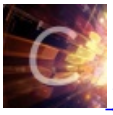
网络安全1-3

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



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：

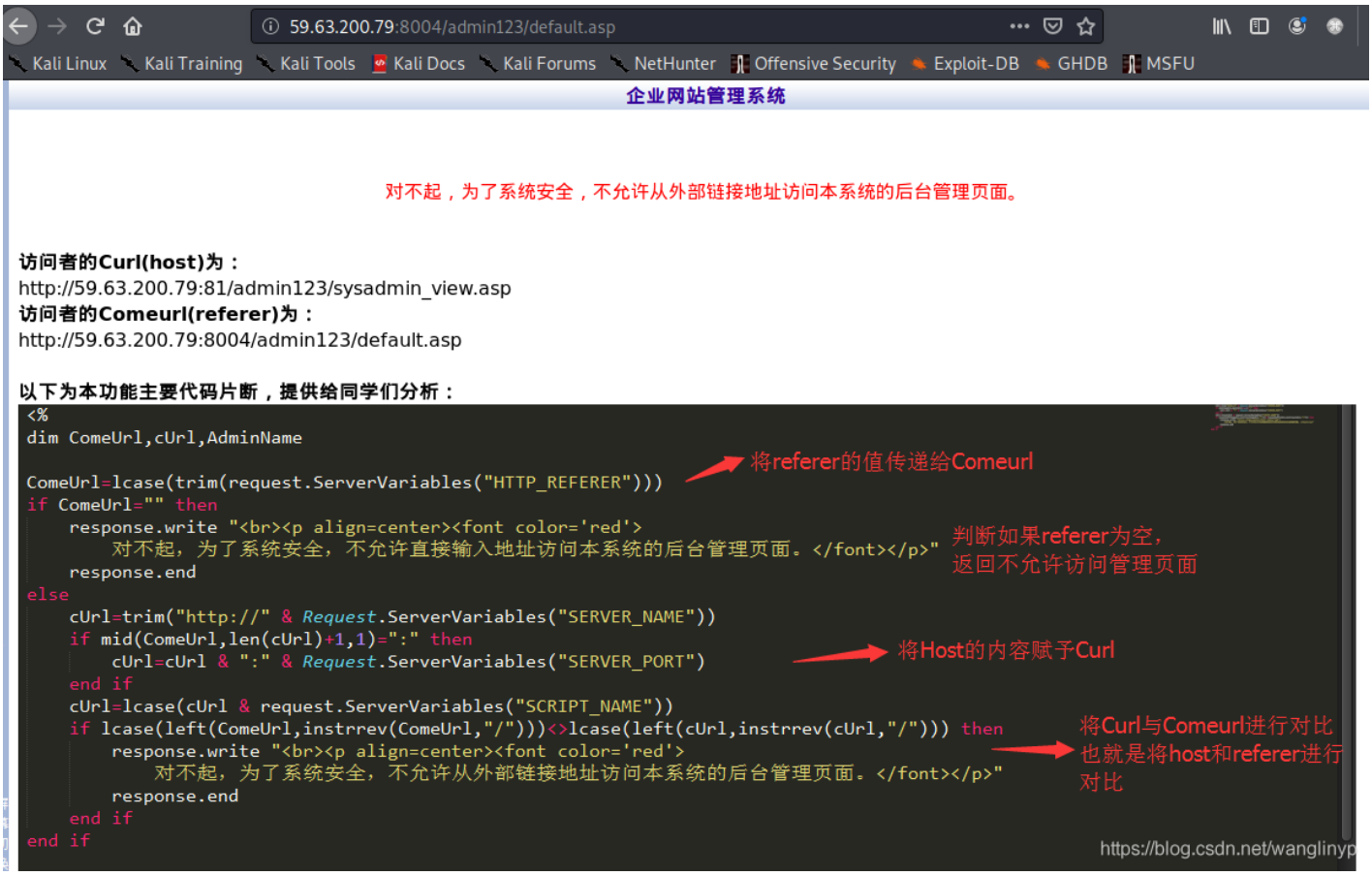
随便点开一条新闻动态：

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

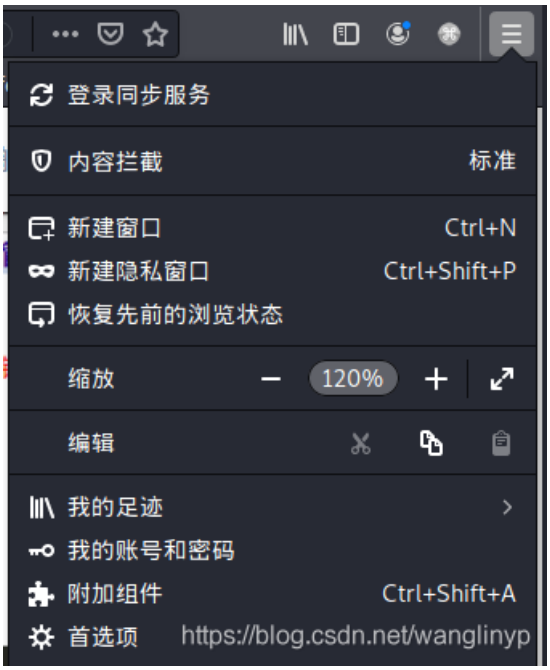


