避措施。

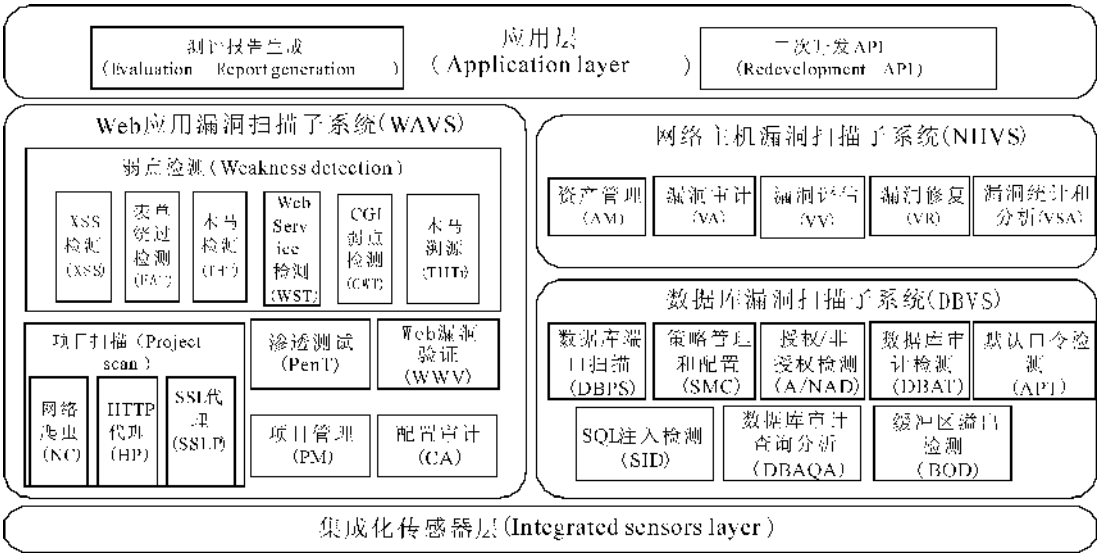

图 1 集约化信息安全测评平台架构

Fig. 1 The architecture of integrated information security evaluation platform

1.1.2 漏洞风险评估

采用风险评估模型,从资产、漏洞和威胁 3 个维度对资产风险进行评估。通过在线报表和离线报表将风险分析结果展示给用户,从多个视角对风险进行深入的分析,评估模型加上评估结果定量和定性分析,从而了解业务系统中存在的风险。

1.1.3 漏洞修复

提供多种二次开发接口供漏洞修复产品或补丁管理产品使用,能及时集中对资产漏洞进行修复。

1.1.4 漏洞审计

用户在实际的漏洞修复的过程中往往很难确认自己的漏洞是否真正修复,即使安装了评估结果中厂商补丁也很难确认补丁程序是否真正安装成功。针对这种情况,平台提供了漏洞审计功能,能够通过发送监督邮件的方式来督促相应的资产管理员对漏洞进行修复,同时启动自动的定时任务对漏洞进行审计,提高了管理人员手工验证漏洞是否修复的效率。

1.1.5 漏洞统计与分析

从多个视角深刻反映网络的整体安全状况,提供“历史数据搜索”与任意扫描任务之间的“汇总查看”和“对比分析”功能,不仅对单个扫描任务的漏洞分布、危害等进行了统计分析,还对多个扫描过程进行综合的风险变化和安全对比评定,为网络安全状况的评定和未来网络建设提供了强有力的决策支持。

主机漏洞扫描子系统采用主机传感器组件,安装于受控的主机系统中,主机漏洞扫描子系统通过对被监控主机资源和重要文件与信息的监管,从系统、应用、网络、资源等多级入手,实现对被审主机的全面监控。由图 2 可知,通过制定与执行非法外联扫描规则,监控网络系统中主机通过调制解调器等通信设备、双网卡、无线等方式连接外网,一旦发现立即禁止并报警。通过制定与执行漏洞扫描设计规则,在特定时间段内扫描主机特定的网络连接行为,如面向特定的 IP 地址、域名、网段、端口的连接行为,并可以限制发起网络连接行为的特定用户与进程。对网络连接信息进行详细的扫描记录,并对违规的网络连接行为进行实时报警与响应。

