# 基于ASP技术的WEB MIS安全系统的设计与实现

高 城 (海军后勤部秦皇岛办事处司令部 066001)

摘要：简要介绍了ASP技术，通过总结Browser/Server体系结构下MIS系统的开发经验，讨论了基于ASP技术下的WEB MIS系统安全策略、安全系统的设计与实现方法。

关键词：ASP WEB MIS 信息安全

随着WEB技术的广泛应用，基于WEB的信息系统越来越多，人们在共享信息的同时，也面临着信息安全的问题。事实上，用户访问网络并获取信息的方式越便捷，保护信息安全的难度也就越大。因此，如何在网络环境下保证MIS系统中的合法用户对资源的安全访问，防止非法访问者的入侵与攻击，同时又不至于产生过多的限制而影响用户的正常使用，正日益成为信息系统开发者所面临的一个重要课题。本文将通过总结Browser/Server体系结构下MIS系统的开发经验，讨论基于ASP技术下的WEB MIS系统安全策略、安全系统的设计与实现方法。

## 1 基于ASP技术的MIS系统安全策略

### 1.1 用户管理—标识和鉴别

在一个多用户的系统中识别授权用户标识是安全控制机制中最重要的一环，也是安全防线的第一个环节。这里的标识（Identification）是指用户向系统出示自己的身份证明，最简单的方法是输入UserID和Password。在基于ASP技术的MIS系统中，可采用form表单提交用户输入的帐号和密码，并与用户标识数据库中相应的字段进行匹配。

### 1.2 存取控制

存取控制机制定义和控制一个对象对另一个对象的存取访问权限。数据库安全最首要的课题就是确实保证只授权给有资格的用户以访问数据库中数据的权限，并能以令人信服的方式证明/测试这一保证的可靠程度。同时，令所有未正常授权人员无法打开数据库。比如在基于ASP技术的MIS系统中，数据库可严格地按单位和专业业务划分，分系统间尽可能做到逻辑上隔离。这样系统中不同角色的权限就可以明确地界定--系统管理员具有新增用户、删除用户并设置初始密码的权利；部门主管在每个分系统的系统权限设置模块中，对用户是否具有对专业数据库的操作权限进行控制和管理。

### 1.3 审计和日志

为了保证数据库中的数据的安全，要求系统保留系统操作的日志文件，以便于事后调查和分析，追查有关责任者，并可发现系统的安全弱点。可采用ASP数据库访问技术，利用专门的数据库来进行审计和日志管理。同时，系统管理员可以根据系统的开销选择是否开启日志记录功能，从而对系统的使用进行严密的监控。

### 1.4 攻击监测

在经典及现代的安全理论中，“存取控制”和“访问控制”都是系统安全策略的最重要的手段，但不可能百分之百地保证一个系统中不存在安全漏洞。由于审计和日志管理都是事后性的，因此为了保证系统能够及时发现并采用适当的防卫和补救措施，必须建立相应的攻击监测系统。可利用ASP数据库技术开发实时监测系统，以使系统管理员及时发现危害系统安全的操作并采取相应的措施。

### 1.5 敏感机要数据的管理

对于系统数据库中的不得公开的机要数据，进行严格的访问控制，保证敏感保密数据不被泄露，即保证其机要性；只允许被授权的用户接触这些数据并防止授权扩

散。机要敏感数据可采用以下两种方式进行管理：对密级较高的数据，其数据库设在使用管理者的PC内，通过PWS单独运行，经主管批准后方可并网调用；对密级一般的数据，通过服务器、操作系统及防火墙严密监控。

### 1.6 限界

限界（Confinement）是指防止在程序之间出现未授权的信息传递，信息的传递应当通过授权通道。与此同时，发现并堵塞系统的隐秘通道，防止信息的异常流动。可通过对日志的分析及进行测试、试用，来发现并堵塞系统的隐通道。

### 1.7 对象重用

所谓对象重用，是指存储对象如内存等，进行重新分配时，由前一个使用这些对象的用户留下的信息被后一个用户非授权地得到，并能够读出其中的数据。解决对象重用问题的办法，是在对象分配时进行初始化操作。

由于在基于ASP技术的MIS系统中，常常使用Session（会话）或Cookie变量来保存用户登录及权限信息，由于Session或Cookie变量在浏览器窗口打开到关闭之间将一直保留，如果新用户使用原来用户的同一浏览器窗口即有发生对象重用的可能性。因此应在登录页面增加初始化所有Session或Cookie变量的代码，并对用户给出相应的提示，以解决对象重用问题。

