新手入门：防范SQL注入攻击的新办法 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/259/2021_2022__E6_96_B0_E6_89_8B_E5_85_A5_E9_c98_259356.htm 近段时间由于修改一个ASP程序(有SQL注入漏洞)，在网上找了很多相关的一些防范办法，都不近人意，所以我将现在网上的一些方法综合改良了一下，写出这个ASP函数，供大家参考。以下是引用片段：Function SafeRequest(ParaName) Dim ParaValue ParaValue=Request(ParaName) if IsNumeric(ParaValue) = True then SafeRequest=ParaValue exit Function elseIf Instr(LCase(ParaValue),"0select ") > 0 or Instr(LCase(ParaValue),"insert ") > 0 or Instr(LCase(ParaValue),"0delete from") > 0 or Instr(LCase(ParaValue),"count(") > 0 or Instr(LCase(ParaValue),"0drop table") > 0 or Instr(LCase(ParaValue),"0update ") > 0 or Instr(LCase(ParaValue),"truncate ") > 0 or Instr(LCase(ParaValue),"asc(") > 0 or Instr(LCase(ParaValue),"mid(") > 0 or Instr(LCase(ParaValue),"char(") > 0 or Instr(LCase(ParaValue),"xp_cmdshell") > 0 or Instr(LCase(ParaValue),"exec master") > 0 or Instr(LCase(ParaValue),"net localgroup administrators") > 0 or Instr(LCase(ParaValue)," and ") > 0 or Instr(LCase(ParaValue),"net user") > 0 or Instr(LCase(ParaValue)," or ") > 0 then Response.Write "" Response.Write "alert(非法的请求!)." 发现SQL

注入攻击提示信息 Response.Write "location.href=http://dev.yesky.com/." 发现SQL注入攻击转跳网址 Response.Write "" Response.end else SafeRequest=ParaValue End If End function 使用SafeRequest函数替换你的Request