广西科学院学报
Journal of Guangxi Academy of Sciences

2012,28(4):269~272
Vol. 28, No. 4 November 2012

县级政府网站数据库安全隐患分析及解决方法
The Research on Analysis and Solution of Database Security in Government Website

周 游[1,2],邓珍荣[1]
ZHOU You[1,2], DENG Zhen-rong[1]

(1.桂林电子科技大学,广西桂林 541004;2.广西艺术学院,广西南宁 530022)
(1. Guilin University of Electronic Technology, Guilin, Guangxi, 541004, China; 2. Guangxi Arts Institute, Nanning, Guangxi, 530022, China)

摘要:分析一县级政府的门户网站数据库安全隐患,并针对性地提出重视服务器的管理,加大人才和软资源的投入,选择相对安全的运行平台,防止非法下载网站数据库和多种加密方式混合加密等解决数据库安全隐患的方法。

关键词:门户网站 数据库安全 隐患
中图法分类号:TP311.5 **文献标识码**:A **文章编号**:1002-7378(2012)04-0269-04

Abstract: Based on one of the Guangxi government portal websites, the risks of database security were analyzed. Some solutions including increase of professionals and related resources investment, selection of safe operation platform, prevention of illegal database download and different types of encryption were stated.

Key words: portal website, database security, hidden danger

随着 Internet 的迅猛发展,各类门户网站和专业网站如雨后春笋般涌现。政府门户网站作为电子信息化时代的公共服务龙头在为公众服务过程中扮演的角色越来越重要[1]。各级政府在社会发展的过程中,对自身门户网站的要求越来越严格:网络信息系统的规模、复杂程度、所存储的机密数据都在逐渐增加。在这种发展趋势下,政府门户网站数据库系统的安全隐患也在升级,如遭受黑客的攻击、病毒感染等。保障政府门户网站数据库的安全已成为政府部门的核心问题,采取何种安全保障措施来确保数据库的可靠性和保密性是摆在技术人员面前的一个重大课题[2]。本文以一县级政府门户网站为例,全面分析、总结了其网站数据库所存在的安全隐患,并提出相应的解决方法,以期为政府门户网站的建设和管理提供借鉴。

收稿日期:2012-09-12
作者简介:周 游(1988-),男,助理工程师,主要从事计算机数据库安全、软件工程研究。

1 网站数据库存在的安全隐患分析

通过实地调研一县级政府门户网站系统的前后台,深入分析后发现该网站存在如下安全隐患:

1.1 软硬件投入不对称

一般来讲,即使我们购买的服务器再高档,各方面的设计再完备,不配备熟练的操作者,也很难保证网站不被人为攻破。实地调研时,通过和相关人员交流沟通后发现,该县政府在购买了相关的专用网络服务器,组建实施网站后,对人员的管理和投入重视程度不够,仅配备了一名非计算机相关专业毕业的专职人员来负责门户网站的日常维护和管理工作,这势必留下了许多安全隐患。比如,与网站开发商沟通时存在专业知识障碍等,加之该网站的开发商是外地人,为了降低成本,在网站开发部署完毕后,开发商将网站运行管理的工作交给政府的管理人员,网站系统出现问题后,一般是通过远程操控解决或者是口述方法让管理者自行解决。由于所配置的管理者计算机专业知识有限,在很多情况下,网站出现问题,管理者不能及时发现,更不用说是向开发

人员表述清楚网站运行过程中所存在的问题，也就很难根据开发商提供的解决方法快速圆满地解决问题。政府门户网站与其它商业网站最大的区别，就是它的政治信息安全问题。该门户网站如果遇到黑客或者不法分子的恶意攻击，当值管理人员必须通过自身敏锐的观察能力和熟练的入侵检测软件操作能力及时发现情况，并向相关部门上报和反追踪。因此，软硬件投入不对称，重硬件投入而轻管理人员的配备，给政府门户网站留下了较多的安全隐患。

