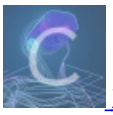
XCTF-dmd-50

原创

永远是深夜有多好。 于 2022-01-21 19:48:50 发布 2262 收藏

分类专栏： XCTF 文章标签： 安全 哈希算法

本文链接：https://blog.csdn.net/qq_37370714/article/details/122628067



看这题目名总感觉给了个md5的提示

查完没壳后静态分析一下（请原谅我看不懂）

通过大致观察分析发现出现了md5，考虑本题和md5有关再继续看看

```
std::operator<<<std::char_traits<char>>(&std::cout, "Enter the valid key!\n", envp);
std::operator>><char,std::char_traits<char>>(&edata, v42);
std::allocator<char>::allocator(&v38);
std::string::string(v39, v42, &v38);
md5(v40, v39);
v41 = std::string::c_str((std::string *)v40);
std::string::~string((std::string *)v40);
std::string::~string((std::string *)v39);
std::allocator<char>::~allocator(&v38);
if ( *(_WORD *)v41 == 14391
  && *(_BYTE *)(v41 + 2) == 48
  && *(_BYTE *)(v41 + 3) == 52
  && *(_BYTE *)(v41 + 4) == 51
  && *(_BYTE *)(v41 + 5) == 56
  && *(_BYTE *)(v41 + 6) == 100
  && *(_BYTE *)(v41 + 7) == 53
  && *(_BYTE *)(v41 + 8) == 98
  && *(_BYTE *)(v41 + 9) == 54
  && *(_BYTE *)(v41 + 10) == 101
  && *(_BYTE *)(v41 + 11) == 50
  && *(_BYTE *)(v41 + 12) == 57
  && *(_BYTE *)(v41 + 13) == 100
```


满足if后

```
:char_traits<char>>(&std::cout, 'T');
:char_traits<char>>(v3, 'h');
:char_traits<char>>(v4, 'e');
:char_traits<char>>(v5, ' ');
:char_traits<char>>(v6, 'k');
:char_traits<char>>(v7, 'e');
:char_traits<char>>(v8, 'y');
::char_traits<char>>(v9, ' ');
::char_traits<char>>(v10, 'i');
::char_traits<char>>(v11, 's');
```

```
::char_traits<char>>(v12, ' ');
::char_traits<char>>(v13, 'v');
::char_traits<char>>(v14, 'a');
::char_traits<char>>(v15, 'l');
::char_traits<char>>(v16, 'i');
::char_traits<char>>(v17, 'd');
::char_traits<char>>(v18, ' ');
::char_traits<char>>(v19, ':');
::char_traits<char>>(v20, ')');
```


会出现`The key is valid :)`
那就想办法满足if

```
if ( *(_WORD *)v41 == '87'
  && *(_BYTE *)(v41 + 2) == '0'
  && *(_BYTE *)(v41 + 3) == '4'
  && *(_BYTE *)(v41 + 4) == '3'
  && *(_BYTE *)(v41 + 5) == '8'
  && *(_BYTE *)(v41 + 6) == 'd'
  && *(_BYTE *)(v41 + 7) == '5'
  && *(_BYTE *)(v41 + 8) == 'b'
  && *(_BYTE *)(v41 + 9) == '6'
  && *(_BYTE *)(v41 + 10) == 'e'
  && *(_BYTE *)(v41 + 11) == '2'
  && *(_BYTE *)(v41 + 12) == '9'
  && *(_BYTE *)(v41 + 13) == 'd'
  && *(_BYTE *)(v41 + 14) == 'b'
  && *(_BYTE *)(v41 + 15) == '0'
  && *(_BYTE *)(v41 + 16) == '8'
  && *(_BYTE *)(v41 + 17) == '9'
  && *(_BYTE *)(v41 + 18) == '8'
  && *(_BYTE *)(v41 + 19) == 'b'
  && *(_BYTE *)(v41 + 20) == 'c'
  && *(_BYTE *)(v41 + 21) == '4'
  && *(_BYTE *)(v41 + 22) == 'f'
  && *(_BYTE *)(v41 + 23) == '0'
```


`v41`和`v40`有关系 `v40`又放着输入的数据 大致能判断`v40`进行md5加密后再进行if判断
由于不怎么看得懂只能猜测
把判断条件内的md5解码后得到

```
# /root/桌面/4907915cc47e4b5bb02bbde6c445c924
Enter the valid key!
b781cbb29054db12f88f08c6e161c199
The key is valid :)
```

看来还有好多要学的啊，加油!