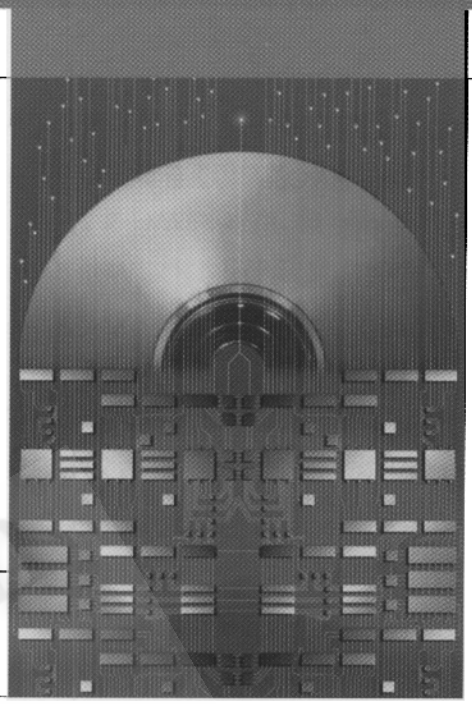
ASP与Access数据库技术在课件开发中的安全性研究

Research of ASP and Access Security in the Development of Courseware



胡光 王敬东 （南京航空航天大学自动化学院 210016）

摘 要： Web环境下的课件开发，需要重视安全问题。本文探讨了Web环境下，利用ASP与Access数据库技术进行课件开发所应考虑的安全性问题，在对开发过程中所遇到的实际问题进行分析和实践验证的基础上，提出了多种技术解决方案，具有实用价值和现实意义。

关键词： 安全 课件 ASP Access 数据库

1 引言

随着网络技术、多媒体技术的日臻成熟，基于Internet的CAI（Computer Assisted Instruction）课件的研究、开发和应用得到了迅速发展，它突破时空限制，大大扩充了教学手段。“ASP”(Active Server Pages)作为一种典型的服务器端网页设计技术，功能强大，得到广泛应用；同时Access数据库作为微软推出的以标准JET为引擎的桌面型数据库系统，由于具有操作简单、界面友好等特点，具有较大的用户群体。因此，ASP＋Access成为许多中小型网上应用系统的首选方案，同时也是远程教学，开发基于Internet的CAI课件的常用技术。但任何Web程序的开发，安全性问题都不容忽视，这是由Internet自身的特点决定的，采用ASP＋Access进行课件开发也不例外，下面分析了开发过程中所应考虑的安全性问题，并提出了相关的解决方案。

2 课件开发中应考虑的安全性问题

任何基于Web的应用程序都会面临安全性的威胁，基于Internet的课件开发中需要考虑的安全性问题主要是防止数据泄露和对课件功能的破坏。课件中的各种数据库系统，如教学管理系统、学生成绩管理系统、试题库等，如果安全措施不当，会使数据库的口令泄露，数据被非法取出和复制，造成信息的泄露，严重时可导致数据被非法删改。另外由于网络的开放性及技术的公开性，恶意用户会通过课件开发中的疏漏进行破坏，使课件不能正常运行。

从以上两个方面考虑，结合作者在利用ASP与Access数据库进行课件开发的实践中所遇到的具体问题，总结出以下需要注意的安全性问题：

2.1 要考虑到Access.mdb有被下载的可能

在知道路径和数据库文件名的情况下，Access数据库文件有被浏览器下载的可能。以课件中的留言系统为例，若将存储有学生的学号、密码和相关留言信息的数据库文件liuyanben.mdb放在目录：“虚拟目录/kejian/”下，则在浏览器端键入“http://服务器主机名/kejian/liuyanben.mdb”，即可进行远程下载。如果事先又没有对数据库文件进行加密，那么该数据库文件的所有重要信息就会被轻易获取。

2.2 权限验证程序设计的安全性问题

在课件开发中，要经常编写ASP代码设置权限验证，使不同类别的用户具有不同级别的操作权限。比如，对于课件中的留言系统，学生可以发布留言和查看留言的回复，而老师可以对留言进行更多的操作，如删除、回复、组合查询等。尤其像成绩管理、在线考试等模块，管理员可以对成绩进行管理，对考试时间、题目等进行设置，权限验证显得尤为重要。对于安全性不强的课件系统，用户在知道相关页面目录的情况下，可以通过在浏览器中敲入相应的地址，绕过验证直接进入该页面，如下面一段ASP权限验证程序：

```
<% '读取用户输入的帐号和密码
UserID=request("yonghu")
```

```
Password=request("mima")
' 检查UserID 及Password 是否正确
set rs=server.createobject("adodb.recordset)
rs.open "select * from infor where yonghu='"&
UserID &"'andmima='"& Password &"'",conn
' 错误定位到error.asp页面
if rs.eof then
response.redirect"error.asp"
end if
' 正确定位到liuyan.asp页面
response.redirect"liuyan.asp"
%>
```

用户只需直接在浏览器端敲入“http://服务器主机名/相对路径/liuyan.asp”就可以饶过权限验证。

2.3 filesystemobject 对象引起的安全性问题

ASP技术的一大优势就是有众多的服务器组件（ActiveX Server Components）的支持。通过使用这些服务器组件，可以高效率地完成各种复杂的功能。filesystemobject 对象是ASP文件存取组件（File Access）中功能强大的一个对象，IIS3、IIS4 的 ASP 的文件操作都可以通过 filesystemobject 实现，包括对目录进行操作，文件的拷贝、修改、删除等。

filesystemobject 对象功能强大，在进行课件开发中，经常被开发者所采用，这就要重视filesystemobject 对象的安全性问题。使用filesystemobjet可以修改、下载 fat 分区上的任何文件。即使是在ntfs分区，如果权限没有设定好的话，文件同样也能被破坏。课件开发完成后进行发布,很多情况是放在学校的信息中心提供的服务器上，"如果网络管理员安全意识不强，比如操作时将Web目录建立在fat分区上、不进行ntfs分区的权限设置等，就会引起filesystemobject方面的安全疏漏。

