国家安全漏洞库的设计与实现

张玉清[1,2]，吴舒平[1,2]，刘奇旭[1,2]，梁芳芳[1,3]

（1.中国科学院研究生院 国家计算机网络入侵防范中心，北京 100049；
2.中国科学院研究生院 信息安全国家重点实验室，北京 100049；
3.西安电子科技大学 计算机网络与信息安全教育部重点实验室，陕西 西安 710071）

摘 要：在研究国内外安全漏洞库的基础上，结合我国国情和安全保障的需求，设计了一个兼容多个漏洞标准的、并将漏洞属性划分为相应群组的漏洞库结构模型。基于此模型，开发实现了国家安全漏洞库，并将其用于国内安全预警和应急响应领域，在实际应用中取得了良好的效果。

关键词：信息安全；安全漏洞；安全漏洞库；漏洞标准

中图分类号：TP393.08 **文献标识码**：B **文章编号**：1000-436X(2011)06-0093-08

Design and implementation of national security vulnerability database

ZHANG Yu-qing[1,2], WU Shu-ping[1,2], LIU Qi-xu[1,2], LIANG Fang-fang[1,3]

(1.National Computer Network Intrusion Protection Center, GUCAS, Beijing 100049, China;
2. State Key Laboratory of Information Security, GUCAS, Beijing 100049, China;
3. Key Lab of Computer Networks and Information Security of Ministry of Education, Xidian University, Xi'an 710071, China)

Abstract: Base on both domestic and overseas research on vulnerability database, considering our national conditions and the security requirements, a security vulnerability database model was proposed. It's compatible with multiple standards, and could be used to classify vulnerability attributes through groups. The national security vulnerability database was implemented based on the model and applied to security warning and emergency response. This work has brought satisfactory effects in practice.

Key words: information security; security vulnerability; security vulnerability database; vulnerability standard

1 引言

近年来，计算机病毒、木马、蠕虫和黑客攻击等日益流行，对国家政治、经济和社会造成危害，并对 Internet 及国家关键信息系统构成严重威胁。这些安全威胁绝大多数是利用系统或软件中存在的安全漏洞来达到破坏系统、窃取机密信息等目的，由此引发的安全事件也层出不穷。如 2009 年 5 月暴风影音软件漏洞导致了南方六省大规模的断网事件，2010 年 1 月微软极光漏洞导致了 Google 公司被攻击事件。

安全漏洞库保存了各类安全漏洞的基本信息、特征和解决方案等属性，是信息安全基础设施中重要的一环。一个结构合理、信息完备的漏洞库有利

收稿日期：2010-08-24；**修回日期**：2010-12-09

基金项目：国家自然科学基金资助项目（60773135, 90718007, 60970140）；中国科学院“十一五”科学数据库子项目(INFO-115-C01-SDB4-31)

Foundation Items: The National Natural Science Foundation of China (60773135, 90718007, 60970140); 11th Five-Year Scientific Database Sub-Project of CAS (INFO-115-C01-SDB4-31)

于为安全厂商基于漏洞发现和攻击防护类的产品提供技术和数据支持；有利于政府部门和安全组织从整体上分析安全漏洞的数量、类型、威胁要素及发展趋势，指导他们制定未来的安全策略；有利于用户确认自身应用环境中可能存在的漏洞，及时采取防护措施，降低网络安全事件发生的可能性。因此，构建安全漏洞库有十分重要的意义。

2 相关工作

欧美发达国家对安全漏洞库的研究投入较早，漏洞挖掘、分类和评级等领域的研究都较为透彻，并形成了行业内有影响力的标准，为安全漏洞库的建立奠定了坚实的基础。经过多年的发展和完善，国外一些安全信息提供机构(SIP, security information provider)在漏洞库的建设上已经具备了很深的资历，积累了丰富的经验，并形成了一批在国际上颇具影响力的漏洞库，如美国国家漏洞库[1] (NVD, national vulnerability database)、知名安全组织 SecurityFocus[2]、IBM 公司的 ISS X-Force[3]和丹麦知名安全公司 Secunia[4]等。

国内安全漏洞库相关领域的研究最早开始于科研机构，有部分研究者从事漏洞库的设计和实现工作[5,6]，但他们的工作重点不是收集和发布漏洞信息，而是通过整合漏洞属性设计合理完善的漏洞库结构，因此这类漏洞库在当时并没有投入实际应用。随着信息安全的发展，部分安全组织、公司和政府机构开始根据自身的需求建立漏洞库。目前影响力较大的中文漏洞库有中国国家信息安全漏洞库[7]、国家信息安全漏洞共享平台[8]等。国内现有中文漏洞库存在如下一些问题。