靶场检测出了异常登陆，为降低难度，靶场给出了登录功能片段，分析给出的功能段，可以知道要想成功访问，访问者的两个url必须一致。因此，下一步需要做的就是修改访问信息，这就需要借助burpsuite截取报文段（建议安装Kali，里边集成很多常用工具）

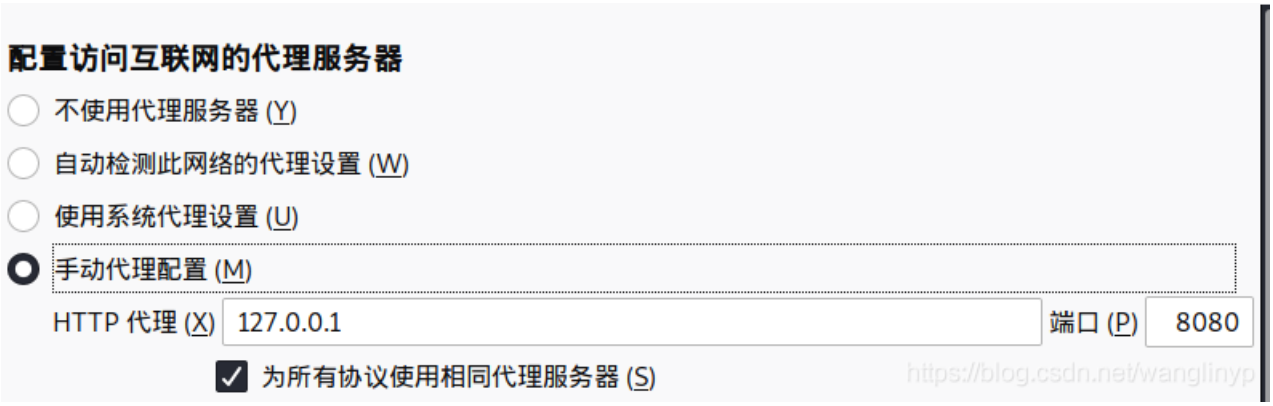
重新回到登录页面（访问前清除一下缓存），访问：

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

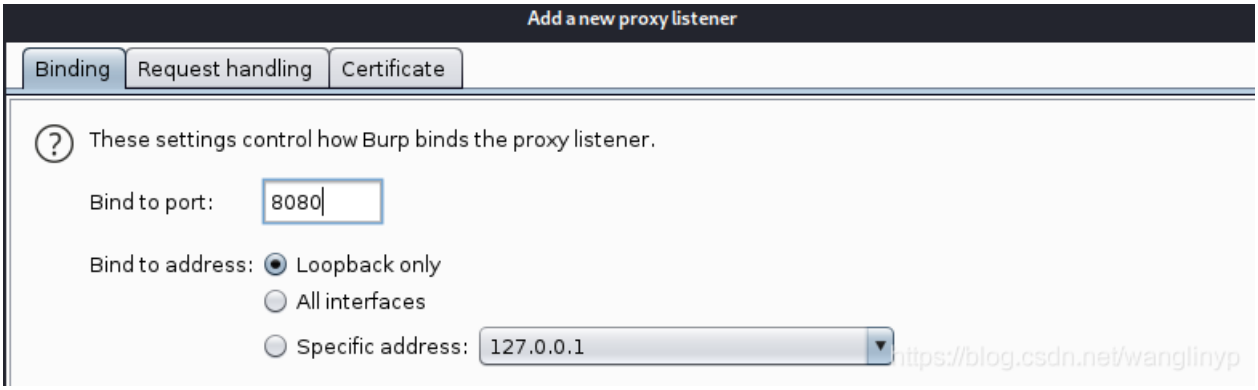
在浏览器中配置代理服务器，ip设置为：127.0.0.1，端口号设置为：8080，以火狐浏览器为例：