2.4 利用表单（form）实现交互的安全性问题

在基于Internet的课件中，经常要实现教学效果的实时反馈，进行师生间的信息交互，用户的在线操作等，开发过程中，ASP代码是利用表单实现相关的交互功能的，通过表单来接收浏览器端用户的输入信息，比如学生的留言，用户的注册信息等。而如果在输入区域中敲入标准的HTML语句或者javascript语句会改变输出结果。比如一个留言本，在留言内容中打入：

```
<font size=10>GOODLUCK! </font>
```

如果ASP程序中没有屏蔽html语句，那么就会改变" GOODLUCK "字体的大小。这种改变问题不大，但是如果在输入框中写个javascript 的死循环，比如：

```
<a  herf="http://someurl" onMouseover="while(1)
{window.close('/')}">最新消息</a>
```

那么其他查看该留言的用户只要移动鼠标到"最新消息"上，就会使用户的浏览器发生死机。

3 安全性的实现

系统安全性的实现主要从提高Access数据库的安全性和加强ASP代码编写的严谨性方面入手。这里给出相关的解决方案：

3.1 非常规命名法

这是防止数据库被找到的有效方法：为Access数据库文件起一个复杂的非常规名字，并把它存放在多层目录下。该实例为了说明方便，将数据库文件名命名为liuyanben.mdb，实际开发过程中，所取文件名与数据库文件的内容没有关联性，不易被识别。例如，对于留言系统的数据库文件，不要简单地命名为“liuyanben.mdb”，而是要起个非常规的名字（建议通过算法），例如：re8qjr56t7b.mdb，再把它放在如/aqwk1kjj6t/kjdpw1/qvd/aqpwcx55 之类的深层目录下。这样，对于一些通过猜测得到Access数据库文件的文件名和路径的非法访问方法起到了有效的阻止作用。

3.2 使用 ODBC 数据源

在ASP程序设计中，应尽量使用ODBC数据源，不要把数据库名直接写在程序中，否则，数据库名将随ASP源代码的失密而一同失密。例如"Driver={Microsoft Access Driver(*.mdb)};

DBQ=C:\Inputb\wwwroot\kejian\liuyanben.mdb"这样就把.mdb文件的路径暴露无遗，相关的.asp文件得到后很容易对数据库进行下载，所以应尽量采用通过ODBC DSN来配置数据源，有效地隐藏.mdb文件路径。

3.3 对数据库文件加密

为Access数据库文件编码及加密是防止数据库信息泄露的有效方式。首先点击菜单"工具->安全->加密/解密数据库"，选取数据库（如：liuyanben.mdb），确定后会出现"数据库加密后另存为"的窗口，存为：liuyanben1.mdb。接着liuyanben.mdb就会被编码，并存为liuyanben1.mdb。以上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。

接下来为数据库加密，首先打开经过编码了的liuyanben1.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liuyanben1.mdb设置密码之后，使用Access数据库文件时，Access会先要求输入密码，验证正确后才能够启动数据库。

3.4 利用 Session 对象进行注册验证

为防止未经注册的用户绕过登陆界面直接进入相关页面，可以采用Session对象进行注册验证。Session对象最大的优点是可以把用户的相关信息保留下来，让后续的网页读取。例如，前述的权限验证模块中，验证用户名和密码无误后，添加一段程序，将Session 对象设置为通过验证状态：

```
<% Session( "Passed" ) = True %>,
```

进入应用程序后，首先验证Session对象

下转第 24 页 >>

<< 上接第 29 页

的状态，如果未通过验证，则将其定位到error页面：

```
<% If Not Session( "Passed" ) Then
response.redirect "error.asp"
End If %>
```

这样，如果绕过登陆界面，Session对象就不会被设置为通过验证状态，无法进入后面的相关页面，保证了权限验证的安全性。

3.5 filesystemobject 安全性问题的解决

为了防止远程客户端利用filesystemobject对象对目录进行操作，对文件进行复制、修改和删除以及下载fat分区上的任何文件，提供虚拟主机服务的信息中心应尽量将 web 目录建在 ntfs 分区上，并对ntfs进行权限设置，目录不要设定为 everyone full control，即使是管理员组的成员一般也没什么必要设为 full control，只要有读取、更改的权限就足够了。 也可以把filesystemobject的组件删除或者改名。

3.6 屏蔽标准 HTML、javascript 语句

使用表单编写类似程序时应该做好对非法键入标准的HTML、javascript语句来改变运行结果的防范，可以写一段程序判断客户端的输入语句，并屏蔽掉所有的 HTML、javaScript语句，这样就有效地防止客户端通过表单来改变课件相关应用程序的功能。

4 结论

安全问题是任何Web程序开发所需要关注的首要问题，基于Internet的课件，需要对安全性问题给予足够的重视，利用ASP和Access数据库是课件开发常用手段，其安全性问题值得深入探讨。

参 考 文 献

1 周恕义、杨晓华、侯洪涛，多媒体CAI及网络化远程教学技术[M]，中国水利水电出版社，2001。

2 彭万波、景丽、周宏敏，ASP开发基础与范例[M]，电子工业出版社，2002。

3 Alan Simpson, Celeste Robinson. Access2000 从入门到精通[M]，电子工业出版社，1999。

4 刘宏峰、陈江波，ASP3.0网络开发技术大全[M]，人民邮电出版社，2001。