【CSICTF】Blaise WriteUp

原创

古月浪子 于 2020-07-23 16:07:19 发布 68 收藏

文章标签： CTF

本文链接：https://blog.csdn.net/tqydyqt/article/details/107478217

Blaise

492

binary reversing

I recovered a binary from my teacher's computer. I tried to reverse it but I couldn't.

nc chall.csivit.com 30808

blaise

这个题我感觉很简单，不知道为什么解题人数比起前面的少了这么多

```
int __cdecl main(int argc, const char **argv, const char **envp)
{
  unsigned int v3; // eax
  unsigned int v4; // ST0C_4

  setbuf(stdout, 0LL);
  setbuf(stdin, 0LL);
  setbuf(stderr, 0LL);
  v3 = time(0LL);
  srand(v3);
  v4 = display_number(15, 20);
  process(v4);
  return 0;
}
```

display_number函数作用是取一个[15,20]的数

```
__int64 __fastcall process(unsigned int a1)
{
  int v1; // eax
  int v3; // [rsp+1Ch] [rbp-14h]
  int v4; // [rsp+20h] [rbp-10h]
  int i; // [rsp+24h] [rbp-Ch]
  unsigned __int64 v6; // [rsp+28h] [rbp-8h]

  v6 = __readfsqword(0x28u);
  v4 = 1;
  for ( i = 0; i <= a1; ++i )
  {
    __isoc99_scanf("%d", &v3);
    v1 = C(a1, i);
    if ( v1 != v3 )
      v4 = 0;
  }
  if ( v4 == 1 )
    system("cat flag.txt");
  return 0LL;
}
```

既然给了你刚刚的随机数，代码又在你手里，直接copy一份run一下，就能跑出答案了，然后cv到远程，大概率直接拿flag

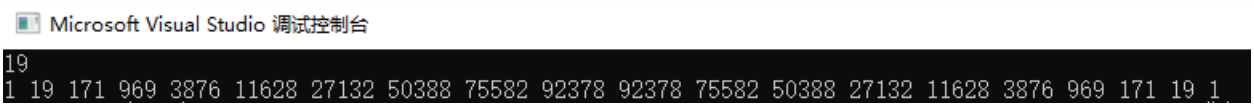
这里直接把IDA里的C函数以及C函数里的f函数全部原封不动的抄到IDE里

```cpp
#include <iostream>

using namespace std;

signed __int64 __fastcall f(signed int a1)
{
 signed int i; // [rsp+8h] [rbp-Ch]
 signed __int64 v3; // [rsp+Ch] [rbp-8h]

 v3 = 1LL;
 for (i = 2; i <= a1; ++i)
  v3 *= i;
 return v3;
}

__int64 __fastcall C(unsigned int a1, unsigned int a2)
{
 signed __int64 v2; // rbx
 signed __int64 v3; // r12

 v2 = f(a1);
 v3 = f(a2);
 return v2 / (f(a1 - a2) * v3);
}

int main()
{
 int i, a1;
 cin >> a1;
 for (i = 0; i <= a1; ++i)
 {
  cout << C(a1, i) << " ";
 }
}
```

连一下远程，获取随机数

```
wesker@ubuntu:~/Desktop$ nc chall.csivit.com 30808
19
```

直接输入run一下，然后复制结果回远程




```
wesker@ubuntu:~/Desktop$ nc chall.csivit.com 30808
19
1 19 171 969 3876 11628 27132 50388 75582 92378 92378 75582 50388 27132 11628 38
76 969 171 19 1
csictf{y0u_d1sc0v3r3d_th3_p4sc4l's_tr14ngl3}
```