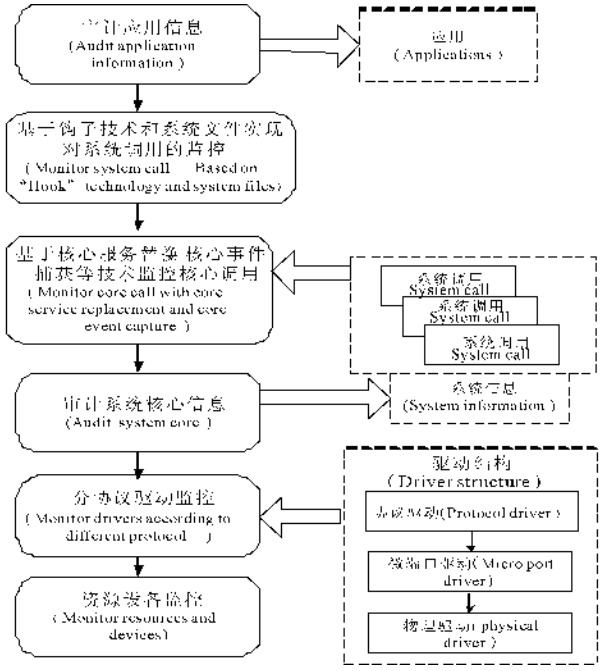

图 2 主机漏洞扫描过程

Fig. 2 Process of host vulnerability scanning

1.2 Web 应用漏洞扫描子系统主要提供的功能

主要功能有:(1)深度扫描。以风险为导向对 WEB 应用进行深度遍历,获得后台数据库信息及 WEB 应用列表。(2)WEB 漏洞检测。对各类典型 Web 漏洞(如:SQL 注入、Xpath 注入、XSS、表单绕过、表单弱口令、各类 CGI 弱点、网页木马、跨站请求伪造等)进行深度检测。(3)WEB 漏洞验证。对 Web 应用安全进行检测与审计,同时提供可靠、简易的漏洞验证框架,可通过漏洞验证技术获得敏感信息,直观的呈现漏洞危害。(4)口令猜解。通过猜测攻击、字典攻击、穷举攻击、混合攻击等方式,对 SMB、TELNET、FTP、POP3、MYSQL、ORACLE、SYSBASE 和 SQL Server 协议进行弱口令检测等。(5)网页木马检测。对各种挂马方式的网页木马进行全自动、高性能、智能化分析,并对网页木马传播的病毒类型做出准确剖析和网页木马宿主做出精确定位。(6)渗透测试。通过当前弱点,完全模拟黑客使用的漏洞发现技术和攻击手段,对目标 WEB 应用的安全性做出深入分析,并实施无害攻击,取得系统安全威胁的直接证据。(7)配置审计。通过当前弱点,模拟黑客攻击,实现数据库的审计功能,获得后台数据库连接信息、数据库实例名、数据库版本、数据字典等配置信息。(8)完整风险评估报告。提供详细的检测扫描报告,包括扫描的 URL 信息、漏洞类型、安全加固建议等。

Web 应用漏洞扫描子系统主要是对某些特定的应用进行监控,通过应用传感器组件,采用代理和非代理两种方式。代理应用漏洞扫描是指与应用程序的开发商进行合作,通过给定的接口实现对应用的控制以及从应用中得到相应的信息;非代理漏洞扫描通过对已有应用对资源使用的监控,从而现实对应用的控制与信息的获取,产生相应的事件。Web 应用漏洞扫描子系统首先通过系统调用获得应用进程的信息和异常,同时通过两种方式对应用进行监管:(1)代理应用漏洞扫描通过开发商提供的监管与控制接口,对应用程序实行监控,从接口中得到应用程序的信息,向控制接口发送一定规则的控制命令起到对应用程序的控制;(2)非代理应用漏洞扫描通过对应用程序的封包技术,生成一个中间组件,应用程序的任何资源操作都将先通过这个组件,从而实现对应用的控制。其结构如图 3 所示。

