在线考试系统的安全漏洞及对策

总计：毕业论文 51 页
插　　图 0 幅
表　　格 0 表

指导教师：张长君
评 阅 人：
完成日期：2006 年 5 月 31 日

摘要

随着网络技术的飞速发展，现在很多国外的大学和社会其他部门都已经开设了远程教育，通过计算机网络实现异地教育和培训。现在，计算机硬件技术的发展已经达到了相当高的水平。但是，远程教育软件的开发目前还处于起步阶段，随着这项技术的不断深入发展，就要求有更好、更完善的软件系统应用到远程教育当中去，目前面向网络编程、数据库访问的多种技术中，比如 JSP、PHP、ASP 中，ASP 以其开发周期短、存取数据简单、运行速度快而成为众多 web 程序员的首选开发技术. 但由于开发手段的直观、快速和高效，也带来了一定的安全隐患。数据库是在线考试系统的基础，通常都保存着重要的信息。大多数教育部门和学校的电子数据都保存在各种数据库中，他们用这些数据库保存一些个人资料，比如学生成绩等。在线考试系统数据库服务器还掌握着敏感的数据，包括考试的时间和考题。数据完整性和合法存取会受到很多方面的安全威胁，包括密码策略、系统后门、数据库操作以及本身的安全方案。但是在线考试系统数据库通常没有象操作系统和网络这样在安全性上受到重视。安全对于在线考试系统更为重要，本文以目前基于 Web 的信息系统最常用的 ASP＋SQL Server 2000 为例，探讨在线考试系统中可能存在的安全隐患，并给出相应的建议。

关键词：ASP；SQL Server 2000；安全漏洞；对策

ABSTRACT

Flying technically along with the network to develop soon, the university of now a lot of abroad all have set up with the social other section the long range educates, passing the calculator network realizes foreign land education with train. Now, the technical development in hardware in calculator has come to a very high horizontal. But, the long range educate the development of the software to still be placed in the stage in start now, along with this technical continuously thorough development, will beg the better and more perfect software system apply to the long range the education center go to, face to now the network plait distance, database visit in various techniques, for example in the JSP, PHP, ASP, ASP with its development cycle short, access data simple, run - time velocity quick and become the head of numerous the member of web procedures chooses to develop the technique. but because of development the means keeps the view, fleetness with efficiently, also brought the certainly safe hidden trouble. The database is the foundation of the on-line examination system, usually all keeping the important information. Educate the section to keep with the electron data of the school all mostly in every kind of database, they keep the some personal data with these databases, for example student score etc. The on-line examination system database server still controls the impressionable data, including the time of the examination with the subject of examination. The data integrity access and would suffer with the legality very in many ways of the safety threatens, including the password strategy, the back door of system, database the operation and oneself of safe project. But the wire examination system database usually has no elephant operate system to suffer to value on the safety like this with the network. The on-line examination system for safety is more important, this text with current according to Web the most in common use ASP in system in information+ SQL Server 2000 for a safe hidden trouble for, inquiring into on-line examination system inside possible to be existence, and give the homologous suggestion.

Key words: ASP; SQL Server 2000; Security Hole; Countermeasure

目录

1.绪论

1.1 本文研究的目的和意义

随着互联网的高速发展，网络的安全问题日益凸现，尤其是近年来出现的在线考试，也由于与互联网密不可分的关系，经常受到安全威胁。尤其以基于ASP＋SQL Server 2000 的在线考试系统的安全问题最为突出，因此研究在线考试系统的安全问题是十分必要的。本文就以基于 ASP＋SQL Server 2000 的在线考试系统的安全问题作为研究对象。通过对ASP 和 SQL Server 2000 安全漏洞的对策的分析与研究，找出的在线考试系统的安全问题的解决方法。

1.2 文献综述

1.2.1ASP 简述

Microsoft Active Server Pages（ASP）是多数在线考试系统服务器端脚本编写环境，使用它可以创建和运行动态、交互的 Web 服务器应用程序。使用 ASP 可以组合 HTML 页 、脚本命令和 ActiveX 组件以创建交互的 Web 页和基于 Web 的功能强大的应用程序。现在很多在线考试方面的网站，在前台上大都用 ASP 来实现。ActiveServerPage 技术为应用开发商提供了基于脚本的直观、快速、高效的应用开发手段，极大地提高了开发的效果。在讨论 ASP 的安全性问题之前，让我们来看看 ASP 是怎么工作的。ASP 脚本是采用明文（plain

