ctf题库--1000

原创

bubblecode 于 2019-08-21 14:33:21 发布 20993 收藏 39

分类专栏： 其它 文章标签： ctf题库 逆向工程 反汇编

本文链接：https://blog.csdn.net/miko2018/article/details/81608424

其它 专栏收录该内容

11 篇文章 1 订阅

订阅专栏

<题目>

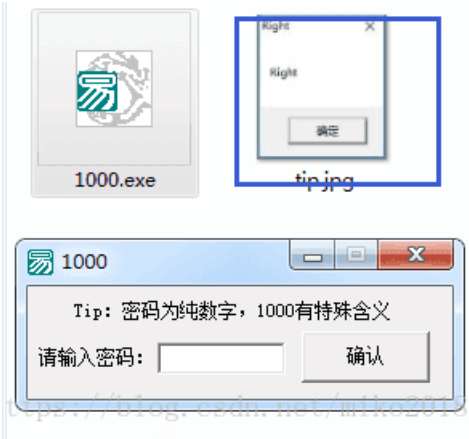
答案格式：CTF{}

解题链接： http://ctf5.shiyanbar.com/misc/1000.exe

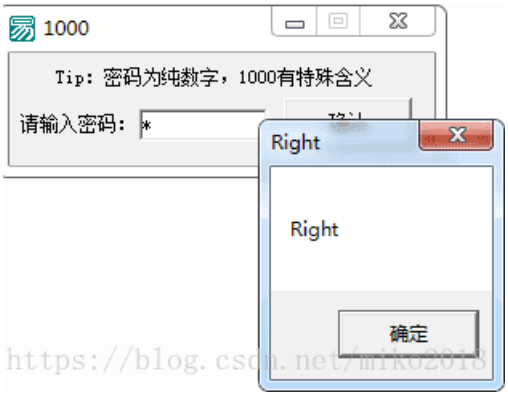
<解答>

打开题目链接下载文件，打开exe，在输入密码之前程序创建了tips.jpg的图片文件。

※程序提示1000有特殊含义，因此我们考虑是二进制，我们将其转换成十进制的8并且输入。



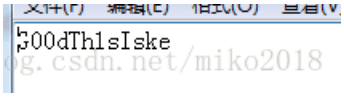
得到了和tips一样的结果。可是点击确定后却没有出现最终值，它一定被藏在了哪里。



※使用PEiD检查发现无壳后，将程序丢到OD中去，右键中文搜索引擎->智能搜索，然后查找“信息”（这里不要查找“Right”，找不到）。

※双击将其定位在反汇编窗口，摁F2设置断点，之后启动程序。
※输入8后程序停在断点处，之后摁f8单步步过，并仔细关注寄存器窗口，直到出现一个绝对路径。的flag.txt的文件。

※我们将路径复制下来并在资源管理器中打开，看到了那个文档，打开文档即得到了最终的值。



ps：在值的最后要加上“Y”才是正确的。不清楚是题目的bug还是出题者有意这样设计的。总之，这是一道很基础的也很有趣的逆向题目。