赛尔网络体检中心

产品白皮书

赛尔网络有限公司

目 录

一. 漏洞的危害和发展趋势

从互联网兴起至今，利用漏洞攻击的网络安全事件不断，并且呈日趋严重的态势。每年全球因漏洞导致的经济损失巨大并且在逐年增加，漏洞已经成为危害互联网的罪魁祸首之一，也成了万众瞩目的焦点。人们也在一次次承受蠕虫爆发、病毒、木马以及恶意代码的危害之后，在不断地寻求着漏洞的解决之道，不断尝试将由漏洞带来的风险降到最低，虽然也取得了一定成效，但是利用漏洞的攻击也在逐渐表现为多种不同的危害形式并且出现了新的攻击趋势。

1.1 漏洞的危害

漏洞是在硬件、软件、协议的具体实现或系统安全策略上存在的缺陷，可以使攻击者在未授权的情况下访问或破坏系统。安全漏洞有很多种分类方式，按照漏洞宿主不同，可以分为三大类：第一类是由于操作系统本身设计缺陷带来的安全漏洞，这类漏洞将被运行在该系统上的应用程序所继承；第二类是应用软件程序的安全漏洞；第三类是应用服务协议的安全漏洞。近年来，针对应用软件程序和应用服务协议安全漏洞的攻击越来越多，同时利用病毒、木马技术进行网络盗窃和诈骗的网络犯罪活动呈快速上升趋势，产生了大范围的危害，由此造成的经济损失也是越发巨大。

针对WEB应用安全漏洞的攻击也在逐渐成为主流的攻击方式。利用网站操作系统的漏洞和WEB服务程序的SQL注入漏洞等，黑客能够得到Web服务器的控制权限，从而轻易篡改网页内容或者窃取重要内部数据，甚至在网页中植入恶意代码（俗称“网页挂马”），使得更多网站访问者受到侵害。

近年来层出不穷的应用软件安全漏洞的危害性已经与操作系统的安全漏洞平分秋色。不断发展和广泛应用的各种应用程序（如IE浏览器、MS Office、多媒体播放器、VMware虚拟机和各种P2P下载软件）中存在的安全漏洞也越来越多的被披露出来。安全漏洞问题日益复杂和严重。

2005－2007年间的主要攻击是针对WEB应用安全漏洞和客户端程序的攻击。来自google、Yahoo、Microsoft以及eBay等著名互联网公司或者提供WEB服务的软件公司都出现了不同程度的漏洞，且都被攻击者成功的加以利用。

例如：

2007年6月份，沪上某高校数千名学生和老师的电子学籍管理系统账号和密码外泄。笔者发现，用这些账号，不仅可查看在校学生的学籍、个人和家庭信息，部分权限大的账号甚至还可对学生的个人信息进行修改。这一情况的出现，不仅威胁到学生的隐私和学籍安全，也可能给骗子以可乘之机。

2008年7月31日，武汉大学招生录取结果查询网页遭到电脑黑客攻击，不法分子利用电脑黑客技术，篡改招生录取查询网页，删除正式录取名单中的11人，恶意添加8人，欺骗考生和家长。据调查，其中1个考生被骗取的金额就达十几万元。学校迅速向公安机关报告并及时对被篡改的录取信息进行了修正。

2008年8月份，清华大学网站遭受到黑客攻击，黑客借用清华校长的名义抨击教育制度，该“新闻”出现在8月24日的“清华新闻”栏目中，该“新闻”中称清华大学校长顾秉林先生在接受学生记者采访的时候，表达了他对现在大学教育状况的担心。文中写顾秉林先生表示，现在的各高校，包括清华与北大在内，已经没有将培养人才作为大学教育的目标。在此条捏造的“新闻”的标题和正文中，还出现了一些不雅的措辞。

2008年9月份，北大校园网上挂出一篇名为“现在的大学校园已被侵蚀”的文章。文中以北大校长许智宏的名义批评了现行教育制度，称中国的高等教育体制改革势在必行，并提出“改革的重点”，其中包括“加强传统的道德文化教育”，“对以教授名义长期盘踞校园的无德无能之辈清理门户”等内容。