### 1.8 多级保护体制

现实的大多数应用都要求对信息本身划分不同的保密级别，在多级保密体系中，对不同数据项赋予不同的保密级别，然后根据数据项的密级给访问该数据的操作赋予不同的级别。而数据的完整性和保密性是通过给予用户一份权限许可来实现的。可在ASP文件的头部嵌入多层数据鉴别文件来过滤数据，实现多级保护。

## 2 基于ASP的MIS安全系统的设计与实现

### 2.1 安全体系结构

一个MIS系统通常是由若干个分系统组成的，在笔者开发的基于ASP技术的MIS安全系统中，分系统是按照业务管理的职能来划分的。这种划分的优点：一是基本上与行政隶属关系一致，符合平时业务习惯，二是职能与责任明确，既便于对下进行业务指导，又便于对上进行业务往来。各分系统之间除公共数据外，完全隔离，不可互通。分系统内部，又划分为两级：一是分系统内部共享数据（第一级），二是业务管理员权限内数据（第二级）。


图 1 MIS系统安全体系结构示意图

业务管理员的权限管理与分配由各分系统的业务主管控制。总体来看，分系统与公共数据之间是第一道保护层，分系统内第一级与第二级之间是第二道保护层。如图1所示。

实现方法：采用ASP的Session技术进行系统隔离保护与用户认证标记保持。其过程是：当用户第一次进入系统时，要求用户输入各自的用户帐号和登录密码，提交后系统将打开用户数据库进行数据匹配，如果数据匹配，则将认证标记交给一个Session对象，用户每转换一次页面都要比较认证标记与预设值是否匹配，程序如下：

```
<%  dim tag
    tag= Session("LoginIdentity") '将身份标记赋给tag变量
    If tag<>"qj12jgk" Then '如果不匹配，将页面导向警告页
    Response.Redirect "../warning.asp"
    End If
    If tag<>"qj12jgk" Then '中止下面的页面执行
      Response.End
    End If
%>
```

该程序作为一个文件check.inc加载在每一个第一级页面的头部，如果认证标记改变只需修改该文件即可。对于第二级页面除在头部加载check.inc，还要加载check2.inc（程序内容与check.inc类似）。

此外，为了避免对象重用，可以在登录成功的进入第一页之前，初始化所有Session对象，也可以在Global.asa文件中使用Session_OnStart事件和Session_OnEnd事件来进行Session对象的初始化操作。

### 2.2 用户身份标识与鉴别

MIS中用户的身份信息是由以下字段组成的：用户ID、姓名、帐号、密码、身份码、权限码、身份描述、是否锁定，如图2所示。这些字段在数据库中做为一个数据表，用户每次登录时，通过数据库访问该数据表，进行身份标识的鉴别。

用户除了拥有所在分系统的身份标识外，在用户数据库另有一标志其对分系统内的子系统所拥有权限的数据表，其结构为：用户帐号、第二级系统密码、对各第二级系统的权限（“permit”为有权，“no”为无权）。用户登录第二级系统采用密码与权限双重鉴别的机制。

用户在进入每一级系统后，均可随时更换自己登录该系统的密码。

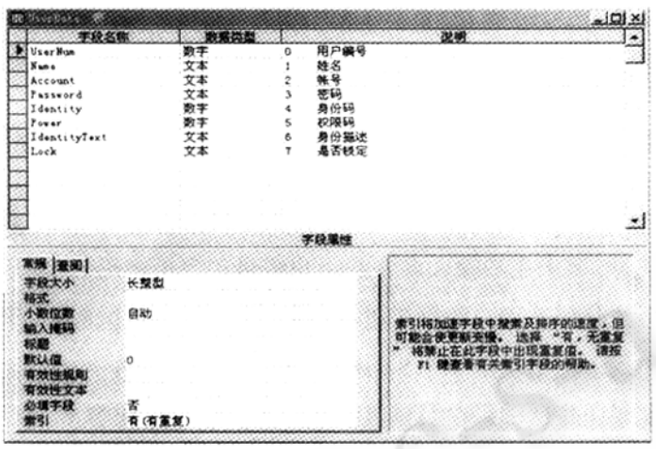


图 2　用户身份标识数据表

## 2.3 系统权限管理

MIS 系统权限管理可分为两部分：一是用户数据管理；二是分系统权限管理。用户数据由系统管理员进行管理，系统管理员可以进行用户信息查询、增加新用户、删除用户、用户数据维护等操作。分系统内权限分配由各分系统业务主管进行管理。分系统业务主管可以对该分系统用户进行授予权限和回收权限的操作，但无操作用户身份标识数据的权限。