text）方式来编写的。ASP 脚本是一系列按特定语法（目前支持 vbscript 和 jscript 两种脚本语言）编写的，与标准 HTML 页面混合在一起的脚本所构成的文本格式的文件。当客户端的最终用户用 WEB 浏览器通过 INTERNET 来访问基于 ASP 脚本的应用时，WEB 浏览器将向 WEB 服务器发出 HTTP 请求。WEB 服务器分析、判断出该请求是 ASP 脚本的应用后，自动通过 ISAPI 接口调用 ASP 脚本的解释运行引擎（ASP.DLL）。ASP.DLL 将从文件系统或内部缓冲区获取指定的 ASP 脚本文件，接着就进行语法分析并解释执行。最终的处理结果将形成 HTML 格式的内容，通过 WEB 服务器"原路"返回给 WEB 浏览器，由 WEB 浏览器在客户端形成最终的结果呈现。这样就完成了一次完整的 ASP 脚本调用。若干个有机的 ASP 脚本调用就组成了一个完整的 ASP 脚本应用。

让我们来看看运行 ASP 所需的环境：

Microsoft Internet Information Server 3.0/4.0/5.0 on NT Server/Linux

Microsoft Internet Information Server 3.0/4.0/5.0 on Win2000/Win2003

Microsoft Personal Web Server on Windows 95/98

WINDOWS 网络操作系统所带的 MicrosoftIIS 提供了强大的功能，但是 IIS 在网络安全方面却是比较危险的。

1.2.2SQL Server 2000 简述

微软的 SQL Server 是一种广泛使用的数据库，很多在线考试系统平台等都是基于 SQL Server 上的，但是在线考试系统数据库的安全性还没有被人们更系统的安全性等同起来，多数管理员认为只要把网络和操作系统的安全搞好了，那么所有的应用程序也就安全了。大多数系统管理员对在线考试系统数据库不熟悉而数据库管理员有对安全问题关心太少，而且一些安全公司也忽略在线考试系统数据库安全，这就使数据库的安全问题更加严峻了。在线考试系统系统中存在的安全漏洞和不当的配置通常会造成严重的后果，而且都难以发现。数据库应用程序通常同操作系统的最高管理员密切相关。广泛 SQL Server 数据库又是属于“端口”型的数据库，这就表示任何人都能够用分析工具试图连接到在线考试系统数据库上，从而绕过操作系统的安全机制，进而闯入系统、破坏和窃取考试资料，甚至破坏整个系统。

2.ASP 漏洞分析和解决方法

ASP 是开发在线考试系统网站应用的快速工具，但是有些网站管理员只看到 ASP 的快速开发能力，却忽视了 ASP 安全问题。ASP 从一开始就一直受到众多漏洞，后门的困扰，包括%81 的噩梦，密码验证问题，IIS 漏洞等等都一直使 ASP 网站开发人员心惊胆跳。本部分试图从开放了 ASP 服务的操作系统漏洞和 ASP 程序本身漏洞，阐述 ASP 安全问题，并给出解决方法。

2.1 在 ASP 程序后加个特殊符号，能看到 ASP 源程序

受影响的版本：

win95+pws 、IIS3.0

98+pws4 不存在这个漏洞

IIS4.0 以上的版本也不存在这个漏洞

问题描述：

这些特殊符号包括小数点，%81，：：$DATA。比如：

http：//someurl/somepage.asp.

http：// someurl/somepage.asp%81

http：// someurl/somepage.asp：：$DATA

http：// someurl/somepage.asp %2e

http：// someurl/somepage %2e%41sp

http：// someurl/somepage%2e%asp

http：// someurl/somepage.asp %2e

http://someurl/msadc/samples/selector/showcode.asp?source=/msadc/samples/../../../../../../boot.ini （可以看到 boot.ini 的文件内容）

那么在安装有 IIS3.0 和 win95+PWS 的浏览中就很容易看到 somepage.asp 的源程序。究竟是什么原因造成了这种可怕的漏洞呢？究其根源其实是 Windows NT 特有的文件系统在做怪。有一点常识的人都知道在 NT 提供了一种完全不同于 FAT 的文件系统：NTFS，这种被称之为新技术文件系统的技术使得 NT 具有了较高的安全机制，但也正是因为它而产生了不少令人头痛的隐患。大家可能不知道， NTFS 支持包含在一个文件中

的多数据流，而这个包含了所有内容的主数据流被称之为"DATA"，因此使得在浏览器 里直接访问 NTFS 系统的这个特性而轻易的捕获在文件中的脚本程序成为了可能。然而 直接导致 ：：$DATA 的原因是由于 IIS 在解析文件名的时候出了问题，它没有很好地规范文件名。

解决方法：

如果是 WinodwsNT 用户，安装 IIS4.0 或者 IIS5.0，Windows2000 不存在这个问题。如果是 win95 用户，安装 WIN98 和 PWS4.0。[1]

