XCTF-Reverse: re1

原创

版权



CTF&Reverse 专栏收录该内容

20 篇文章 0 订阅 订阅专栏

题目地址: https://adworld.xctf.org.cn/task/answer?type=reverse&number=4&grade=0&id=5073&page=1

	答题	竞赛	排行榜 ~	队伍	商城	
「 「CE1 13 最佳Writeup由Lord of rings • 令狐提供						┓ ■ WP ● 建议
难度系数: ◆★★★★4.0						
题目来源: DUTCTF						
题目描述:菜鸡开始学习逆向工程,首先是最简单的题目						
题目场景: 暂无						
题目附件: 附件1					http:	s://blog.csdn.net/Waffle666

工具: IDA notepad++

IDA Pro 能把软件翻译成C语言代码

> 此目	此电脑 〉 Windows-SSD (C:) 〉 用户 〉 mi 〉 桌面 〉 XCTF 〉 reverse 〉 re1 ~							
^	名称 ^	修改日期	类型	大小				
	b5c583c7d2664a4da42ef2d790732f	2020/11/18 10:04	应用程序	89 KB				
	C:\Users\mi\Desktop\XCTF\reverse\re1\k	2d790732f09.exe						
ł	欢迎来到DUTCTF呦 这是一道很可爱很简单的逆向题呦 输入flag吧:							
			https://bl	log.csdn.net/W	affle666	6		

将下载下来的文件拖入IDA



思路:可以先用IDA shift+F12——》搜索中文字符串,找到关键的地方

双击flag get

F5生成C语言的伪代码			
:00413E12	•		
:00413E14 alSnan	🛛 🦅 War	rning ×	
:00413E1B			
:00413E1C alInd		Please position the cursor within a function	
:00413E22		Don't display this message again (for this session only)	
:00413E24 ; char a	a:		
:00413E24 alInf		07	
:00413E2A		UK	
:00413E2C ; char a	aivnanti		
::00413E2C a1Qnan		<pre>db '1#QNAN',0 ; DATA XREF: _\$I10_OUTPUT:loc_40F130</pre>	C†c
:00413E33		align 4	
:00413E34 xmmword	_413E34	xmmword 3074656D30633165577B465443545544h 300 csdn.net/Waille	

警告:请将光标放在一个函数

解决方法:跳转——》交叉引用列表——》出现图形结构界面,再将光标放函数上,按F5

生成了一个C语言的伪代码:



C 库函数 - strcmp()

描述

C 库函数 int strcmp(const char *str1, const char *str2) 把 str1 所指向的字符串和 str2 所指向的字符串进行比较。

声明

下面是 strcmp() 函数的声明。

int strcmp(const char *str1, const char *str2)

参数

- str1 -- 要进行比较的第一个字符串。
- str2 -- 要进行比较的第二个字符串。

返回值

该函数返回值如下:

- 如果返回值小于 0,则表示 str1 小于 str2。
- 如果返回值大于 0, 则表示 str1 大于 str2。
- 如果返回值等于 0, 则表示 str1 等于 str2。

双击: xmmword_413E34, 就跳转到如下界面

ugger Options Windows Help

😠 🖾 👁 🗴 📾 📾 🕼 📌 🖛 🗙 🕨 🗈 🖬 No debugger 💿 🤨 🔁 🛐 🚏 🏠									
;ion 📕 Instruction 📕 Data 📕 Unexplored 📕 External symbol									
	這 IDA View	-A 🗵 📑 P:	seudocode-A 🗵	🔄 Strings window 🗵	🖸 Hex View	-1 🗵 🗖	🛚 Structures 🔳	🗄 Enums	
Se ^	• .rc	lata:00413E2A	ł	align 4					
. t.	.rc	lata:00413E20	C ; char a1Qna	n[]					
. t	• .rc	lata:00413E20	a1Qnan	db '1#QNAN',0	; DAT	A XREF: _	<pre>\$I10_OUTPUT:loc_</pre>	_40F13C↑o	
. t	• .rc	lata:00413E33	}	align 4					
.t	• .rc	lata:00413E34	1 xmmword_413E	34 xmmword <mark>3074656D</mark>)30633165 <mark>577B</mark> 4	6544354554	<mark>14h</mark>		
. t	.rc	lata:00413E34	ŀ		; DAT	A XREF: _n	nain+10↑r		
. t	• .rc	lata:00413E44	l qword_413E44	dq 7D46544354554	l 4h ; D AT	A XREF: _n	nain+27↑r		
. t	.rc	lata:00413E40	; char byte_	413E4C					
.t	• .rc	lata:00413E40	byte_413E4C	db 0BBh	; DAT	A XREF: _n	nain+1A↑o		
.t	• .rc	lata:00413E4D)	db 0B6h					
. t	• rc	lata:00413F4F	1	dh 0D3h					

