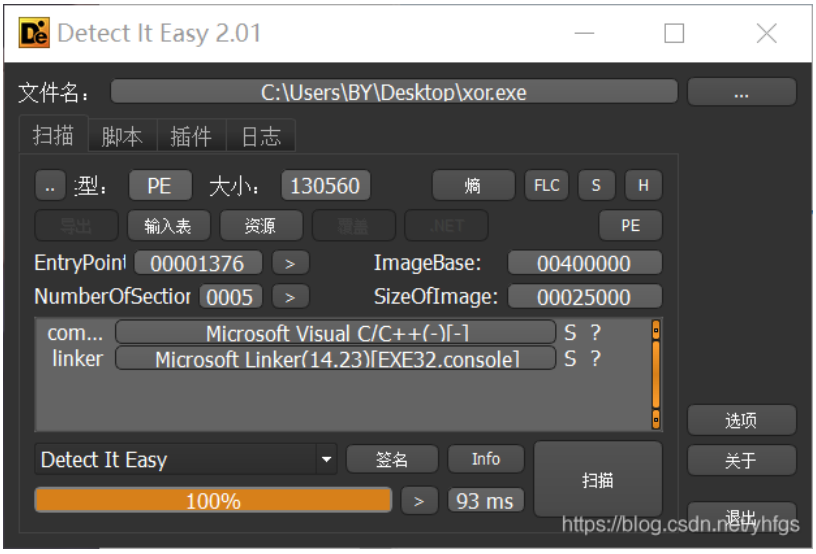
buuctf——（MRCTF2020）Xor

原创

re3sry 于 2021-06-06 13:55:52 发布 73 收藏 1
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/yhfgs/article/details/117625690
版权

1.查壳。

无壳，32位。



2.丢到IDA中反编译。

分析代码。就是一个很简单的异或运算。

第一个if表明flag是27位，for循环是将flag按位与对应下表取异或（逻辑很简单），并与byte_41EA08中的值比较。

```
int __cdecl main(int argc, const char **argv, const char **envp)
{
  unsigned int i; // eax

  sub_401020((int)"Give Me Your Flag String:\n");
  sub_401050("%s", byte_4212C0);
  if ( strlen(byte_4212C0) != 27 )
  {
LABEL_6:
    sub_401020((int)"Wrong!\n");
    sub_404B7E("pause");
    _loaddll(0);
    __debugbreak();
  }
  for ( i = 0; i < 0x1B; ++i )
  {
    if ( ((unsigned __int8)i ^ (unsigned __int8)byte_4212C0[i]) != byte_41EA08[i] )
      goto LABEL_6;
  }
  sub_401020((int)"Right!\n");
  sub_404B7E("pause");
  return 0;
}
```

查看byte_41EA08中的值。（不要忘记4Dh这个值）

```
.rdata:0041EA08 byte_41EA08     db 4Dh                  ; DATA XREF: _main+48↑r
.rdata:0041EA09 aSawbFxzJTqjNBp db 'SAWB~FXZ:J:`tQJ"N@ bpdd}8g',0
.rdata:0041EA24                 db    0
```

3.写脚本。

```
x="MSAWB^FXZ:J:`tQJ\"N@ bpdd}8g"
flag=""
for i in range(len(x)):
    flag+=chr(ord(x[i])^i)
print(flag)
```

4.get flag

flag{@_R3@1ly_E2_R3verse!}

（应为MRCTF{@_R3@1ly_E2_R3verse!}，由于我是在buuctf中做的MRCTF改为flag）。