ctf实战 封神台的靶场 第三关通关记录

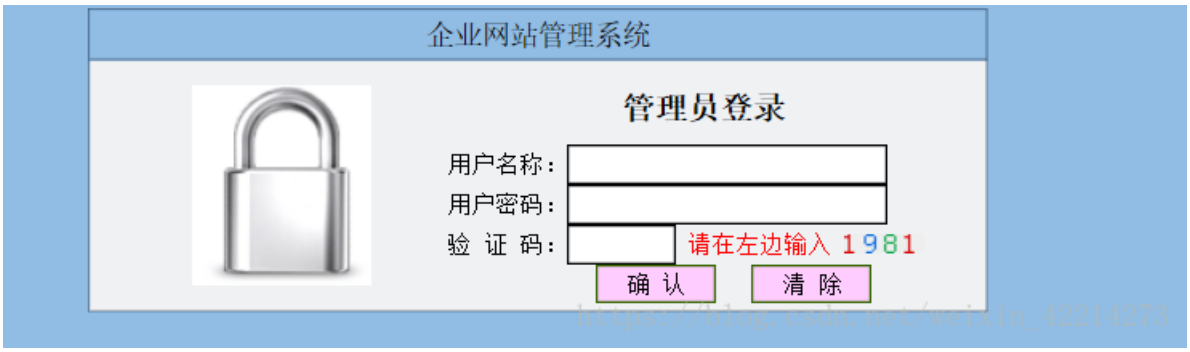
转载

weixin_30498807 于 2019-05-28 00:57:00 发布 1546 收藏 1
原文链接：http://www.cnblogs.com/jackzz/p/10934727.html

封神台第三关

根据题目可能要用burp进行抓包，点击传送门进入题目主页

之前题目说的扫描到新的后台地址admin123 在网址后加入admin123 进入新的后台管理页面



根据第二关得到的用户和密码进行登录 进入后得到这样一个页面

抓包结果如

根据代码分析只需要修改host和referer的ip地址

修改以后结果还是进不去

```
<%
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
```

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

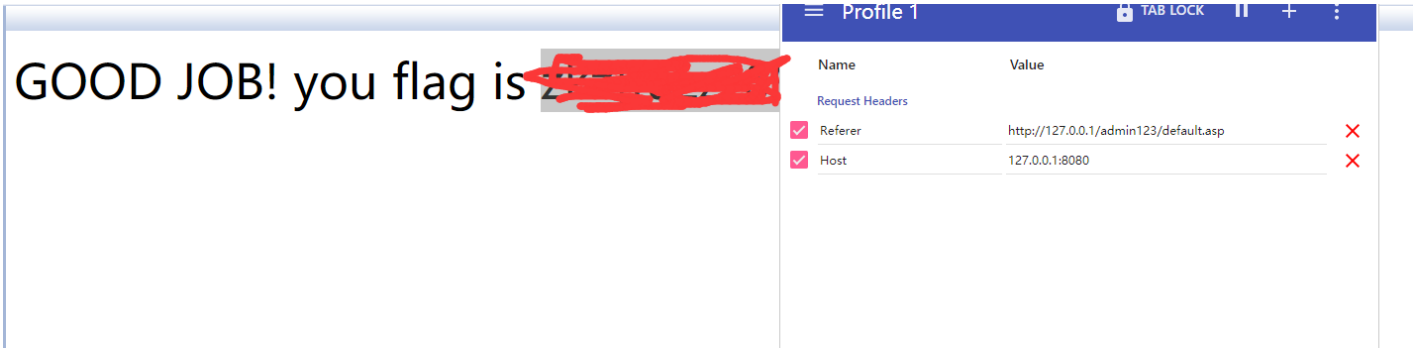
将Curl与Comeurl进行对比也就是将host和referer进行对比

分析一下问题 打开Firefox的网路检测 F12 发现可能用的是8080端口进行通信

用Modify Headers 修改host和refere

host改为：127.0.0.1：8080

refere改为http://127.0.0.1/admin123/default.asp



成功弹出flag值

转载于:https://www.cnblogs.com/jackzz/p/10934727.html