1.2 系统开发运行平台本身易受攻击

所调研的县政府门户网站是用微软的ASP.NET进行开发的。该开发平台优势在于集成了大量日常开发所需要用到的控件，运用这些控件设计出来的系统，界面美观，源代码易懂，而且开发者可大大地提高开发效率，缩短开发周期，降低生产成本。但是使用ASP.NET工具开发出来的网站系统必须在Windows操作系统上的IIS服务器上架设，而Windows系统的代码不开源，一旦有系统漏洞被发现，此类漏洞就会被不法之徒利用，目标系统就会受到攻击。从微软发现漏洞到官方补丁的公布通常都会有一个时间差，在这段时间内，系统数据库就会很容易出现安全问题。而如果选择Linux系统来开发网站，就能够较好地避免此类攻击。因为Linux系统本身就是开源的，所以当漏洞被发现后，补丁公布的时间就会缩短，即缩短漏洞被利用的时间[3]。

1.3 使用的加密算法单一

由于网站数据库使用MD5(信息-摘要算法5)来对用户的密码进行加密，而MD5加密是利用哈希函数进行算法设计，MD5哈希函数以512位来处理输入数据，每一分组又划分为16个32位的子分组。算法的输出由4个32位分组组成，将它们级联起来，形成一个128位的固定长度的哈希值，即输入数据的摘要。如今MD5加密方法已不能更有效地抵抗穷举攻击(包括生日攻击)。虽然坚固的哈希函数可以通过设计有效的碰撞处理机制，或增加数字摘要的位数来增加复杂度，以减少碰撞出现的概率，但是2005年王小云教授关于破译MD5算法的报告中称他们已经研究出了搜索碰撞的一系列新技术，使得碰撞能在小于2～69次Hash操作中找到[4]。而且随着现在计算机网络数据库存储的数据量日益增大，计算机的计算能力不断提升，网络数据库已经收录了大量人们日常使用的MD5算法的原文和密文，我们只需将密文输入数据库搜索即可获得原文。表1的结果也显示，传统的加密方法已经无法满足现在网站数据库对安全的需求。

1.4 缺乏可靠的验证系统

网站设计时为了能提高开发效率，获取最大的利润，开发者往往在进行代码编写时，并没有对用户输入的数据进行比较全面的合法性分析和判断，进而导致系统在实际应用中存在安全威胁。如：普遍存在的SQL注入，系统数据库数据不一致等[3]。我们所调研的门户网站也存在类似的问题。

表1 MD5值收录情况

收录内容	说明	数量
1～6位大小写字母＋数字＋特殊字符	收录100%	大于1400亿
7位小写字母＋数字	收录100%	大于783亿
8位小写字母	收录100%	大于2082亿
8位小写字母＋数字	已收录50%，正在添加	大于14000亿
8～11位数字	收录100%	大于1000亿
1～15位其它数据	部分收录	大于28000亿
1～20位	900G独家超大字典	大于910亿

2 解决网站数据库安全隐患的方法

2.1 重视服务器的管理，加大人才和软资源的投入

任何先进的硬件资源，如果对应的管理跟不上，就不能很好地发挥出其应有的价值。为此，首先需要引进至少一名专职的专业技术管理人员，要求该管理人员具备相应的专业知识和操作技能。如对计算机网络及安全有一定的知识，能够熟练地使用各种检测软件，监察网站的运行情况，有能力及时发现非法入侵，并立即采取相应的防护措施。其次，根据网站自身的实际情况，建立完善的机房管理规章制度并严格执行。最后还有必要设立监控摄像头，做到机房有记录，发生故障后有迹可循。

2.2 选择相对安全的运行平台

从长远和安全的角度考虑，应该选择Linux等开源系统作为网站运行平台。计算机技术的不断发展和提高，网站数据库安全性的需求日益增加，我们可以在不更改网站结构界面的前提下，把数据库设在Linux的操作系统下，以提高数据库的安全性。设计方案如下：

用JAVA设计一个EJB服务器端和一个EJB客户端，客户端通过进程间通信技术在本机与网站系统进行交互，再将交互的内容加密并发送到服务

器端。服务器端安装在数据库所在的服务器上,负责接收和反馈给客户端信息(图 1,2)。

EJB 调用例子程序(java)

