18.10.10 实验吧----easycreakme

原创

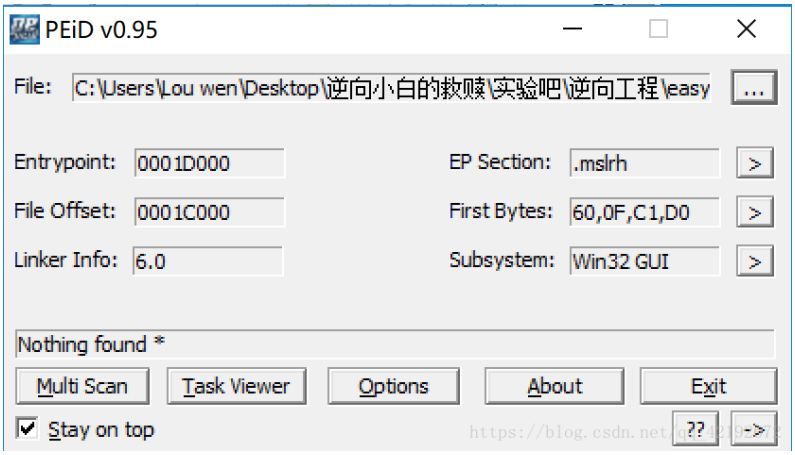
xiaoyuyulala 于 2018-10-10 10:37:37 发布 153 收藏 1
分类专栏： RE_WP 文章标签： easycreakme 实验吧

提示：

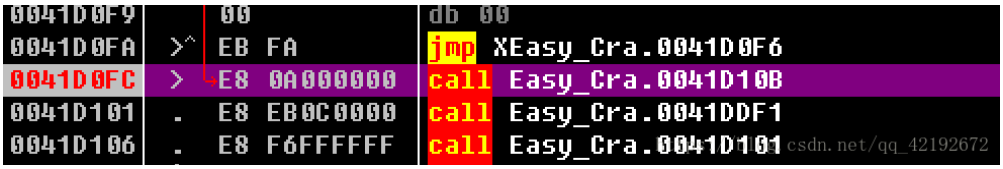
这是一个简单程序，但需要花费时间去进行分析，找出攻击的指令。

格式是ctf{}

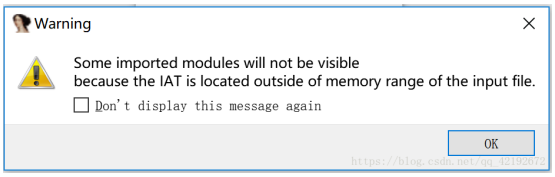
是一个exe文件，我自己是无法打开的，用PEID查看一下



存在保护措施，尝试着脱壳吧，拖进OD尝试脱壳，但是程序会崩掉，仔细观察一下.....如下

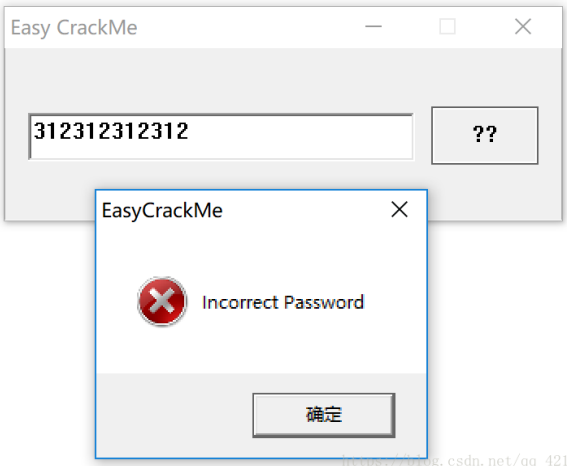


这个函数执行后会直接崩掉，拖到IDA看一下吧



IAT地址输入表尽然写在内存外？题目怕不是坏了，题目作者在底下评论了正确题目的地址.....

正确程序如下



直接对GetWindowTextA设置断点，然后单步执行回到代码段，直接回调，在4010A3设置断点，重新分析，可以看到要求我们输入的字符长度是100

看一下对应地址的伪C码好了

```
  String = 0;
  memset(&v3, 0, 0x60u);
  v6 = 0;
  v7 = 0;
  GetDlgItemTextA(hDlg, 1000, &String, 100);
  if ( v3 != 'a' || strncmp(&v4, a5y, 2u) || strcmp(&v5, aR3versing) || String != 'E' )
    return MessageBoxA(hDlg, aIncorrectPassw, Caption, 0x10u);
  MessageBoxA(hDlg, Text, Caption, 0x40u);
  return EndDialog(hDlg, 0);
}
```

基本就是判断一下输入的是否等于这些就好，排列组合一下，入下

```
.text:00401080 String          = byte ptr -64h
.text:00401080 var_63          = byte ptr -63h
.text:00401080 var_62          = byte ptr -62h
.text:00401080 var_60          = byte ptr -60h
```

分析完之后就是这四个连着的内存存放的字符就是答案