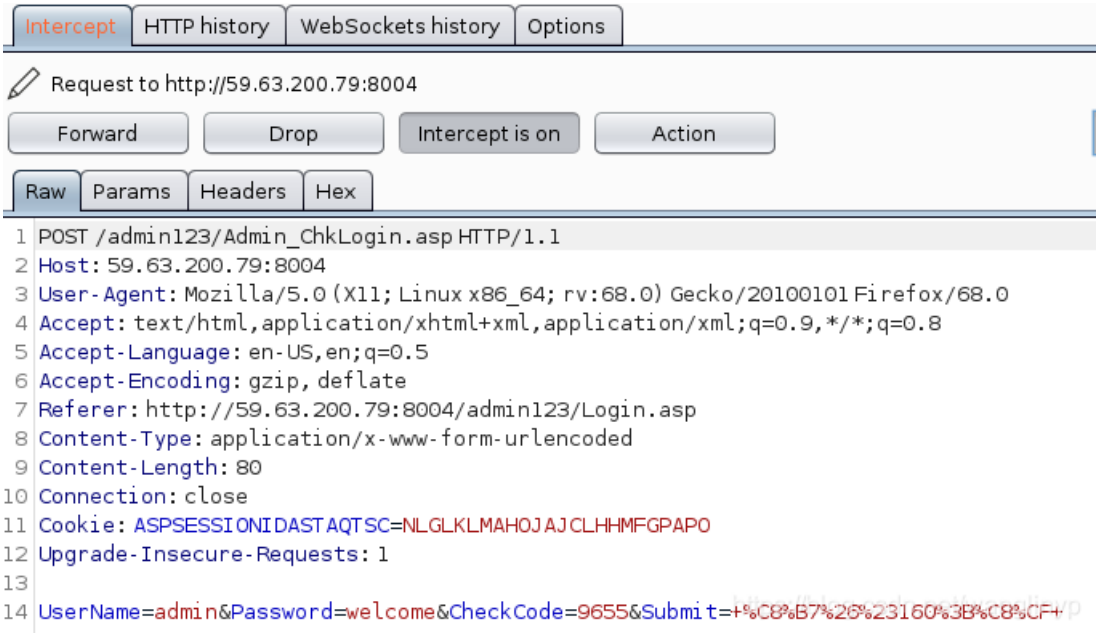
打开首选项->常规，滑到最低端->网络设置



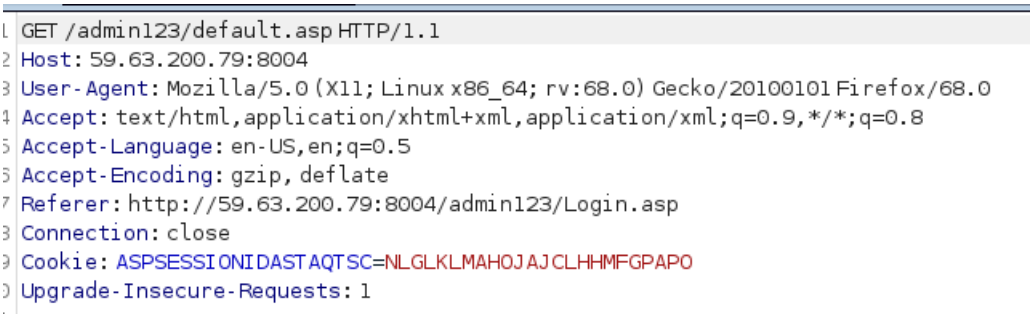
打开burpsuite->proxy->Options->Add



