Advances in Computer and Autonomous Intelligence Research
计算机与自主智能研究进展
第 2 卷◆第 4 期◆版本 1.0◆2024 年
文章类型：论文|刊号（ISSN）：2972-4236(P) / 2972-4244(O)

# 计算机软件安全漏洞检测技术的实际应用

万振华
深圳开源互联网安全技术有限公司
DOI:10.12238/acair.v2i4.10340

[摘　要] 在科技的持续发展和进步下,相对应的计算机软件安全漏洞检测技术也得到了有效的优化升级,目前计算机软件安全漏洞检测技术主要可以分为静态、动态、交互式三大类。计算机软件安全漏洞检测技术的应用在于能够通过格式化的方式处理安全漏洞以及竞争机制安全漏洞,并对缓冲区域的安全漏洞、随机安全漏洞进行检测和处理,对于信息安全而言至关重要。基于此,本文将对计算机软件安全漏洞检测技术的实际应用展开研究。
[关键词] 计算机软件；安全漏洞检测技术；应用方法；优化研究
中图分类号：P633.6　文献标识码：A

## The practical application of computer software security vulnerability detection technology

Zhenhua Wan
Shenzhen Kaiyuan Internet Security Technology Co., Ltd.

[Abstract] With the continuous development and progress of technology, corresponding computer software security vulnerability detection technologies have also been effectively optimized and upgraded. Currently, computer software security vulnerability detection technologies can be mainly divided into three categories: static, dynamic, and interactive. The design and application of computer software security vulnerability detection technology is to handle security vulnerabilities and competition mechanism security vulnerabilities through formatted methods, and to detect and handle security vulnerabilities in buffer areas and random security vulnerabilities, which is crucial for information security. Based on this, this article will conduct research on the practical application of computer software security vulnerability detection technology.
[Key words] computer software; Security vulnerability detection technology; Application methods; Optimization research

## 前言

计算机软件安全漏洞检测技术实现了对多种技术、方法的有机整合,能够做到对计算机软件的全面化系统化的安全评估,及时的发现安全漏洞并采取针对性的举措进行修复处理,以此避免被攻击者利用,造成信息安全威胁或其他损失[1]。在安全漏洞检测技术的应用下,网络安全、个人和企业的信息安全都能够得到良好的保障,在科技的加速发展下信息安全保护也更加重要[2]。由此可见,对计算机软件安全漏洞检测技术的实际应用进行探究具有较高的必要性,具体策略综述如下。

## 1 影响计算机安全的主要因素

1.1系统本身存在的安全隐患

系统本身存在的安全隐患有系统漏洞和外部移动存储设备。第一,系统漏洞。在对计算机软件普遍存在的安全隐患问题的综合化分析中发现,大部分计算机软件的安全隐患是由系统漏洞导致的[3]。而系统漏洞产生的原因则在于程序逻辑阶段存在着一定的疏忽问题,部分特殊情况并未被充分的考虑在内,进而导致漏洞的生成,致使系统运行过程中时序、同步等方面出现了明显的问题[4]。第二,外部移动存储设备。目前越来越多的计算机软件会采用外部移动存储设备,不仅具备便捷性的优势,还在操作上进行了优化,操作性大大提升,在实际生活中的应用范围也较为广泛。不过移动存储介质在保密机构的使用中缺乏可靠的安全检测机制,实名认证等方面也有所欠缺,极大的增加了信息安全管理的难度,为计算机网络的安全性带来了一定的隐患。

1.2系统外部的安全隐患

计算机软件系统外部的安全隐患主要包括计算机病毒、黑客入侵两个方面。第一,计算机病毒。计算机病毒的传播途径多种多样,如：硬盘、U盘、网络等都隶属其中,这些病毒往往具备潜伏性的特点,且传染性较强,容易造成计算机软件数据的丢失或系统的崩盘损坏,带来一系列的经济损失。随着互联网的不断

进步发展,相对应的计算机软件病毒也在更新迭代,稍有不慎就会带来较大的损失和威胁,不利于计算机网络的安全[5]。第二,黑客入侵。黑客是具备较为丰富的计算机技术和知识的群体,其能够做到熟练的应用各类软件,并通过编写各类程序恶意的侵入各类网站中,对网站的使用权限进行非法篡改,或对网站中的数据资料进行盗取,以及造成网站信息的缺失等,对于网络安全的威胁性极大。

1.3管理与维护中存在的安全隐患

管理与维护中存在的安全隐患有故意泄密、违规操作两个方面。第一,因违规操作而泄密。比如在对计算机软件信息的管理和维护中,工作人员将移动存储介质上的信息删除后通过技术将其复原,这也就属于违规操作行为,在此基础上将未完全清除数据的移动存储介质外借,这也就会导致计算机软件信息泄露的情况出现,威胁到计算机软件信息的安全。第二,故意泄密。故意泄密是指负责计算机软件系统维护和管理的工作人员,故意将网络安全机密外泄、破坏的行为。在计算机软件系统开发的过程中,团队中的工作人员很容易获取和掌控计算机软件系统的保密措施,进而更容易进入内部的界面利用口令、密钥得到计算机软件网络的内部窃取机密信息,并且还能够对机密信息进行修改、删除等操作,对于计算机软件安全来说威胁较大。