1）各个安全漏洞库在描述程度、收录数量和更新速度等方面各有所长，但由于各个漏洞库隶属于不同的政府部门，相互之间没有交流，导致漏洞信息不够全面；

2）由于没有遵从统一的标准，现有的安全漏洞库采用各不相同的标识、分类和评级方法，使得同一漏洞经不同机构发布后，其漏洞信息差别较大，对漏洞数据的共享和交流造成影响，也给用户理解带来困扰。

因此，本文在广泛调研国内外安全漏洞库的基础上，设计了一个与标准兼容的，基于群组对漏洞属性进行划分的安全漏洞库模型。该模型结构清晰合理，兼容漏洞领域的多个标准，有利于建设安全漏洞领域专业的、权威的、标准的漏洞资源，满足我国信息安全领域对安全漏洞进行统一引用的需求，增强不同网络安全工具之间的互操作性。

在此模型的基础上，本文实现了基于 Web 站点提供服务的国家安全漏洞库[9]。该系统综合了漏洞信息收集、管理和发布的重要功能，使得高效便捷地完成安全漏洞信息的整合集成与公开共享成为可能，大大提高了漏洞库维护的效率，缩短了漏洞更新的周期。

本文第 3 节介绍了国家安全漏洞库的设计目标；第 4 节详细介绍了系统设计方案，包括总体架构，系统主要功能模块、安全漏洞库的结构模型和系统访问权限控制方案；第 5 节分析了国家安全漏洞库的实现平台和建设中的关键技术；第 6 节介绍了国家安全漏洞库的应用效果和应用实例；第 7 节将本文建设的漏洞库与国内外其他漏洞库进行比较，说明了本文提出的漏洞库模型的优点和特性，并展望了下一步的工作；第 8 节是结束语。

3 国家安全漏洞库的设计目标

国家安全漏洞库定位于为国家建立一个安全漏洞信息共享与交流的平台，为公众和社会提供权威、标准、及时的安全漏洞信息，充分发挥漏洞库在安全预警和应急响应领域的作用。

安全漏洞库的建立和维护需要大量长期的工作，必须事先确立合理明确的设计目标，为今后能够积累到有价值的漏洞数据资源，及漏洞库的维护和管理奠定基础。国家安全漏洞库在设计时满足了以下几个高层次的设计目标。

3.1 兼容国内外多个漏洞标准

规范、标准的数据才能够在不同的漏洞库和安全工具之间共享和流通，才具有更大的价值。国际上安全漏洞领域最有影响力的标准是 CVE[10,11] (common vulnerability and exposures)。CVE 是为了寻求国际间安全企业、组织、机构对漏洞进行统一命名与解释而形成的，由于实际中所起到的巨大的沟通与规范作用，在国际安全界享有绝对的权威。CVE 本质上是一个检索目录或者称为漏洞的标准化名称列表，使用 CVE 编号可以方便地在兼容 CVE 标准的不同数据库中访问和检索漏洞信息。CVE 本身提供的漏洞信息并不详尽，仅包含 CVE 编号、漏洞描述、参考资源、状态信息和发布时间这 5 个属性。国际上主流漏洞库都与 CVE 标准保持兼容

和交叉引用。国家安全漏洞库在设计时支持 CVE 标准，实现了漏洞资源与国际接轨，通过 CVE 编号就能获取到相应的中文漏洞信息。

为了进一步规范漏洞数据，使得漏洞描述、评级和分类更加合理，同时考虑到近年来国内软件行业发展迅猛，国产软件漏洞数量逐年走高，而部分国产软件漏洞并未被 CVE 标准收录的情况，国家安全漏洞库的设计同时支持国际和国家标准。目前国内尚未有漏洞相关的国家标准出台。正在制订的标准有由国家计算机网络入侵防范中心负责及参与起草的《漏洞标识与描述规范》（草案）[12]及《安全漏洞等级划分指南》（草案）[13]。国家安全漏洞库的漏洞属性覆盖了《漏洞标识与描述规范》（草案）的全部字段，漏洞评级按照《安全漏洞等级划分指南》（草案）分为紧急、高、中、低 4 个级别。为了提供更多漏洞评级的细节，国家安全漏洞库支持国际标准 CVSS[14,15](common vulnerability scoring system)；漏洞分类由于尚未有国家标准提出，因此按照国际标准 CWE[16](common weakness enumeration)划分。对国际国内标准的全面支持，为漏洞数据共享、流通和推广奠定了坚实的基础。

3.2　漏洞数据全面、详尽、更新及时

国家安全漏洞库覆盖了近万种软件和产品。主流的应用软件、操作系统和网络设备都包含在内。尤其关注在国内应用广泛的系统、软件产生的漏洞。这些漏洞一旦被大量利用，会给国家互联网基础设施造成重大损失。国家安全漏洞库为用户提供详尽的漏洞信息，帮助用户定位和修复漏洞，关键的信息包括漏洞影响的软件版本、可能造成的威胁、是否可远程利用及相应的解决方案等。国家安全漏洞库每个工作日都会更新漏洞信息，第一时间帮助用户修补安全威胁。

