# bugkuCTF平台逆向题第五道love题解

原创

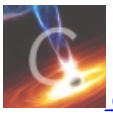
Megrez_ 于 2019-03-26 14:15:31 发布 470 收藏

分类专栏： ctf



本文链接：https://blog.csdn.net/qq_43445167/article/details/88818579

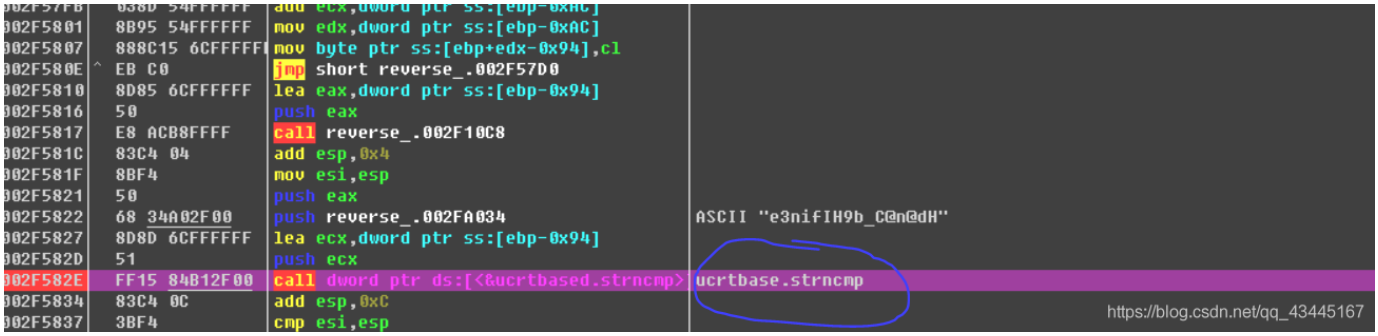




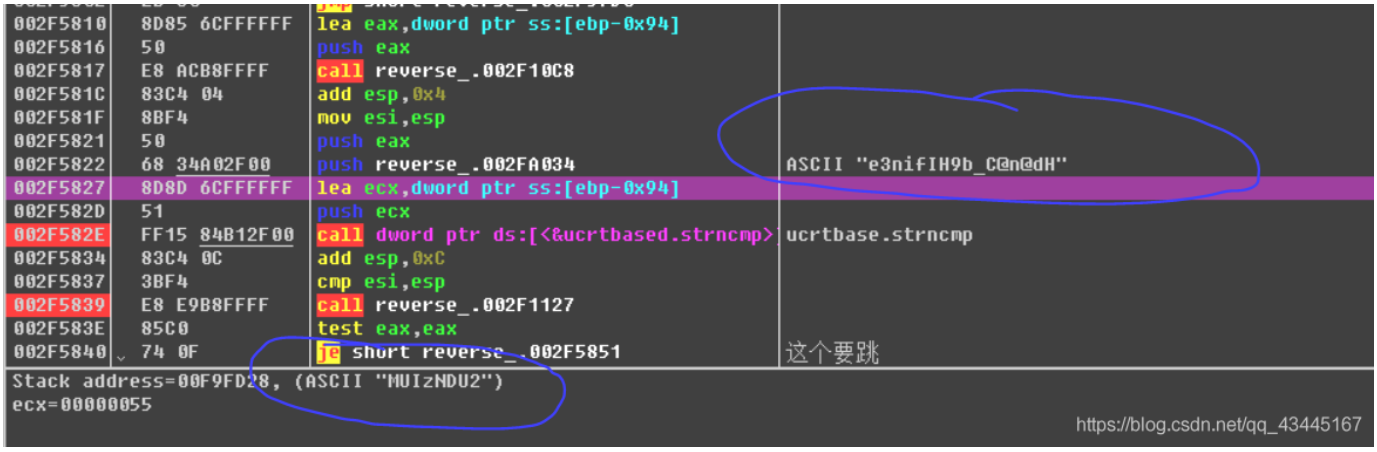


看了看网上的writeup 这尼玛都不是人的思维，自己写个writeup

1. 首先 第一件事 看标题 标题一般有提示 对吧。 然而看不出个卵。
2. 运行一波 嗯哼 盲猜调strcmp进行比对，flag就会入栈，打开od，开始疯狂寻找




