 数据库被挂马我相信很多人都碰到过。在这里，我讲下我处理的方法。 第一步：为现有数据库做好备份。 第二步：执行如下ASP文件，这样就可以去掉数据库当中的JS木马： 注：conn.asp自己去写了。 ’ 这里放入JS木马内容：请记得改为自己数据库中的JS木马内容。 gt. amp.".gt.gt."amp. "gt.gt.:" ’ 显示表名Set rs=Server.CreateObject("ADODB.Recordset") sql="0select * from ["amp."]" rs.open sql,conn,1,3 For i=0 to rs.fields.count-1 ’ 遍历表中字段If int(rs(i).Type)=129 or int(rs(i).Type)=130 or int(rs(i).Type)=200 or int(rs(i).Type)=201 or int(rs(i).Type)=202 or int(rs(i).Type)=203 Then ’ 只处理字段类型为字符型的字段 conn.execute("0update ["amp."] set "amp." =replace(cast("amp." as varchar(8000)), ’ 这里放入JS木马内容 ’ , ’ ’)") response.write rs(i).name amp.rs(i).Type lt.brgt. 如果数据库表很多的话，上面的遍历数据库结构未执行完就被IIS给停止了。在这时候可以在： If rstSchema("TABLE_TYPE")="TABLE" Then 当中适当加入k值的范围，如： If rstSchema("TABLE_TYPE")="TABLE" klt.20 Then 这样的话就一次只操作9个表。 第三步： 根据数据库JS注入的特性(会包括lt./scriptlt.lt.script")gt.0 or Instr(LCase(Request.Form(F_Post)),"gt.")gt.0) and Instr(LCase(Request.Form(F_Post)),"http://")gt.0 Then Cheack_Sqljs=True Exit For End If Next End If If Request.QueryStringgt."" Then ’ QueryString提交时的检测For

Each F_Get In Request.QueryString If (Instr(LCase(Request.Form(F_Get)),"lt.lt./scriptlt.lt.lt.lt.Script Language=JavaScriptlt./Script&gt." Response.End() End If 编辑特别推荐: WinXP不能访问Windows7共享文件 诊断:电脑中毒后的一些表现 Windows7的新快速键 100Test 下载频道开通，各类考试题目直接下载。详细请访问 www.100test.com