在2009年10月份，西南民大学的学报邮箱被黑，利用学报邮箱要每个作者发表文章的版面费。在西南民大学报编辑室，学报副主编王珏说“两个投稿邮箱都被黑了，现在还在想办法找回。”从10月5日起，投稿邮箱登录失败，提示密码错误。邮箱被黑客入侵了！”王珏说，随后他们便陆续接到一些作者电话，询问学报是否要收版面费。想到这里，他立刻向已经登录不上的邮箱发了邮件，果然收到了一些作者所看到的邮件。大家这才发现，这是一起黑客入侵邮箱骗取钱财的网络诈骗。目前，网络上已经有网友发帖指责他们利用学报赚钱，王珏表示，这对学校的声誉影响极大。

2009年高考网上录取前后，20多所知名高校的二级网页屡遭“挂马”，而浏览这些高校网页的学生和家长，存在被盗取网游、网银等账号信息，此事件引发了不小的震动。期间，中央财经大学招生网页被挂马，招生数据被恶意篡改，同时，8月份又有多所高校的成人教育网站被恶意“挂马”，这些情况引发了各大高校的高度戒备。

从上可以看出，安全漏洞的危害范围在逐渐扩大，由系统层扩展到应用层，由服务器端扩展到客户端，由少数操作系统扩展到绝大多数操作系统；由此造成的经济损失也越来越大，尤其是用户不易察觉的隐性攻击造成的损失是无法衡量的。

1.2 漏洞的发展趋势

随着技术的不断进步，漏洞的发现、漏洞利用技术也发展到一个较高水平，从总体上来看，漏洞的发展趋势主要表现为以下几个方面：

漏洞的发现技术更加自动化和智能化，漏洞发现技术的革新导致了发现的漏洞数量剧增，下面是国际组织CERT/CC从1995年到2007年的漏洞统计数据。该组织2007 年全年收到信息系统安全漏洞报告7236个，自1995年以来，漏洞报告总数已达38016个。

表 1.1 1995-1999 CERT/CC漏洞统计数据表

Year	**1995**	**1996**	**1997**	**1998**	**1999**
Vulnerabilities	171	345	311	262	417

Year	**2000**	**2001**	**2002**	**2003**	**2004**	**2005**	**2006**	**2007**
Vulnerabilities	1,090	2,437	4,129	3,784	3,780	5,990	8064	7236

表 1.2 2000-2007 CERT/CC漏洞统计数据表

其中，除Windows操作系统漏洞外，安全漏洞更多的集中出现在了IE浏览器和MS Office等应用软件上。国际上出现大量的专业漏洞研究组织，漏洞的出现到漏洞被利用的时间在不断的缩短，同时0-day攻击的数量在逐渐增加。利用漏洞攻击的重心由服务器端向客户端过渡，由系统层和网络层逐渐向应用层扩展；WEB应用安全漏洞造成危害日益凸显。漏洞的发现、利用不仅仅局限于常见的网络设备、操作系统，而且不断的向新的应用领域扩散。利用漏洞的蠕虫逐渐减少，利用漏洞攻击的手法越来越诡异，越来越隐蔽。

二. 漏洞修复的必要性与重要性

漏洞的危害越来越严重，发展的趋势也日益严峻。归根结底，产生这些问题的原因是系统漏洞的存在并被攻击者恶意利用。软件由于在设计初期考虑不周导致的问题仍然没有得到很好的解决，人们依然用着“亡羊补牢”的方法来度过每一次攻击，利用漏洞的攻击成为人们心中永远的痛。

统计表明，19.4%的攻击来自于利用管理配置错误，而利用已知的一个系统漏洞入侵成功的占到了15.3%。事实证明，绝大多数的网络攻击事件都是利用厂商已经公布而用户未及时修补的漏洞。已经公布的漏洞未得到及时的修补和用户的安全意识有很大的关系，一个漏洞从厂商公布到漏洞被大规模利用之间的时间虽然在逐渐的缩短，但是最短的也有18天之久，18天对于一些安全意识高的用户来说，修补一个安全漏洞应该没有任何问题。