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

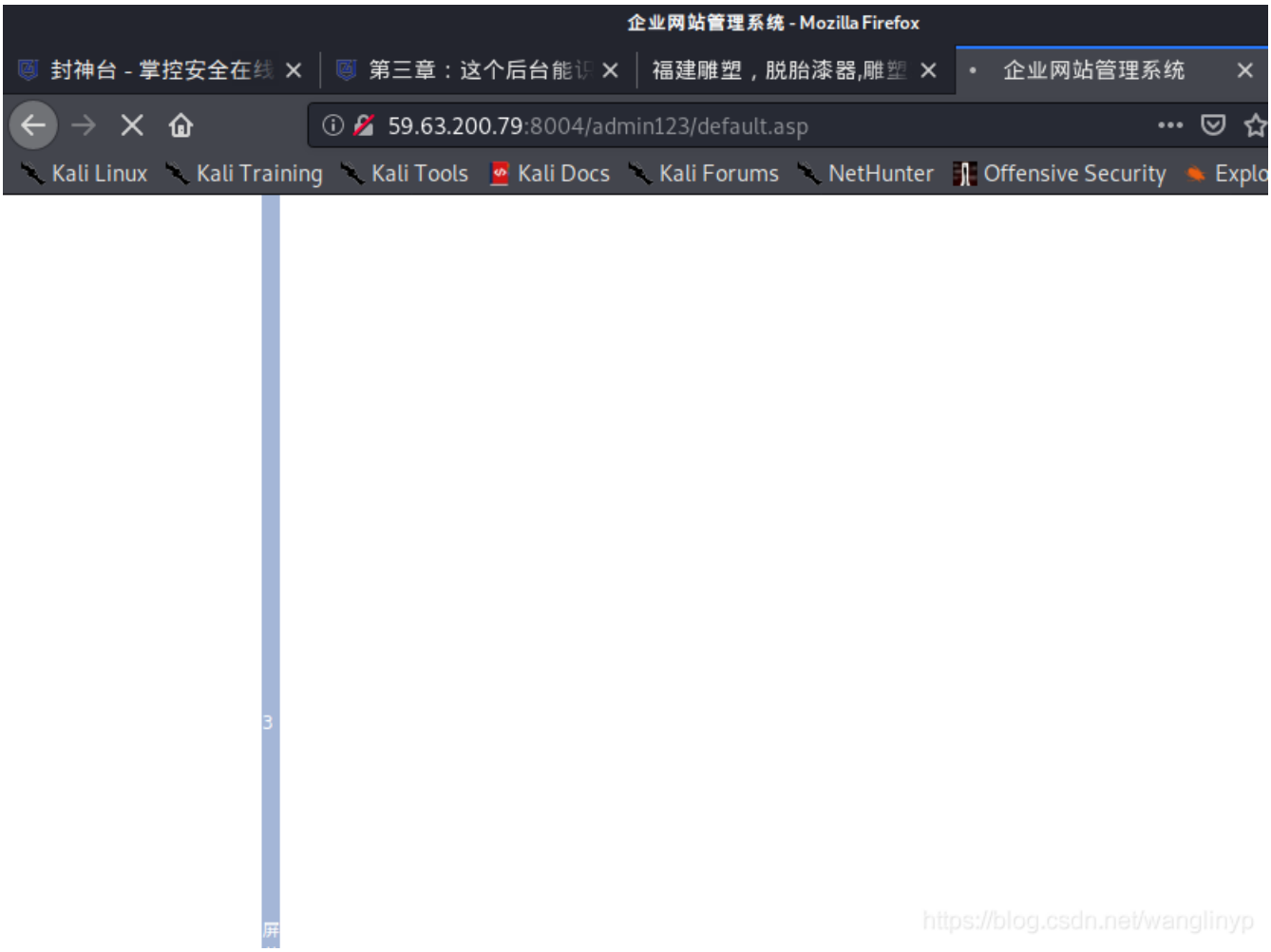


我们点击forward提交当前页面数据