## 2 计算机软件中的安全漏洞检测技术

2.1静态安全漏洞检测技术

就计算机软件安全漏洞检测技术中的静态安全漏洞检测技术而言,其主要是由功能测试技术、代码验证技术、渗透测试技术三个部分沟通构成。在静态安全漏洞检测技术的应用下会先对软件的源程序、代码进行检测,而后从中提取出关键词对检测程序进行要点、特性方面的进一步检测分析,找出其中存在着的异常数据段,进行预防并做出相应的警示。静态安全漏洞检测技术具有快捷性的优势,实用效果相对较好,有利于计算机软件安全漏洞检测成本的控制,不过在精准性上静态安全漏洞检测技术还需要持续提升,目前无法保证十分的精确。

2.2动态安全漏洞检测技术

就计算机软件安全漏洞检测技术中的动态安全漏洞检测技术而言,其主要是采取对运行中的计算机软件的各项功能作用下的运行环境的改变,对软件运行结果进行分析,并将其和检测软件技术的预期的结果进行对比分析,以此确定差异性,判断计算机软件安全漏洞的存在。动态安全漏洞检测技术方法具备方便快捷、针对性强等一系列的优势,但同时也可能会因动态安全漏洞检测而导致软件运行过程中出现一些新的漏洞问题。

2.3交互式安全漏洞检测技术

通常指的是交互式应用程序安全测试(Interactive Application Security Testing,IAST)。这是一种在应用和API中自动化识别和诊断软件漏洞的技术,通过插桩技术收集安全信息,持续地从内部运行的代码中发现其安全及逻辑问题,并提供实时的报警展示。IAST技术通过插桩技术收集安全信息,直接从运行中的代码发现问题。它不是源代码扫描(SAST),也不是HTTP扫描(DAST)。IAST能够访问代码本身,在每行代码执行SAST；同时,IAST也能访问HTTP流量,在每一次请求和响应时执行类DAST的分析。因此,IAST的规则可以被看作是SAST和DAST的功能合集。IAST技术主要应用于软件开发和测试阶段,帮助企业在DevOps阶段解决漏洞问题。它可以自动化地分析应用和API中的自有代码以及开源库和框架的安全性,找出以前没有发现的漏洞,包括并不限于OWASP Top 10等复杂漏洞。目前市场上已有多种IAST产品可供选择,如开源网安的VulHunter等。这些产品通过使用插桩技术和流量代理,在研发测试阶段对运行时的应用及API进行漏洞实时检测。它们支持对软件漏洞进行全生命周期管理,实施多维度应用安全管控,具有“高覆盖、低误报、实时检测”等优点。

## 3 计算机软件中安全漏洞检测技术的应用

3.1处理格式化安全漏洞

在多种多样的计算机软件安全漏洞检测中,格式化漏洞是较为常见的一种类型。在计算机软件中格式化漏洞通常以字符的形式存在,容易导致计算机软件中保存的信息的丢失,且无法通过常规技术手段恢复。想要有效的解决计算机软件中的格式化漏洞问题,还需要以计算机软件的基础参数作为检测的着手点,利用计算机应用代码进行软件的初始格式计算,从而发现格式化漏洞问题并解决格式化漏洞问题,实现对计算机软件安全漏洞检测技术的有效应用。

3.2处理竞争机制安全漏洞

在计算机领域的持续进步和发展下,越来越多的计算机软件功能随之出现,这些软件聚集在一起往往会形成激烈的竞争关系,进而导致计算机软件程序遭到破坏,并且引发一定的安全漏洞问题的出现。这一部分的安全漏洞也被称之为竞争安全漏洞问题。针对因软件功能之间的相互竞争矛盾而导致的竞争安全漏洞,应当通过原子化的处理方式进行解决,对计算机软件的编码进行检测,从而有效的突出部分代码的特征和特性,对存在安全问题的部分进行锁定和进行进一步的检测。在应用计算机软件安全漏洞检测技术进行漏洞运行检测的过程中,代码原子化通常不会受到其他外界条件的干扰或影响,因此,通过性、通过效率都相对较高。

3.3处理缓冲区域安全漏洞

当计算机软件系统中出现了安全漏洞,则代表着计算机软件系统中原有的检测系统已经无法有效的检测软件漏洞问题。当出现此类问题时,技术工作人员需要针对计算机软件函数进行检测,并且在这一过程中还需将计算机软件系统升级到最高的安全版本,摒弃原本的无法有效检测计算机软件安全的旧版本,从而更好的对计算机软件系统缓冲区的漏洞进行防治,实现计算机软件安全漏洞检测技术的有效应用,达到保护计算机软件系统运行安全与可靠的目的。