目前大多数用户的安全意识也提高了，但是“冲击波”蠕虫和“震荡波”蠕虫的爆发还造成如此之大的损失，病毒、特洛伊木马及恶意代码逐渐成为严重的安全问题，这说明仅仅提高用户的安全意识是完全不够的。同时由于客户端、第三方软件安全漏洞危害日益增大，传统的远程扫

描已经不能满足日益变化的安全漏洞形式，需要一套有效的管理机制并通过一定安全技术手段辅助自动完成整个过程，才能有效地对漏洞进行动态地管理。

目前，从技术和管理两个角度来看，漏洞问题已经有了较为成熟的解决方案。漏洞管理就是这样一套能够有效避免由漏洞攻击导致的安全问题的解决方案，它从漏洞的整个生命周期着手，在周期的不同阶段采取不同的措施，是一个循环、周期执行的工作流程。一个相对完整的漏洞管理过程包含以下步骤：

1. 对用户网络中的资产进行自动发现并按照资产重要性进行分类；

2. 自动周期对网络资产的漏洞进行评估并将结果自动发送和保存；

3. 采用业界权威的分析模型对漏洞评估的结果进行定性和定量的风险分析，并根据资产重要性给出可操作性强的漏洞修复方案；

4. 根据漏洞修复方案，对网络资产中存在的漏洞进行合理的修复或者调整网络的整体安全策略进行规避；

5. 对修复完毕的漏洞进行修复确认；

6. 定期重复上述步骤1-5。

漏洞管理能够对预防已知安全漏洞的攻击起到很好的作用，做到真正的“未雨绸缪”。相对于传统的漏洞扫描产品而言，漏洞管理产品能够为用户带来更多的价值。

漏洞管理产品从漏洞生命周期出发，提供一套有效的漏洞管理工作流程，实现了由漏洞扫描到漏洞管理的转变，实现了“治标”到“治本”的飞跃。通过漏洞管理产品，集中、及时找出漏洞并详细了解漏洞相关信息，不需要用户每天去关注不同厂商的漏洞公告，因为各个厂商的漏洞公告不会定期发布，即使发布了漏洞公告绝大多数用户也不能够及时地获得相关信息。通过漏洞管理产品将网络资产按照重要性进行分类，自动周期升级并对网络资产进行评估，最后自动将风险评估结果自动发送给相关责任人，大大降低人工维护成本。漏洞管理产品根据评估结果定性、定量分析网络资产风险，反映用户网络安全问题，并把问题的重要性和优先级进行分类，方便用户有效地落实漏洞修补和风险规避的工作流程，并为补丁管理产品提供相应的接口。漏洞管理产品能够提供完整的漏洞管理机制，方便管理者跟踪、记录和验证评估的成效。

三. 产品评价指标

由于漏洞管理和漏洞扫描产品之间具有较大的差异性，用户在购买一款漏洞管理类产品时需要考虑以下因素：

服务商是否具备漏洞跟踪和漏洞前瞻性研究能力，具体可考察漏洞知识库的完备性、权威性

和更新及时性；产品是否支持漏洞管理工作流程，包括是否支持相应的开放接口；漏洞评估的性能，主要考察漏洞检测的速度、准确性和覆盖，其中覆盖的漏洞是否包含常见的本地及远程安全漏洞；产品是否具备资产管理能力，是否具备对资产风险的定性、定量分析能力；产品是否具备针对复杂大型网络的分布式部署和集中管理能力；产品的报告内容、形式是否灵活，报告是否具备多角度统计分析的能力；是否获得国际上第三方权威测试机构的认证。

四．赛尔网络体检中心产品

基于多年的安全服务实践经验，同时结合用户对安全评估产品的实际应用需求，赛尔网络体检中心自主研发了弱点扫描及评估系统、网站木马检测及清除系统，它们采用高效、智能的漏洞识别和木马识别技术，第一时间主动对网络中的资产进行细致深入的漏洞和木马检测、分析，并给用户提供专业、有效的漏洞防护建议，让攻击者无机可乘，是您身边专业的“漏洞管理专家”。

