攻防世界-MISC：embarrass

原创

LY613313 于 2021-11-26 15:18:41 发布 157 收藏

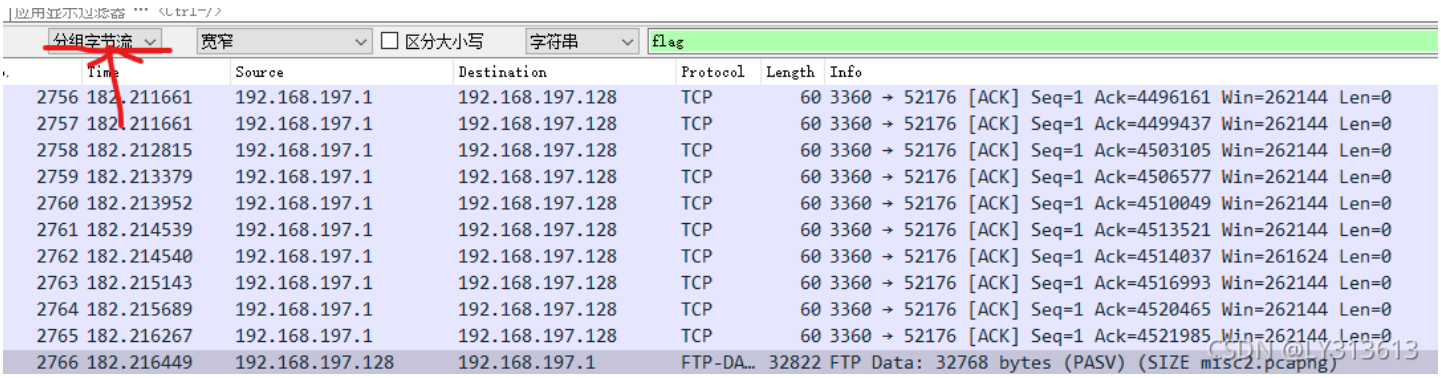
文章标签： 安全

本文链接：https://blog.csdn.net/m0_56161093/article/details/121559955

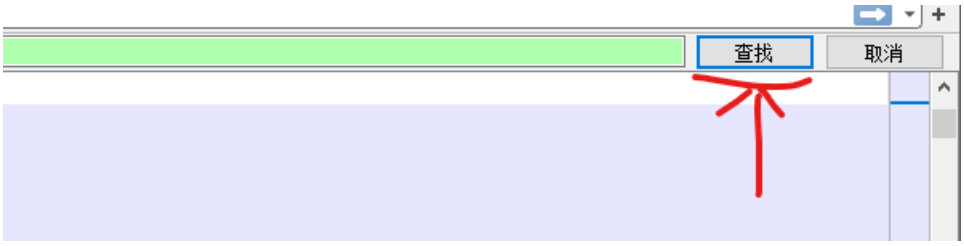
这是攻防世界高手进阶区的第二题，题目如下：

点击下载附件一，得到一个压缩包，解压后得到一个流量包

用wireshake打开，CTRL+F搜索字符串flag,记住要选择分组字节流



点击查找



在点击几次过后即可看到flag（我记我是点了6次）

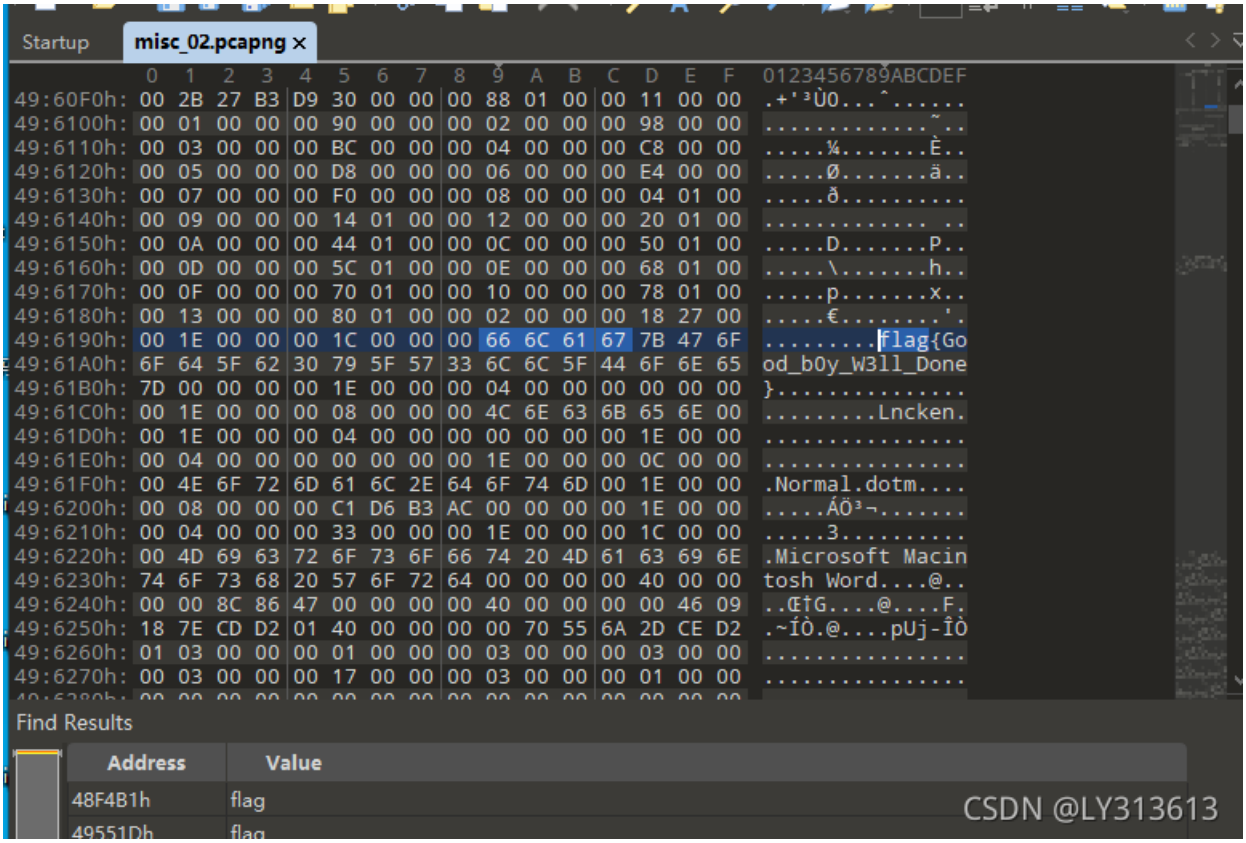
```
[Time since first frame in this TCP stream: 0.724521000 seconds]
[Time since previous frame in this TCP stream: 0.000182000 seconds]
P payload (32768 bytes)
Data (32768 bytes data)
up frame: 1236]
un method: PASV]
00 66 6c 61 67 7b 47 6f  6f 64 5f 62 30 79 5f 57   flag{Go od_b0y_W
33 6c 6c 5f 44 6f 6e 65  7d 00 0c 10 00 00 02 00   3ll_Done }·····
00 00 1e 00 00 00 05 00  00 00 b1 ea cc e2 00 03   ···· ····
00 00 00 01 00 00 00 00  00 00 00 00 00 00 00 00   ···· ····
00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ···· ····
00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ···· ····
```


复制提交成功，如果复制不了，可以先右键，选择将字节复制为16进制+ASCII转储，将其复制到文本文档里面再查找复制。

```
Go od_b0y_W
ne }·····
·· ····
·· ····
·· ····
·· ····
·· ····
·· ····
·· ····
·· ····
·· ····
·· ····
·· ····
·· ····
·· ····
·· ····
·· ····
```


```
flag{Good_b0y_W3ll_Done}
```

提交过后查看一下WP发现其实用16进制编辑器打开直接查找即可，用010editor打开查找flag，直接就可以得到flag（学到了□□□□）



以上就是我对这道题的解法。因本人菜鸡一只，如果有什么不对的地方，实属正常。还请各位大佬予以指正，谢谢！