第6卷第4期 辽宁省交通高等专科学校学报 Vol.6 No.4
2004年12月 JOURNAL OF LIAONING PROVINCIAL COLLEGE OF COMMUNICATIONS Dec.2004

文章编号:1008－3812(2004)04－0055－03

Web数据库中信息的安全策略

张翠玲 高 晗 杨 玲
(辽宁省交通高等专科学校,辽宁沈阳 110122)

摘 要 网站数据库中的口令字段简单地采用明文,数据库泄密后,其中的信息一目了然。本文对数据库中的有关信息的加密进行了研究。

关键词 数据库 安全 MD5算法
中图分类号:TP393.092 **文献标识码**:B

0 引言

随着Internet/Intranet技术的蓬勃发展,人们已不再满足于传统的静态Web技术,ASP技术的出现给动态Web网络的开发带来新机,越来越多的网站利用ASP技术开发出动态、交互和高效的Web服务器应用程序。网站的后台管理则采用ASP与数据库的有机结合来动态管理网站信息,目前通常使用的是在登陆管理界面时需要提交用名、密码和验证码进行身份验证。

由于网站的建设者的安全意识不强,多数直接利用网上的开放源码,通过少量修改甚至不加任何修改便直接应用到自己的网站,这样的做法存在着很大的安全隐患,有可能导致数据库被下载,口令被破解等,使网站失去控制权。本文着重从密码的安全性来介绍如何对数据库中口令字段信息的加密,以达到保护信息安全。

1 MD5用于口令的加密方法

1.1 MD5简介

MD5的全称是Message－Digest Algorithm 5(信息－摘要算法),在90年代初由MIT Laboratory for Computer Science和RSA Data Security Inc的Ronald L. Rivest开发出来,经MD2、MD3和MD4发展而来。它的作用是让大容量信息在用数字签名软件签署私人密匙前被"压缩"成一种保密的格式(就是把一个任意长度的字节串变换成一定长的大整数)。不管是MD2、MD4还是MD5,它们都需要获得一个随机长度的信息并产生一个128位的信息摘要。虽然这些算法的结构或多或少有些相似,但MD2的设计与MD4和MD5完全不同,那是因为MD2是为8位机器做过设计优化的,而MD4和MD5却是面向32位的电脑。这三个算法的描述和C语言源代码在Internet RFCs 1321中有详细的描述,这是一份最权威的文档,由Ronald L. Rivest在1992年8月向IEFT提交。

1991年,Rivest开发出技术上更为趋近成熟的MD5算法。它在MD4的基础上增加了"安全－带子"(Safety－Belts)的概念。虽然MD5比MD4稍微慢一些,但却更为安全。这个算法很明显的由四个和MD4设计有少许不同的步骤组成。在MD5算法中,信息－摘要的大小和填充的必要条件与MD4完全相同。Den Boer和Bosselaers曾发现MD5算法中的假冲突(Pseudo－Collisions),但除此之外就没有其他被发现的加密后结果了。

MD5的典型应用是对一段信息(Message)产生信息摘要(Message－Digest),以防止被篡改。比如,在UNIX下有很多软件在下载的时候都有一个文件名相同,文件扩展名为.md5的文件,在这个文件中通常只有一行文本,大致结构如:

MD5 (tanajiya.tar.gz) =
0ca175b9c0f726a831d895e269332461

这就是tanajiya.tar.gz文件的数字签名。MD5将整个文件当作一个大文本信息,通过其不可逆的字符串变换算法,产生了这个唯一的MD5信息摘要。如果在以后传播这个文件的过程中,无论文件的内容发生了任何形式的改变(包括人为修改或者下载过程中线路不稳定引起的传输错误等),只要你对这个文件重新计算MD5时就会发现信息摘要不相同,由此可以确定你得到的只是一个不正确的文件。如果再有一个第三方的认证机构,用MD5还可以防止文件作者的"抵赖",这就是所谓的数字签名应用。

MD5还广泛用于加密和解密技术上。比如在UNIX系统中用户的密码就是以MD5(或其它类似的算法)经加密后存储在文件系统中。当用户登录的时候,系统把用户输入的密码计算成MD5值,然后再去和保存在文件系统中的MD5值进行比较,进而确定输入的密码是否正确。通过这样的步骤,系统在并不知道用户密码的明码的情况下就可以确定用户登录系统的合法性。这不但可以避免用户的密码被具有系统管理员权限的用户知道,而且还在一定程度上增加了密码被破解的难度。