2.2ACCESS 数据库有可能被下载的漏洞

问题描述：

在用 ACCESS 做后台数据库时，如果有人通过各种方法知道或者猜到了服务器的 ACCESS 数据库的路径和数据库名称，那么他能够下载这个 ACCESS 数据库文件，这是非常危险的。比如：如果你的 ACCESS 数据库 book.mdb 放在虚拟目录下的 database 目录下，那么有人在浏览器中打入：http：//someurl/database/book.mdb，

如果你的 book.mdb 数据库没有事先加密的话，那 book.mdb 中所有重要的数据都掌握在别人的手中。

解决方法：

(1)为你的数据库文件名称起个复杂的非常规的名字，并把他放在几目录下。

所谓"非常规"，打个比方：比如有个数据库要保存的是有关书籍的信息，可不要把他起个"book.mdb"的名字，起个怪怪的名称，比如 d34ksfslf.mdb，再把他放在如./kdslf/i44/studi/ 的几层目录下，这样黑客要想通过猜的方式得到你的 ACCESS 数据库文件就难上加难了。

(2)不要把数据库名写在程序中

有些人喜欢把 DSN 写在程序中，比如：

```
DBPath = Server.MapPath("cmddb.mdb")
conn.Open "driver={Microsoft Access Driver (*.mdb)};dbq=" & DBPath
```

假如万一给人拿到了源程序，ACCESS 数据库的名字就一览无余。因此使用 ODBC 里设置数据源，再在程序中这样写：

```
conn.open "shujiyuan"
```

(3)使用 ACCESS 来为数据库文件编码及加密

首先在选取"工具->安全->加密/解密数据库，选取数据库（如：employer.mdb)，然后接确定，接着会出现"数据库加密后另存为"的窗口，存为：employer1.mdb。接着 employer.mdb 就会被编码，然后存为 employer1.mdb.。要注意的是，以上的动作并不是对数据库设置密码，而只是对数据库文件加以编码，目的是为了防止他人使用别的工具来查看数据库文件的内容。接下来我们为数据库加密，首先以打开经过编码了的 employer1.mdb，在打开时，选择"独占"方式。然后选取功能表的"工具->安全->设置数据库密码"，接着输入密码即可。为 employer1.mdb 设置密码之后，接下来如果再使用 ACCEES 数据库文件时，则 ACCESS 会先要求输入密码，验证正确后才能够启动数据库。不过要在 ASP 程序中的 connection 对象的 open 方法中增加 PWD 的参数即可，例如：

```
param="driver={Microsoft Access Driver (*.mdb)};Pwd=yfdsfs"
param=param&";dbq="&server.mappath("employer1.mdb")
conn.open param
```

这样即使他人得到了 employer1.mdb 文件，没有密码他是无法看到 employer1.mdb 的。[2]

2.3code.asp 文件会泄漏 ASP 代码

问题描述：

举个很简单的例子，在微软提供的 ASP1.0 的例程里有一个 .asp 文件专门用来查看其它 .asp 文件的源代码，该文件为 ASPSamp/Samples/code.asp。如果有人把这个程序上传到服务器，而服务器端没有任何防范措施的话，他就可以很容易地查看他人的程序。例如：code.asp?source=/directory/file.asp，不过这是个比较旧的漏洞了，相信现在很少会出现这种漏洞。下面这命令是比较新的：

http://someurl/iissamples/exair/howitworks/code.asp?/lunwen/soushuo.asp=xxx.asp。

最大的危害莫过于 asp 文件可以被上述方式读出；数据库密码以明文形式暴露在黑客眼前。

问题解决：

对于 IIS 自带的 showasp code 的 asp 程序文件，删除该文件或者禁止访问该目录即可。[3]

2.4file system object 组件篡改下载 fat 分区上的任何文件的漏洞

问题描述：

IIS3、 IIS4 的 ASP 的文件操作都可以通过 file system object 实现，包括文本文件的读写目录操作、文件的拷贝改名删除等，但是这个强大的功能也留下了非常危险的 "后门"。利用 file system objet 可以篡改下载 fat 分区上的任何文件。即使是 ntfs 分区，如果权限没有设定好的话，同样也能破坏，一不小心你就可能遭受"灭顶之灾 "。遗憾的是很多网络管理人员只知道让 web 服务器运行起来，很少对 ntfs 进行权限 设置，而 NT 目录权限的默认设置偏偏安全性又低得可怕。

问题解决：

作为考试系统的管理人员必须密切关注服务器的设置，尽量将 web 目录建在 ntfs 分区上，目录不要设定 everyone full control，即使是是管理员组的成员一般也没什么必要 full control，只要有读取、更改权限就足够了。也可以把 file system object 的组件删除或者改名。[4]

2.5 输入标准的 HTML 语句或者 javascript 语句会改变输出结果

问题描述：

在输入框中打入标准的 HTML 语句会得到什么相的结果呢？比如一个留言本，我们留言内容中打入：

你好！

如果你的 ASP 程序中没有屏蔽 html 语句，那么就会改变"你好"字体的大小。在留言本中改变字体大小和贴图有时并不是什么坏事，反而可以使留言本生动。但是如果在输入框中写个 javascript 的死循环，比如：

