

# xctf攻防世界 MISC高手进阶区 embarrass

原创

18947943 于 2022-01-17 14:04:56 发布 5532 收藏

分类专栏: [攻防世界misc之路](#) 文章标签: [misc](#)

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/18947943/article/details/122538493>

版权



[攻防世界misc之路](#) 专栏收录该内容

68 篇文章 2 订阅

订阅专栏

## 1. 进入环境, 下载附件

给的是一个pcapng文件, 果断使用wireshark打开, 直接尝试搜索关键词flag试一试, 如图:

The screenshot shows the Wireshark interface with a search for 'flag' in a pcapng file named 'misc\_02.pcapng'. The search results are displayed in the packet list pane, showing a match in the payload of an FTP data packet (No. 2766). The packet details pane shows the FTP data structure, and the packet bytes pane shows the raw data with the search results highlighted.

No.	Time	Source	Destination	Protocol	Length	Info
2761	182.214539	192.168.197.1	192.168.197.128	TCP	60	3360 → 52176 [ACK] Seq=1 Ack=451
2762	182.214540	192.168.197.1	192.168.197.128	TCP	60	3360 → 52176 [ACK] Seq=1 Ack=451
2763	182.215143	192.168.197.1	192.168.197.128	TCP	60	3360 → 52176 [ACK] Seq=1 Ack=451
2764	182.215689	192.168.197.1	192.168.197.128	TCP	60	3360 → 52176 [ACK] Seq=1 Ack=452
2765	182.216267	192.168.197.1	192.168.197.128	TCP	60	3360 → 52176 [ACK] Seq=1 Ack=452
2766	182.216449	192.168.197.128	192.168.197.1	FTP-DA...	32822	FTP Data: 32768 bytes (PASV) (SI
2767	182.216830	192.168.197.1	192.168.197.128	TCP	60	3360 → 52176 [ACK] Seq=1 Ack=452

Packet details for No. 2766:

```
Checksum: 0xbda [unverified]
[Checksum Status: Unverified]
Urgent Pointer: 0
> [Timestamps]
> [SEQ/ACK analysis]
TCP payload (32768 bytes)
FTP Data (32768 bytes data)
[Status: Complete]

08e0  00 66 6c 61 67 7b 47 6f 6f 64 5f 62 30 79 5f 57  ·flag{Go od_b0y_W
08f0  33 6c 6c 5f 44 6f 6e 65 7d 00 0c 10 00 00 02 00  311_Done }.....
0900  00 00 1e 00 00 00 05 00 00 00 b1 ea cc e2 00 03  .....
0910  00 00 00 01 00 00 00 00 00 00 00 00 00 00 00  .....
0920  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
0930  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
0940  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
0950  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
0960  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
0970  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
0980  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
```

??? 这就出来了??? 试了一下, 还特么的真的是。。。人麻了

最终答案为: `flag{Good_b0y_W311_Done}`

## 2. 换个做法玩玩吧，都尝试一下

将文件丢入kali中，输入命令：

```
strings misc_02.pcapng | grep flag
```

结果如图：

```
(zhangfa@kali)-[~/下载]
└─$ strings misc_02.pcapng | grep flag
GET /flag.php HTTP/1.1
GET /flag.doc HTTP/1.1
flag{Good_b0y_W3ll_Done}
flag{Good_b0y_W3ll_Done}
flag{Good_b0y_W3ll_Done}
flag{Good_b0y_W3ll_Done}
<p>Some antivirus programs mistake XAMPP for a virus, typically flagging the
file xampp-manager.exe This is a false positive meaning that the antivirus erroneously
identified it as a virus, when it is not. Before we release each new version of
XAMPP we run it through virus scanning software. At the moment we are using
Kaspersky Online Virus Scanner.
You can also use the online tool Virus Total
for scanning XAMPP or send us an email to security (at) apachefriends (dot)
org if you find any issue.</p>
<tr><td class="e">filter.default_flags</td><td class="v"><i>no value</i></td><td
class="v"><i>no value</i></td></tr>
<tr><td class="e">windows_tracing_flags </td><td class="v">3 03D11@18947943
```