1.3 数据库漏洞扫描子系统主要提供以下功能

数据库漏洞扫描子系统通过创建和执行安全策略来保护数据库安全,能够自动地鉴别在数据库系统中存在的安全隐患,能够扫描口令过于简单、权限控制、系统配置等一系列问题,内置的知识库能够对违背和不遵循安全性策略的做法推荐修正的操作。

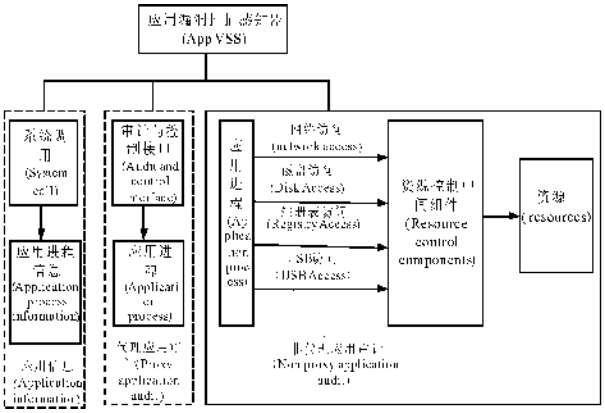

图 3 Web 应用漏洞扫描子系统结构

Fig. 3 The structure of Web application vulnerability scanning subsystem

1.3.1 端口扫描

可以扫描指定 IP 或指定 IP 范围内的活动数据库(如 IP 地址,数据库类型,服务名,端口号等);提供自动搜索数据库服务器的功能,能够自动搜索出数据库的服务器的 IP 地址、数据库类型、服务名。

1.3.2 策略管理

策略即数据库检测的依据和标准,分为授权检测策略和非授权检测策略两类。策略管理可以制定不同的检测标准,并可以自己设置检测参数。授权检测是使用具有 DBA 权限的数据库帐户,按照选定的授权检测策略对目标数据库进行漏洞检测。非授权检测是依据数据库版本号按照选定的非授权检测策略对目标数据库进行检测。

1.3.3 策略配置

根据用户的实际测试目的,定制不同的策略。分别对应 3 个模块:默认口令检测、sql 注入、缓冲区溢出。根据策略进行数据库默认口令的检测,检测出的结果应用于 SQL 注入和渗透检测。SQL 注入通过数据库默认口令的检测可以查找出一些低权限的用户,通过把低权限用户提升为拥有 DBA 权限的用户,可以以 DBA 的身份查看数据库资源或运行 SQL 语句。

1.3.4 数据库审计监测

实时审计用户对数据库系统所有操作,如登录、注销、插入、删除、执行存储过程、用户自定义操作等,支持分析、提取 SQL 语句中绑定变量,并可完全监测还原 SQL 操作语句包括源 IP 地址、目的 IP 地址、访问时间、MAC 地址、数据库用户名、客户端类

型、数据库操作类型、数据库表名、字段名等。

1.3.5 数据库审计查询分析

可以支持基于 IP 地址、时间、用户名、数据库操作类型、操作命令、数据库名、数据表名、字段名、关键字等条件的审计日志搜索查询分析。

数据库漏洞扫描子系统对数据库操作行为进行监管,主要是通过分离网络数据包中的 SQL 语句,分析操作行为、操作对象等信息,对违规行为进行阻断。分析的数据库操作行为主要包括增加/修改/删除数据、创建/修改/删除数据库、创建/修改/删除表等。对于这些操作行为的控制还可以增加参数,如 IP 地址、用户名、操作对象(表、数据库)、操作字段等。