1.2 MD5的算法描述

对MD5算法简要的叙述可以为:MD5以512位分组来处理输入的信息,且每一分组又被划分为16个32位子分组,经过了一系列的处理后,算法的输出由四个32位分组组成,将这四个32位分组级联后将生成一个128位散列值。

在MD5算法中,首先需要对信息进行填充,使其字节长度对512求余的结果等于448。因此,信息的字节长度(Bits Length)将被扩展至N＊512＋448,即N＊64＋56个字节(Bytes),N为一个正整数。填充的方法如下,在信息的后面填充一个1和无数个0,直到满足上面的条件时才停止用0对信息的填充。然后,在在这个结果后面附加一个以64位二进制表示的填充前信息长度。经过这两步的处理,现在的

收稿日期:2004－10－21

信息字节长度=N*512+448+64=(N+1)*512,即长度恰好是512的整数倍。这样做的原因是为满足后面处理中对信息长度的要求。

MD5中有四个32位被称作链接变量(Chaining Variable)的整数参数,他们分别为:A=0x01234567,B=0x89abcdef,C=0xfedcba98,D=0x76543210。

当设置好这四个链接变量后,就开始进入算法的四轮循环运算。循环的次数是信息中512位信息分组的数目。

将上面四个链接变量复制到另外四个变量中:A到a,B到b,C到c,D到d。

主循环有四轮(MD4只有三轮),每轮循环都很相似。第一轮进行16次操作。每次操作对a、b、c和d中的其中三个作一次非线性函数运算,然后将所得结果加上第四个变量,文本的一个子分组和一个常数。再将所得结果向右环移一个不定的数,并加上a、b、c或d中之一。最后用该结果取代a、b、c或d中之一。

实现MD5算法的各种语言子程序可以在网上找到。

1.3 口令字段加密的ASP程序

MD5算法正常的输出顺序为abcd,如明文admin经MD5加密后为

a=21232f29 b=7a57a5a7 c=43894a0e d=4a801fc3

测试程序如下:

```
<! -- #include file="../inc/md5.asp" -->
<%
  GetUserName=request.form("FormUserName")
  md5order=request.form("order")
  result=md5(GetUserName,md5order)
%>
<html><head>
<title>MD5 算法的 ASP 实现</title>
<meta http-equiv="Content-Type" content="text/html; charset=gb2312">
<style type="text/css"><! --'此处省略了样式定义--></style></head>
<body>
<table width="750" border="0" cellpadding="2" cellspacing="1" class="table01">
  <tr><td class="tr01"><table width="100%" border="0" cellspacing="0" cellpadding="0">
    <tr class="tr01"><td><font face="webdings">8</font> <strong>MD5 加密</strong></td>
      <td align="right"></td></tr></table></td></tr>
  <tr><td><table width="100%" border="0" cellpadding="1" cellspacing="1" class="table02">
    <tr><td colspan="2" class="tr02"> 描述:排列顺序数用 abcd 表示</td></tr>
    <tr><form name="form1" method="post" action="test1.asp">
      <td class="tr03"><p>请输入原码:
        <input type="text" name="FormUserName" value="<%=GetUserName%>"></p>
        <p>排列顺序数:<input type="text" name="order" value="<%=md5order%>" ></p>
        <p align="center"><input type="submit" name="Submit2" value="加密"></p>
      </td>
      <td class="tr03"> 经 MD5 转换后为:
        <%if result<>"" then%>
        <input type="text" name="result" readonly="true" value="<%=result %>" size="35">
        <% else%><input type="text" name="result" readonly="true" value="" size="35">
        <%end if%>
      </td>
    </form>
  </tr></table></td></tr>
  <tr><td class="tr01" height="3"></td></tr>
</table>
```

上述代码中的引用程序md5.asp为通用子程序,可在网上找到。在子程序计算出abcd数值后,需要添加以下代码

```
dim i,s,o,n
  s=iorder
  n=len(s)
for i=1 to n
  Select Case mid(s,i,1)
  Case "a"o=o & WordToHex(a)
  Case "b"o=o & WordToHex(b)
  Case "c"o=o & WordToHex(c)
  Case "d"o=o & WordToHex(d)
  end select
next
MD5=LCase(o) 'md5 重排序
```

