

网络安全1-3

原创

小开心007 于 2020-04-05 10:40:25 发布 163 收藏

分类专栏: [Web安全](#) 文章标签: [web](#)

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/wanglinyp/article/details/105323277>

版权



[Web安全](#) 专栏收录该内容

3 篇文章 0 订阅

订阅专栏

声明: 练习仅可在靶场, 不可用于非法操作。

封神台靶场练习之↓

第三章 这个后台能识别登录者... 【抓包和CSRF伪造】

先看一下题目要求:

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.....

按照要求进入题目靶场:



随便点开一条新闻动态:



根据题目要求，管理员登录端口为admin123,因此，修改url如下：

```
http://59.63.200.79:8004/admin123
```

回车，出现了管理员的登录界面



在上一篇文章中，我们获取了管理员账号密码（admin: welcome），在这里输入进行尝试

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

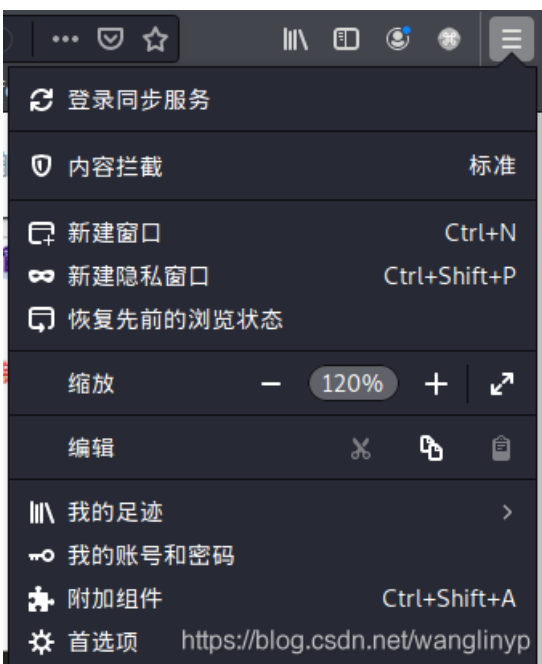
<https://blog.csdn.net/wanglinyp>

靶场检测出了异常登陆，为降低难度，靶场给出了登录功能片段，分析给出的功能段，可以知道要想成功访问，访问者的两个url必须一致。因此，下一步需要做的就是修改访问信息，这就需要借助burpsuite截取报文段（建议安装Kali，里边集成很多常用工具）

重新回到登录页面（访问前清除一下缓存），访问：

http://59.63.200.79:8004/admin123

在浏览器中配置代理服务器，ip设置为：127.0.0.1，端口号设置为：8080，以火狐浏览器为例：



打开首选项->常规，滑到最低端->网络设置

配置访问互联网的代理服务器

- 不使用代理服务器 (Y)
- 自动检测此网络的代理设置 (W)
- 使用系统代理设置 (U)
- 手动代理配置 (M)

HTTP 代理 (X) 端口 (P)

为所有协议使用相同代理服务器 (S)

<https://blog.csdn.net/wanglinyp>

打开burpsuite->proxy->Options->Add

Add a new proxy listener

Binding Request handling Certificate

? These settings control how Burp binds the proxy listener.

Bind to port:

Bind to address: Loopback only
 All interfaces
 Specific address:

<https://blog.csdn.net/wanglinyp>

保存后，回到登录页面，输入账号密码，确定，这时候看一下burpsuite->proxy->intercept,网站信息已经被捕获

Intercept HTTP history WebSockets history Options

Request to http://59.63.200.79:8004

Forward Drop Intercept is on Action

Raw Params Headers Hex

```
1 POST /admin123/Admin_ChkLogin.asp HTTP/1.1
2 Host: 59.63.200.79:8004
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Referer: http://59.63.200.79:8004/admin123/Login.asp
8 Content-Type: application/x-www-form-urlencoded
9 Content-Length: 80
10 Connection: close
11 Cookie: ASPSESSIONIDASTAQTSC=NLGLKLMHAHOJAJCLHHMFGPAPO
12 Upgrade-Insecure-Requests: 1
13
14 UserName=admin&Password=welcome&CheckCode=9655&Submit=+%C8%B7%28%23160%3B%C8%CF%0
```