## 2.4 系统监测与审计

对系统进行监测与审计，对系统的安全具有至关重要的影响。通过对系统的监测，可以及时发现外界对系统的攻击并在第一时间采取应急措施，保证系统安全，同时可以给企图入侵者以一定的威慑；通过系统审计和日志分析，可以确定非法操作者的身份及攻击 PC 的 IP 地址，籍此追究其责任，还可以通过分析日志发现异常的数据操作，找到系统漏洞，进而促进系统的完善。

系统监测主要通过实时监测（Real-Time Scan）的方式，监测系统的设计借鉴了 Windows NT 用户审计和“防火墙”实时监测的思想，运用了 ASP 服务器访问、ADO 数据库存取等技术。系统监测主要包括以下两部分：一是对非法操作的数据采集和记录，二是对监测数据库的动态扫描。

(1) 非法操作的数据采集和记录。对非法操作的数据采集和记录与系统日志类似，不同的是前者针对外部攻击的记录，后者是针对内部操作的记录。当用户对某一页面发出请求后（无论该用户是合法用户还是非法入侵），系统通过访问服务器常量参数首先记录下该用户的访问信息，包括该用户登录服务器的帐号、发出请求的 PC 的 IP 地址、响应请求的服务器 IP 地址、被请求页面的 URL 等信息，该程序段作为一个文件加载在被请求页面 ASP 文件的头部。

之后进行用户身份鉴别，有两种非法操作的情况：一是多次登录，可能是猜测系统用户帐号和密码；二是非法登录非登录页。非法操作可通过程序段记录到相应的非法操作数据库，该程序段作为一个文件加载在错误处理页面 ASP 文件的头部。


图 3　系统实时监测（左：未有报警；右：报警界面）

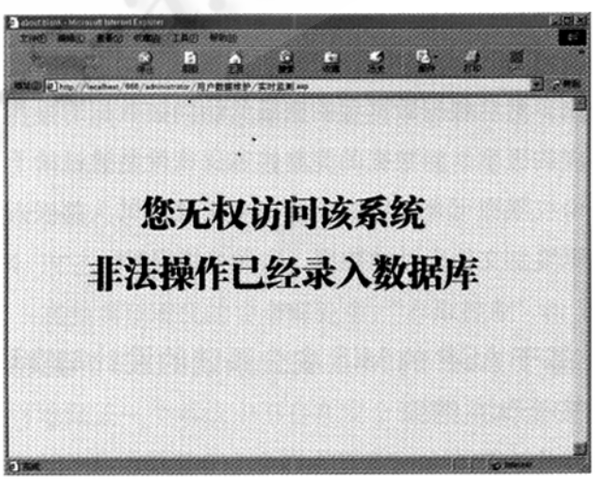


图 4　系统警告页面

(2) 动态扫描非法操作数据库。系统根据设定的刷新频率和监测时段，定时访问数据库并动态计算查询条件，发现符合条件的记录即向系统管理员报警，并显示非法操作信息。系统管理员可以根据提示信息进行日志查询，做出相应处理。系统监测如图 3、图 4 所示。

## 3 结束语

基于ASP技术实现MIS安全系统，是ASP数据库开发应用的一种新形式。通过ASP页面保护、日志管理、非法操作审计和系统实时监测等手段，可以使整个系统的安全级别达到系统审计保护级—公安部标准的第二级或美国TCSEC（Trusted Computer System Evaluation Criteria，《可信计算机系统评估标准》[4]）橘皮书的C2级，对该领域的应用具有一定的参考价值。■

参考文献

1 陈传波、梅雪莲，WWW方式的动态页面的原理及制作，[J] 计算机应用研究，1999，12：104–106。

2 Simson Garfinkel and Gene Spafford, Practical Unix & Internet Security, [M] 电子工业出版社，1999：134–150。

3 吴应良，管理信息系统的安全问题与对策研究，[J] 计算机应用研究，1999，11：22–31。

4 刘启原、刘怡，数据库与信息系统的安全，[M] 科学出版社，2000，1：20–28。