

[bugku逆向] love WriteUp

原创

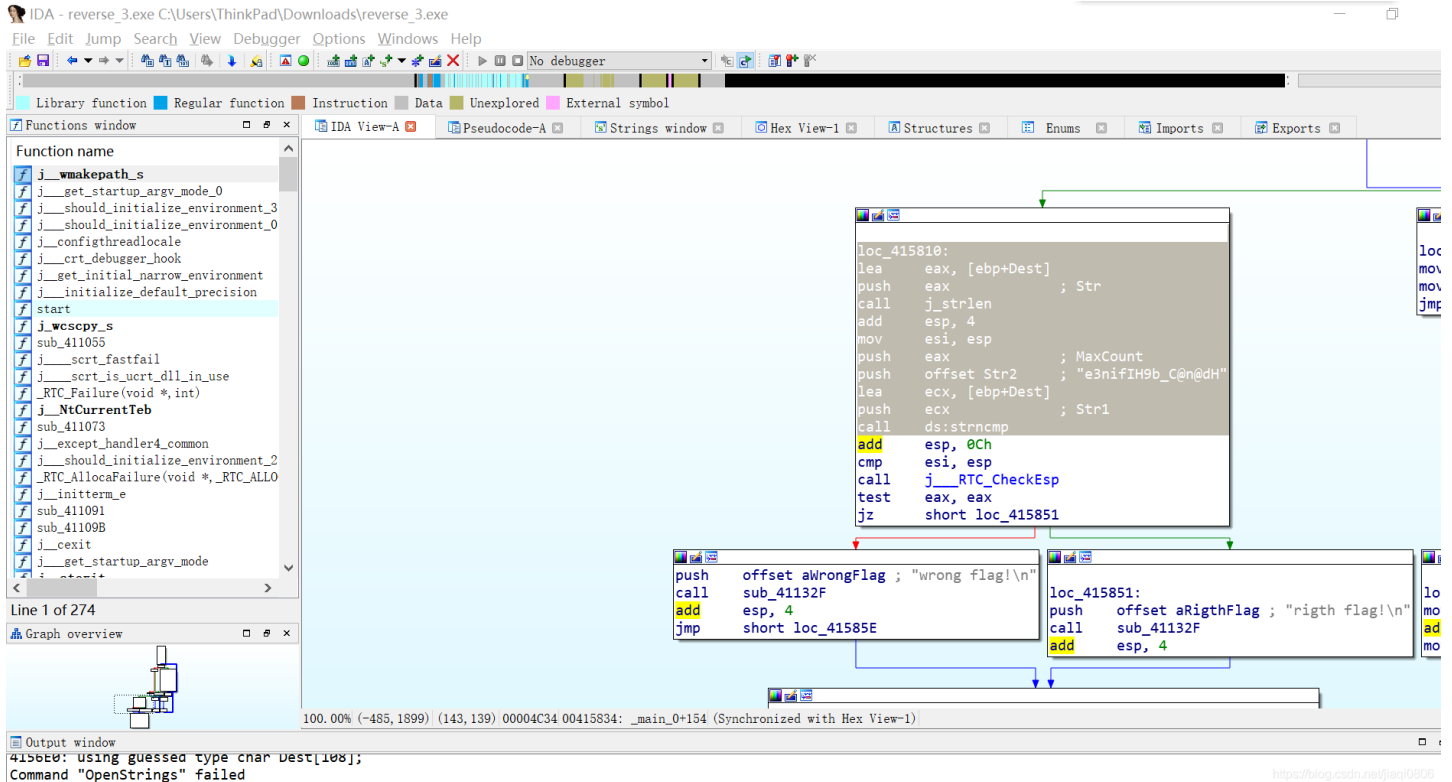
球球球你了 于 2020-02-23 18:16:25 发布 124 收藏

版权声明：本文为博主原创文章，遵循 [CC 4.0 BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) 版权协议，转载请附上原文出处链接和本声明。

本文链接：<https://blog.csdn.net/jiaqi0806/article/details/104464297>

版权

用IDA打开reverse.exe 界面如下



快捷键 **shift+F12** 打开字符串视图

File Edit Jump Search View Debugger Options Windows Help

Library function Regular function Instruction Data Unexplored External symbol

Functions window

Function name

- j_wmakepath_s
- j__get_startup_argv_mode_0
- j__should_initialize_environment_3
- j__should_initialize_environment_0
- j__configthreadlocale
- j__crt_debugger_hook
- j__get_initial_narrow_environment
- j__initialize_default_precision
- start
- j_wscopy_s
- sub_411055
- j__scrt_fastfail
- j__scrt_is_ucrt_dll_in_use
- _RTC_Failure(void *,int)
- j__NtCurrentTeb
- sub_411073
- j__except_handler4_common
- j__should_initialize_environment_2
- _RTC_AllocFailure(void *,_RTC_ALLO
- j__initterm_e
- sub_411091
- sub_41109B
- j__cexit
- j__get_startup_argv_mode
- j__scrt_is_ucrt_dll_in_use