2 集约化信息安全测评平台应用

集约化信息安全测评平台已投入使用,已为社会提供信息系统测评服务,测试软件系统和网站是否存在常见的应用安全漏洞。我们以某个业务领域事件预警及报告系统为例,对平台的运行效果进行验证说明。首先说明测试环境,如图 4 所示,网络环境分成内部服务器区、用户终端区、网络边界区、远程接入区等部分,主要包括以下设备:

(1)客户端硬件为 Intel Core2 CPU T7500@2.20GHz 2.19GHz,2GB 内存;软件:Microsoft Windows XP Professional,IE8。

(2)服务器端硬件:Dell PE R210 服务器:Intel Xeon X3430@2.4GHz,4GB 内存;IBM HS22 刀片服务器:Intel Xeon E5620@2.4GHz,6GB 内存;融信 FW4000 防火墙;绿盟 SG600 安全网关;绿盟 AF P300A 应用防火墙;绿盟 NIPS600A-C 入侵防御系统等。软件:MySQL5.1 数据库,Web 服务器为 IIS7。

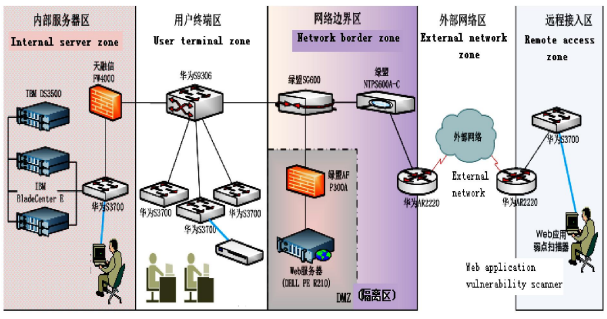

图 4 实验环境拓扑结构

Fig. 4 The topology of testing environment

受测应用系统部署在独立的服务器上。根据该应用系统的安全设计需求,以及其对业务信息的安全要求和系统服务的连续性要求的特点,选取测评指标时,从保护数据在生成、存储、传输、处理过程中不被泄露、破坏和免受未授权修改的要求;保护系统连续正常的运行,免受对系统的未授权修改、破坏而导致系统不可用的要求;通用的信息安全保护要求等 3 个方面考虑,在应用系统安全层面从身份鉴别、访问控制、安全审计、通信完整性、通信保密性、软件容错等方面的测评指标着手工作,同时对被测系统进行基于 Web 的漏洞扫描。

如表 1 所示,受测系统在用户身份鉴别、访问控制、安全审计、通信保密性及资源控制等方面设计和实现了安全保障策略,不存在后门和高、中风险漏洞,基本具备了保护系统内业务数据、保证系统正常服务的能力。但是系统在访问控制粒度、服务器配置等方面存在一定的不足。根据本平台自动生成的报告(如图 5)中提出问题和修改建议,用户可以结合系统的应用需求和实际运行环境继续完善系统的安全保存措施。

表 1 服务器漏洞扫描结果统计

Table 1 Statistics of server vulnerability scanning

序号 No.	IP 地址 IP Address	主机名 Host name	安全漏洞数 Number of security vulnerability			
			高 High	中 Medium	低 Low	小计 Sum
1	192.168.0.27	WEBSERVER3	0	0	11	11
2	192.168.0.29	WEBSERVER1	0	0	11	11
3	192.168.0.30	WEBSERVER2	0	0	12	12
4	192.168.0.251	NETWORK-SERVER	0	0	20	20
5	192.168.0.252	DSVIEW-S	6	0	6	12
6	192.168.0.253	DSVIEW-M	4	0	6	10
7	192.168.10.28	DATASERVER3	0	0	13	13
8	10.45.0.6	WIN-8GE9EC4JCOR	0	0	11	11
9	10.45.0.5	WINDOWS-Q3BFCBW	0	0	13	13