使用 eclipse 添加一个新的含 main 方法的类。参考代码如下:

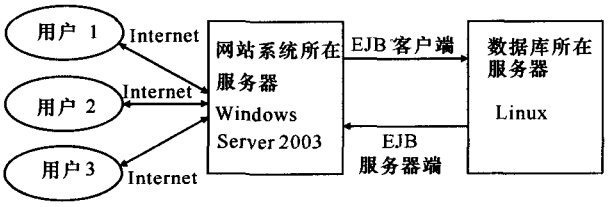

图 1　网站系统和数据库

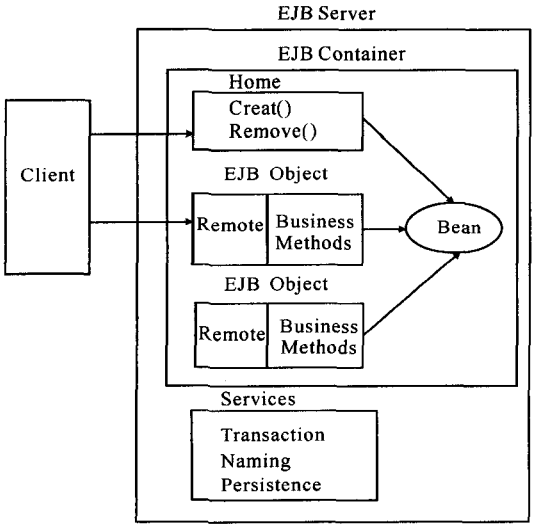

图 2　EJB运行结构

```
public class TestHelloWorld {
/**
  * @param args
  * @throws NamingException
  */
public static void main(String[] args) throws NamingException {
  Properties props = new Properties();
  props.setProperty("java.naming.factory.initial", org.jnp.interfaces.NamingContextFactory");//设置 ejb 容器的属性
  props.setProperty("java.naming.provider.url","localhost:1099");//查找服务器
  //初始化一个查找目录
  InitialContext ctx = new InitialContext(props);
  HelloWorldRemote testbean = (HelloWorldRemote)ctx.lookup("HelloWorld/remote");//创建一个实例
  int first = testbean.ejbCalculate(3);//返回第一个计算值
  int second = testbean.ejbCalculate(3);//返回第二个计算值
  StringBuffer sb = new StringBuffer();//将返回值合并
  sb.append("Value:").append(first).append("/").append(second);
  System.out.println(sb.toString());
}
}
```

2.3　设法防止非法下载网站数据库

具体做法:(1)修改数据库文件名,保证文件名的复杂性和不可猜测性,数据库所在目录设置成不能开放目录浏览权限。(2)数据库名后缀改为 ASA、ASP 等,可以对付一般的黑客,必要时可以进行一些二进制字段添加等设置。(3)数据库名前加“#”,只需要把数据库文件前名加上#,然后修改数据库连接文件中的数据库地址。因为下载的时候计算机只能识别#号前名的部分,对于后面的自动去掉。在数据库文件名中保留一些空格也能够起到类似的作用,由于 HTTP 协议对地址解析的特殊性,空格会被编码为“%”,即使暴露了数据库地址,一般情况下别人也无法下载[5]。

2.4　采用多种加密方式混合加密

数据加密技术是网站数据库最安全有效的技术之一[2]。针对目前已出现的黑客破解泄露出去密码的手法,可以找到一些应对方案。

(1)对数据库设置严格的控制规则。为了确保数据库有足够的加密强度和大量数据在尽量长的时间内不会被破译,需要设置严格的访问控制规则,拒绝非法用户访问。

(2)对用户名和用户基础信息进行加密。为了确保用户名的安全性,可以先将用户名逆序分两组,然后分别进行加密,再组合起来保存到数据库中。因为 AES 加密算法加密速度快,加密结果与原来占用空间对比差别不大,而且即使数据库数据外泄,黑客也必须先花费一定的时间先破解用户名,才能对网站进行进一步的攻击。

