攻防世界 Reverse

原创

pipixia233333 于 2019-04-28 16:31:43 发布 652 收藏
分类专栏： 逆向之旅


逆向之旅 专栏收录该内容
128 篇文章 2 订阅
订阅专栏

看pwn 看不下去 没事做做逆向题　想想 后天就要回家了~~ 想想还是有点小激动

这个题 其实逻辑很简单

```
unsigned int v0; // eax
int len; // eax
FILE *v2; // eax
FILE *v3; // eax
signed int result; // eax
char strr[25]; // [esp+10h] [ebp-44h]
int v6; // [esp+2Ch] [ebp-28h]
int input[8]; // [esp+30h] [ebp-24h]

sub_401AD0();
strcpy(strr, "1A2F943C4D8C5B6EA3C9BCAD7E");
v0 = 0;
v6 = 0;
do
{
  input[v0] = 0;
  ++v0;
}
while ( v0 < 8 );
puts("input your key:");
scanf("%s", input);
len = strlen(input);
if ( len <= 19 )
{
  printf("too short!");
  result = -1;
}
else if ( len > 30 )
{
  printf("too long!");
  result = -1;
}
else
{
  if ( check(input, strr, len) )
    printf("congratulations, your input is the flag ^_^");
  else
```


我们看一下 check函数

```
strr[8] = 0x30;
strr[9] = 0x11;
strr[10] = 0x50;
strr[11] = 0xD0u;
strr[12] = 0x82u;
strr[13] = 0x23;
strr[14] = 0xAEu;
strr[15] = 0x23;
strr[16] = 0xEEu;
strr[17] = 0xA9u;
strr[18] = 0xB4u;
strr[19] = 0x52;
strr[20] = 120;
strr[21] = 0x57;
strr[22] = 0xC;
strr[23] = 0x86u;
strr[24] = 0x8Bu;
if ( len == 25 )
{
  v5 = 0;
  do
  {
    v11[v5] = __ROL1__(input[v5], 2);
    ++v5;
  }
  while ( v5 != 25 );
  v6 = 0;
  do
  {
    v11[v6] ^= strtohex(str, v6);
    ++v6;
  }
  while ( v6 != 25 );
  v7 = 15;
  for ( i = 0; v11[i] == v7; v7 = strr[i] )
  {
    if ( ++i == 25 )
```

)000905 check:28 (401505)

其中那个 strtohex 就是把两个字符 转化成一个 16进制的数字

然后我们 写一个脚本就可以了

```
#include <stdio.h>
#include<iostream>
#include<iomanip>
#include<stdio.h>
#include<string.h>
#include<algorithm>
#include<vector>
#include<iostream>
#include<map>
#include<time.h>
#include<queue>
#include "windows.h"
using namespace std;
unsigned char strr[25];
char str[]="1A2F943C4D8C5B6EA3C9BCAD7E";
int strtohex(int index)
{
    char v2; // al
    char v3; // cl
    int v4; // eax
    int v5; // edx

    v2 = str[index];
    v3 = str[index + 1];
    if ( (v2 - 48) > 9u )
        v2 -= 55;
    v4 = v2 & 0xF;
    v5 = (v3 - 55) & 0xF;
```

```
    if ( (v3 - 48) <= 9u )
        v5 = v3 & 0xF;
    return v5 | 16 * v4;
}
int main()
{
    strr[0] = 15;
    strr[1] = -121;
    strr[2] = 98;
    strr[3] = 20;
    strr[4] = 1;
    strr[5] = -58;
    strr[6] = -16;
    strr[7] = 33;
    strr[8] = 48;
    strr[9] = 17;
    strr[10] = 80;
    strr[11] = -48;
    strr[12] = -126;
    strr[13] = 35;
    strr[14] = -82;
    strr[15] = 35;
    strr[16] = -18;
    strr[17] = -87;
    strr[18] = -76;
    strr[19] = 82;
    strr[20] = 120;
    strr[21] = 87;
    strr[22] = 12;
    strr[23] = -122;
    strr[24] = -117;
    for(int i=0;i<25;i++)
    {
        strr[i]^=strtohex(i);
        //printf("%x\n",strtohex(i));
        strr[i]=((strr[i]>>2)|(strr[i]<<6));
        printf("%c",strr[i]);
    }
    //printf("%s\n",strr);
}
```

得出flag

```
EIS{ea3y_r7EveOrSe_r1ghT}
```