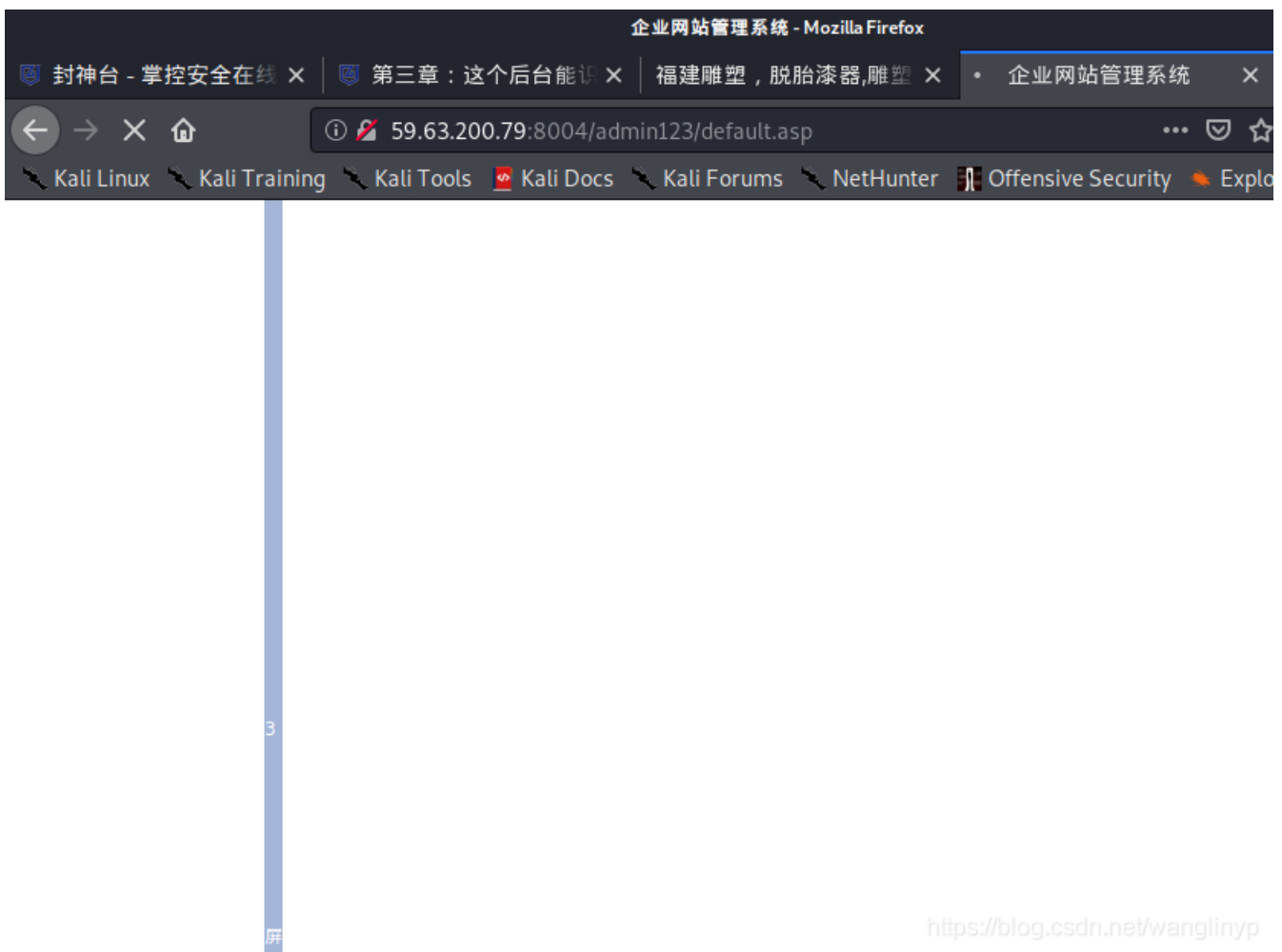
我们点击forward提交当前页面数据

```
1 GET /admin123/default.asp HTTP/1.1
2 Host: 59.63.200.79:8004
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Referer: http://59.63.200.79:8004/admin123/Login.asp
8 Connection: close
9 Cookie: ASPSESSIONIDASTAQTSC=NLGLKLMHAHOJAJCLHHMFGPAPO
10 Upgrade-Insecure-Requests: 1
```