Line 1 of 274

Graph overview

Output window

Address	Length	Type	String
.text:00...	00000007	C	offset
.text:00...	0000000C	C	base64input
.text:00...	00000006	C	input
.text:00...	00000005	C	nlen
.rdata:0...	00000042	C	ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/=
.rdata:0...	00000017	C	please enter the flag:
.rdata:0...	00000005	C	%20s
.rdata:0...	0000000D	C	wrong flag!\n
.rdata:0...	0000001B	C	tack around the variable '
.rdata:0...	00000011	C	' was corrupted.
.rdata:0...	0000000E	C	he variable '
.rdata:0...	0000002B	C	' is being used without being initialized.
.rdata:0...	0000000D	C	righ flag!\n
.rdata:0...	000000DD	C	The value of ESP was not properly saved across a function call. ...
.rdata:0...	0000011D	C	A cast to a smaller data type has caused a loss of data. If this...
.rdata:0...	0000001D	C	Stack memory was corrupted\n\r
.rdata:0...	00000036	C	A local variable was used before it was initialized\n\r
.rdata:0...	0000002C	C	Stack memory around _alloca was corrupted\n\r
.rdata:0...	0000001E	C	Unknown Runtime Check Error\n\r
.rdata:0...	00000011	C	Unknown Filename
.rdata:0...	00000014	C	Unknown Module Name
.rdata:0...	00000020	C	Run-Time Check Failure #%- %s
.rdata:0...	00000026	C	Stack corrupted near unknown variable
.rdata:0...	00000006	C	% 2X
.rdata:0...	00000049	C	Stack area around _alloca memory reserved by this function is cor...
.rdata:0...	00000009	C	\nData: <
.rdata:0...	0000002A	C	\nAllocation number within this function:
.rdata:0...	00000008	C	\nSize:
.rdata:0...	0000000D	C	\nAddress: 0x
.rdata:0...	00000048	C	Stack area around _alloca memory reserved by this function is cor...
.rdata:0...	00000012	C	%s%s%p%s%zd%s%d%s
.rdata:0...	00000009	C	%s%s%s

Line 1 of 43

<https://blog.csdn.net/jiaojiaojiao>

找到关键词：base64（考虑是否是base64编码？）以及wrong/right flag的判断

双击wrong flag！找到对应函数 ctrlX 后再F5可以打开对应的伪代码

```
IDA Vie... Pseudocode-B Pseudocod... Strings w
6 int v3; // edx
7 __int64 v4; // ST08_8
8 signed int j; // [esp+DCh] [ebp-ACh]
9 signed int i; // [esp+E8h] [ebp-A0h]
10 signed int v8; // [esp+E8h] [ebp-A0h]
11 char Dest[108]; // [esp+F4h] [ebp-94h]
12 char Str; // [esp+160h] [ebp-28h]
13 char v11; // [esp+17Ch] [ebp-Ch]
14
15 for ( i = 0; i < 100; ++i )
16 {
17     if ( (unsigned int)i >= 0x64 )
18         j__report_rangecheckfailure();
19     Dest[i] = 0;
20 }
21 sub_41132F("please enter the flag:");
22 sub_411375("%20s", &Str);
23 v0 = j_strlen(&Str);
24 v1 = (const char *)sub_4110BE(&Str, v0, &v11);
25 strncpy(Dest, v1, 0x28u);
26 v8 = j_strlen(Dest);
27 for ( j = 0; j < v8; ++j )
28     Dest[j] += j;
29 v2 = j_strlen(Dest);
30 if ( !strcmp(Dest, Str2, v2) )
31     sub_41132F("righth flag!\n");
32 else
33     sub_41132F("wrong flag!\n");
34 HIDWORD(v4) = v3;
35 LODWORD(v4) = 0;
36 return v4;
37 }
```

<https://blog.csdn.net/jiaqi0806>

观察代码成分 copy输入到dest并做了个累加 比较和str2的值

这里再根据之前base64的判断 可能是输入的字符base64加密后加上index值, 再转化成字符串, 与e3nifH9b_C@n@dH (点击str2就会定位到str2的字符串) 比较 若一致则输出right flag

可以写一个python脚本进行计算

```
import base64
s='e3nifIH9b_C@n@dH'
f=''
n=len(s)
for i in range(n):
    f+=chr(ord(s[i])-i)
print(f)
print(base64.b64decode(f))
```

```
C:\Users\ThinkPad\AppData\Local\Programs\Python\Python39-64\python.exe
e21fbDB2ZV95b3V9
b' {i_10ve_you}'
Press any key to continue . . .
https://blog.csdn.net/jiaqi0806
```

拿到flag



[创作打卡挑战赛](#) >

[赢取流量/现金/CSDN周边激励大奖](#)