XCTF 攻防世界 Reverse新手题（game)

原创

sherlockjjobs 于 2020-12-12 17:06:32 发布 682 收藏 2

分类专栏： CTF 网络安全 渗透测试 文章标签： 反汇编 反编译 网络安全 渗透测试 安全

本文链接：https://blog.csdn.net/weixin_43456810/article/details/111073497

XCTF 攻防世界 Reverse新手题（game)

这道题目按照一般IDA静态分析的思路走，应该不难做出来

首先，找到main函数，F5反编译一下

发现main_0()函数，进入此函数，反编译一下

对main_0()的代码进行分析，可以看到最后一部分的if段，当8个值都为1时，调用sub_457AB4()函数，代码如下：

```
if ( byte_532E28[0] == 1
      && byte_532E28[1] == 1
      && byte_532E28[2] == 1
      && byte_532E28[3] == 1
      && byte_532E28[4] == 1
      && byte_532E28[5] == 1
      && byte_532E28[6] == 1
      && byte_532E28[7] == 1 )
    {
      sub_457AB4();
    }
```

这时，可以猜测sub_457AB4()函数中有flag的信息，双击进入，可以发现确实存在flag的信息:

```
sub_45A7BE("done!!! the flag is ");
```

接着，继续往下看，分析得到有两个数组，进行两次异或运算:

```
for ( i = 0; i < 56; ++i )
  {
    *(&v2 + i) ^= *(&v59 + i);
    *(&v2 + i) ^= 0x13u;
  }
```

编写exp代码如下：

```
a = [18, 64, 98, 5, 2, 4, 6, 3, 6, 48, 49, 65, 32, 12, 48, 65, 31, 78, 62, 32, 49, 32,
     1, 57, 96, 3, 21, 9, 4, 62, 3, 5, 4, 1, 2, 3, 44, 65, 78, 32, 16, 97, 54, 16, 44,
     52, 32, 64, 89, 45, 32, 65, 15, 34, 18, 16, 0]
b = [123, 32, 18, 98, 119, 108, 65, 41, 124, 80, 125, 38, 124, 111, 74, 49,
     83, 108, 94, 108, 84, 6, 96, 83, 44, 121, 104, 110, 32, 95, 117, 101, 99,
     123, 127, 119, 96, 48, 107, 71, 92, 29, 81, 107, 90, 85, 64, 12, 43, 76, 86,
     13, 114, 1, 117, 126, 0]
i = 0
c = ''
while (i < 56):
    a[i] ^= b[i]
    a[i] ^= 0x13
    c = c + chr(a[i])
    i = i + 1
print(c)
```

代码应该不难理解，a和b是将上面的值组合到一起，接着进行两次异或运算，最后将十六进制转换为字符串，得到flag