

2021年中国工业互联网安全大赛核能行业赛道writeup之hacker

原创

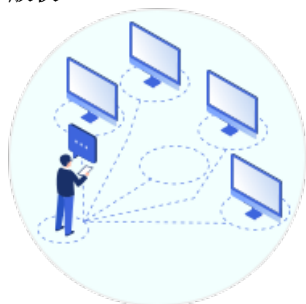
苦行僧(csdn) 于 2021-10-18 00:28:06 发布 77 收藏 1

分类专栏: [信息安全](#) 文章标签: [CTF](#) [DIE](#) [IDA](#) [UPX](#) [writeup](#)

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/qpeity/article/details/120800313>

版权



[信息安全](#) 专栏收录该内容

12 篇文章 0 订阅

订阅专栏

附加题 hacker, 题目描述: hacker, 附件下载

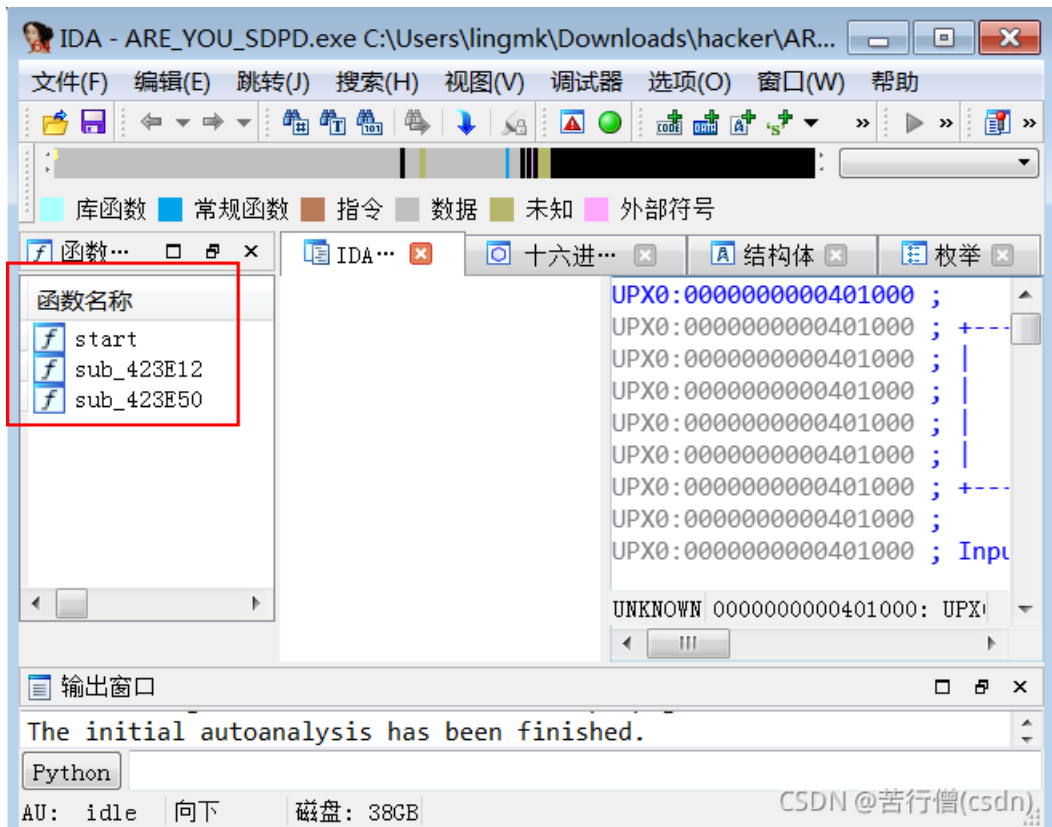
[hacker](#) <https://download.csdn.net/download/qpeity/33230528>解压缩得到一个EXE文件 ARE_YOU_SDPD.exe, 在一个文件夹下运行看一下。

```
C:\Windows\system32\cmd.exe

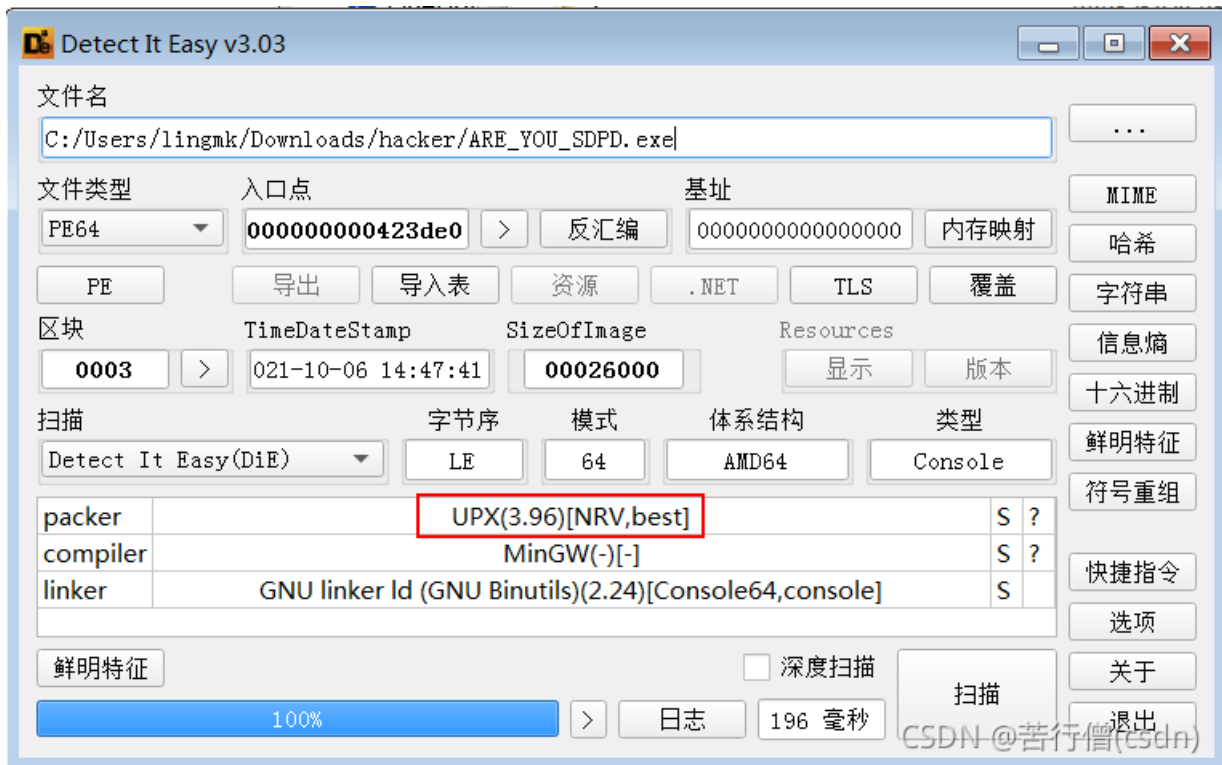
C:\Users\lingmk\Downloads\hacker>ARE_YOU_SDPD.exe
输入的flag为: abc

C:\Users\lingmk\Downloads\hacker>
```

