

封神台----尤里的复仇I-第三章：这个后台能识别登录者...

原创

向那风 于 2019-07-18 15:20:31 发布 1575 收藏 3

分类专栏: [渗透学习 靶场练习](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: https://blog.csdn.net/x_yhy/article/details/96430600

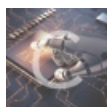
版权



[渗透学习](#) 同时被 2 个专栏收录

10 篇文章 0 订阅

订阅专栏



[靶场练习](#)

7 篇文章 0 订阅

订阅专栏

根据提示, 真正的后台地址为admin123, 输入上一关的账号、密码进去。

后台 59.63.200.79:8004/admin123/default.asp

企业网站管理系统

对不起, 为了系统安全, 不允许从外部链接地址访问本系统的后台管理页面。

访问者的Curl(host)为:
http://59.63.200.79:81/admin123/sysadmin_view.asp
访问者的Comeurl(referer)为:
http://59.63.200.79:8004/admin123/default.asp

以下为本功能主要代码片断, 提供给同学们分析:

```
<%  
dim ComeUrl, cUrl, AdminName  
ComeUrl=lcase(trim(request.ServerVariables("HTTP_REFERER")))   
if ComeUrl="" then   
response.write "<br><p align=center><font color='red'>  
对不起, 为了系统安全, 不允许直接输入地址访问本系统的后台管理页面。</font></p>"   
response.end   
else   
cUrl=trim("http://" & Request.ServerVariables("SERVER_NAME"))   
if mid(ComeUrl,len(cUrl)+1,1)=":" then   
cUrl=cUrl & ":" & Request.ServerVariables("SERVER_PORT")   
end if   
cUrl=lcase(cUrl & request.ServerVariables("SCRIPT_NAME"))   
if lcase(left(ComeUrl,instrrev(ComeUrl,"/")))<>lcase(left(cUrl,instrrev(cUrl,"/"))) then   
response.write "<br><p align=center><font color='red'>  
对不起, 为了系统安全, 不允许从外部链接地址访问本系统的后台管理页面。</font></p>"   
response.end   
end if   
end if   
end if
```

将referer的值传递给Comeurl

判断如果referer为空, 返回不允许访问管理页面

将Host的内容赋予Curl

将Curl与Comeurl进行对比 也就是将host和referer进行对比

https://blog.csdn.net/x_yhy

分析代码:

1. 从请求头中拿到Referer，并赋值给ComeUrl。
2. 判断ComeUrl是否为空，若是空，则表明是直接输入地址访问。本题不允许
3. ComeUrl不为空，读取Host，并在前面拼接 http:// 赋值给cUrl，如果ComeUrl有 ":",表明有端口号，在为cUrl 加上端口号。
4. 最后判断cUrl和ComeUrl中从右边看，第一次出现"/"的位置，返回的是从左数的下标。比如：

```
str="123456.78.9.txt"
response.write(InstrRev(str, "."))           #输出: 12
```

5. 就是说Referer的ip、port和host的ip、port必须一样。