特大新闻 ，那么其他查看该留言的客人只要移动鼠标到"特大新闻"，上就会使用户的浏览器因死循环而死掉。

解决方法：

编写类似程序时应该做好对此类操作的防范，譬如可以写一段程序判断客户端的输入，并屏蔽掉所有的 HTML、 javascript 语句。[5]

2.6ASP 程序密码验证漏洞

漏洞描述：

很多在线考试系统把密码放到数据库中，在登陆验证中用以下 sql,(以 asp 为例)

sql="select * from user where username='"&username&"'and pass='"& pass &'" 此时，您只要根据 sql 构造一个特殊的用户名和密码，如: ben' or '1'='1 就可以进入本来你没有特权的页面。再来看看上面那个语句吧：

sql="select * from user where username='"&username&"'and pass='"& pass&'" 此时，您只要根据 sql 构造一个特殊的用户名和密码，如：ben' or '1'='1

这样,程序将会变成这样：

sql="select*from username where username="&ben'or'1'=1&"and pass="&pass&" or 是一个逻辑运算符,作用是在判断两个条件的时候,只要其中一个条件成立,那么等式将会成立.而在语言中,是以 1 来代表真的(成立).那么在这行语句中,原语句的"and"验证将不再继续,而因为"1=1"和"or"令语句返回为真值.。另外我们也可以构造以下的用户名：

username='aa' or username<>'aa', pass='aa' or pass<>'aa'

相应的在浏览器端的用户名框内写入：

aa' or username<>'aa

口令框内写入：

aa' or pass<>'aa,

注意这两个字符串两头是没有'的。这样就可以成功的骗过系统而进入。后一种方法理论虽然如此，但要实践是非常困难的，下面两个条件都必须具备：

（1）首先要能够准确的知道系统在表中是用哪两个字段存储用户名和口令的，只有这样才能准确的构造出这个进攻性的字符串。实际上这是很难猜中的。

（2）系统对输入的字符串不进行有效性检查。

问题解决： 对输入的内容验证和"'"号的处理。[6]

2.7INDEX SERVER 服务会漏洞 ASP 源程序

问题描述：

在运行 IIS4 或者 IIS5 的 Index Server，输入特殊的字符格式可以看到 ASP 源程序或者其它页面的程序。甚至以及添打了最近关于参看源代码的补丁程序的系统，或者没有.htw 文件的系统，一样存在该问题。获得 asp 程序，甚至 global.asa 文件的源代码,无疑对考试系统是一个非常重大的安全隐患。往往这些代码中包含了用户密码和 ID，以及数据库的源路径和名称等等。这对于攻击者收集系统信息，进行下一步的入侵都是非常重要的。通过构建下面的特殊程序可以参看该程序源代码：

http://202.116.26.38/null.htw?CiWebHitsFile=/default.asp&CiRestriction=none&CiHiliteType=Full

这样只是返回一些 html 格式的文件代码，但是当你添加%20 到 CiWebHitsFile 的参数后面，如下：

http://someurl/null.htw?CiWebHitsFile=/default.asp%20&CiRestriction=none&CiHiliteType=Full

这将获得该程序的源代码。

（注意：/default.asp 是以 web 的根开始计算。如某站点的

http：//welcome/welcome.asp

那么对应就是：

http://someurl/null.htw?CiWebHitsFile=/welcome/welcome.asp%20&CiRestriction=none&CiHiliteType=Full)

由于'null.htw'文件并非真正的系统映射文件，所以只是一个储存在系统内存中的虚拟文件。哪怕你已经从你的系统中删除了所有的真实的.htw 文件，但是由于对 null.htw 文件的请求默认是由 webhits.dll 来处理。所以，IIS 仍然受到该漏洞的威胁。

问题解决：

如果该 webhits 提供的功能是系统必须的，请到

http://www.microsoft.com/downloads/search.aspx?displaylang=zh-cn（微软中国下载中心）下载相应的补丁程序。如果没必要，请用 IIS 的 MMC 管理工具简单移除.htw 的映象文件。[7]

2.8 存在后门允许用户查看 ASP 文件源程序和下载整个网站

问题描述：

随 IIS 和 Frontpage Extention server 而来的动态库程序存在后门，允许用户远程读取 asp、asa 和 CGI 程序的源代码。但这个动态库要求有密码，这个后门的密码是： "Netscape engineers are weenies!"