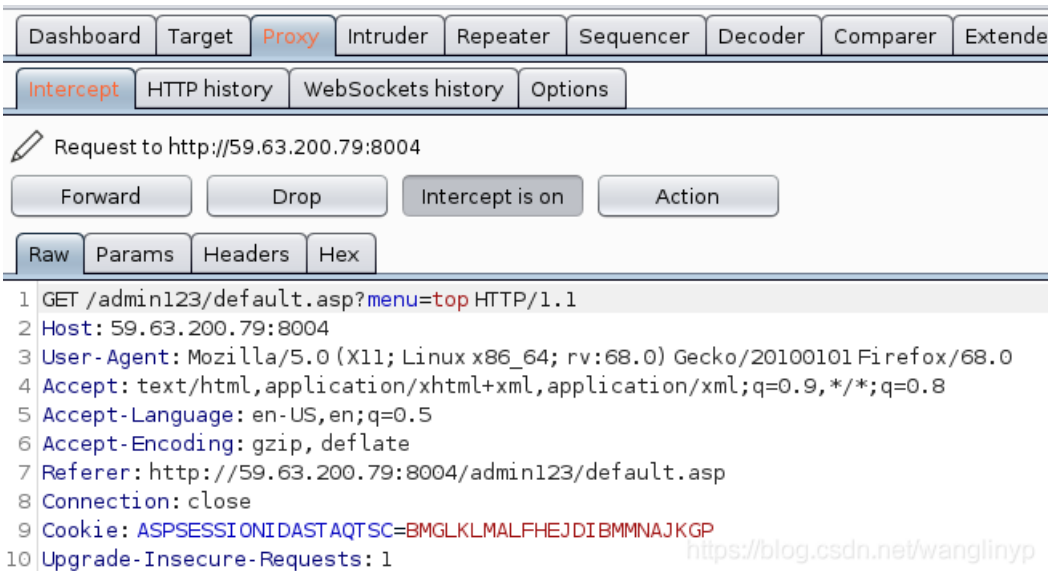
可以看到页面默认跳转到default.asp,继续点击forward



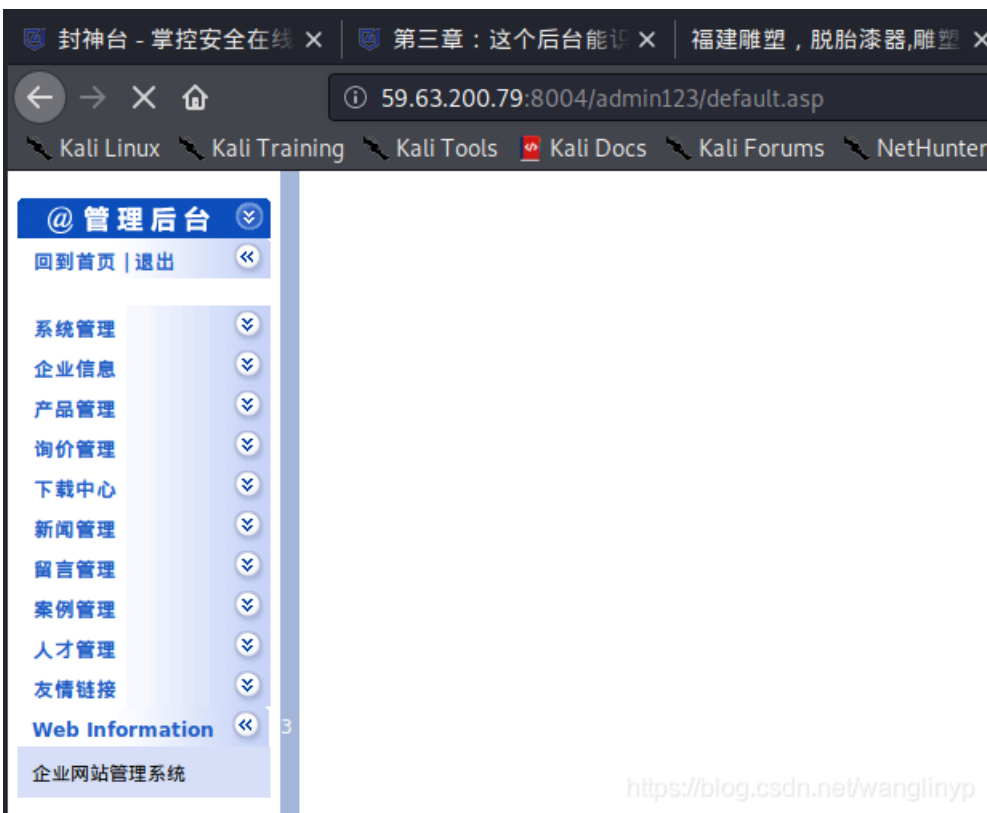
可以看到，页面开始请求访问LeftTree.asp回到浏览器：



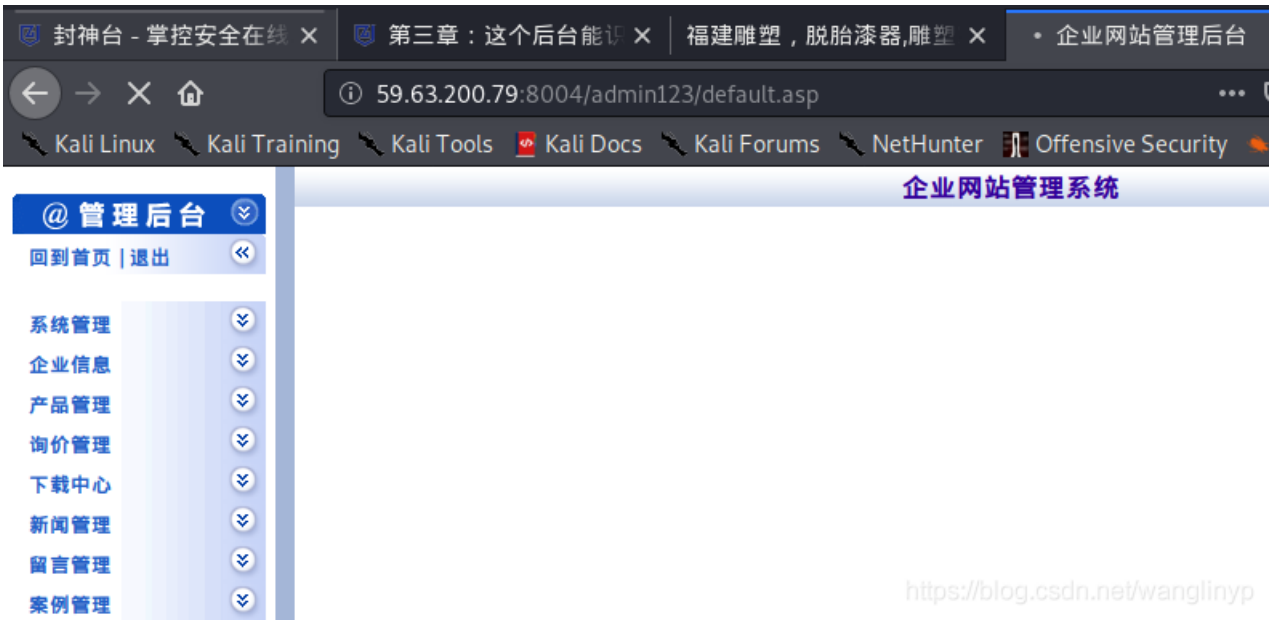
出现网站页面且title 发生变化，这时，在burpsuite端继续点击forward：



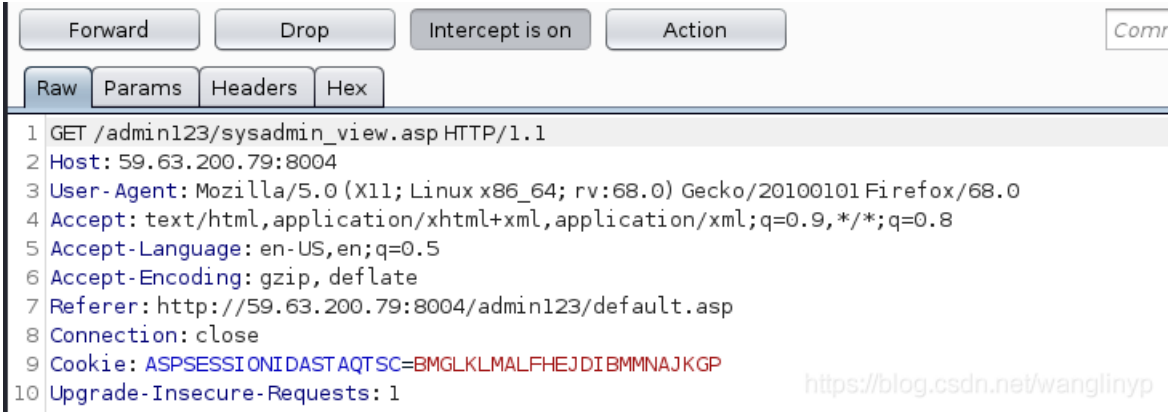
回到浏览器，出现了页面信息，页面下一步将要请求default.asp?menu=top



回到burpsuite继续点击forward,让浏览器去访问default.asp?menu=top, 浏览器页面如下:



burpsuite捕获到下一条要提交的信息:



可以看到浏览器请求sysadmin_view.asp, 继续点击forward, 让浏览器请求sysadmin_view.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/wanglinyp>

页面继续回到出错页面，页面提示中说明，服务器会对请求信息进行拼接判断，要求我们的访问Comurl(referer)与Curl (host)一致（端口）。因此，重新进行上面的操作，在最后一步访问请求时，在burpsuite修改请求信息：

Forward Drop Intercept is on Action

Raw Params Headers Hex

```

1 GET /admin123/sysadmin_view.asp HTTP/1.1
2 Host: 59.63.200.79:8004 8004修改为81
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Referer: http://59.63.200.79:8004/admin123/default.asp
8 Connection: close 8004修改为81
9 Cookie: ASPSESSIONIDASTAQTSC=BMGLKLMALFHEJDI BMMNAJKGP
10 Upgrade-Insecure-Requests: 1

```

<https://blog.csdn.net/wanglinyp>

点击提交：

企业网站管理系统

GOOD JOB! you flag is

成功获取网址后台。