数据库服务器是什么:数据库是Web服务器的命脉

数据库是Web服务器命脉对于Web站点正常运行起着至关重要作用但是数据库在Web结合存在着诸多安全隐患它往往攻击者入侵Web入口如何来加固Web数据库呢?我们就以当前使用比较广泛Access和MSSQL数据库为例说是如何加强Web数据库安全性

1、Access数据库防下载

数据库被下载这对Web来说几乎是毁灭性攻击者从中可以获取包括管理员帐户及密码等在内敏感信息然后实施进步攻击可被下载数据库主要是Access数据库采用这种数据库Web站点不在少数防止Access数据库下载可以从以下几个方面入手

(1).数据库改名

数据库改名包括两部分首先将其改成比较生僻名称建议名字足够长并使用某些特殊以防被攻击者猜中另外将mdb后缀改为asp以防数据库被下载当然数据库改名后数据库连接配置文件也要进行修改(图1)

(2).改变数据库路径

站点系统都有默认数据库路径由于安全意识淡薄部署Web站点时有很多人不去修改数据库路径因而攻击者很容易地猜到该站点数据库路径

更改数据库路径大家可以在站点目录下创建比较生僻目录然后将数据库文件拷贝到该目录中当然更改数据库路径后需要修改站点系统数据库连接文件般asp站点系统数据库连接文件是conn.asp打开该文件后然后根据实际情况进行修改使得其跟当前数据库路径相致(图2)

(3).设置好目录权限

要设置好数据库目录访问权限原则是权限最小化以防止非正常访问Web是通过IIS用户运行我们只要给IIS用户读取和写入权限然后通过“IIS管理器”把这个目录脚本执行权限去掉防止入侵者在该目录中通过上传获得webshell了(图3)

(4).添加mdb扩展映射

IIS对于不能解析文件类型就会弹出下载对话框让用户下载我们可以通过在IIS管理器中添加对mdb扩展映射防止数据库被下载其设置思路方法是:打开IIS管理器定位到相应Web站点右键选择“属性”然后依次点击“主目录→配置→映射”在“应用扩展”里面添加.mdb文件应用解析至于用于解析它可执行文件大家可以自己进行选择只要让攻击者无法访问数据库文件就可以了(图4)

(5).数据库改造

思路是将数据库后缀名(.mdb)修改为.asp然后在数据库中加上个NotDownLoad表以防数据库被下载具体操作思路方法如下:

首先新建个.asp文件(notdown.asp)其代码如下:

```
db="DataShop.asp" '这里改成你数据库地址这是相对根目录地址
 conn=server.createobject("Adodb.Connection")
connstr="Provider=Microsoft.Jet.OLEDB.4.0;Data Source="&Server.MapPath(db)
```

```
conn.open connstr

conn.execute("create table notdownload(notdown oleobject)")

 rs=server.createobject("adodb.record")

sql="select * from notdownload"

rs.open sql,conn,1,3

rs.add

rs("notdown").appendchunk(chrB(asc("<")) & chrB(asc("%")))

rs.update

rs.close

 rs=nothing

conn.close

 conn=nothing
```

然后在服务器端运行notdown.asp这样在数据库添加了包含notdown字段notdownload数据表即可防止数据库下载notdown有个值是"< %",asp运行是因缺少"% >"关闭标记而拒绝访问下载当然会失败(图5)

2、MSSQL数据库防注入

MSSQL数据库是大中型Web站点常采用数据库对于SQL数据最大威胁是注入攻击者通过注入来SQL语句

执行系统命令因此其危险性更大个注入点有可能造成整个Web服务器沦陷防MSSQL注入可以从下面几个方面入手

(1).慎重选择建站系统

通过站点系统建立个Web站点是非常容易但是某些站点系统代码编写不够严谨考虑不周变量过滤不严等使得可被攻击者利用因此选择款安全站点系统是至关重要当然没有百分的百安全站点系统管理员如果懂代码话可以进行检测分析看看是否有漏洞另外可以扮演入侵者进行入侵检测最后及时打补丁也是非常重要

(2).最小权限连接数据库

Web站点连接数据库都是通过相应帐户进行连接在这些帐户中SA是权限最大也是最危险数据库不要用SA帐户使用SA帐户连接数据库对服务器来说就是场灾难般来说可以使用DB_OWNER权限帐户连接数据库如果可以正常运行使用public用户最安全设置成dbo权限连接数据库的后入侵者基本就只能通过猜解用户名和密码或者是差异备份来获得webshell了对于前者我们可以通过加密和修改管理后台默认登陆地址来防御对于差异备份我们知道它条件是有备份权限并且要知道web目录这样被攻击可能性大大地降低(图6)

(3).删除危险存储过程

MSSQL数据库系统集成了较多存储过程这些命令集方便了我们操作当然也为攻击者入侵Web提供了便利因此我们要根据需要删除某些在Web中用不到并且可被攻击者利用才存储过程比如xp_regread和xp_dirtree这两个存储过程可被攻击者用来读取注册表信息和列目录我们可以删除另外xp_cmdshell可被用来执行DOS命令比如建立系统帐户等等是非常危险sp_makwebtask过程可以读取SQL SELECT命令所得到结果到表格形式HTML文件中这些比较危险可被攻击者利用存储过程我们可以删除比如删除xp_cmdshell可以执行“exec master..sp_dropextendedproc xp_cmdshell”其它类似(图7)

(4).修改页误导攻击者

SQL注入入侵是根据IIS给出ASP提示信息来入侵如果我们把IIS设置成不管出什么样ASP只给出种提示信息即http 500那么攻击者就无法获得敏感信息实施入侵了打开IIS管理器选择相应Web站点打开其站点属性窗口在“自定义”选项卡下选择“500:100”点击“编辑”打开“编辑自定义属性”窗口消息类型选择“文件”然后通过浏览定位到自己构造页比如“c:\test.htm”然后确定即可(图8)

整理总结:防下载、防注入这是从Web安全角度出发实施非常规措施在常态下我们定要做好Web数据库备份这才是最基本相信做好了这两方面工作才能未雨绸缪让数据库更好地为Web服务

2009-2-12 5:28:25
疯狂代码 http://www.crazycoder.cn/