程序路径为：

/_vti_bin/_vti_aut/dvwssr.dll

一般安装了 Frontpage98 的 IIS 服务器都有这个路径和文件。这个程序要求解码后才能发挥读取 asp 等源程序，有趣的是，这个密码正是嘲弄其竞争对手 Netscape 的。现提供一个有该漏洞的国外网站给安全技术人员参考：

http：//62.236.90.195

关于读取源程序，请下载这个测试程序，用法为：

[john@Linux john]$ ./dvwssr1.pl 62.236.90.195 /cqsdoc/showcode.asp

测试程序：

http：//www.cnns.net/exploits/nt/dvwssr1.pl[8]

2.9IIS4.0 受 HTTP 的 D.O.S 攻击漏洞

问题描述：

受影响的版本：IIS 4.0 以及更早的版本

这是一个很简单的方法.发送很多的

"Host：aaaaa...aa"到 IIS：

GET / HTTP/1.1

Host： aaaaaaaaaaaaaaaaaaaaaa....(200 bytes)

Host： aaaaaaaaaaaaaaaaaaaaaa....(200 bytes)

...10,000 lines

Host： aaaaaaaaaaaaaaaaaaaaaa....(200 bytes)

发送了象上面所写的两次请求后，对方的 IIS 在接受了这些请求后就会导致内存溢出.当然，它就不能对更多的请求作出反应。因为对方正缺乏虚拟内存，服务器也将停止运行。事后，对方不能通过重起 webservice 来解决问题，而必须重启服务器。[9]

2.10IIS5.0 超长 URL 拒绝服务漏洞

问题描述：

Microsoft IIS 5.0 在处理以".ida"为扩展名的 URL 请求时，它会有两种结果。一个可能的结果是服务器回复"URL String too long"的信息；或类似"Cannot find the specified path" 的信息。另一种可能就是服务器端服务停止，并返回"Access Violation"信息(即成功的实现了对服务器端的拒绝服务攻击)当远端攻击者发出类似如下的请求时：

http：//someurl/...[25kb of '.']...ida

服务器端会崩溃(导致拒绝服务攻击)或返回该文件不在当前路径的信息(暴露文件物理地址)

问题解决：

大多数情况下，站点很少使用扩展名为".ida"和".idq"的文件，可在 ISAPI 脚本映射中，将扩展名为".ida"和".idq"的应用程序映射删除。[10]

2.11 请求不存在的 idq 或 ida 文件会暴露服务器的物理地址

问题描述：

通过请求一个不存在的扩展名为 idq 或 ida 得文件，IIS 会暴露文件在服务器上得物理地址.这样会给攻击者提供了不必要的信息，而且，这对攻击一个 Web 站点来说，是很有价值的第一步。

测试程序： 通过请求如：http：//someurl/anything.ida

http：//someurl/lunwen/anything.ida

或：

http：//someurl/anything.idq

一个远端用户可以收到类似：

'The IDQ d：\http\anything.idq could not be found'

的响应。这样的一个响应就会让攻击者获得了 Web 站点的物理路径，并且还可以获得更多的有关该站点在服务器上的组织与结构。[11]

2.12NT Index Server 存在返回上级目录的漏洞

受影响的版本：Microsoft Index Server2.0 [WinNT4.0,WinNT 2000.0]

Index Sserver2.0 是 WinNT4.0 Option Pack 中附带的一个软件的工具,其中的功能已经被 WinNT 2000 中的 Indexing Services 所包含。当与 IIS 结合使用时,Index Server 和 Indexing Services 便可以在最初的环境来浏览 Web Search 的结果,它将生成一个 HTML 文件,其中包含了查找后所返回页面内容的简短引用,并将其连接至所返回的页面[即符合查询内容的页面],也就是超级连接。要做到这一点,它便需要支持由 webhits.dll ISAPI 程序处理的.htw 文件类型。这个 dll 允许在一个模版中使用"../"用做返回上级目录的字符串.这样,了解服务器文件结构的攻击者便可以远程的阅读该机器上的任意文件了。

漏洞的利用：

(1)系统中存在.htw 文件

Index Server 提供的这种超级连接允许 Web 用户获得一个关于他搜寻结果的返回页,这个页面的名字是与 CiWebHitsFile 变量一起通过.htw 文件的,webhits.dll 这个 ISAPI 程序将处理这个请求,对其进行超级连接并返回该页面。因此用户便可以控制通过.htw 文件的 CiWebHits 变量,请求到任何所希望获得的信息。另外存在的一个问题便是 ASP 或其他脚本文件的源代码也可以利用该方法来获得。上面我们说过 webhits.dll 后接上"../"便可以访问到 Web 虚拟目录外的文件,下面我们来看个例子：

http：//somerul/iissamples/issamples/oop/qfullhit.dll?CiWebHitsFile=/../../winnt/system32/logfiles/w3svc1/ex000121.log&CiRestriction=none&CiHiliteType=Full 在浏览器中输入该地址,便可以获得该服务器上给定日期的 Web 日志文件.在系统常见的.htw 样本文件有：