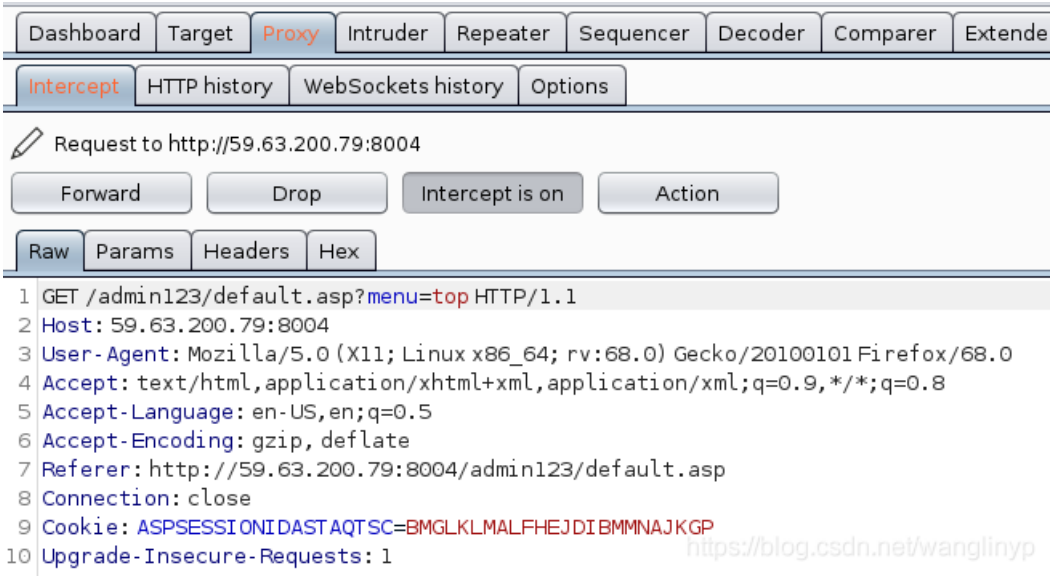


可以看到页面默认跳转到default.asp,继续点击forward

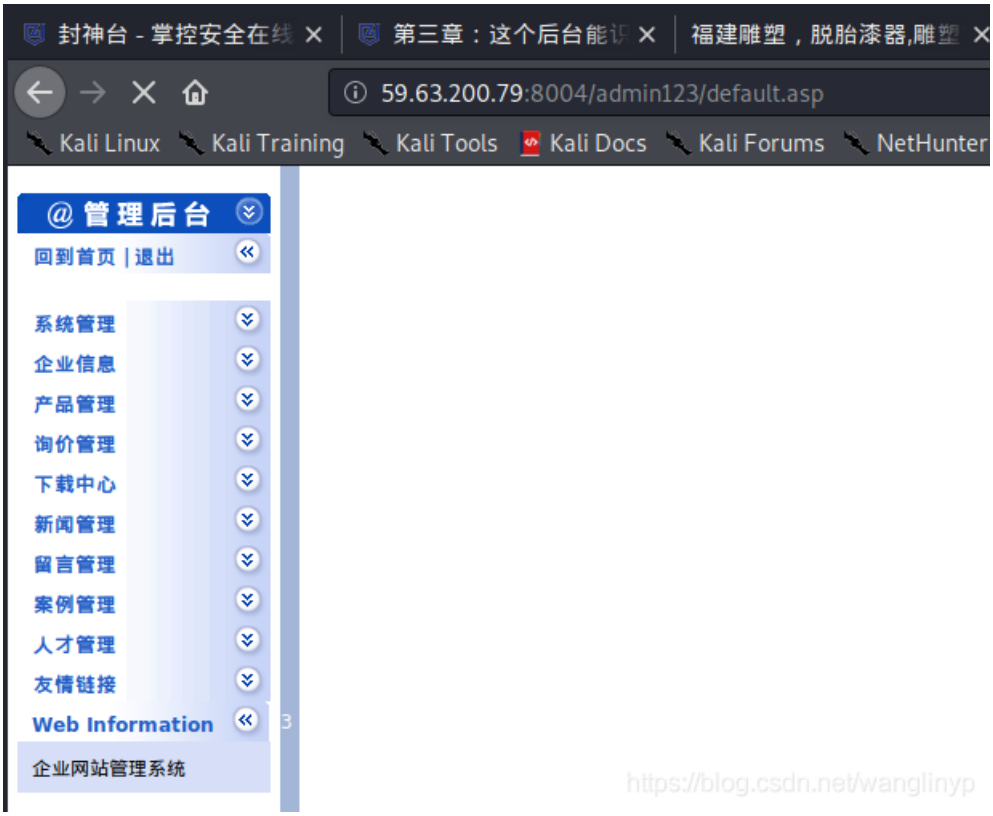
