攻防世界 逆向 666

原创

与日平肩以头抢地 于 2020-02-17 10:03:41 发布 594 收藏 1

分类专栏： 逆向 文章标签： 安全

本文链接：https://blog.csdn.net/fool_best/article/details/104353319

逆向 专栏收录该内容

12 篇文章 0 订阅

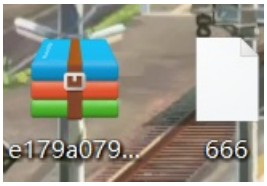
订阅专栏

攻防世界 逆向 666

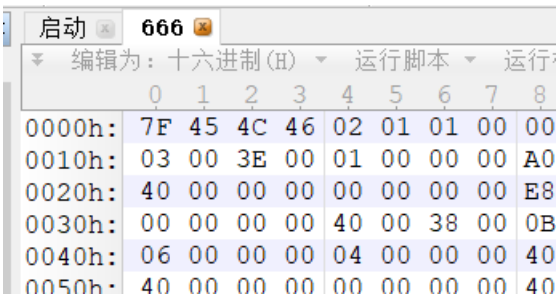
（原创）

原题如下：

下载附件解压：



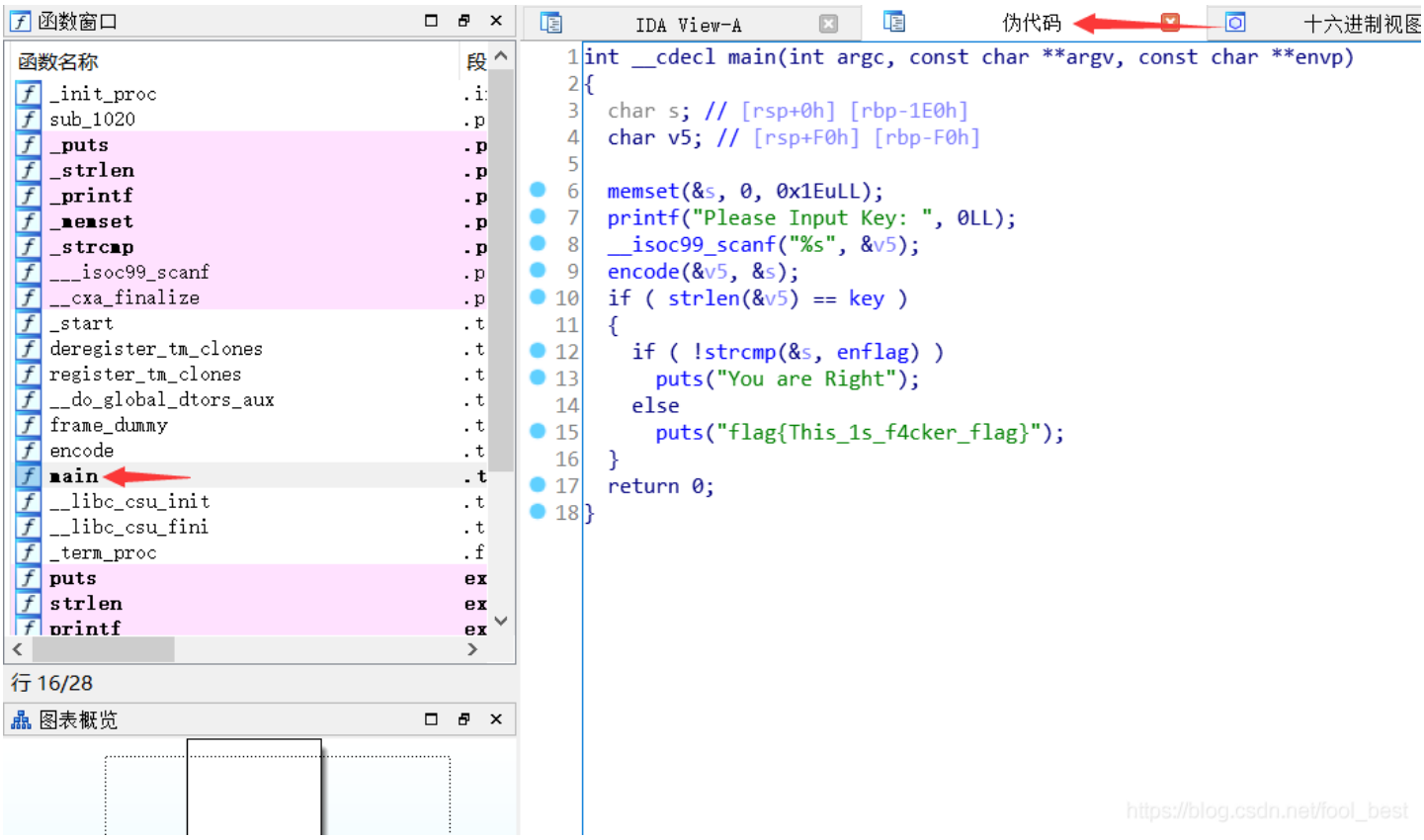
查看16进制的头文件，7F 45 4C 46，我不认识是啥文件，百度一下。



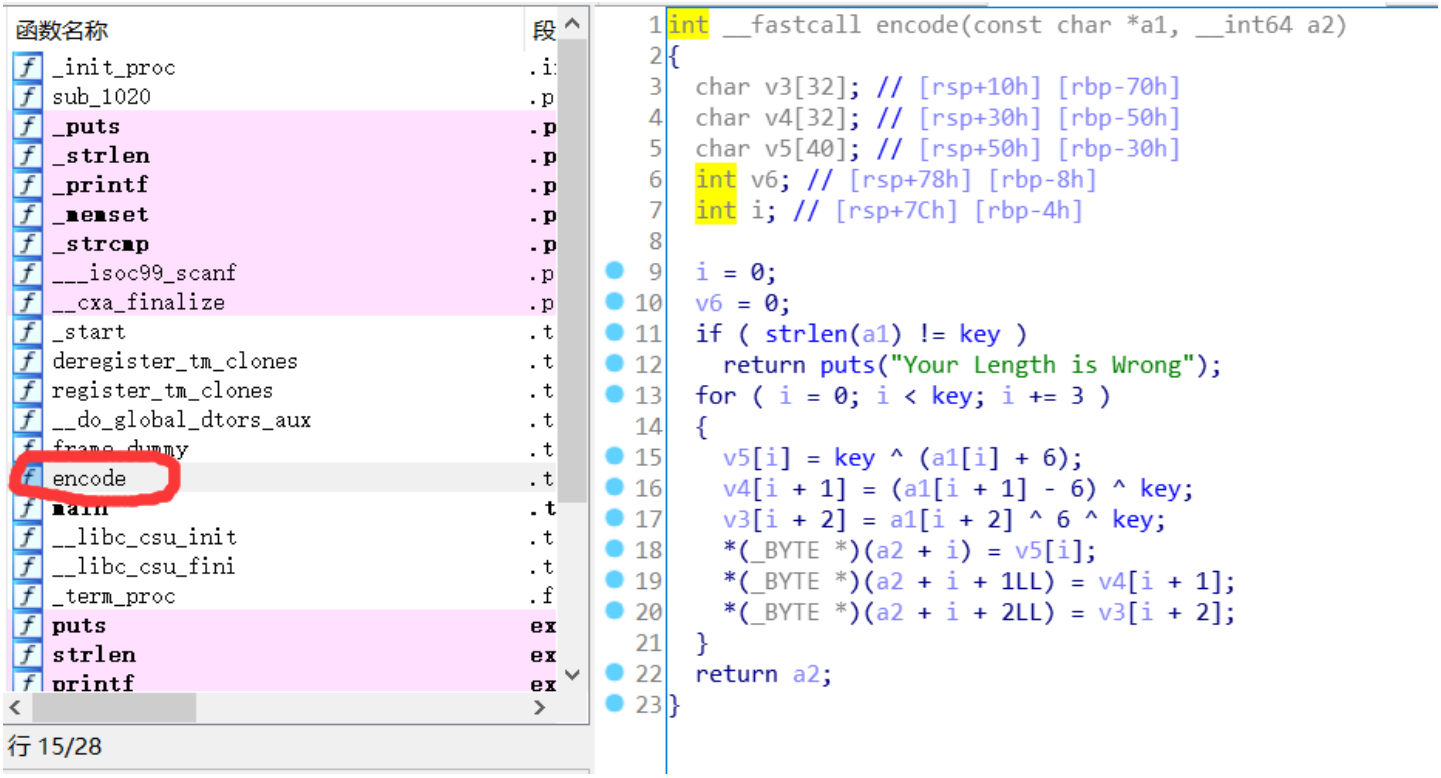
原来是一个可执行的文件。
（文件类型，16进制的文件头，以及Ascii数字信息，如下部分表）

Unix elf		7f 45 4c 46	.ELF

我们用IDA打开找到main函数查看伪代码。
其中有一个encode的函数。



我们再查看一下encode函数的伪代码。看懂代码之后就会发现了线索了。



下面是python写出脚本。

```
enflag=[105, 122, 119, 104, 114, 111, 122, 34, 34, 119, 34, 118, 46, 75, 34, 46, 78, 105, 0]
flag=''
for i in range(0,18,3):
flag+=chr((18^enflag[i])-6)
flag+=chr((18^enflag[i+1])+6)
flag+=chr(18^enflag[i+2]6)
print(flag)
```

运行即可。

最终得到flag：unctf{b66_6b6_66b}