用 IDA 反汇编一下, 发现找不到程序入口, 大概率加壳了。



用 DIE (Detect It Easy) 查壳，发现是 UPX 加壳。



那就用 UPX 脱壳，得到 a.exe。

```
upx -d ARE_YOU_SDPD.exe -o a.exe
```

```

(kali@kali)-[~/Desktop]
└─$ upx -d ARE_YOU_SDPD.exe -o a.exe
Ultimate Packer for eXecutables
Copyright (C) 1996 - 2020
UPX 3.96      Markus Oberhumer, Laszlo Molnar & John Reiser   Jan 23rd 2020

  File size      Ratio      Format      Name
  ────┬───┬───┬───┬───┬───
132922 ← 67386 50.70% win64/pe  a.exe

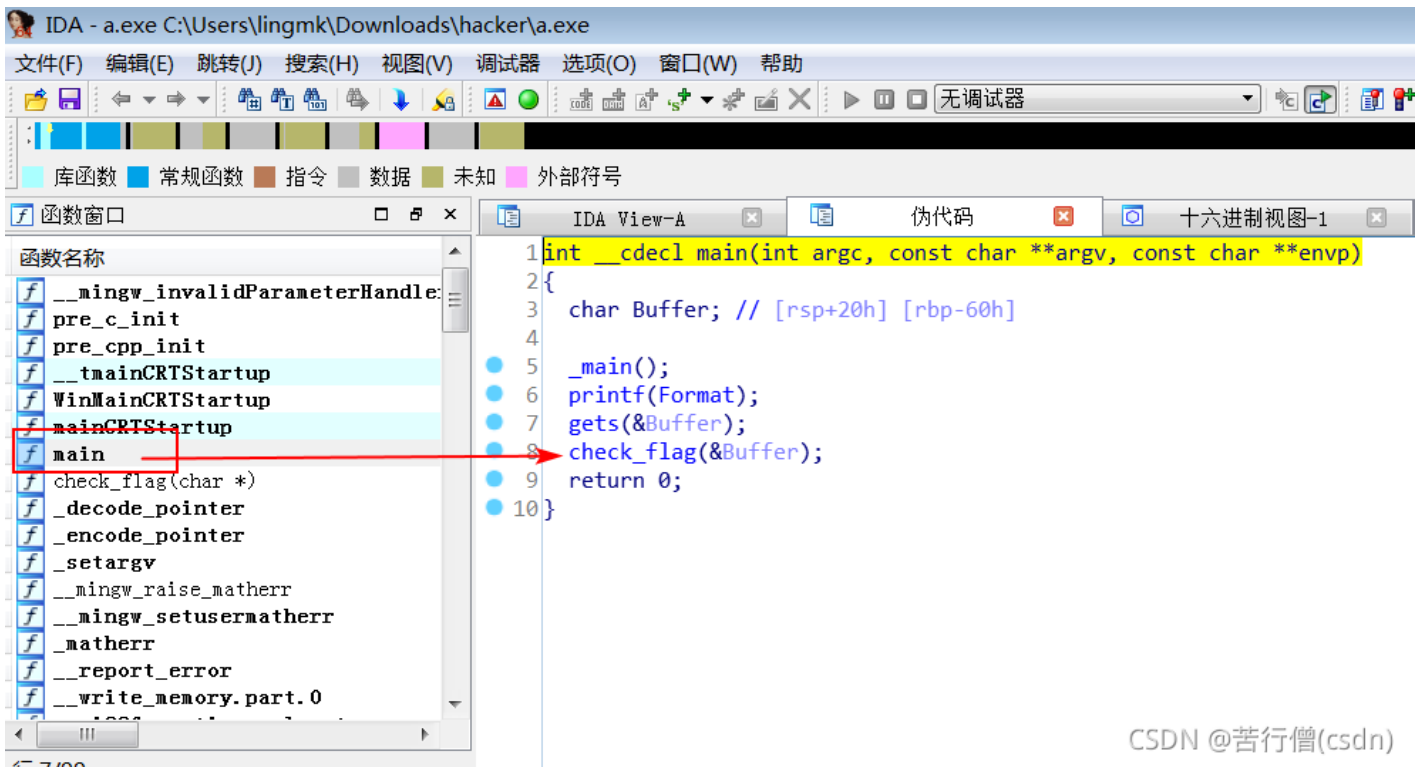
Unpacked 1 file.

(kali@kali)-[~/Desktop]
└─$

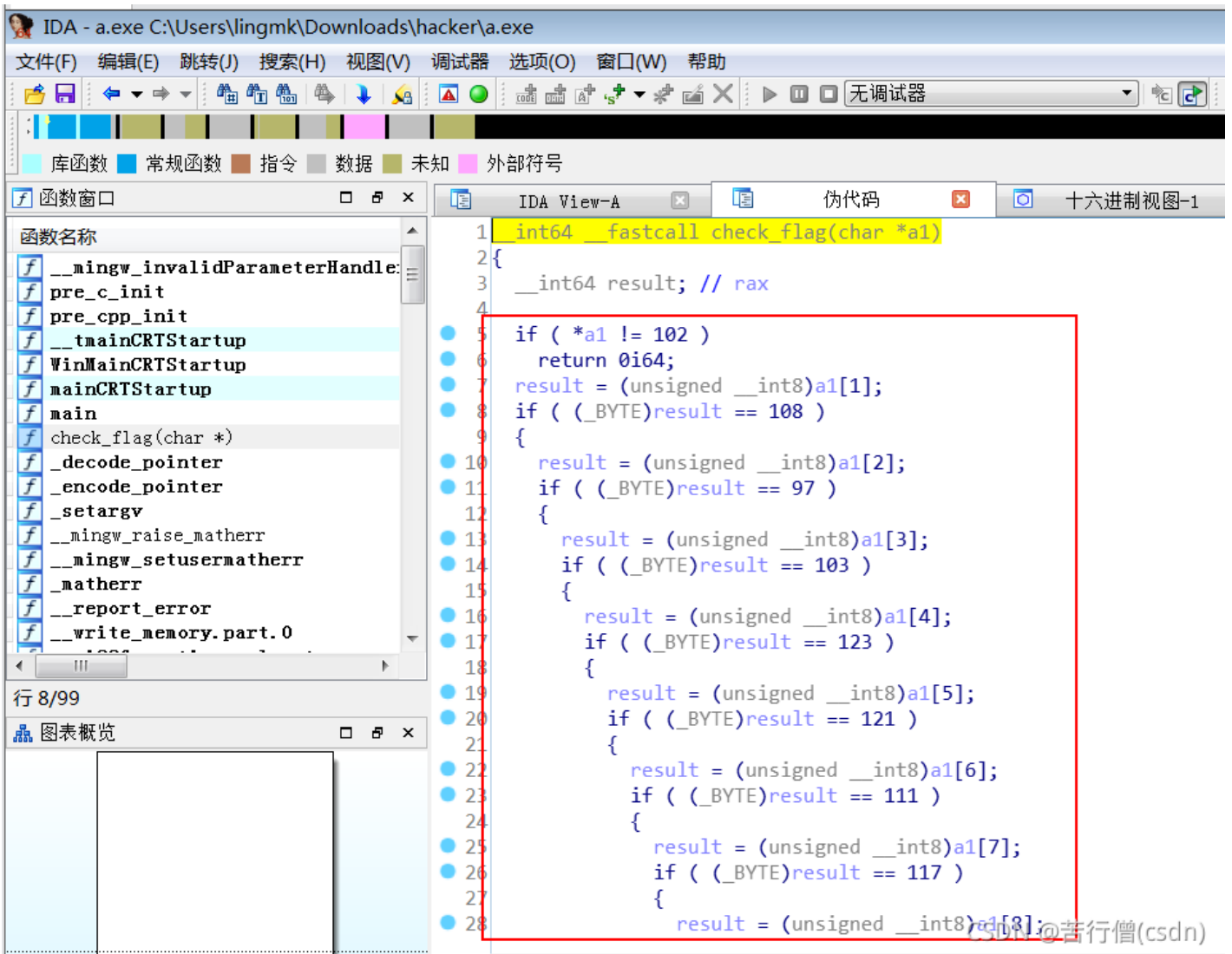
```

CSDN @苦行僧(csdn)

用 IDA 反汇编一下 a.exe，可以找到入口 main 函数，在 main 函数的汇编代码上按F5键看到main 函数的代码。程序逻辑是打印一行，等待用户输入字符串并保存到 Buffer，再在 check_flag 函数里检查用户的输入。



双击 check_flag 函数，看到 check_flag 函数逐位检查字符是否匹配，只要把检查的整型转换成对应的 ASCII 字符，就得到了 flag。整型数组为{102,108,97,103,123,121,111,117,45,97,114,101,95,97,95,104,97,99,107,125}



写一段简单的C代码，显示一下 flag 为 flag{you-are_a_hack}

```
#include "stdio.h"

int main(int argc, int** argv) {
    int a[] = {102,108,97,103,123,121,111,117,45,97,114,101,95,97,95,104,97,99,107,125};
    for(int i = 0; i < sizeof(a) / sizeof(a[0]); i++) {
        printf("%c", a[i]);
    }
    return 0;
}
```

