

buuctf被嗅探的流量

原创

lierpang_ 于 2021-04-20 16:49:06 发布 176 收藏

分类专栏: [CTF](#) 文章标签: [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/lixin_1010/article/details/115912769

版权



[CTF 专栏收录该内容](#)

10 篇文章 0 订阅

订阅专栏

被嗅探的流量

下载下来为一个压缩包, 解压缩发现为pcapng文件

名称	大小	压缩后大小	类型	修改时间	CRC32
..			文件夹		
被嗅探的流量.pcapng	211,264	180,629	Wireshark captur...	2015/8/18 10:...	DE606567

使用wireshark打开文件, 发现有一个明显的upload.php

No.	Time	Source	Destination	Protocol	Length	Info
139410	172.16.66.100	172.16.80.120	HTTP	375	POST /upload.php HTTP/1.1 (JPEG JFIF image)	

并且后面提示了有图片文件, 邮件追踪流-TCP流拉到最后发现flag

```
7..s..?.....d\..x..A..P...M...'. (.lou.#s>..
C.*..j..E.....?.....z... (...o....?Y_.00....EW..
Q..9...R3.....M.....V.....x.S._x.Z=...xI.....
.....H/.a.....j<9Zu0..T.#OKG..E[...
a.....?...J.....flag{da73d88936010da1eeeb36e945ec4b97}.
-----WebKitFormBoundaryIeRPZp2QAo2zkI2U--
HTTP/1.0 500 Internal Server Error
Date: Tue, 18 Aug 2015 10:40:44 GMT
Server: Apache
X-Powered-By: PHP/5.3.3
```

https://blog.csdn.net/lixin_1010