

# BUUCTF Reverse 内涵的软件 WriteUp

原创

PlumpBoy 于 2021-09-10 18:36:52 发布 27 收藏

分类专栏: [BUUCTF 逆向题解](#) 文章标签: [系统安全](#) [安全](#) [经验分享](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 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/weixin\\_45723661/article/details/120227827](https://blog.csdn.net/weixin_45723661/article/details/120227827)

版权



[BUUCTF 逆向题解 专栏收录该内容](#)

18 篇文章 1 订阅

订阅专栏

## 内涵的软件

先打开看一看, 发现不管输入啥都报错退出。拖到x32dbg中, 执行到exe本体中, 搜索字符串找到每次输出语句, 向上看一看, 发现flag

00401057	56	push esi	esi:EntryPoint
00401058	57	push edi	edi:EntryPoint
00401059	8D7D B4	lea edi,dword ptr ss:[ebp-4C]	edi:EntryPoint
0040105C	B9 13000000	mov ecx,13	
00401061	B8 CCCCCCCC	mov eax,CCCCCCCC	
00401066	F3:AB	rep stosd	
00401068	C745 FC 05000000	mov dword ptr ss:[ebp-4],5	
0040106F	C745 F8 18514200	mov dword ptr ss:[ebp-8],70125468-0786-425118:"DBAPP{49d3c93df25caad81232130f3d2ebfad}"	
00401076	EB 09	jmp 70125468-0786-4705-bd91-87037f8f3e16	
00401078	8B45 FC	mov eax,dword ptr ss:[ebp-4]	
0040107B	83E8 01	sub eax,1	
0040107E	8945 FC	mov dword ptr ss:[ebp-4],eax	
00401081	837D FC 00	cmp dword ptr ss:[ebp-4],0	
00401085	7C 18	j1 70125468-0786-4705-bd91-87037f8f3e16	
00401087	8B4D FC	mov ecx,dword ptr ss:[ebp-4]	
0040108A	51	push ecx	
0040108B	68 EC504200	push 70125468-0786-4705-bd91-87037f8f3e16	4250EC:"距离出现答案还有%d秒, 请耐心等待! \n"
00401090	E8 EB000000	call 70125468-0786-4705-bd91-87037f8f3e16	
00401095	83C4 08	add esp,8	
00401098	E8 6DFFFFFF	call 70125468-0786-4705-bd91-87037f8f3e16	
0040109D	EB D9	jmp 70125468-0786-4705-bd91-87037f8f3e16	
0040109F	68 88504200	push 70125468-0786-4705-bd91-87037f8f3e16	425088:"\n\n\n这里本来应该是答案的,但是粗心的程序员忘记把变
004010A4	E8 D7000000	call 70125468-0786-4705-bd91-87037f8f3e16	
004010A9	83C4 04	add esp,4	
004010AC	C645 F4 01	mov byte ptr ss:[ebp-C],1	
004010B0	8D55 F4	lea ebx,dword ptr ss:[ebp-C]	

CSDN @PlumpBoy