/iissamples/issamples/oop/qfullhit.htw

/iissamples/issamples/oop/qsumrhit.htw

/iissamples/exair/search/qfullhit.htw

/iissamples/exair/search/qsumrhit.hw

/iishelp/iis/misc/iirturnh.htw

[这个文件通常受 loopback 限制]

(2)系统中不存在.htw 文件

调用一个 webhits.dll ISAPI 程序需要通过.htw 文件来完成,如果您的系统中不存在.htw 文件,虽然请求一个不存在的.htw 文件将失败,但是您的仍然存在可被利用的漏洞。其中的窍门便是利用 inetinfo.exe 来调用 webhits.dll,这样同样能访问到 Web 虚拟目录外的文件。但我们需要通过制作一个的特殊的 URL 来完成该漏洞的利用。首先我们需要一个有效的文件资源,这个文件必须是一个静态的文件,如".htm",".html",".txt"或者".gif",".jpg"。这些文件将用作模版来被 webhits.dll 打开。现在我们需要获得 inetinfo.exe 来利用 webhits.dll,唯一可以做到这点的便是请求一个.htw 文件:

http://url/default.htm.htw?CiWebHitsFile=/../../winnt/system32/logfiles/w3svc1/ex000121.log&CiRestriction=none&CiHiliteType=Full

很明显,这个请求肯定会失败,因为系统上不存在这个文件。但请注意,我们现在已经调用到了 webhits.dll,我们只要在一个存在的文件资源后面[也就是在.htw 前面]加上一串特殊的数字(%20s),[就是在例子中 default.htm 后面加上这个代表空格的特殊数字],这样我们便可以欺骗过 web 服务器从而达到我们的目的.由于在缓冲部分中.htw 文件名字部分被删除掉[由于%20s 这个符号],所以,当请求传送到 webhits.dll 的时候,便可以成功的打开该文件,并返回给客户端,而且过程中并不要求系统中真的存在.htw 文件。

问题解决:请到

http://www.microsoft.com/downloads/search.aspx?displaylang=zh-cn

(微软中国下载中心)下载相应的补丁程序。[12]

2.13 绕过验证直接进入 ASP 页面

漏洞描述:

如果用户知道了一个 ASP 页面的路径和文件名，而这个文件又是要经过验证才能进去的，但是用户直接输入这个 ASP 页面的文件名，就有可能通过绕过验证.比如：我在一些网站上这样试过：首先关闭所有的浏览器，窗口，输入：

http：//someurl/system_search.asp?page=1

就样就看到了只能系统员才能看到的页面。当然有些人为了防止这种情况也会在 system_search.asp 的开头加个判断，比如：判断 session("system_name"),如果不为空时就能进入，这样上面的 url 请求就不能直接进入管理员页面了。但是这种方法也有一个漏洞，如果攻击者先用一个合法的帐号，或者在本机上生成一个 session, 如 session("system_name")="admi"，那因为 session("system_name")不为空，这样也能直接进入绕过密码，直接进入管理员页面。

解决方法：

在需要验证的 ASP 页面开头处进行相应的处理。比如：可跟踪上一个页面的文件名，只有从上一页面转进来的会话才能读取这个页面。

2.14IIS4.0/5.0 特殊数据格式的 URL 请求远程 DOS 攻击

漏洞描述：

当在安装有有 IIS4.0 或者 IIS5.0 的 web 服务上,请求一个具有特殊数据格式的 URL,会拖慢受攻击 web 服务器的响应速度,或许会使其暂时停止响应。

受影响的版本:

Microsoft Internet Information Server 4.0

Microsoft Internet Information Server 5.0

漏洞测试程序如下：

http：//202.96.168.51/download/exploits/iisdos.exe

源代码如下：

http：//202.96.168.51/download/exploits/iisdos.zip

测试程序：只要打入：iisdos <***.***.**.**> 就能攻击对方 web 服务器

问题解决：请到

http://www.microsoft.com/downloads/search.aspx?displaylang=zh-cn

（微软中国下载中心）下载相应的补丁程序。

2.15IIS Web Server DOS

漏洞描述：

默认情况下，IIS 容易被拒绝服务攻击。如果注册表中有一个叫"MaxClientRequestBuffer"的键未被创建，针对这种 NT 系统的攻击通常能奏效。"MaxClientRequestBuffer"这个键用于设置 IIS 允许接受的输入量。如果"MaxClientRequestBuffer"设置为 256(bytes)，则攻击者通过输入大量的字符请求 IIS 将被限制在 256 字节以内。而系统的缺省设置对此不加限制，因此，可以很容易地对 IISserver 实行 DOS 攻击，攻击结果将导致 NT 系统的 CPU 占用率达到 100%