3.3　满足不同层次用户的需求

漏洞信息的用户层面很广，主要包括公共互联网用户、政府部门及信息安全研究人员。上述 3 类用户具有的漏洞背景知识不同，对漏洞信息的理解和接受的能力也不同。因此，为了满足不同层次用户的需求，国家安全漏洞库的用户接口在设计时分为两部分，安全漏洞发布站点及安全漏洞论坛。

安全漏洞发布站点主要面向公共互联网用户和政府部门。公共互联网用户由于不具备专业的漏洞知识，因此该站点发布已验证且经过专业人员整理后的漏洞信息，使用通俗易懂的语言描述，提示漏洞的危害并附有详尽的、便于实施的漏洞解决方案。对于政府部门，他们更加关注漏洞的危害性和对互联网整体安全形势的潜在影响，因此，由专业人员对漏洞数据进行统计，分析当前的漏洞形势，并对网络安全的发展趋势做出预测，将上述内容撰写成相应的报告发布在网站上，供政府部门查阅。

安全漏洞论坛主要面向漏洞领域的研究人员。设有技术文章、漏洞研讨等版面，提供漏洞领域的最新研究进展和前沿技术，旨在带动漏洞研究人员的交流，推动信息共享和技术进步。安全漏洞论坛同时发布攻击利用代码和补丁的细节信息，使得系统管理人员能够及时地定位、验证和修复漏洞。安全漏洞论坛提供漏洞上报的渠道，鼓励漏洞挖掘人员及时上报漏洞，这部分未公开的漏洞也叫 0day 漏洞，是最有价值的漏洞资源。

4　国家安全漏洞库的设计方案

国家安全漏洞库的系统结构如图 1 所示。系统采用 B/S (browser/server)架构，分为表示层、功能层和数据层。表示层面向用户，是漏洞信息共享和发布的平台；功能层面向漏洞库的技术人员和维护人员，负责漏洞信息的收集和管理；数据层存储漏洞库的相关数据。

4.1　系统主要功能模块

4.1.1　安全漏洞论坛及安全漏洞发布站点

安全漏洞论坛主要服务于技术用户。漏洞上报模块提供漏洞的上报渠道，可以通过网页提交表单的方式上报，也可以通过电子邮件上报。两种上报方式均采用加密方式传输敏感的漏洞信息，防止未知漏洞信息被截获，造成用户损失。在漏洞研讨版面，用户可以通过邮件列表、RSS 订阅和访问站点等方式参与漏洞技术交流。攻击利用代码及补丁细节信息与漏洞信息互为补充并保持交叉引用，通过 Web 站点和邮件订阅 2 种方式同时发布。

安全漏洞发布站点面向公共互联网用户和政府部门发布漏洞信息和漏洞报告。漏洞发布站点提供友好的用户界面、完善的检索和数据统计功能，方便用户获取和使用漏洞数据。漏洞报告则分为漏洞周报，漏洞月报和漏洞年报，分析本周、本月和本年度漏洞数量，各危害级别及不同类型的漏洞数目的分布情况，与前一阶段相比呈现出的趋势及对下一阶段安全形势的预测，并评选出重大漏洞，为政府部门制定安全事件应急响应策略提供参考。