可以看到，页面开始请求访问LeftTree.asp回到浏览器：



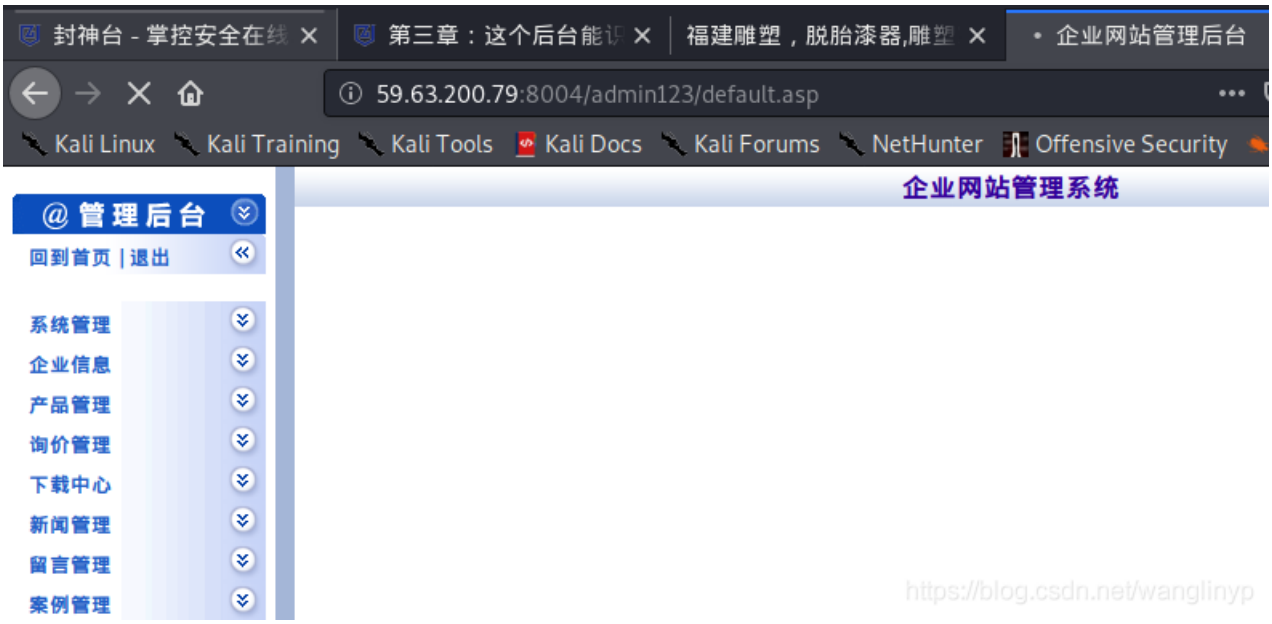
出现网站页面且title 发生变化，这时，在burpsuite端继续点击forward：