解决方案：

运行

Regedt32.exe 在：

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\w3svc\parameters

增加一个值：value Name： MaxClientRequestBuffer Data Type： REG_DWORD 设置为十进制，具体数值设置为你想设定的 IIS 允许接受的 URL 最大长度。CNNS 的设置为 256。

2.16MS ODBC 数据库连接溢出导致 NT/9x 拒绝服务攻击

引语：在线考试系统使用数据库时，应该使用 ODBC

漏洞描述：

Microsoft ODBC 数据库在连接和断开时可能存在潜在的溢出问题(Microsoft ACCESS 数据库相关)。如果不取消连接而直接和第二个数据库相连接，可能导致服务停止。

影响系统：

ODBC 版本： 3.510.3711.0

ODBC Access 驱动版本： 3.51.1029.00

OS 版本： Windows NT 4.0 Service Pack 5, IIS 4.0 (i386)

Microsoft Office 97 Professional (MSO97.dll： 8.0.0.3507)

漏洞检测方法如下：

ODBC 连接源名称： miscdb

ODBC 数据库型号： MS Access

ODBC 假设路径： d：\data\misc.mdb

ASP 代码如下：

```
<%
set connVB = server.createobject("ADODB.Connection")
connVB.open "DRIVER={Microsoft Access Driver (*.mdb)}; DSN=miscdb"
%>
<html>
<body>
...lots of html removed...
<!-- We Connect to DB1 -->
<%
set connGlobal = server.createobject("ADODB.Connection")
connGlobal.Open "DSN=miscdb;User=sa"
mSQL = "arb SQL Statement"
set rsGlobal = connGlobal.execute(mSQL)
While not rsGlobal.eof
Response.Write rsGlobal("resultfrommiscdb")
rsGlobal.movenext
wend
'rsGlobal.close
'set rsGlobal = nothing
'connGlobal.close
'set connGlobal = nothing
' Note we do NOT close the connection
%>
<!-- Call the same database by means of DBQ direct file access -->
```

```
<%
set connGlobal = server.createobject("ADODB.Connection")
connGlobal.Open "DRIVER={Microsoft Access Driver (*.mdb)};
DBQ=d: \data\misc.mdb"
mSQL = "arb SQL Statement"
set rsGlobal = connGlobal.execute(mSQL)
While not rsGlobal.eof
Response.Write rsGlobal("resultfrommiscdb")
rsGlobal.movenext
wend
rsGlobal.close
set rsGlobal = nothing
connGlobal.close
set connGlobal = nothing
' Note we DO close the connection
%>
```

在这种情况下，IIS 处理进程将会停顿，CPU 使用率由于 inetinfo.exe 进程将达到 100%。只有重新启动计算机才能恢复。

2.17ASP 主页.inc 文件泄露问题

受影响的版本：任何提供 ASP 服务的系统

远程：YES / 本地：YES

内容摘要：当存在 asp 的主页正在制作并没有进行最后调试完成以前，可以被某些搜索引擎机动追加为搜索对象，如果这时候有人利用搜索引擎对这些网页进行查找，会得到有关文件的定位，并能在浏览器中察看到数据库地点和结构的细节揭示完整的源代码。具体操作过程是：利用搜索引擎查找包含+"Microsoft VBScript 运行时刻错误执行搜索" +".inc ，" 的关键字，搜索引擎会自动查找包含 asp 的包含文件(.inc)并显示给用户，利用浏览器观看包含文件的源代码，其中可能会有某些敏感信息

解决方案：

(1)搜索引擎应该不索引有 asp 运行时刻错误的页

(2) 程序员应该在网页发布前对其进行彻底的调试

(3) 安全专家需要固定 asp 包含文件以便外部的用户不能看他们

asp 新闻组、站点提供两个解决方案对这个漏洞进行修正，首先对 .inc 文件内容进行加密，其次也可以使用 .asp 文件代替 .inc 文件使用户无法从浏览器直接观看文件的源代码。.inc 文件的文件名不用使用系统默认的或者有特殊含义容易被用户猜测到的，尽量使用无规则的英文字母。

2.18 利用 Activer server explorer 可对文件进行读写访问

漏洞描述：

chinaasp 的 Activerserverexplorer 可以很方便的对本地文件在线查看服务器上的目录在线查看文件的名称、大小、类型、修改时间,在线编辑纯文本文件，如.txt、.htm、.asp、.pl、.cgi 等等,直接执行服务器上的文件。Activer server explorer 要求填写相对路径或者绝对路径，但是假如：有一个攻击者把 Activer server explorer 上传到目标服务器上的某个目录，并且这个目录支持 ASP 的话，那么他就可以通过 Activer server explorer 修改、执行目标服务器上的文件。这种情况可以发生在一个攻击者拥有目标 NT 服务器上的一个可写目录帐号，并且这个目录又支持 ASP。比如一些支持 ASP 的个人免费主页服务器，把 Activer server explorer 先传上你申请的免费主页空间，再通过各种方法得到目标服务器的路径，(比如可通过漏洞：″请求不存在的扩展名为 idq 或 ida 文件，会暴露文件在服务器上的物理地址.″).或者直接在相对路径上填″.″，一般是默认。这样攻击者就能任意修改，执行目标服务器上的文件，不管他对这个文件有无读写访问权。所以那些提供有 ASP 服务的个人主页或者其它服务的服务器，就要加倍小心这种攻击了。