程序运行结果见图1

图1 MD5加密处理

2 密文的运用

在管理程序的登陆程序中,首先对用户提交的口令进行md5转换处理,将转换结果与保存在数据库中口令字段的密文进行比较,如果二者一致方可转入下一步。通过这样的验证措施,即使数据库泄露,口令也不会被轻易破解。

当然为了加强防护措施,还可以对转换的结果进行重排序,如将abcd的顺序打乱,或仅使用其中的几个数,如代码MD5=LCase(WordToHex(b) & WordToHex(c))仅使用了b和c。

实际上任何一种算法都会有其漏洞,即使是目前大行其道的MD5和SHA-1,当对漏洞的研究发展到其能够被有

文章编号:1008-3812(2004)04-0057-02

现代企业薪酬设计初探

刘纪东
(国家开发银行辽宁省分行,辽宁沈阳 110014)

摘 要 本文简要介绍了薪酬的概念与薪酬设计的目的,说明了现代企业薪酬设计的原则,对薪酬体系的设计和薪酬策略的选择进行了初步的分析,对现代薪酬管理发展趋势进行了展望。

关键词 薪酬设计 薪酬体系 薪酬策略
中图分类号:F272.92 **文献标识码**:B

面对未来竞争激烈且快速变迁的经营环境,人力资源管理将成为企业成败的关键,健全的薪酬制度是吸引、激励、发展与留住人才的最有力的工具。而传统的薪酬设计理念将不足以满足现代高素质员工的要求,这就要求企业经营者转变观念,从而改善管理,提供符合现代企业特点的薪酬设计方案。

1 薪酬的概念与薪酬设计的目的

所谓薪酬是指员工从事企业所需要的劳动,而得到的以货币形式和非货币形式所表现的补偿,是企业支付给员工的劳动报酬。与传统的工资概念所不同的是,薪酬还包含了非货币形式的报酬。

2 薪酬设计的原则

企业设计薪酬时必须遵循一定的原则,这些原则包括战略导向、经济性、体现员工价值、激励作用、相对公平、外部竞争性等。

2.1 战略导向原则

战略导向原则强调企业设计薪酬时必须从企业战略的角度进行分析,制定的薪酬政策和制度必须体现企业发展战略的要求。

2.2 经济性原则

薪酬设计的经济性原则强调企业设计薪酬时必须充分考虑企业自身发展的特点和支付能力。

2.3 体现员工价值原则

企业在设计薪酬时,必须要能充分体现员工的价值,要使员工的发展与企业的发展充分协调起来,保持员工创造与员工待遇之间短期和长期的平衡。

2.4 激励作用原则

激励作用原则就是强调企业在设计薪酬时必须充分考虑薪酬的激励作用,即薪酬的激励效果。

2.5 内部一致性原则

内部一致性原则包含几个方面。一是横向公平,即企业所有员工之间的薪酬标准、尺度应该是一致的;二是纵向公平,即企业设计薪酬时必须考虑到历史的延续性,一个员工过去的投入产出比和现在乃至将来都应该基本上是一致的,而且还应该是有所增长的。

2.6 外部竞争性原则

外部竞争性原则前文已经提到过,它强调企业在设计薪酬时必须考虑到同行业薪酬市场的薪酬水平和竞争对手的薪酬水平,保证企业的薪酬水平在市场上具有一定的竞争力,能充分地吸引和留住企业发展所需的战略、关键性人才。

3 典型的薪酬体系

3.1 职务工资制

收稿日期:2004-09-30

效利用时,则标志着该算法灭亡的时候到了。长期以来,密码界一直在致力于对新加密算法的研究,而且在高度机密的安全领域,所采用的加密算法也绝非 MD5,各国政府、各大公司都在研究拥有独立技术的加密算法,其中比较出色的代表有 SHA-1、SHA-224 等。

3 结语

随着一些黑客软件的出现,如 ASP 网站管理员帐号密码探测器,利用 ASP 中 SQL 语句的漏洞,自动猜测运算,并获取网站的管理员帐号和密码。因此保护网站信息显得十分重要。

本文仅就网站管理后台程序中的口令安全性问题进行了研究,通过使用 MD5 加密算法对口令进行加密转换可以有效地防止信息泄露,当然网站中的重要信息也可以采用此方法进行处理。

Security Policies of Informations about Web Database

Zhang Cuiling Gao Han Yang Ling

〔**Abstract**〕The password field in database of a Website using plain text simply, it can be read after the database was downloaded. The method Encrypting some informations in database was introduced in this paper.

〔**Keywords**〕database security md5 arithmetic