依托专业的CCERT响应组和北大信安中心，综合运用信息重整化（NSIP）等多种领先技术，自动、高效、及时准确地发现网络资产存在的安全漏洞；提供Open VM（Open Vulnerability Management开放漏洞管理）工作流程平台，将先进的漏洞管理理念贯穿整个服务产品实现过程中；对发现的网络资产的安全漏洞进行详细分析并采用权威的风险评估模型将风险量化，给出专业的解决方案；方便的资产风险管理功能，帮助安全管理员全面、快速定位企业信息资产中的风险情况，并为用户提供全方面的治疗、培训服务。

4.1 产品体系结构

是基于WEB的管理方式，用户使用浏览器通过SSL加密通道和系统WEB界面模块进行交互，方便用户管理。系统采用模块化设计，内部整体工作架构如图4.1所示。

图 4.1 漏洞管理系列整体架构图

4.1.1 扫描核心模块

扫描核心模块是系统最重要的模块之一，它负责完成目标的探测评估工作，包括判定主机存活状态、操作系统识别、规则解析匹配等。

4.1.2 漏洞知识库

漏洞知识库包含漏洞相关信息，是系统运行的基础，扫描调度模块和WEB管理模块都依赖它进行工作。

4.1.3 扫描结果库

扫描结果库包含了扫描任务的结果信息，是扫描结果报告生成的基础，也是查询和分析结果的数据来源。

4.1.4 数据分析模块

数据分析模块是综合分析、趋势分析和报表合并的统计信息的数据来源，是任务合并、分布式数据汇总之后的结果。

4.1.5 风险管理模块

管理员通过此模块可以对网络风险进行全方位管理、定位和分析，并进行漏洞审计，自动验证漏洞是否修复。另外，通过资产管理，能够方便用户掌握风险分布情况、定位风险和高效实施风险降低或规避措施。

4.1.6 WEB 界面模块

WEB界面模块负责和用户进行交互，配合用户的请求完成管理工作。

4.1.7 系统升级模块

有网络自动升级和用户手动升级的策略，系统的各个模块都可以通过升级模块进行升级。

4.1.8 辅助模块

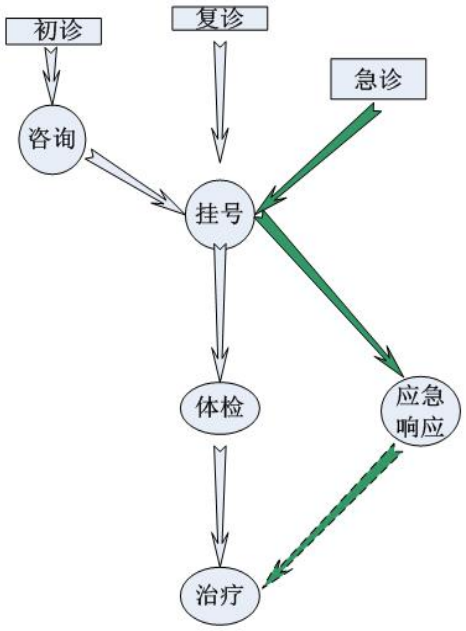
支持分布式部署功能。在下级设备完成扫描得到结果数据后，会向上级管理系统上传数据，数据传输过程中使用SSL加密传输通道，保证了数据的保密性。汇总的数据可以进行集中统一的分析。

4.1.9 扩展模块、WEB 扫描模块

推出了WEB应用安全漏洞检测模块，通过对被检测站点进行深度内容分析，找出可被浏览的ASP、JSP、PHP、CGI等页面，同时可以分析被检测站点页面源代码，以检测网站是否存在跨站脚本和SQL注入等漏洞。