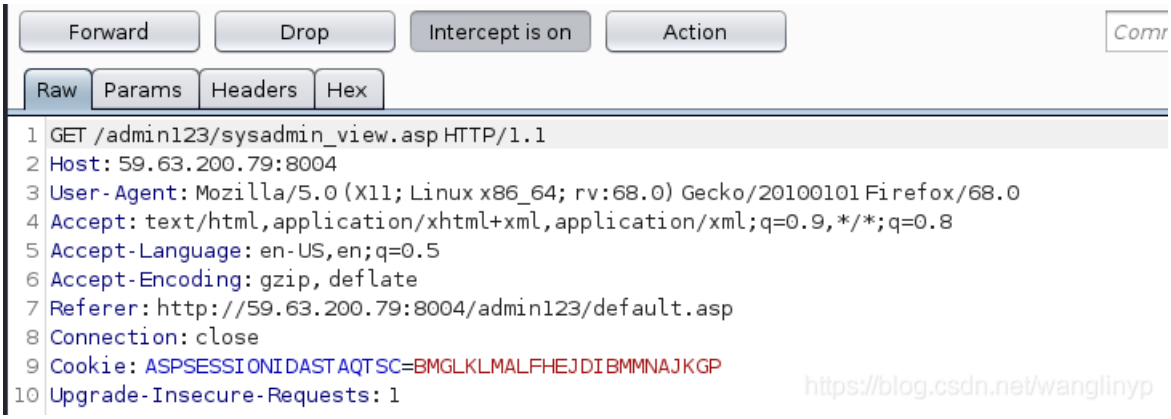
回到浏览器，出现了页面信息，页面下一步将要请求default.asp?menu=top



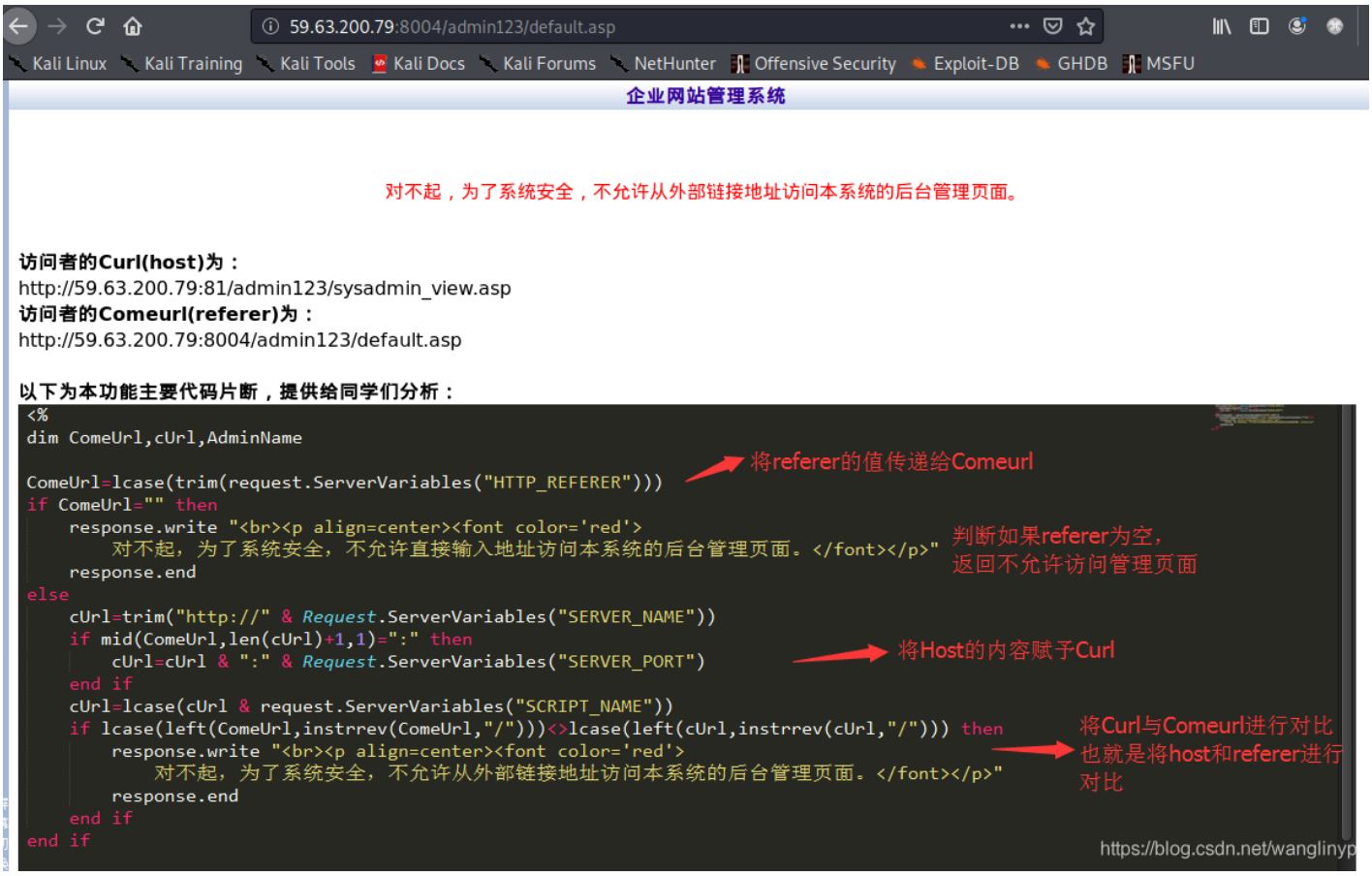
回到burpsuite继续点击forward,让浏览器去访问default.asp?menu=top，l浏览器页面如下：