3.4处理随机安全漏洞

当计算机软件系统运行时出现随机安全漏洞问题时,技术工作人员需要及时的对软件发生器的故障点进行锁定和进行针

对性的调整修复处理。而后，对随机安全漏洞问题进行进一步的预防检测，增强计算机软件运行防护的安全指数。就当下的相关研究成果分析可知，技术工作人员已经研发出了对于随机漏洞问题更具针对性的设备，此类专用设备能够第一时间发现随机漏洞的存在，以及检测到其对计算机软件所发起的恶意攻击，通过专业设备及时的发出干扰信号切断恶意攻击指令，从而实现对计算机软件系统运行安全的有效保护，避免信息泄露或故障问题的出现。

## 4 保护计算机网络安全的应对措施

想要实现对计算机网络安全的有效保护，就必须要积极的落实针对性的应对措施。经过分析与整合，以下将从在先进技术层面的应对策略、在硬件设备方面的应对策略、在管理层面的应对策略方面着手对此展开几点研究：

第一，在先进技术层面的应对策略。这一部分包含了入侵检测技术、漏洞扫描技术两个部分。首先，入侵检查技术。其主要是指针对计算机软件系统中的信息进行检测的程序，入侵检查技术应用的目的在于保护计算机软件系统运行的安全。在入侵检查技术应用下的计算机软件程序启动后，能够快速且准确的发现入侵程序的存在，并对该入侵程序进行安全检测，如果发现任何不稳定或不安全的因素会立即报告，并且对于入侵行为进行针对性的打击拦截，切断入侵对象的进入通道，有效的避免了病毒等对计算机软件系统运行安全的威胁。其次，漏洞扫描技术。其能够实现对计算机软件系统本身以及其他网络设备的有效扫描，全方位的找出存在安全隐患的部分，以此维护计算机软件的安全。在计算机软件系统中都或多或少的存在着一定的漏洞，通过漏洞扫描技术能够更好的锁定这些漏洞，并对系统的安全指数进行评估，根据最终的评估结果反馈来判断计算机软件系统的安全状况，从而更好的制定针对性的策略进行安全指数的提升。

第二，在硬件设备方面的应对策略。移动硬件设备强化是提高计算机网络安全的重要路径，除了要进行加密处理之外，加强对移动硬件设备的管理也至关重要。当今时代背景下，更多的企业和单位选择使用移动存储设备安全管理平台，能够通过平台实现远程访问和信息的保护加固，并且此类平台具备实名认证等一系列的保护手段，能够更好的保证移动存储介质的安全性，并且具备便捷性和一体化的优势，能够有效的防止资料外泄。因此，想要增强内部资料的安全，还需加强对移动存储设备安全管理平台的应用。

第三，在管理层面的应对策略。在实际的计算机软件系统维护和管理中，需要通过人力来完成部分工作，在其中存在着一定的人为操作失误的几率，以及存在着人为故意损坏的情况。这些问题很难从根本上避免。目前，行之有效的措施是对计算机网络安全管理体系进行进一步的完善，推动计算机软件系统安全性能方面的优化提升，以此尽可能的减少管理层方面的安全隐患，确保个人、社会、以及国家信息能够得到良好的安全保护。除此之外，对于个人操作方面的培训也应当积极的加强，并建立起针对性的责任制度，将责任划分到个人，从而进一步降低故意损坏等行为的出现几率，让计算机网络安全能够得到更大的保证，能够发挥更大的效果，得到广泛的认可，创造出更多的优良成果。

## 5 结语

综上所述，计算机软件安全漏洞检测技术的应用能够有效的提高用户信息安全指数，为软件安全提供更加坚实可靠的保障。因此，必须要对计算机软件安全漏洞检测技术的实际应用起到高度的重视，加强对安全漏洞检测技术的优化研究，不断的提高安全防护水平，更好的维护用户权益，创造出更多的良性成果。

## [参考文献]

[1]李寅杰.计算机软件中安全漏洞检测技术研究[J].软件,2023,44(07):108-111.

[2]曹道通.计算机软件中安全漏洞检测技术与应用分析[J].软件,2022,43(09):180-182.

[3]李世庆.计算机软件安全检测技术探讨[J].信息技术与信息化,2021,(05):172-173.

[4]李云.安全漏洞检测技术在计算机软件中的应用[J].无线互联科技,2021,18(09):76-77.

[5]张睿腾.刍议计算机软件安全漏洞检测技术[J].电子测试,2021,(06):123-124.

## 作者简介：

万振华(1983--),男,汉族,武汉人,本科,助理工程师,研究方向：专注于软件安全领域的技术研究,包括应用安全技术、软件供应链安全技术的研究,对软件安全开发生命周期(S-SDLC)全链有深厚经验。