

攻防世界MISC进阶之easycap

原创

[harry_c](#) 于 2019-08-16 22:45:41 发布 2416 收藏

分类专栏: [攻防世界](#) 文章标签: [攻防世界](#) [MISC进阶](#) [easycap](#) [攻防世界进阶](#) [渗透](#)

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/harry_c/article/details/99686762

版权



[攻防世界](#) 专栏收录该内容

29 篇文章 2 订阅

订阅专栏

攻防世界MISC进阶之easycap

第一步: [分析](#)

第二步: [实操](#)

第三步: [答案](#)

第一步: 分析

难度系数: 2星

题目来源: bsidessf-ctf-2017

题目描述: 你能从截取的数据包中得到flag吗?

题目场景: 暂无

题目附件: 附件1

给的信息是截取的数据包, 在再结合附件的文件, 我们知道需要使用数据流分析软件进行查看,

第二步: 实操

使用winshark进行查看

右键追踪TCP流

第三步: 答案

至此最终的flag为: FLAG:385b87afc8671dee07550290d16a8071