利用i tr()函数防止SQL注入攻击 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_88_A9_E7_94_A8i_tr_c98_454842.htm 学asp也有一段时间了，这几天一直在写自己的程序，也遇到了好多问题，我就不得不得考虑到一些现在的漏洞，比如，‘ 或 and 1=1等等的一些漏洞！别的先不管，今天我就来说说如何堵这个漏洞！ 记得看了一篇文章（不记得什么时候看的了），他用到了instr这个函数，具体的应该是这样的。 If instr(Request("id")," ")>0 or instr(Request("id"),"")>0 then response.redirect "index.asp" 当然，也也可以在then后面写你想要的！这个先不管！ 让我们先来学习instr这个函数吧： 语法 InStr([start, ]string1, string2[, compare]) InStr 函数的语法有以下参数： 参数 描述 start 可选。数值表达式，用于设置每次搜索的开始位置。如果省略，将从第一个字符的位置开始搜索。如果 start 包含 Null，则会出现错误。如果已指定 compare，则必须要有 start 参数。 String1 必选。接受搜索的字符串表达式。 String2 必选。要搜索的字符串表达式。 Compare 可选。指示在计算子字符串时使用的比较类型的数值。有关数值，请参阅"设置"部分。如果省略，将执行二进制比较。 compare 参数可以有以下值： 常数 值 描述 vbBinaryCompare 0 执行二进制比较。 vbTextCompare 1 执行文本比较。 [返回值] InStr 函数返回以下值： 如果 InStr 返回 string1 为零长度 0 string1 为 Null Null string2 为零长度 start string2 为 Null Null string2 没有找到 0 在 string1 中找到 string2 找到匹配字符串的位置 start > Len(string2) 0 下面的示例利用 InStr 搜索字符串: Dim SearchString,

SearchChar, MyPos SearchString ="XXpXXpXXPXXP" 要在其中搜索的字符串。 SearchChar = "P" 搜索 "P"。 MyPos = Instr(4, SearchString, SearchChar, 1) 文本比较从第四个字符开始返回 6。 MyPos = Instr(1, SearchString, SearchChar, 0) 二进制比较从第1个字符开始返回 9。 MyPos = Instr(SearchString, SearchChar) 返回 9。 缺省为二进制比较(最后一个参数省略)。 MyPos = Instr(1, SearchString, "W") 二进制比较从第1个字符开始返回 0 (没有找到 "W")。 注意 InStrB 函数使用包含在字符串中的字节数据，所以 InStrB 返回的不是一个字符串在另一个字符串中第一次出现的字符位置，而是字节位置。 总结概括：instr的功能就是： 返回字符或字符串在另一个字符串中第一次出现的位置，好了，让我们在看看哪个代码： if instr(Request("id")," ")>0 or instr(Request("id"),"")>0 then 含义：比较 字符（空格）与字符（）在request（"id"）中的具体位置（进行二进制制比较），假如找到了（空格）与（‘ ）字符，那么就是then 后的语句！ 现在大家理解这个含义了吧！ 当我看第一眼的时候我就说，假如在asp？Id=90加上字符（；或,）等等一些字符时不是造样出错吗？（是，回答的肯定的：） 估计又有人说，那我会在if instr(Request("id")," ")>0 or instr(Request("id"),"")>0 then 语句中在加些字符，比如改为：if instr(Request("id")," ")>0 or instr(Request("id"),"")>0 or instr(Request("id"),".")>0 or instr(Request("id"),", ")>0 then 等等，你还可以在后面加，呵呵！（这个好啊！不过比较烂：） 是，这样加上后，确实能桃过一些所谓的黑客们的手的！ 其实没必要，大家忘了instr(Request("id")," ")>0这句话了吗，他还和（空格）比较了啊！只要有这句话，那些所谓的黑客们的

，and 1 = 1 不就没用了吗？ 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