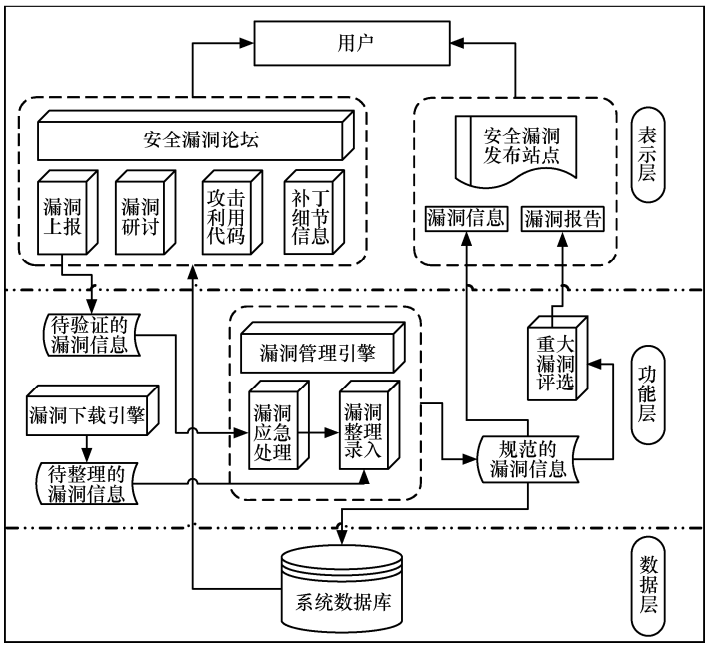


图 1　系统结构图

4.1.2　漏洞下载引擎

已公布的漏洞信息由维护人员使用漏洞下载引擎从国外权威的漏洞信息发布站点采集。为保证采集的漏洞数据质量，本文选择国际知名漏洞库 NVD、SecurityFocus、ISS X-Force 和 Secunia 作为主要的数据源。漏洞下载引擎能够自动下载指定的漏洞数据，智能地辨别重复条目，自动跟踪漏洞信息并及时更新，大大提高了漏洞库的维护效率。

4.1.3　漏洞管理引擎

漏洞管理引擎负责处理由漏洞论坛上报的未知漏洞信息和由漏洞下载引擎收集的已公布的漏洞信息。包含漏洞应急处理和漏洞整理录入 2 个子模块。

对于上报的未知漏洞信息（0day 漏洞）首先要做的工作就是应急处理，包含漏洞验证、漏洞报告、漏洞分析、漏洞整理录入、漏洞公布、致谢、反馈及更新等 7 个步骤。各步骤主要功能和职责如下。

1) 漏洞验证：由专业的漏洞技术研究人员负责验证漏洞论坛上报的国内外系统和软件产生的漏洞。由于提交上来的大部分漏洞信息一般只有简单的描述和 POC (proof of concept)代码，而 POC 一般只展示攻击的可能性，并不加载 shellcode，且不保证适用于各种环境。这就需要依靠漏洞研究人员丰富的漏洞分析经验来确认漏洞的真实性。漏洞验证是漏洞应急处理的关键，需要漏洞技术研究人员有快速的响应能力。

2) 漏洞报告：确定漏洞存在之后，将漏洞通告给软件厂商和相关的安全协调组织，并且敦促厂商尽快修复漏洞，提供软件补丁。

3) 漏洞分析：漏洞技术人员会对漏洞进行全面的研究，确定漏洞影响的系统和软件的版本、漏洞的危害级别、漏洞类型、可否远程利用、造成的影响、有无解决方案等关键要素。

4) 漏洞整理录入：漏洞库维护人员将分析得到的漏洞信息进行整理和完善，添加参考链接、漏洞编号和漏洞描述等信息并录入数据库。

5）漏洞公布：和软件厂商协调漏洞发布的时间后，再将漏洞在合适的时间公布出来。

6）致谢：对漏洞报告提交者表示感谢，并同发现者保持联系，以便进行进一步的研究与合作。

7）反馈及更新：将与漏洞相关的恶意利用代码和补丁对用户配置的影响等信息反馈给厂商。关注最新的漏洞公告，并根据最新的漏洞信息更新漏洞库。

对于已公布的漏洞信息，由于这部分漏洞已经得到验证，因此对其整理完善后录入数据库即可。

4.1.4　重大漏洞评选系统

由于各种操作系统、应用软件、网络设备上每天都会暴露出大量的漏洞，因此定期发布网络上发现的最普遍而且风险最高的漏洞是必要的。笔者研究了微软、SANS 等众多机构的重大漏洞评选机制，确定了如下评选原则：重大漏洞应根据漏洞的危害等级、漏

洞类型、攻击类型、攻击效果、攻击复杂度、受影响系统、漏洞实际可利用的程度和漏洞修复情况等因素综合评出最普遍和最具影响性的漏洞。

重大漏洞评选系统将上述影响因素取不同的权值，为已公布的漏洞评分并排序，按照分数的高低，每周评选 5 个重要漏洞，每月评选 10 个重要漏洞，对上述漏洞详细分析危害、受影响的软件、被利用情况及补丁信息，并点评一周或一月的漏洞趋势，最后撰写为漏洞周报或漏洞月报。经评选的重大漏洞往往是危害最严重，利用最广泛的漏洞。国家安全漏洞库将漏洞周报和漏洞月报公布在漏洞发布站点，起到了很好的安全预警作用。

4.2　漏洞库结构模型

为了实现和国内国际漏洞标准的兼容，并使得漏洞库的结构清晰合理，便于漏洞发布和今后的建设管理。笔者深入研究了《漏洞标识与描述规范》（草案），该规范明确规定漏洞描述至少应包括标识（CVD 编号）、名称、发布时间、发布单位、摘要、类别、等级、影响系统和解决方案这 9 个属性。可以看到《漏洞标识与描述规范》（草案）作为一个标准，规定的是漏洞库的基础结构，但是如果仅用它描述漏洞信息则不够全面。因此本文分析了国内外主流漏洞库的结构模型，对漏洞属性进行了全面的归纳，提炼出 36 个属性。在此基础上，提出一种基于群组分类描述漏洞属性的方法，将全部的漏洞属性划分为 8 个群组，漏洞库结构模型如图 2 所示。

