论网站信息管理存在安全问题及防御措施

闫亚琦

（吉林省科学技术协会信息中心，吉林　长春　130021）

摘　要：随着信息技术的飞速发展，人类对电脑的依赖性日益增强，尽管计算机网站技术为人类的日常生活提供了极大的便利，但它也有一些缺点。随着网站技术的普及，网站安全问题越来越突出。鉴于此，本文首先分析影响网站信息管理的主要因素，其次论述网络信息安全存在的问题，最后提出网站安全管理的相应策略。

关键词：网站信息管理　安全问题　防御措施

中图分类号：TN948.61　　**文献标识码：**A　　**文章编号：**1003-9082（2023）01-0007-03

随着计算机网站技术的飞速发展，因特网进行信息发布、获取信息的方式日益融入人们的日常生活和工作中。然而，网站的安全问题却时时受到威胁，网站安全的管理迫在眉睫。网站安全由通信技术、网站技术、计算机软件、硬件设计、密码学、网站安全技术等多学科综合。网站安全袭击使人们不得不对新的防御手段进行研究，新的防御手段会引来新的攻击者，如此周而复始，网站安全技术在双方的斗争中逐渐完善和发展。

一、影响网站信息管理的主要因素

网站安全是通过技术手段对网站进行有效的管理与控制，因此，在一个站点环境下，可以有效地保证信息和数据的机密性、完整性和易用性。它的主要目的是保证通过该站点传递的信息始终不会增加、改变、丢失或被其他用户非法阅读。要实现这一目标，就需要确保网站系统软件和数据库系统具有一定的安全防护能力，并且确保诸如终端、数据链路等站点部件的功能不会改变，只有被授权的用户才能使用。因此，从某种程度上来说，网站的安全问题实际上就是网站的安全漏洞，它的缺陷主要来源于以下几个方面。

1.自然因素

1.1软件漏洞。即使是最完善的软件和应用程序，也不可能百分百的没有漏洞。而正是这种漏洞，成为非法用户、黑客窃取秘密和恶意攻击的方式。针对内部安全缺陷的攻击，主要包括：

1.1.1协议漏洞。比如，IMAP和POP3必须在Unix的根目录下执行，攻击者可以通过这个弱点来攻击IMAP，使其无法访问到系统的根目录。

1.1.2缓冲区溢出。许多系统可以接收任意长度的数据，而不用检查程序和缓冲的改变，将溢出的部分放置到堆叠中，而系统仍然能够正常地执行指令。

攻击者会使用这个弱点来发出命令，这些命令的长度超过了缓冲的能力，导致系统的不稳定。

1.1.3口令攻击。比如Unix系统的软件经常会将密码存储在一个可以被复制或者密码破解的文件里。所以，如果系统没有及时的升级，很可能会遭到攻击。

1.2病毒攻击。电脑病毒的主要危害是：对电脑的数据和信息产生直接的损害，使使用者遭受巨大的损害：对系统资源的消耗和运行速度的降低：产生其他未预料到的危险：使使用者承受巨大的精神压力。电脑病毒一般有四种类型：①文件类型的病毒；②引导病毒（系统启动系统）；③链病毒；④宏病毒。

2.人为因素

2.1操作失误。由于操作人员的安全意识不强，安全配置不合理，用户口令的选择不正确，账号的任意外借、与他人分享，这些安全隐患都会危及网站的安全。但在建立了网站管理系统和员工培训后，这种现象逐步消失，不再是对网站安全的主要威胁[1]。

2.2黑客攻击。这是目前电脑网络所面对的最大威胁，其中包括敌方电脑的攻击及电脑犯罪。这种攻击有两种类型：一类是主动攻击，通过多种途径选择性地摧毁信息的正确性和完整性；第二种是被动式攻击，即通过截取、窃取、破译来获取关键的保密信息，而不会对网站的正常运行造成干扰。

2.3用户输入验证不够全面。在网站设计中，一定要对使用者和使用者的输入持怀疑的态度，而不是绝对的信赖。因此，不能简单地使用使用者的信息，而要进行严格的验证。判断使用者的输入是否符合输入规则，以便输入资料库。使用者输入确认应包含下列内容：

2.3.1输入信息长度验证。程序员倾向于相信普通的使用者不会刻意地把输入拖得太长，而且不做输入确认也不会

造成伤害。但是，当使用者输入了数万亿的数据时，如果程序没有校验长度，就会导致程序的校验错误，或者使用了很多的变量，导致内存溢出，致使服务器服务中断，或者是关闭。.