3. 卧槽 上面那串奇异的字符一定是flag。提交 你懂的
4. 开始思考 我发现我输入的字符串没有入栈，这其中一定有蹊跷！

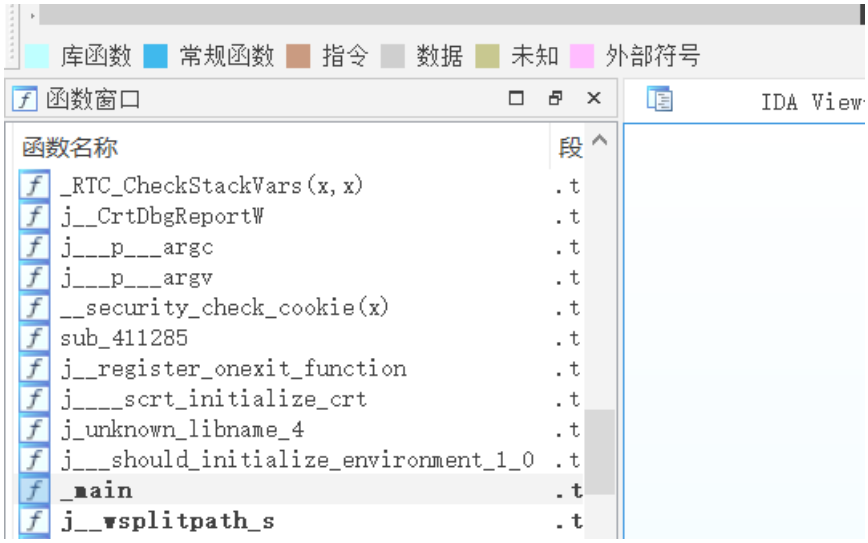



5. 然后我选择去找输入函数，跟踪我输入的字符串。


6. 如图 我发现我的字符串出现了 我就觉得它对我的字符串动了手脚 事实证明...我错了 是它的下一个函数对我的字符串动了手脚...（我就是f8看出来的）

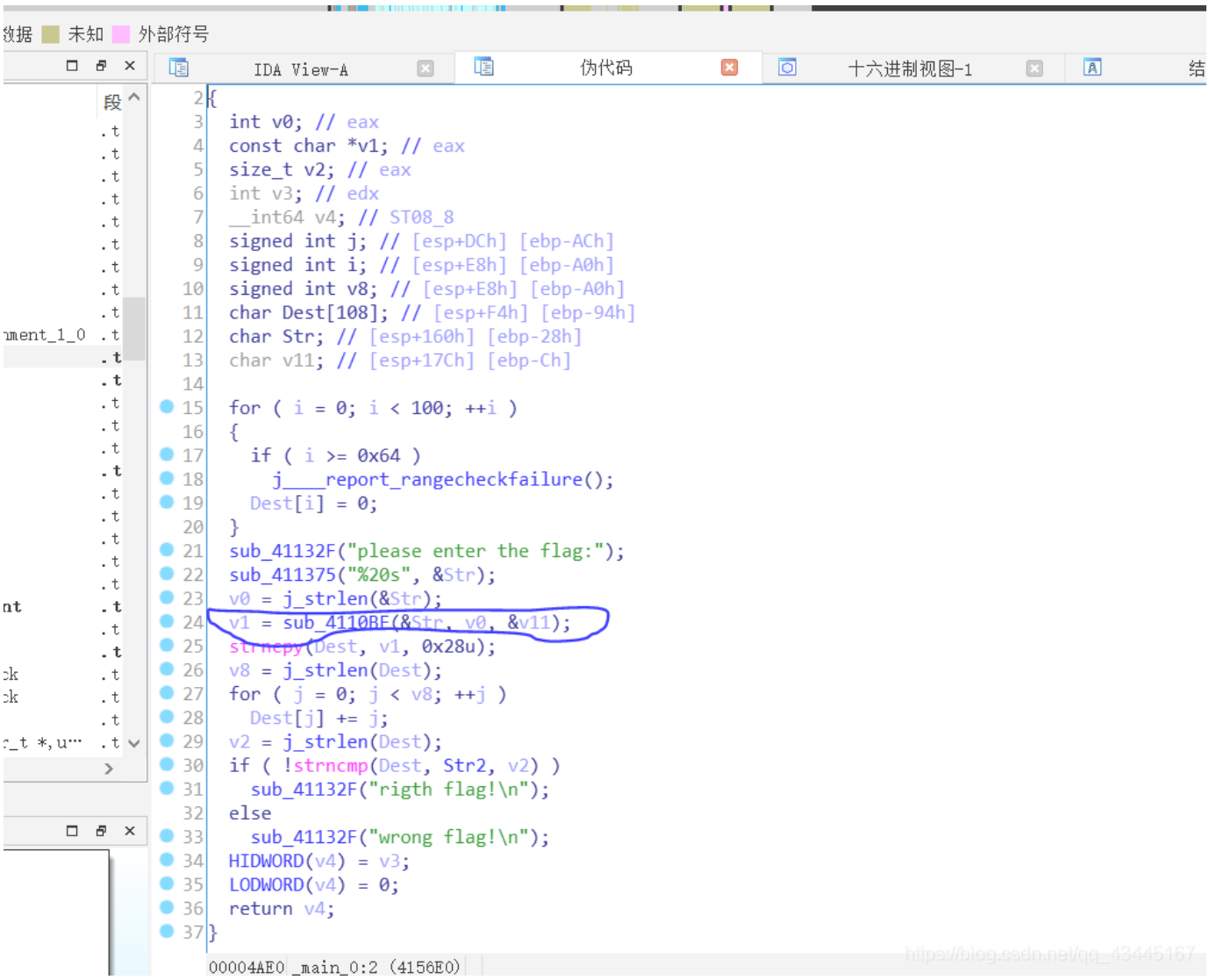

7.

8. 这个字符串与图2中的字符串像的一匹，尼玛脉络出来了。题目将输入的flag加密后与另一个字符串比较。开IDA！逆向算




法！（先找主函数）

9. 直接f5看伪码，往里跟




10.自己分析一边就知道这个函数有问题了，往里跟就能看到加密函数。

然后 算法逆向不出来。。。。。。。。。

去看writeup了，base64，气得我吐血。就当熟悉base64的加密过程了。