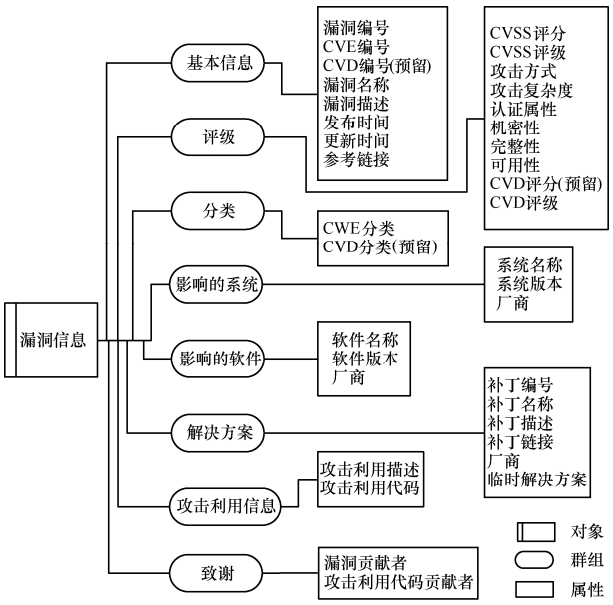


图 2　漏洞库结构模型

该方法的思想是将多维漏洞属性划分成相应的群组。群组是漏洞若干个关联紧密的属性的集合。每个漏洞对应多个群组，每个群组包含多个属性。各个群组之间相互独立，群组内部的属性相互关联。

使用基于群组的方法分类描述漏洞，使得漏洞信息更加结构化。这种模型不仅方便用户有选择地获取自身关注的那部分漏洞信息，还使得漏洞库管理人员能够灵活地挑选对应领域的专家对漏洞信息进行分析和维护，如漏洞评级领域的专家可以仅负责维护漏洞评级群组对应的属性。

该模型与漏洞标准紧密结合。每条漏洞信息均对应有 CVE 编号、CVD 编号和内部编号，满足在不同范围内对漏洞统一引用的需求。对于没有被 CVE 收录的国产系统和软件的漏洞使用 CVD 编号索引。暂无 CVE 编号和 CVD 编号的漏洞使用内部编号索引。漏洞评级群组同时支持 CVSS 标准和《安全漏洞等级划分指南》（草案），漏洞分类群组目前仅支持 CWE 分类，但预留有国内漏洞分类方法的接口。

4.3　访问权限控制方案

考虑到漏洞信息的敏感性，如何将不同级别的漏洞信息通过合适的方式传递给正确的用户是漏洞库设计时必须要考虑的关键因素。

国家安全漏洞库中存储的漏洞信息按其生命周期可分为 3 类：已上报未验证的漏洞、已验证未公开的漏洞和已公开的漏洞。前两类都属于未公布的漏洞，这部分漏洞厂商往往没有相应的补丁提供，一旦提前泄露，很可能被黑客大量利用，造成巨大危害。因此本文设计了一个基于用户角色的权限控制方案，如图 3 所示。

由于不同用户拥有不同程度的漏洞知识和技能，因此被赋予不同的角色，享有的权限也不同。

普通用户：不具备漏洞领域的专业知识，仅能浏览已公布的漏洞信息。

注册用户：拥有一定程度的漏洞专业知识和技能，可以是安全爱好者或漏洞研究人员。他们拥有普通用户的权限，同时可以通过注册获得相应的权限后提交新的漏洞。在新漏洞验证公布之前，注册用户仅能查看本人提交的漏洞信息，不能浏览其他注册用户提交的漏洞信息。

领域专家：精通漏洞领域专业知识和技能，达到一定的信任级别，一般为漏洞领域的专家学者。领域专家通过注册获得相应权限后能够验证和分

析注册用户提交的全部漏洞，但不能对已发布的漏洞进行任何操作。

系统管理员：是漏洞库的拥有者。系统管理员拥有全部的权限，可以管理已发布和未公开发布的所有漏洞信息，包括决定新漏洞的发布时间，修改漏洞库结构，添加、修改和删除漏洞信息。同时还能够为其他角色的用户授予相应的权限。

