ASP＋Access的安全隐患及对策access教程 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/181/2021_2022_ASP_EF_BC_8BAcce_c97_181036.htm ASP＋Access解决方案的主要安全隐患来自Access数据库的安全性，其次在于ASP网页设计过程中的安全漏洞。 1.Access数据库的存储隐患 在ASP＋Access应用系统中，如果获得或者猜到Access数据库的存储路径和数据库名，则该数据库就可以被下载到本地。例如：对于网上书店的Access数据库，人们一般命名为book.mdb、store.mdb等，而存储的路径一般为“ URL/database ”或干脆放在根目录（“ URL/ ”）下。这样，只要在浏览器地址栏中敲入地址：“ URL/database/store.mdb ”，就可以轻易地把store.mdb下载到本地的机器中。 2.Access数据库的解密隐患 由于Access数据库的加密机制非常简单，所以即使数据库设置了密码，解密也很容易。该数据库系统通过将用户输入的密码与某一固定密钥进行异或来形成一个加密串，并将其存储在＊.mdb文件中从地址“ &H42 ”开始的区域内。由于异或操作的特点是“ 经过两次异或就恢复原值 ”，因此，用这一密钥与＊.mdb文件中的加密串进行第二次异或操作，就可以轻松地得到Access数据库的密码。基于这种原理，可以很容易地编制出解密程序。 由此可见，无论是否设置了数据库密码，只要数据库被下载，其信息就没有任何安全性可言了。 3.源代码的安全隐患 由于ASP程序采用的是非编译性语言，这大大降低了程序源代码的安全性。任何人只要进入站点，就可以获得源代码，从而造成ASP应用程序源代码的泄露。 4.程序设计中的安全隐患 ASP代码利用表单（form）实现与用户交互的功

能，而相应的内容会反映在浏览器的地址栏中，如果不采用适当的安全措施，只要记下这些内容，就可以绕过验证直接进入某一页面。例如在浏览器中敲入“……page.asp?x=1”，即可不经过表单页面直接进入满足“x=1”条件的页面。因此，在设计验证或注册页面时，必须采取特殊措施来避免此类问题的发生。 提高数据库的安全性 由于Access数据库加密机制过于简单，因此，如何有效地防止Access数据库被下载,就成了提高ASP＋Access解决方案安全性的重中之重。 1.非常规命名法 防止数据库被找到的简便方法是为Access数据库文件起一个复杂的非常规名字，并把它存放在多层目录下。例如，对于网上书店的数据库文件，不要简单地命名为“book.mdb”或“store.mdb”，而是要起个非常规的名字，例如：faq19jhsvzbal.mdb，再把它放在如./akkjj16t/kjhgb661/acd/avccx55 之类的深层目录下。这样，对于一些通过猜的方式得到Access数据库文件名的非法访问方法起到了有效的阻止作用。 2.使用ODBC数据源 在ASP程序设计中，应尽量使用ODBC数据源，不要把数据库名直接写在程序中，否则，数据库名将随ASP源代码的失密而一同失密。例如： DBPath = Server.MapPath(“./akkjj16t/kjhgb661/acd/avccx55/faq19jhsvzbal.mdb ”) conn.Open “driver={Microsoft Access Driver (＊.mdb)}.dbq=” & DBPath 可见，即使数据库名字起得再怪异，隐藏的目录再深，ASP源代码失密后，数据库也很容易被下载下来。如果使用ODBC数据源，就不会存在这样的问题了： conn.open “ODBC－DSN名”