

推荐：A Acce 数据库安全隐患及对策 PDF转换可能丢失图片或格式，建议阅读原文

[https://www.100test.com/kao\\_ti2020/251/2021\\_2022\\_\\_E6\\_8E\\_A8\\_E8\\_8D\\_90\\_EF\\_BC\\_9AA\\_c97\\_251794.htm](https://www.100test.com/kao_ti2020/251/2021_2022__E6_8E_A8_E8_8D_90_EF_BC_9AA_c97_251794.htm)

随着Internet的发展，Web技术日新月异。继通用网关接口(CGI)之后，“ASP” (Active Server Pages)作为一种典型的服务器端网页设计技术，被广泛地应用在网上银行、电子商务、搜索引擎等各种互联网应用中。同时Access数据库作为微软推出的以标准JET为引擎的桌面型数据库系统，由于具有操作简单、界面友好等特点，具有较大的用户群体。因此ASP Access成为许多中小型网上应用系统的首选方案。但ASP Access解决方案在为我们带来便捷的同时，也带来了不容忽视的安全问题。ASP Access的安全隐患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。

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](http://www.100test.com)