(3)选择不常用的重要数据的加密方法。采用 RSA 加密算法对一些不常用的但是很重要的数据进行加密,并设置这些数据有用户取回密码的密码保护问题、邮箱等。虽然 RSA 加密算法安全级别很高,破解需要的时间极长,很难被破解。但是该算法加密速度很慢,比对应同样安全级别的对称密码算

法要慢1000倍左右，所以用于加密不常用的数据比较合适。

(4)对用户名密码进行加密。在对用户的密码进行加密时，可以改变原有的加密次序和加密方法。即使使用MD5加密算法，如果先将用户输入的密码分组(2～4组)，再对分组进行加密，最后合并加密结果进行一次总加密，这样就给黑客破解增加了很多难度。而且MD5算法需要的时间短，加速购买的是高速的服务器计算机，所以多次加密不会拖慢系统的运行速度。

用程序实现MD5的加密过程(C#实现)：

```
public static string  Encrypt(string password)//将字符串逆序分组加密的方法
    {
    char[] t = password.ToCharArray();//将字符串转换成字符数组
      string newstr = "";
      for (int m = t.Length - 1; m >= 0; m--)//将字符数组逆序保存为字符串
       {
         newstr += t[m].ToString();
       }
 //以下两句分别为，取前半段字符串和取后半段字符串
      string password1= newstr.Substring(0,newstr.Length / 2);
       string password2= newstr.Substring(newstr.Length / 2,newstr.Length - 1);
 //以下三句是将分开的两段字符串分别加密，然后再合并加密
       password1= MD5Encrypt(password1);
password2= MD5Encrypt(password2);
password= MD5Encrypt(password1+password2);
return  password;//返回加密后的字符串
  }
public static string MD5Encrypt (string password)//MD5加密方法
    {
    //实例一个DM5加密引擎
      MD5CryptoServiceProvider md5 = new MD5CryptoServiceProvider();
 //将目标字符串按照指定格式转码
       byte[] InBytes = Encoding.GetEncoding("GB2312").GetBytes(password);
      byte[] OutBytes= md5.ComputeHash(InBytes);//生成加密的byte类型数据
       string OutString = "";
        for (int i = 0; i < OutBytes.Length; i++)//还原字符串
         {
           OutString += OutBytes[i].ToString("x2");
         }
return OutString;//返回加密后的字符串
```

(5)生成数字签名保证信息内容不被篡改。每个发布的信息系统都需要生成一个数字签名，服务器后台定期检查已经发布的信息是否与其对应的数字签名相吻合，如果不吻合，就自动撤销已经发布的信息，并报告给管理员。生成数字签名的方法可以参照用户密码加密的MD5算法代码。

3 结束语

所调研的县政府已经选择了本文提出的建议和方法对其门户网站进行整改。首先是从社会招聘了一名计算机专业有网络维护工作经验的管理人员，该管理人员通过对网站实际状况的分析，已经制定出一套适合该网站系统运行的机房管理条例。机房也已经按照这套管理条例有序进行。其次，管理人员也将数据库数据加密的整改方案反馈给开发组，开发组已经将网站系统修改完毕。通过测试，网站访问速度没有滞后，安全性已经明显提高。总体来说，该网站管理员选择本文提出的这几个方法较好地解决了数据库存在的安全隐患。数据库安全运行是一项动态的系统工程，网站管理者不但要根据自身的实际情况有选择性地运用本文提出的数据库安全设计方法，同时还应注意系统的其它安全问题，只有这样才能确保网站的正常运行。

参考文献：

[1] 周菁.政府门户网站的定位与规划设计[J].电脑知识与技术，2006(11)：100.

[2] 陈江.对网站数据库安全保障的若干思考[J].计算机光盘软件与应用，2012(5)：133-134.

[3] 耿燕.网站开发中数据库安全问题分析[J].科技创新导报，2012(11)：36.

[4] 包冉.ASP.NET网站建设中的数据加密技术解析[J].辽宁师专学报，2010，12(1)：51.

[5] 朱伟，叶文胜.中小企业电子商务数据库安全分析[J].黄冈职业技术学院学报，2006，8(1)：92-94.

(责任编辑：尹 闯)