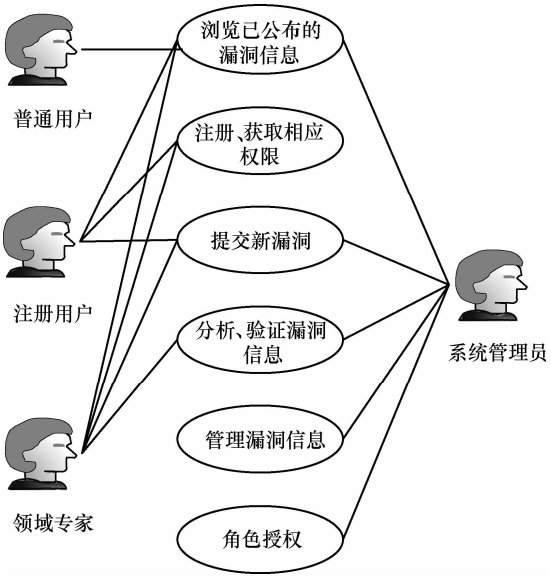


图3 访问权限控制方案

5 国家安全漏洞库的系统实现

系统表示层的安全漏洞论坛和安全漏洞发布站点基于Windows平台和微软ASP.NET技术开发，Web 服务器使用 IIS。系统功能层的漏洞下载引擎和漏洞管理引擎基于 Windows 平台，使用 C#语言开发。系统数据库选择 SQL 服务器关系数据库。

5.1 漏洞下载引擎

漏洞数据下载是漏洞信息的重要来源。传统的漏洞下载工具将包含漏洞信息的 Web 页视为没有结构的纯文本，使用程序中硬编码的抽取规则对漏洞信息进行抽取。这种方式容易实现，但无法灵活定义抽取规则，当 Web 页的格式频繁改变时，代码维护工作变得相当困难。本文基于 HTML 文档结构，使用可扩展 XML 路径语言(XPath)技术实现从漏洞发布页面中抽取相应的漏洞属性。XPath 具有强大的表达能力，通过构造适当的 XPath 表达式对 XML/HTML 文档树进行匹配，从而得到该文档树结点集的一个子集，其中包含需要抽取的漏洞信息。该方法的抽取规则可以通过外部的配置文件来定义，Web页的格式改变后只需修改配置文件即可，方便了系统的使用和维护。

5.2 漏洞管理引擎

漏洞管理引擎采用 ASP.NET 技术，基于 Web 动态页面实现。数据库管理员使用浏览器，通过向服务器端的漏洞库提交请求，以实现对漏洞相关数据的查询、插入、更新、删除等操作。漏洞管理引擎实现了良好的人机交互界面，方便管理员维护存储在漏洞库中的数据。

漏洞管理引擎使用 ADO.NET 数据库访问技术和漏洞库建立连接。ADO.NET 是微软针对网络数据库应用和 Visual 系列开发工具所开发的数据对象，具有高性能、可扩展和面向对象的特性。

5.3 数据备份与恢复策略

安全漏洞库的建设是一个长期而艰巨的任务，漏洞数据是经过许多专家的辛苦工作积累的宝贵资源。由于人为错误、硬盘损坏、黑客攻击等都有可能造成数据的丢失，影响漏洞库持续稳定的提供服务，因此漏洞数据的备份与恢复工作十分重要。本文采用了 3 种备份恢复策略。

1) 启用SQL服务器数据库自动备份和恢复机制。

2) 使用冗余磁盘阵列 RAID 进行备份与恢复。

3) 使用远程镜像技术定期将本地数据镜像备份到远程服务器。

5.4 系统安全防护措施

为保证国家安全漏洞库 Web 服务站点的安全性，本文采取了以下防护措施。

1) 代码级的安全防护：使用过滤输入中的危险字符和参数化查询的方式防御 SQL 注入漏洞；使用过滤输入中的危险字符，结合微软 Anti-XSS 库，对 Web 应用程序的输出进行编码的方法防御 XSS 攻击；使用加入随机 token 的方式抵御 CSRF 攻击。

2) 网站安全防护：部署基于网络可生存性的网站保护系统[17]。该系统基于网络可生存性的事后恢复思想，利用实时监控和基于 NDIS 中间层驱动过滤的方式实现对网页文件的保护；利用数据库管理系统中的触发器机制，通过权限管理，实现对数据库中数据的保护。系统还对普通用户的数据库访问权限严格控制，防止用户破坏漏洞数据。

6 应用效果及案例

国家安全漏洞库[9]于 2009 年 11 月 27 日开通访问，运行近一年时间，目前现有漏洞数据 33 286 条，

发布漏洞周报 60 则，漏洞月报 12 则。

鉴于国家安全漏洞库以网站为应用平台，以发布漏洞信息和漏洞报告为主要服务形式，因此漏洞库的访问情况很大程度上反映了漏洞库的应用效果。了解和掌握国家安全漏洞库的访问情况，根据访问数据改进网站服务是十分必要的。因此本文部署了漏洞数据服务监测与统计系统，通过统计访问数据评价漏洞库的应用情况，具体统计数据见表 1。