漏洞解决方法：

其实 Activer server explorer 就是利用了上面讲的漏洞 4 filesystemobject 组件篡改下载 fat 分区上的任何文件的漏洞。那么我们如何才能限制用户使用 FileSystemObject 对象呢？一种极端的做法是完全反注册掉提供 FileSystemObject 对象的那个组件，也就是 Scrrun.dll。具体的方法如下：

在 MS-DOS 状态下面键入：

Regsvr32 /u c：\windows\system\scrrun.dll

（注意：在实际操作的时候要更改成为系统本地的实际路径） 但是这样的话，就不能使用 FileSystemObject 对象了，有时利用 FileSystemObject 对象来管理文件是很方便，有什么办法能两全其美呢？我们可以做到禁止他人非法使用 FileSystemObject 对象,但是我们自己仍然可以使用这个对象. 方法如下： 查找注册表中 HKEY_CLASSES_ROOT\Scripting.FileSystemObject 键值，将其更改成为想要的字符串(右键-->"重命名"),比如更改成 HKEY_CLASSES_ROOT\Scripting.FileSystemObject2

这样,在 ASP 就必须这样引用这个对象了：

Set fso = CreateObject("Scripting.FileSystemObject2")

而不能使用：

Set fso = CreateObject("Scripting.FileSystemObject")

如果使用通常的方法来调用 FileSystemObject 对象就会无法使用了。只要不告诉别人这个更改过的对象名称，其他人是无法使用 FileSystemObject 对象的。这样，作为站点管理者我们就杜绝了他人非法使用 FileSystemObject 对象，而我们自己仍然可以使用这个对象来方便的实现在线考试系统在线管理等功能了！

2.19IIS4.0/IIS5.0 超长文件名请求存在漏洞

受影响的版本：

Microsoft IIS 5.0+ Microsoft Windows NT 2000

Microsoft IIS 4.0+ Microsoft Windows NT 4.0+ Microsoft BackOffice 4.5

Microsoft Windows NT 4.0+ Microsoft BackOffice 4.0

Microsoft Windows NT 4.0

当在一个已知的文件名后加 230 个"%20"再加个.htr，会使安装有 Microsoft IIS 4.0/5.0 泄漏该文件的内容。这是由 ISM.dll 映射的.htr 文件引起的.比如：

http：//target/filename%20<重复 230 次>.htr

这种请求只有当.htr 请求是第一次调用或者 ISM.dll 第一次装载进内存，才能起作用。

解决方法：请到 http://www.microsoft.com/downloads/search.aspx?displaylang=zh-cn（微软中国下载中心）下载相应的补丁程序。

3.SQL Server 2000 的安全漏洞

在进行 SQL Server 2000 数据库的安全配置之前，首先你必须对操作系统进行安全配置，保证你的操作系统处于安全状态。然后对你要使用的操作数据库软件（程序）进行必要的安全审核，比如对 ASP、PHP 等脚本，这是很多基于数据库的 WEB 应用常出现的安全隐患，对于脚本主要是一个过滤问题，需要过滤一些类似，‘;@/等字符，防止破坏者构造恶意的 SQL 语句。接着，安装 SQL Server2000 后请打上补丁 sp1 以及最新的 sp2。

下载地址是：

http://www.microsoft.com/sql/downloads/2000/sp1.asp

和

http://www.microsoft.com/sql/downloads/2000/sp2.asp

在做完上面三步基础之后，我们再来讨论 SQL Server 的安全配置。

3.1 使用安全的密码策略

我们把密码策略摆在所有安全配置的第一步，请注意，很多数据库帐号的密码过于简单，这跟系统密码过于简单是一个道理。对于 sa 更应该注意，同时不要让 sa 帐号的密码写于应用程序或者脚本中。健壮的密码是安全的第一步！

SQL Server2000 安装的时候，如果是使用混合模式，那么就需要输入 sa 的密码，除非你确认必须使用空密码。这比以前的版本有所改进。

同时养成定期修改密码的好习惯。数据库管理员应该定期查看是否有不符合密码要求的帐号。比如使用下面的 SQL 语句：

```
Use master
Select name,Password from syslogins where password is null
```

3.2 使用安全的帐号策略

由于 SQL