

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

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

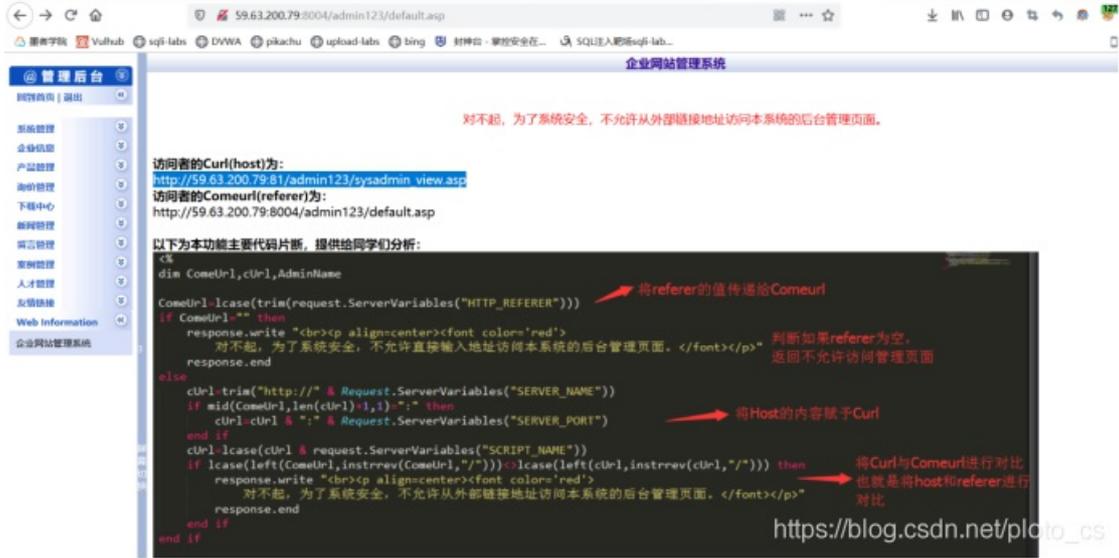
ID	地址	HTTP响应
33	http://59.63.200.79:8004/index.asp	200
34	http://59.63.200.79:8004/8010/Guide/.....	200
35	http://59.63.200.79:8004/AboutUs.asp	200
36	http://59.63.200.79:8004/admin/southideeditor/popup.asp	200
37	http://59.63.200.79:8004/admin/southideeditor/upload.asp	200
38	http://59.63.200.79:8004/admin123/admin.asp	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

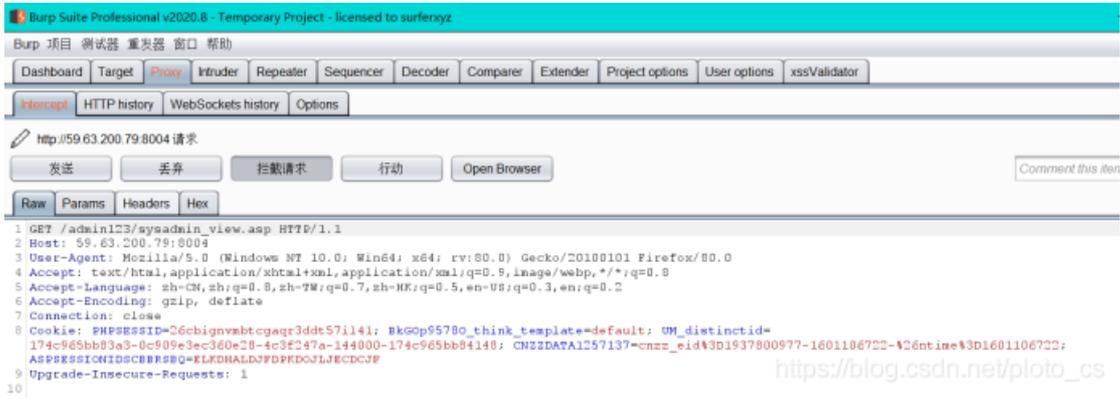


4.分析代码

- 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

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