表 1　国家安全漏洞库访问情况数据统计

数据项	数据量
累计独立 IP 数	59 754 次
累计访问人次	85 975 次
累计页面访问数	745 878 次
累计请求数	1 876 721 次
累计下载量	35.58G

注：数据统计截止至 2010 年 11 月 24 日。

国家安全漏洞库开通访问一年来，保持了平稳连续运行，Alexa 排名在中文漏洞库中靠前，在中国科学院科学数据库系统中访问排名靠前，总体访问情况良好，受到众多用户的持续关注和访问，达到了预期的应用效果。访问 IP 来自国内、美国、台湾、日本、韩国、英国等地区，说明国家安全漏洞库不仅在国内发挥着安全预警作用，也受到国外同行的关注。

为拓展国家安全漏洞库的应用范畴，依托安全漏洞库的漏洞资源，为政府相关部门、社会团体、科研机构提供及时而专业的安全漏洞咨询服务，得到了相关单位的良好反馈，在信息安全预警和应急响应领域发挥了重要作用。典型应用案例如下。

1) 为公安部国家网络与信息安全信息通报中心提供每周、每月、季度、年度的安全漏洞形势分析报告，以及特殊时期如两会、国庆期间的每日漏洞通报。目前共提供漏洞周报 100 余份、漏洞月报 20 余份、漏洞年报 2 份。为国家政府部门掌握网络安全态势，制定相应的应急响应方案提供技术支持。

2) 为公安部和中国计算机学会计算机安全专业委员会主办的《信息网络安全》杂志撰写安全漏洞分析与预警的专栏文章 14 篇，通过该杂志为用户提供漏洞信息和防护建议。

3) 为中国科学院提供重大漏洞，关键补丁以及网络安全事件通报服务。使其能够根据漏洞信息对中科院内部计算机网络进行安全防护。

4) 为新华社提供每周安全漏洞预警新闻。新华社是中国政府官方的国家通讯社，在世界各地有一百多个分社，在中国大陆的每个省、直辖市、自治区都设有分社，是中文媒体的主要新闻来源之一。漏洞预警新闻通过新华社在大范围的用户中传播，发挥了良好的预警效果，大大降低网络中安全漏洞风险。

7　讨论和展望

目前，我国颇具规模的中文漏洞库有中国国家信息安全漏洞库、国家信息安全漏洞共享平台、国家安全漏洞库等。国外最著名的漏洞库为美国国家漏洞库 NVD，表 2 从数据规模、对标准的支持程度和漏洞属性全面性 3 个角度对上述漏洞库做如下比较。

表 2　漏洞库比较

漏洞库	数据规模/条	CVE 标准	CVSS 标准	CWE 标准	漏洞属性个数/个
中国国家信息安全漏洞库	37 262	支持	不支持	不支持	14
国家信息安全漏洞共享平台	28 950	支持	不支持	不支持	14
国家安全漏洞库	33 286	支持	支持	支持	36
美国国家漏洞库 NVD	44 477	支持	支持	支持	15

注：数据统计截止至 2010 年 11 月 24 日。

相对于其他中文漏洞库，国家安全漏洞库具有以下优点：数据资源丰富，数据量达到一定规模；与国内外标准保持高度兼容，特别是对国内标准的支持，使得未被 CVE 收录的国产软件漏洞能够标识并及时公布；漏洞属性更加全面、漏洞信息更加详尽。

本文提出的基于群组的漏洞属性划分方法，使得漏洞信息更加结构化，漏洞库模型更加清晰，方便用户使用漏洞数据和漏洞库的管理。

安全漏洞库拥有高质量的漏洞数据资源，是漏洞发布和安全预警的重要平台，但安全漏洞库的功能并不仅限于此。如美国基于漏洞库提出了 SCAP[18,19]（security content automation protocol）计划。SCAP 是一种使用安全标准进行自动化漏洞管理、度量，以及安全策略符合性评估的方法。该方法和 CVE\CVSS\CWE 等标准紧密结合，应用结构化、形式化的漏洞信息进行自动化的安全风险评估和终端安全配置检查，大大提高了漏洞检测和修复的效率。

本文在做好漏洞库数据资源建设的同时，会进一步研究类似 SCAP 模式的基于漏洞库的安全审计、风险评估、软件安全性评测的方法及工具，将漏洞库融入国家信息安全战略的整体框架中，充分

发挥漏洞库数据资源的效用，为各类围绕安全漏洞的工具和服务提供支持。

8 结束语

安全漏洞是很多恶意攻击的主要根源。对漏洞信息进行分析、总结、积累，建立安全漏洞库是十分必要的。本文设计了一种兼容国内外多个漏洞标准的、基于群组进行漏洞属性划分的漏洞库结构模型，并在 Windows 平台下实现了国家安全漏洞库。该系统作为漏洞信息共享发布的平台，在安全预警和应急响应领域扮演着重要角色。同时，国家安全漏洞库存储的规范而标准的漏洞信息也为风险评估、漏洞扫描等领域的研究提供了重要的数据支持。

参考文献：

[1] National vulnerability database[EB/OL]. http://nvd.nist.gov/.