转化成字符串: convert to string

. . 1.5 ger Options Windows Help y 🔺 🕥 🛛 📾 📾 🗗 😴 🗸 🏄 🗡 🕨 🔲 🗔 No Convert to string n 📕 Instruction 📗 Data 📒 Unexplored Extern rdata:00413E2C ; char a1Qnan[] db '1#QNAN',0 rdata:00413E2C **a1Qnan** ; DATA XREF: _\$I10_OUTPUT:log rdata:00413E33 align 4 rdata:00413E34 aDutctfWe1c0met db 'DUTCTF{We1c0met0DUTCTF}',0 rdata:00413E34 ; DATA XREF: main+101r rdata:00413E4C ; char byte_413E4C rdata:00413E4C byte_413E4C db 0BBh ; DATA XREF: _main+1A^o rdata:00413E4D db 0B6h

得到flag值: DUTCTF{We1c0met0DUTCTF}

14 nrintf

C:\Users\mi\Desktop\XCTF\reverse\re1\b5c583c7d2664a4da42ef2d790732f09.exe

欢迎来到DUTCTF呦 这是一道很可爱很简单的逆向题呦 h输入flag吧:DUTCTF{WelcOmetODUTCTF} hflag get√ 请按任意键继续	
	https://blog.csdn.net/Waffle666

另一种方法

用记事本或者notepad++打开刚下载的可执行文件exe

搜索flag

38	< <u>NULNULT5ANULSOH@NULNUL</u> `5ANUL					
39	@NULNUL15ANUL	查找				×
40	DNULNULx5ANUL	土北				_
11	HNULNULx845ANUL	旦14	首换 又什宣找 你记			_
12	LNULNULx905ANUL		查找目标(F) : <mark>flag</mark>	~	查找下一个	
13	PNULNULx9C5ANULEOT NULNULxA85ANULSUB) Likker -	C
14	NULNUL\$9ANULLNULNUL0-ANUL.NULNUL			选取范围内(I	计数(T)	U
15	NULNULNULXCC9ANULONULNULNULNUL-ANUL (N				杏找所有打开文件(0)	ЭA
16	NUTNUTNUT这是一道很可爱很简单的逆向。	_				
17	NUL输入flag吧:NUL%sNULNULflag get√				在当前文件中查找	
48	WII flag 不太 对吻,再试试则,加油吻		全词匹配(W)			
19	NULpauseNULNULNULNULNULNULHNULNULN		匹配大小与(C)		取消	UI
50	袤x99BSDxA79彦xC4ETXNULNULE:\c\Cons		值坏宣找(P)			JU:
51	4@NULNULNULNULXFEXFFXFFNULNULNU	一查打	戈模式	\checkmark	透明度(Y)	I
52	ENOSetLastErrorNULNULSOSTXGetCurrentThm		普通(N)		● 失去焦点后	W
53	STXGetCurrentProcessIdNULxD6STXGetSyste	0	扩展(X) (\n, \r, \t, \0, \x)		○始终	x 9
54	NULNULNULACKNULNULNUL NULNULNULBELNUI	0	正则表达式(G) 匹配新行			JU:
55	NULNULNULBELNULNULNULVTNULNULBSNUL					
56	NULNULSYNNULNULSINULNULSTNUL				https://blogteschunat/W/s	afft edi 66
	hurthurthurthathurthurthathurthurthurthath		TT burn amuburn burn burn			

JULNUL1#QNANNULNULDUTCTF{WelcOmetODUTCTF}NUL次迎来到DU

DUTCTF{We1c0met0DUTCTF}