mbp 封神台靶场 三 （笔记）

原创

qq_43558415 于 2020-02-09 18:10:55 发布 773 收藏

分类专栏： 封神台靶场

本文链接：https://blog.csdn.net/qq_43558415/article/details/104237912

打开链接，根据提示进行操作

Tips:

1、提交flag格式为zkz{……}
2、绕过后台登录识别
3、burpsuite

第二关拿到密码后，虽然在admin路径中成功登录后台，但那竟然是一个假后台！
不过没关系，尤里也遇到过不少假后台，他拿出了后台扫描工具…… 扫描到了另一个后台登陆地址(admin123)
然而登陆上去后……尤里竟然发现这个管理系统能识别登录者的身份……
传送门

备用传送门

由上可知后台登陆地址为admin123,需要准备的工具是大名鼎鼎的burp（抓包软件）根据提示登录admin123的后台。

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://117.167.136.245:81/admin123/sysadmin_view.asp
访问者的Comeurl(referer)为：
http://117.167.136.245:10181/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
```

将referer的值传递给Comeurl

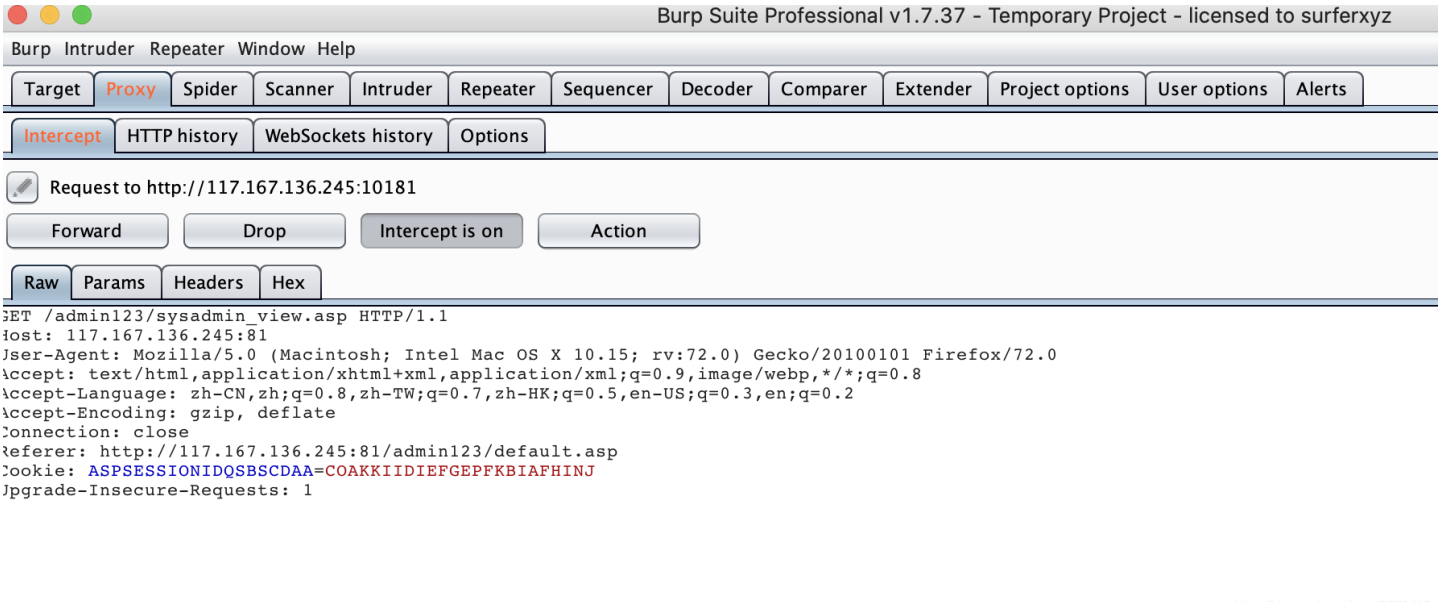
判断如果referer为空，返回不允许访问管理页面

将Host的内容赋于Curl

将Curl与Comeurl进行对比也就是将host和referer进行对比

```
end if
```

需要显示的是sysadmin_view.asp，但返回的是default.asp，区别是端口号不同。接着发现这里有代码片段，其中还有提示，根据理解是要curl和comeurl进行比对，也就是host和refer进行对比，打开burp看看包。对访问sysadmin_view.asp的端口号修改为81即可拿到flag。



总结：在做这个时候需要使用抓包软件，抓包软件通过设置代理对通过的数据包进行抓取，推荐一个代理插件foxyproxy（ssr代理也可以用到，切换特别方便）本关主要看代码理解和抓包修改，在复现的时候没遇到什么问题。