图 5 平台运行结果界面

Fig. 5 The interface of running result

3 结论

本文主要给出集约化信息安全测评平台的架构，并阐述其功能。该平台融合了网络主机、数据库、Web 应用漏洞检测等多种关键技术，集网络攻防演练和演示、管理安全测试、数据安全测试、外部安全测试及网站系统内容测试、产品与系统测评、信息安全应急响应为一体，可以在信息系统功能、性能、安全等方面为政府各部门及社会各界提供测试和评估服务。在今后的平台建设中，我们计划进一步增加平台的智能化、自动化功能，借助大数据等技术优化各种漏洞扫描和报告的数据挖掘，增加漏洞发现的能力和效率。

参考文献：

[1] 阙华坤，杨劲锋，肖勇，等. 基于一体化平台的信息安全等级评估[J]. 计算机工程，2013，39(10)：133-137.
Que H K，Yang J F，Xiao Y，et al. Information security level assessment based on integrated platform [J]. Computer Engineering，2013，39(10)：133-137.

[2] 李建华，张爱新，薛质，等. 信息安全实验室的建设方案[J]. 实验室研究与探索，2009，28(3)：65-67.
Li J H，Zhang A X，Xue Z，et al. Design of an information security laboratory[J]. Research and Exploration in Laboratory，2009，28(3)：65-67.

[3] 王春元，杨善林，周永务. 信息安全等级测评系统设计[J]. 计算机工程与设计，2006，27(23)：4457-4460.
Wang C Y，Yang S L，Zhou Y W. Testing and evaluation design of information security grades[J]. Computer Engineering and Design，2006，27(23)：4457-4460.

[4] 袁静，任卫红，李明. 基于测评知识库的自动评价系统研究[J]. 信息网络安全，2010(10)：74-76.
Yuan J，Ren W H，Li M. Research on automatic evaluation system evaluation based on knowledge base[J]. Netinfo Security，2010(10)：74-76.

[5] 李明，朱建平，金波，等. 信息系统安全等级测评工具的研究与实现[C]//第 18 届全国信息保密学术会议论文集. 北京：金城出版社，2008：95-103.
Li M，Zhu J P，Jin B，et al. Research and implementation of information system security evaluation tool[C]. In：Proceeding of 18th National Information Security Conference. Beijing：Gold Wall Press，2008，95-103.

[6] 黄洪，任卫红，余达太，等. 基于故障树的等级测评专家系统模型研究[J]. 计算机应用研究，2010，27(1)：204-208.
Huang H，Ren W H，Yu D T，et al. Expert system model research for classified evaluation based on fault tree[J]. Application Research of Computers，2010，27(1)：204-208.

[7] 范建华，薛岩龙. 基于业务的信息安全等级保护风险评估方法[J]. 计算机与数字工程，2010，38(3)：112-115.
Fan J H，Xue Y L. Information security risk assessment method based on traffic and classified protection [J]. Computer & Digital Engineering，2010，38(3)：112-115.

[8] 吴震，崔建，周昌令，等. 基于 OWASP 和 WASC 的多维度 Web 应用安全体系[J]. 广西大学学报：自然科学版，2011，36(s1)：148-154.
Wu Z，Cui J，Zhou C L，et al. Architecture of multi-dimension web application security based on OWASP and WASC[J]. Journal of Guangxi University：Natural Science Edition，2011，36(s1)：148-154.

[9] 陈煜欣. 基于等级保护的政府 Web 应用安全建设实践[J]. 信息安全与通信保密，2012(10)：30-34.
Chen Y X. Classified protection building-up practice for governmental web application security [J]. China Information Security，2012(10)：30-34.

[10] 李茜. 一个基于等级保护的高校数据中心信息系统安全方案[J]. 广西科学院学报，2013，29(2)：89-91.
Li Q. A scheme for information system security of college data center based on classified protection[J]. Journal of Guangxi Academy of Science，2013，29(2)：89-91.

（责任编辑：尹 闯）