

攻防世界 Misc 心仪的公司

原创

==Microsoft== 于 2022-03-12 13:29:37 发布 41 收藏

分类专栏: [Misc](#) 文章标签: [ctf misc](#)

欢迎转载, 请保留作者的链接, 文章会同步更新到微信公众号: 欢迎转载, 请保留作者的链接, 文章会同步更新到个人微信公众号: IT技术分享社区, 个人网站 <https://programmerblog.xyz/>

本文链接: <https://blog.csdn.net/MrTreebook/article/details/123442355>

版权



[Misc 专栏收录该内容](#)

50 篇文章 0 订阅

订阅专栏

攻防世界 Misc 心仪的公司

1.wireshark分析流量包

2.strings命令

1.wireshark分析流量包

No.	Time	Source	Destination	Protocol	Length	Info
2296	9.768650	113.215.6.151	192.168.1.111	HTTP	532	HTTP/1.1 200 OK (text/html)
12863	140.967482	192.168.1.108	192.168.1.111	HTTP	71	HTTP/1.1 200 OK (text/html)
12923	144.004050	192.168.1.108	192.168.1.111	HTTP	71	HTTP/1.1 200 OK (text/html)
13079	151.835067	192.168.1.108	192.168.1.111	HTTP	71	HTTP/1.1 200 OK (text/html)
13237	156.789419	192.168.1.108	192.168.1.111	HTTP	71	HTTP/1.1 200 OK (text/html)
13314	161.964644	192.168.1.111	192.168.1.108	HTTP	789	POST /conf1g.php HTTP/1.1 (application/x-www-form-urlencoded)
13330	161.978150	192.168.1.108	192.168.1.111	HTTP	639	HTTP/1.1 200 OK (JPEG JFIF image)

CSDN @==Microsoft==

```
00 00 00 00 00 00 28 00 4e e0 00 4c 75 01 15 05 c4 ,.01. 00 .LS...
00 ee 71 3b 9c 4e e7 13 b9 ff 00 b9 10 69 1c ec ff .q;.N... ....i...
00 00 63 7f ff d9 66 6c 34 67 3a 7b 66 74 6f 70 5f .c...f14 g:{ftop_
00 49 73 5f 57 61 69 74 69 6e 67 5f 34 5f 79 7d Is_Waiti ng_4_y}
```

- 在搜索栏搜shell
- 看到有一个jpg
- 得到flag

2.strings命令

- 放到ubuntu下

```
strings webshell.pcapng | grep "{"
```

- 这个方法似乎有撞运气的感觉

```
function mssqlinfo(dbname) {  
  !sf{  
  QiJ{  
  fl4g:{ftop_Is_Waiting_4_y}  
  !{6S  
  Je, {d
```

- 轻松获取flag



[创作打卡挑战赛](#) >

[赢取流量/现金/CSDN周边激励大奖](#)