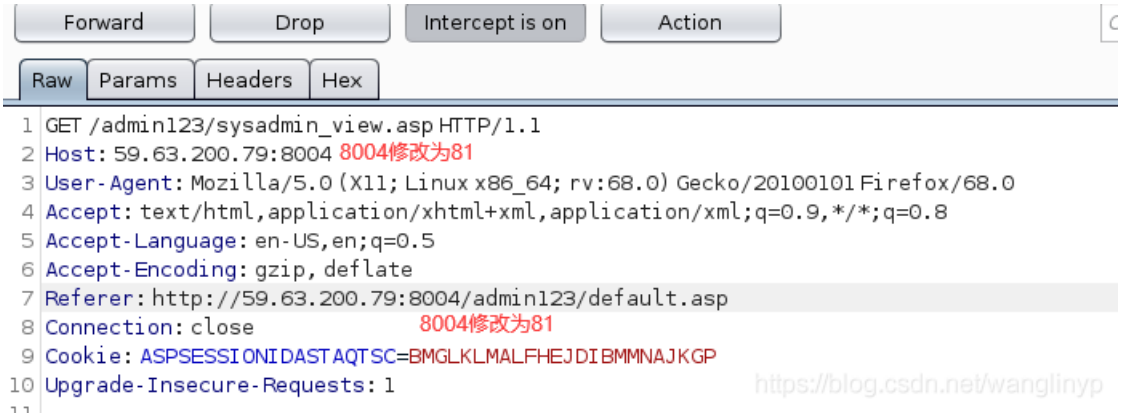
burpsuite捕获到下一条要提交的信息：



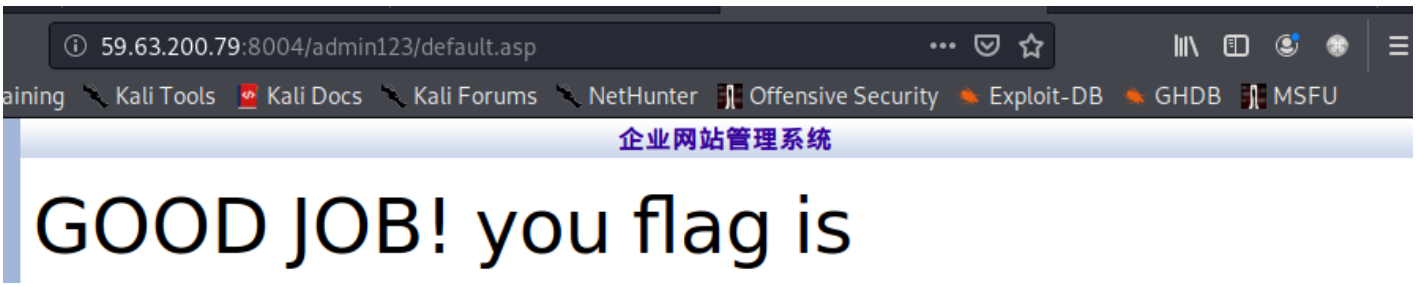
可以看到浏览器请求sysadmin_view.asp，继续点击forward，让浏览器请求sysadmin_view.asp



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：



点击提交：



成功获取网址后台。