xctf攻防世界 MISC高手进阶区 心仪的公司

原创

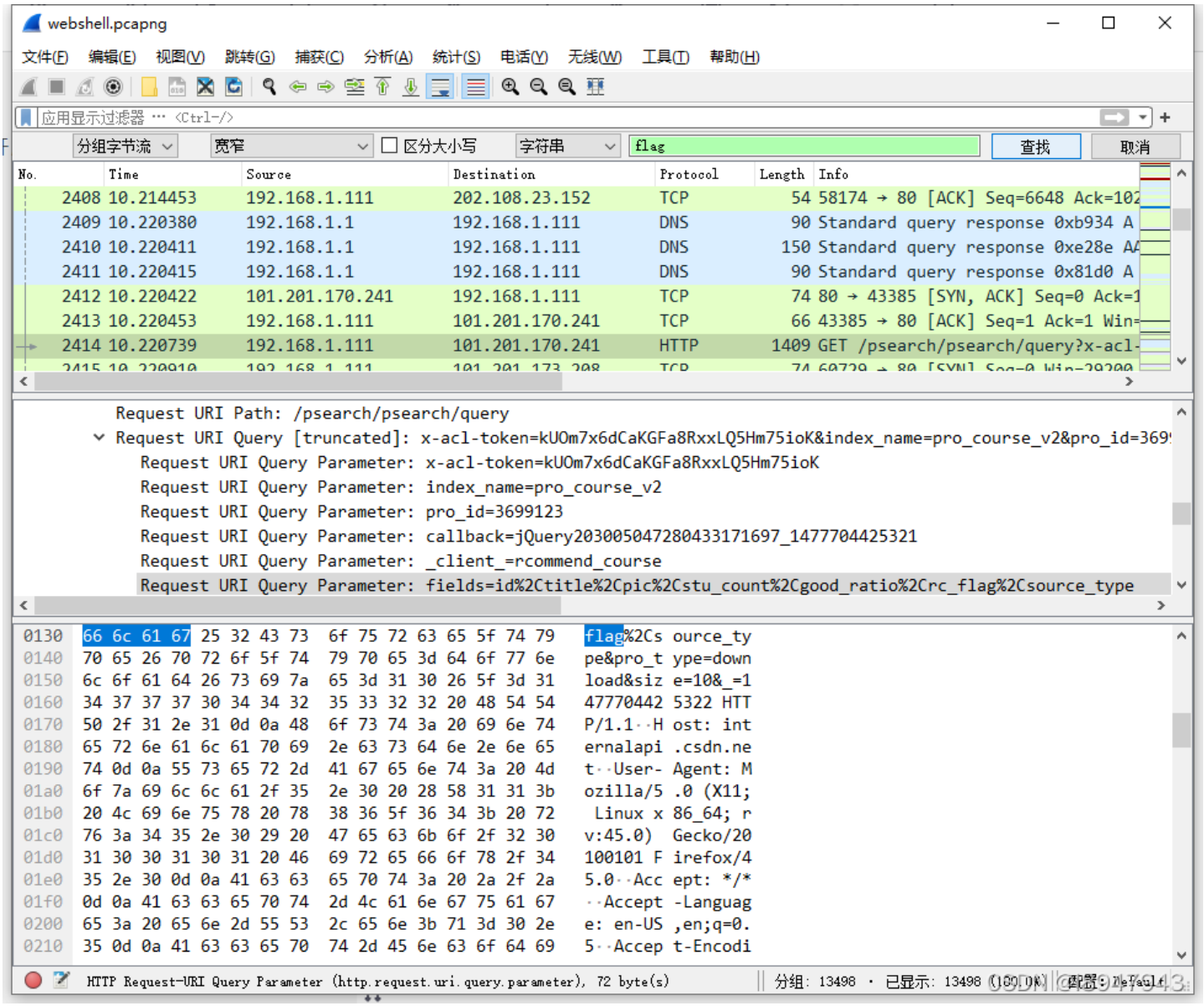
l8947943 于 2022-01-25 21:56:30 发布 10770 收藏

分类专栏： 攻防世界misc之路 文章标签： 安全 misc

本文链接：https://blog.csdn.net/l8947943/article/details/122692571

1. 进入环境，下载附件

给的是一个rar压缩包，里面是个抓包流量文件，使用wireshark打开，如图：

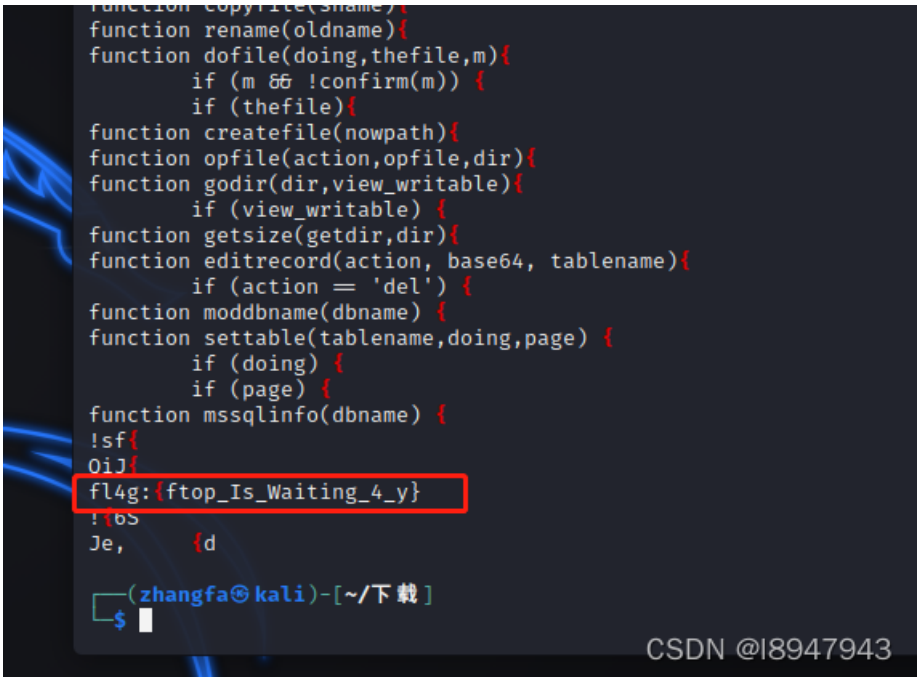


一通关键词搜索后无果

2. 问题分析

扔到kali中，使用strings命令，进行过滤尝试

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



或者使用正则过滤：

```
# 贪婪模式，前置几个字符，{}中字符长度在1到20之间，并且以}符号结尾
strings webshell.pcapng | grep -E '^.*?:{.{1,20}}$'
```

结果如图：

最终答案为：`fl4g:{ftop_Is_Waiting_4_y}`