




CTF 逆向crackme

原创

[yoyo_573](#)  于 2020-08-15 20:19:32 发布  391  收藏 1

分类专栏: [ctf](#)

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/yoyo_573/article/details/108027334

版权



[ctf](#) 专栏收录该内容

8 篇文章 0 订阅

订阅专栏

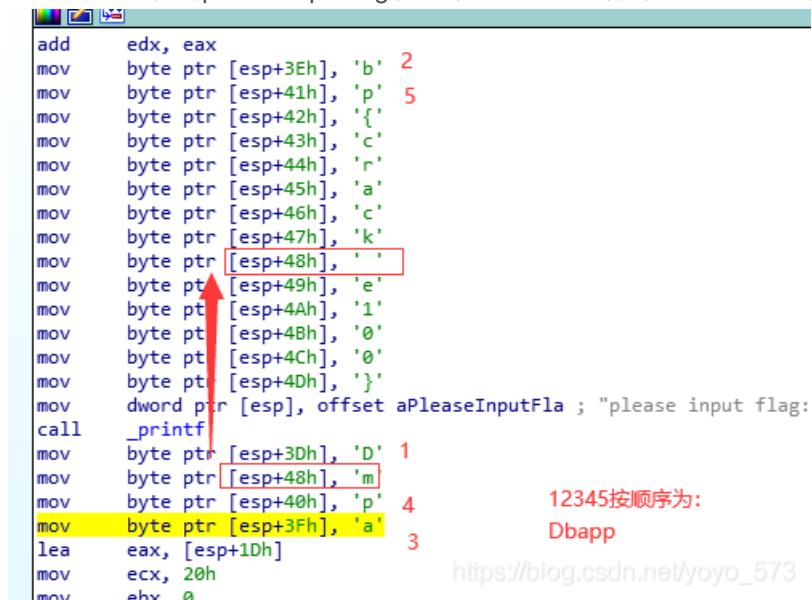
CTF 逆向crackme

通过IDA进行编译，查看MAIN函数按F5生成伪代码



然后右键转成字符。这时候已经差不多能知道flag了

验证下结果，我们可以查看IDA-view-A，找到please in put flag:关键字。我们可以看到ESP入口地址依次为3D, 3E,3F,40,41。



步骤12345的顺序Dbapp，其中48h为'm'

得到结果为Dbapp{crackme100}

注意到一个细节 伪代码 `LOWORD(v19) = '0'`;在字符串根据偏移地址依次入栈 "0"然后是 "{" "



[创作打卡挑战赛](#)

[赢取流量/现金/CSDN周边激励大奖](#)