4.2 赛尔网络体检中心服务流程

赛尔网络体检中心



服务	名称	内容
咨询	中心服务介绍	
	安全方案建议	
	用户疑难解答	
体检	系统检测	系统弱点漏洞检测
	Web 检测	木马、病毒、不良信息检测
	数据库检测	据库安全配置检测
	网络设备检测	交换机、路由器等设备配置检测
治疗	系统安全加固	弱点漏洞修复、服务安全配置等
	Web 安全加固	木马清除、病毒查杀、代码校正等
	数据库安全加固	数据库系统安全修复
	网络设备安全加固	网络设备服务配置
	网站升级及重建	
	安全产品	安全软件、安全设备
急诊	应急响应	分析及取证、灾难恢复及入侵追踪等
培训	培训交流	网站安全、灾难恢复培训

图 4.2 赛尔网络体检中心服务流程

4.2.1 咨询

咨询内容有：中心服务介绍、安全方案建议和用户疑难解答。您如果对我们体检中心不了解的情况下，可以联系我们，我们会给你解答您心中的疑问！

4.2.2 挂号

您对我们体检中心有了了解，如果您想让我们体检中心为您检查，您要给我们体检中心提供您网站的域名。这样我们就会为您检查了。

4.2.3 体检

根据用户所给的域名，来检查用户的系统检测、WEB检测、数据库检测和网络设备检测，这样全面的检测用户所给的域名，并把所检测出来的报告发送给用户。用户可以查看报告，知道自己网站的情况。

4.2.4 治疗

我们可以给用户提供技术支持，来帮住用户解决报告上的所有问题。这样就是用户的网站更加安全。方法有：系统安全加固、数据库安全加固、网络设备安全加固、网站升级及重建和安全产品。

4.2.5 急诊

如果用户遇到了资料的丢失或损坏，我们体检中心可以对用户进行急诊，并用最快的速度对用户的网站进行分析和取证、灾难恢复及入侵追踪等，以使用户的损失降到最小。

4.2.6 培训

用户对自己的技术存在担心，我们可以通过培训的方式，使用户的技术提高，以应对一些特殊情况，这样就可以解决用户网站的安全后顾之忧了。

4.3 产品特色

4.3.1 基于用户行为模式的管理架构

作为用户体验性很强的产品，始终秉承“以人为本”的理念，在产品设计过程充分考虑了实际用户需求和使用习惯，从用户角度完善了很多管理功能。“一键式”智能任务模式、快速结果报表、智能摘要技术等，最大限度的满足了易用性和高效性的需求。

采用B/S管理架构，能够以SSL加密通讯方式通过浏览器来远程进行管理。的专用硬件能够长期稳定地运行，很好地保证了任务的周期性自动处理。能够自动处理的任务包括：评估任务下发、扫描结果自动分析、处理和发送、系统检测插件的自动升级等。同时，支持多用户管理模式，能够对用户的权限做出严格的限制，并且提供了登录、操作和异常等日志审计功能，方便用户对系统的审计和管理。

4.3.2 高效、智能的漏洞识别技术

赛尔网络体检中心应用先进的智能漏洞识别技术，在提高的网络安全的评估速度和准确率方面都起到了很大的促进作用。智能漏洞识别技术就是采用多种技术通过不同途径收集目标系统的多种信息，在进行漏洞评估过程中，不断地对中间的结果数据进行调整，保障了最后评估结果的准确性。

通过漏洞识别技术、开放端口服务的智能识别、检测规则依赖关系的自动扫描等技术的运用，在检测速度和检测准确性之间找到了最佳的平衡点。加载全部检测规则，对同样的目标系统进行检测时，扫描速度为常见同类产品4－6倍，同时仍能保证误报率低于1%。

4.3.3 精确的 WEB 应用安全分析

考虑到目前WEB应用安全漏洞所带来的巨大危害，推出了WEB应用安全漏洞检测模块，通过对被检测站点进行深度内容分析，找出可被浏览的ASP、JSP、PHP、CGI等页面，同时还在漏洞检测中提供了专用的CGI漏洞检测插件规则类别以及专用的SQL注入和跨站脚本等检测插件，用来发现一些特定、常见的站点隐藏的页面并发现一些文件路径信息泄露的安全隐患，并能深入的分析一些CGI的漏洞问题。

4.3.5 基于实践的风险管理及展示

单纯的漏洞扫描产品因没有与资产关联，只能扫描出漏洞并不能反映客户环境中资产的真实的风险状况。远程安全评估系统将资产、漏洞和威胁紧密结合，提供了图形化的资产管理方式，

