BUUCTF -re -[ACTF新生赛2020]rome

原创

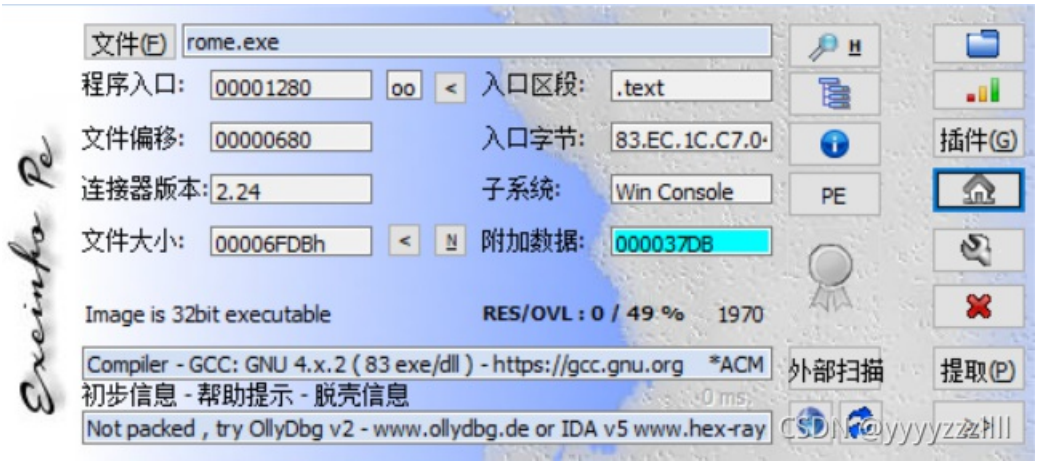
yyyzzzllll 于 2021-11-08 17:41:56 发布 35 收藏

分类专栏： # re 文章标签： re

本文链接：https://blog.csdn.net/yzl_007/article/details/121212582

BUUCTF -re -[ACTF新生赛2020]rome

无壳



定位到主函数

```
int func()
{
  int result; // eax
  int v1[4]; // [esp+14h] [ebp-44h]
  unsigned __int8 v2; // [esp+24h] [ebp-34h] BYREF
  unsigned __int8 v3; // [esp+25h] [ebp-33h]
  unsigned __int8 v4; // [esp+26h] [ebp-32h]
  unsigned __int8 v5; // [esp+27h] [ebp-31h]
  unsigned __int8 v6; // [esp+28h] [ebp-30h]
  int v7; // [esp+29h] [ebp-2Fh]
  int v8; // [esp+2Dh] [ebp-2Bh]
  int v9; // [esp+31h] [ebp-27h]
  int v10; // [esp+35h] [ebp-23h]
  unsigned __int8 v11; // [esp+39h] [ebp-1Fh]
  char v12[29]; // [esp+3Bh] [ebp-1Dh] BYREF

  strcpy(v12, "Qsw3sj_lz4_Ujw@l");
  printf("Please input:");
  scanf("%s", &v2);
  result = v2;
  if ( v2 == 65 )
```

```
{
  result = v3;
  if ( v3 == 67 )
  {
    result = v4;
    if ( v4 == 84 )
    {
      result = v5;
      if ( v5 == 70 )
      {
        result = v6;
        if ( v6 == 123 )
        {
          result = v11;
          if ( v11 == 125 )
          {
            v1[0] = v7;
            v1[1] = v8;
            v1[2] = v9;
            v1[3] = v10;
            *(_DWORD *)&v12[17] = 0;
            while ( *(int *)&v12[17] <= 15 )
            {
              if ( *((char *)v1 + *(_DWORD *)&v12[17]) > 64 && *((char *)v1 + *(_DWORD *)&v12[17]) <= 90 )
                *((_BYTE *)v1 + *(_DWORD *)&v12[17]) = (*((char *)v1 + *(_DWORD *)&v12[17]) - 51) % 26 + 65;
              if ( *((char *)v1 + *(_DWORD *)&v12[17]) > 96 && *((char *)v1 + *(_DWORD *)&v12[17]) <= 122 )
                *((_BYTE *)v1 + *(_DWORD *)&v12[17]) = (*((char *)v1 + *(_DWORD *)&v12[17]) - 79) % 26 + 97;
              ++*(_DWORD *)&v12[17];
            }
            *(_DWORD *)&v12[17] = 0;
            while ( *(int *)&v12[17] <= 15 )
            {
              result = (unsigned __int8)v12[*(_DWORD *)&v12[17]];
              if ( *((_BYTE *)v1 + *(_DWORD *)&v12[17]) != (_BYTE)result )
                return result;
              ++*(_DWORD *)&v12[17];
            }
            return printf("You are correct!");
          }
        }
      }
    }
  }
  return result;
}
```

关键的就是这一段

```
*(_DWORD *)&v12[17] = 0;
while ( *(int *)&v12[17] <= 15 )
{
  if ( *((char *)v1 + *(_DWORD *)&v12[17]) > 64 && *((char *)v1 + *(_DWORD *)&v12[17]) <= 90 )
    *((_BYTE *)v1 + *(_DWORD *)&v12[17]) = (*((char *)v1 + *(_DWORD *)&v12[17]) - 51) % 26 + 65;
  if ( *((char *)v1 + *(_DWORD *)&v12[17]) > 96 && *((char *)v1 + *(_DWORD *)&v12[17]) <= 122 )
    *((_BYTE *)v1 + *(_DWORD *)&v12[17]) = (*((char *)v1 + *(_DWORD *)&v12[17]) - 79) % 26 + 97;
  ++*(_DWORD *)&v12[17];
}
*(_DWORD *)&v12[17] = 0;
while ( *(int *)&v12[17] <= 15 )
{
  result = (unsigned __int8)v12[*(_DWORD *)&v12[17]];
  if ( *((_BYTE *)v1 + *(_DWORD *)&v12[17]) != (_BYTE)result )
    return result;
  ++*(_DWORD *)&v12[17];
}
return printf("You are correct!");
```


给了一段字符"Qsw3sj_lz4_Ujw@l"，之间爆破吧

```
s = "Qsw3sj_lz4_Ujw@l"

flag=''
for i in range(0,16):
    for k in range(0,127):
        z=k
        if k>64 and k<=90:
            k=(k-51)%26+65
        if k>96 and k<=122:
            k=(k-79)%26+97
        if k==ord(s[i]):
            flag+=chr(z)
print(flag)
#Cae3ar_th4_Gre@t
```