2.3.2输入信息敏感字符检查。程序员在设计软件时，很有可能会注意到 JavaScript中的一些敏感的字符，比如在设计消息时，会把诸如“<”之类的信息过滤掉，这样就不会给用户带来网页炸弹了。但是，要特别关注的是，对留言板的内容进行筛选。二是筛选用户姓名。在编程过程中，用户名的校验通常仅限于校验长度，而不能校验JavaScript和HTML标签，因此很容易产生缺陷。三是邮件信息的核实，邮件中的邮件通常也只是确认是否包含了“@”，其余的都没有，这就造成了两个缺陷：内存溢出漏洞，输入信息太多；包含诸如JavaScript之类的文字信息，在显示用户邮件时会产生网页爆炸等。四是对检索资料进行确认。虽然不能将搜索结果直接存储在网站上，但这些信息都和数据库、服务器的文件有着千丝万缕的联系，一旦出现了问题，很可能会泄露出一些不该被发现的数据。如果使用者对程式有一定的认识，可以设定特定的搜寻资讯，以撷取不该搜寻的资料库，如使用者账号密码表等。所以，通常要确认一些常用的数据库操作语句，比如搜索信息中是否包含“Select”之类的，以限制用户的输入，防止信息泄漏[2]。

二、网络信息安全存在的问题

网络的安全隐患主要是利用网络自身的安全漏洞，而网络使用、管理过程中的不正当行为，会使网络的安全问题更加严重。目前存在着许多问题，其中技术问题、管理问题和人为问题。

1.技术问题

在技术方面，主要有3种类型的安全问题：硬件系统安全、软件系统安全、系统安全配置不合理等。

1.1硬件系统的安全缺陷。由于技术和理论上的限制，电脑和硬件设备都有一定的缺陷，从而在实际应用中出现了各种安全隐患。

1.2软件系统的安全漏洞，在软件开发过程中，为了方便地对所使用的系统软件、应用软件进行不断地改进和完善，而在软件开发过程中，经常会有“后门”来进行软件的升级和修改，而这些“后门”一旦被黑客利用，就会对系统的安全造成威胁。同时，在软件开发中，由于结构设计上的不足，或者程序编制上的不规范，也容易造成安全漏洞。

1.3系统安全配置不当造成的其他安全漏洞。一般情况下，系统中会有一个缺省的组态，而且缺省组态的安全性一般会比较低。另外，由于网络组态过程中的一些问题，如匿名FTP、Telnet的开放、密码文件的安全保护、命令的不合理使用等，都会造成安全上的安全隐患。黑客可以通过这些弱点进行攻击，从而破坏网络的安全[3]。

2.管理问题

管理上的问题，主要是由于网络的管理上的缺陷。通常，许多组织在设计内部网络时，都会把注意力集中在外部的威胁上，由于没有考虑到来自内部的攻击，造成了内部网络中缺少稽核追踪机制，而网管人员对日志及其他信息的关注不够。此外，管理人员素质差、管理措施不健全、使用者的安全意识薄弱等因素也是造成网络安全问题的主要原因。安全问题的根本原因在于人类。以上所述的技术与管理问题，都可以归结为人的问题。网络安全问题按人类行为的不同可划分为人为故意错误和人为无意错误。人为的无意失误，这些问题主要是由于系统本身的错误，操作上的错误，或者是软件上的错误。其中，安全漏洞是由管理员的安全配置问题引起的，也是网络用户安全意识薄弱所导致的。预处理问题是指利用系统中的漏洞进行的攻击，或者是对实体设备造成的直接的损害。比如，该病毒能够攻破网络的安全防护，入侵到网络主机，从而导致网络的安全问题。

三、网站安全管理的相应策略

1.网站安全的管理

1.1使用防火墙。防火墙作为一种新型的网站安全技术，在整个网站的安全中占有举足轻重的位置，是当前应用最为广泛和高效的一种网站安全技术。

1.2与因特网接入处增设网站入侵检测系统。IDS是一种对网站的实时违反进行自动识别和响应的系统，它所处的位置是一个具有敏感数据的网站，或者是任何有危险的网站，能够识别、记录入侵或破坏的代码，查找网站违法行为和未经许可的网站接入，一旦被发现，系统就会按照系统的安全政策进行响应，包括实时报警、自动切断通信联系、以及用户定制的安全政策。

1.3病毒防御。纯粹的抗病毒，并非公司的终极目的。只有明确市场的需求，注重产品的使用与管理，将其融入系统的整体防御系统中，才能真正提高企业的信息安全。我们必须选择合适的技术，将各种技术有机地结合起来，以实现目标。