[2] Securityfoucs[EB/OL]. http://www.securityfocus.com/bid/.

[3] IBM ISS X-force[EB/OL]. http://xforce.iss.net/.

[4] Secunia[EB/OL]. http://secunia.com/.

[5] 翟钰，张玉清，武维善等. 系统安全漏洞研究及数据库实现[J]. 计算机工程，2004，30(8)：68-70.
ZHAI Y, ZHANG Y Q, WU W S. Research of system security vulnerability and implementation of database[J]. Computer Engineering, 2004,30(8):68-70.

[6] 赵鑫. 漏洞攻击防范技术与漏洞数据库设计[D]. 北京：北京邮电大学,2008.
ZHAO X. Vulnerability Attack and Defense and Vulnerability Database Design[D]. Beijing: Beijing University of Posts and Telecommunications, 2008.

[7] 中国国家信息安全漏洞库[EB/OL]. http://www.cnnvd.org.cn/.
China national vulnerability database of information security[EB/OL]. http://www.cnnvd.org.cn/.

[8] 国家信息安全漏洞共享平台[EB/OL]. http://www.cnvd.org.cn/.
China national vulnerability database[EB/OL]. http://www.cnvd. org.cn/.

[9] 国家安全漏洞库[EB/OL]. http://www.nipc.org.cn/.
National security vulnerability database[EB/OL]. http://www.nipc.org.cn/.

[10] Common vulnerabilities and exposures[EB/OL]. http://cve.mitre.org/.

[11] PETER M, TIM G. NIST special publication 800-51, use of common vulnerabilities and exposures(CVE) vulnerability naming scheme[EB/OL]. http://csrc.nist.gov/publications/nistpubs/800-51/sp800-51.pdf. 2002.

[12] 中华人民共和国国家标准. 漏洞标识与描述规范(草案)[S]. 2010.
National Standard of the People's Republic of China. Vulnerability Identification and Description Specification[S]. 2010

[13] 中华人民共和国国家标准. 安全漏洞等级划分指南(草案)[S]. 2010.
National Standard of the People's Republic of China. Classification of Security Vulnerabilities Guide[S].2010.

[14] JOHN C, JOHN T. Common vulnerability scoring system[EB/OL]. http://www.first.org/cvss/v1/guide.html. 2004.

[15] PETER M, KAREN S, SASHA R. A complete guide to the common vulnerability scoring system version 2.0[EB/OL]. http://www.first.org/ cvss/cvss-guide.pdf. 2007.

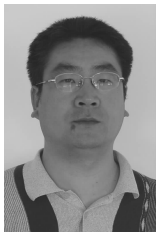
[16] Common weakness enumeration[EB/OL]. http://cwe.mitre.org/.

[17] 刘宇, 张玉清. 基于网络可生存性的网站保护系统[J]. 计算机工程, 2008, 34(19):167-169.
LIU Y, ZHANG Y Q. Website protection system based on network survivability[J]. Computer Engineering, 2008，34(19)：167-169.

[18] STEPHEN Q, DAVID W, CHRISTOPHER J. NIST special publication 800-126, the technical specification for the security content automation protocol (SCAP): SCAP version 1.1[EB/OL]. http://csrc.nist.gov/publications/drafts/800-126-r1/second-public-draft_sp800-126r1-may2010.pdf. 2010.

[19] STEPHEN Q, KAREN S, MATTHEW B. NIST special publication 800-117, guide to adopting and using the security content automation protocol (SCAP) version 1.0[EB/OL]. http://csrc.nist.gov/ publications/nistpubs/800-117/sp800-117.pdf. 2010.

作者简介：



张玉清（1966-），男，陕西宝鸡人，博士，中国科学院研究生院教授、博士生导师，主要研究方向为网络与信息系统安全。

吴舒平（1985-），女，湖北襄樊人，中国科学院研究生院硕士生，主要研究方向为网络与信息系统安全。

刘奇旭（1984-），男，江苏徐州人，中国科学院研究生院博士生，主要研究方向为网络与信息系统安全。

梁芳芳（1985-），女，山西临汾人，西安电子科技大学通信工程学院硕士生，主要研究方向为网络与信息系统安全。