并通过可量化的模型呈现，帮助用户对网络中存在的风险有一个整体、直观的认识，做到真正意义上的风险量化。

在每次安全评估之前，用户需要根据自己的业务系统确定需要进行评估的资产，并且划分资产的重要性。根据用户的资产及其重要性会自动在其内部对目标评估系统建立基于时间和基于风险等多种安全评估模型。在对目标完成评估之后，模型输出的结果数据不但有定性的趋势分析，而且有定量的风险分析，用户能够清楚地看到单个资产、整个网络的资产存在的风险，还能够看到网络中漏洞的分布情况、风险级别排名较高的资产、不同操作系统和不同应用漏洞分布等详细统计信息，用户能够很直观地了解自己网络安全状况。

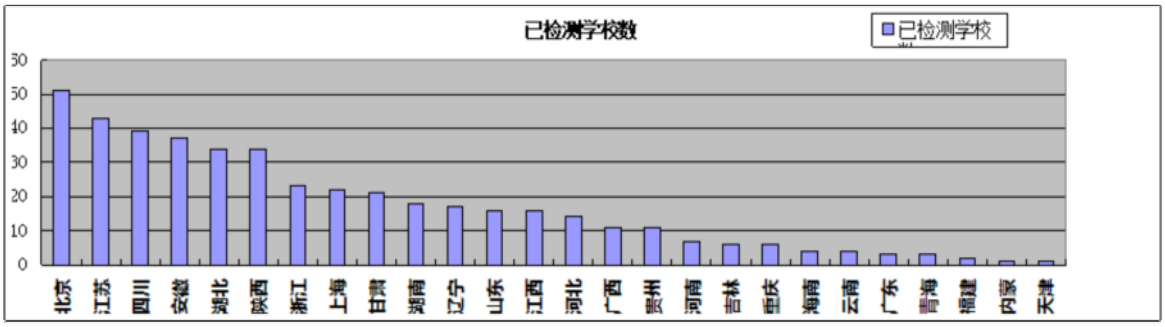
4.4 典型应用方式

用户只需要登录：www.nhcc.edu.cn 点击体检指南挂号，填写如下信息

用户名、所在省份、域名或 IP、联系人、联系电话、管理员邮箱

即可获得全面的网络信息安全检测服务，让您尽情享受赛尔网络体检中心的专业支持，并为您提供一份全面详实的安全检测报告。根据用户需求，我们将提供全面的治疗、紧急响应及培训服务。

已接受检测高校分布如下：



五. 结论

每年都有数以千计的网络安全漏洞被发现和公布，再加上攻击者手段的不断变化，用户的网络安全状况也随着被公布安全漏洞的增加而日益严峻。因此，安全评估对于绝大多数用户都是不容忽视的，用户必须比攻击者更早掌握自己网络安全漏洞并且做好适当的修补，才能够有效地预防入侵事件的发生。

事实证明，99%的攻击事件都是利用未修补的漏洞。许多已经部署防火墙、入侵检测系统和防病毒软件的企业仍然饱受漏洞入侵之苦，其中有更多受到蠕虫及其变种的破坏，造成巨大的经济损失。归根结底，其原因是用户缺乏一套完整的漏洞管理体系，未能落实定期评估与漏洞修补工作，忽视了漏洞的管理，最终漏洞成为攻击者实施攻击的有效途径，甚至成为蠕虫攻击的目标。

依托国内权威漏洞知识库及中国计算机教育科研网络、CCERT和北大信安中心，赛尔网络体检中心将以优质的安全检测服务，定期和持续地给用户提供可靠的安全评估和治疗服务，并且提供完整的漏洞管理机制，有效降低用户网络和主机风险，更大限度地保证用户网络和系统的安全性和稳定性。

联系方式：

北京市中关村东路 1 号院清华科技园科技大厦 B 座 8 层

信息技术部 宁雄雁

电话：01062603794/62603044

邮编：100084

公司网址：www.cernet.com

电子邮件：ningxy@cernet.com