2.网站自身的安全管理

2.1网站服务器的安全管理。网站服务器的日常维护和管理工作主要有：更新网页服务器的内容，审计日志文

件，安装一些新的工具和软件，修改服务器的配置，以及服务器的安全检查。主要注意以下几点：

2.1.1网站的安全问题要从网站的结构设计入手。从网站的基本安全性出发，可以从网站的架构入手，首先，安装一个强有力的防火墙，能够有效地抵御外部入侵，其次，可以通过设置非法入侵监控系统，提高防火墙的性能，实现对网站进行实时拦截，并对数据包和内容进行分析。在受到入侵时，可以立即有效地中断服务。再一次，应该限制非法使用者进入网络，指定IP位址的客户可以存取局域网服务器，以阻止非法修改来自外部的网站服务器配置。

2.1.2解决网站安全问题应定期对网站服务器进行安全检查。由于该站点的服务器是开放的，每天都有数以千计的用户来浏览，因此，必须对服务器进行例行的安全审查，并采用漏洞扫描和IDS工具加强对服务器的安全管理与检查。此外，当新的安全漏洞不断涌现时，我们必须适时地对各种新的安全漏洞进行补丁，以防止服务器遭到攻击或其他异常状况。

2.1.3解决网站安全问题应定期进行必要的数据备份。一个网站的核心就是资料，一旦资料被毁，将会造成严重的后果。因此，在设定对应的权限时，应该制定一套正规的备用计划，并且，在网站升级的同时，也要随时修改备份计划。

2.2数据库安全管理。资料库的安全，就是要对资料库进行保护，避免因非法使用而导致的资料泄漏与损毁。为保障企业应用系统的后台数据安全，利用客户机/服务器的方式对后台数据库进行访问，为各种应用程序创建不同的业务流程和进程用户识别。后台资料库系统利用服务器处理来识别存取使用者的身份，以决定存取的存取。本文采用了以下几种方式和技术，对后台数据库进行存取控制。

2.2.1访问矩阵。访问矩阵是指在不同的数据对象中，由不同的主体（使用者或者使用者过程）可以进行的操作，而每个人都可以通过自己的权限访问这些数据。它使用body行、存取物件表、存取矩阵元素的矩阵。Informix提供二级许可：资料库许可和资料表许可，可以将选择和更新授权给资料表中的具体栏位。所以，我们在存取矩阵中定义一个精确到字段级别的存取控制。

2.2.3视图的使用。可以透过检视来指定使用者的资料使用范围，将使用者限制于表格中的具体栏位或资料表，而检视与基本资料表相同，也可作为授权单位。对于不同的使用者，在一个被授权的使用者的视图中，没有包含不可存取的保密资料，以增加系统的安全。

2.2.4数据验证码DAC。在后台资料库中几个关键资料表格，设定资料验证DAC栏位，该栏位是由银行金钥及相关关键字段值所产生。DAC字段的数值在不同的记录中也是不同的。若使用者在资料库内非法更改资料，则会造成DAC效能错误，增加资料之安全性。

2.3在程序编码中进行安全管理。

2.3.1避免恶意代码的入侵。首先要做的是确认输入，这样攻击者就不能插入脚本代码或者让缓冲区溢出；其次，编码所有的输出，包括输入，可阻止客户机以程式码的形式转换潜在的恶意程式码；第三个方法是采用一个接收参数的储存程序，避免资料库把SQL输入到一个可执行的陈述式中。同时使用具有最低权限的处理程序账户和仿真账户。当攻击者试图在应用程式的安全性环境中执行程式码时，可以减轻危险，并降低伤害。

2.3.2要防止会话劫持。首先，将个人cookie与认证cookie分开；其次，将认证cookie通过HTTPS连接进行传输；第三个不会在查询字串中传送使用者识别码，该使用者识别码表示已经经过认证。

作为一个网站的管理者，既要做好自己的网站，又要承担起维护和管理的职责，这就要求我们的管理者要时刻保持谦虚的态度，不断地关注着新的管理技术.和安全防护技术。针对现有的安全问题，要采取最快、最有效的办法，对尚未发生的安全问题进行预测，从而保证对网站的安全风险。

结语

综上所述，随着互联网时代的来临以及信息的普及，人们每天都要访问一些网站，因此，对互联网的管理和维护也变得更加重要。在实际工作中，网站管理中出现了许多问题，强调建设，忽视管理，这是一个很常见的问题。另外，为了保障网站的正常运作，我们需要对站点的管理员进行监控，并对其进行实时的修改和修改，以保证网站的安全和稳定。

参考文献

[1]王宇.论网站信息管理存在安全问题及防御措施[J].科学与财富,2020(5):54.

[2]罗鹏.论网站信息管理存在安全问题及防御措施[J].魅力中国,2021(7):544-545.

[3]续晓冬,李斌.网站信息管理系统功能完善与安全性探讨[J].企业文化(下旬刊),2013(9):189.

作者简介：闫亚琦（1988—）女，吉林省长春市人。研究生学历。研究方向：档案管理。