

Re

0xre0

re0 [已完成]

描述

URL <http://ol795rwtm.bkt.clouddn.com/re0.exe>

基准分数 50

当前分数 50

完成人数 131

用 od 打开得到 flag

<pre>mov [local.1],eax push re0.01072124 call re0.01071020 push re0.01072138 call re0.01071020 push 0x20 lea eax,[local.9] push eax push re0.0107214C call re0.01071050 add esp,0x14 lea eax,[local.9] mov ecx,re0.01072108 nop mov dl,byte ptr ds:[ecx]</pre>	<pre>ASCII "Welcome to hgame\n" ASCII "\nInput your flag: " Arg3 = 00000020 Arg2 = 79887538 Arg1 = 0107214C ASCII "%s" re0.00E51050 ASCII "hctf{F1r5t_St5p_Ls_Ea5y}"</pre>
--	--

0x1 sc2_player

sc2_player [已完成]

描述

知识点: hotkey: n

URL http://ol795rwtm.bkt.clouddn.com/sc2_player.exe

基准分数 100

当前分数 100

完成人数 33

用 od 打开，查找字符串 input your flag 来到输入处，发现先对输入位数处理，得到输入位数为 28 位

00A1122F	. 8845 FB	mov byte ptr ss:[ebp-0x5],al	<pre>Arg1 = 00A13108 ASCII "Input your flag: " sc2_play.00A1470 Arg3 = 00000000 Arg2 = 009EF772 ASCII "11111111111111111111111111111111" Arg1 = 00A1311C ASCII "%s" sc2_play.00A313E0</pre>
00A11232	. E8 0831A100	push sc2_play.00A13108	
00A11237	. F8 34020000	call sc2_play.00A11470	
00A1123C	. 83C4 04	add esp,0x4	
00A1123F	. 6A 20	push 0x20	
00A11241	. 8D4D DC	lea ecx,dword ptr ss:[ebp-0x24]	
00A11244	. 51	push ecx	
00A11245	. E8 1C31A100	push sc2_play.00A1311C	
00A1124A	. F8 91010000	call sc2_play.00A113E0	
00A1124F	. 83C4 0C	add esp,0xC	
00A11252	. 8D55 DC	lea edx,dword ptr ss:[ebp-0x24]	
00A11255	. 8955 D4	mov dword ptr ss:[ebp-0x2C],edx	
00A11258	. 8B45 D4	mov eax,dword ptr ss:[ebp-0x2C]	
00A1125B	. 83C0 01	add eax,0x1	
00A1125E	. 8945 D0	mov dword ptr ss:[ebp-0x30],eax	
00A11261	> 8B4D D4	mov ecx,dword ptr ss:[ebp-0x2C]	
00A11264	. 8A11	mov dl,byte ptr ds:[ecx]	
00A11266	. 8855 DB	mov byte ptr ss:[ebp-0x25],dl	
00A11269	. 8345 D4 01	add dword ptr ss:[ebp-0x2C],0x1	
00A1126D	. 807D DB 00	cmp byte ptr ss:[ebp-0x25],0x0	
00A11271	. 75 EE	jnz short sc2_play.00A11261	
00A11273	. 8B45 D4	mov eax,dword ptr ss:[ebp-0x2C]	
00A11276	. 2B45 D0	sub eax,dword ptr ss:[ebp-0x30]	
00A11279	. 8945 CC	mov dword ptr ss:[ebp-0x34],eax	
00A1127C	. 837D CC 1C	cmp dword ptr ss:[ebp-0x34],0x1C	

00A11000	> 55	push ebp	
00A11001	- 8BEC	mov ebp,esp	
00A11003	- 51	push ecx	
00A11004	- C745 FC 0000	mov [local.1],0x0	
00A1100B	- EB 09	jmp short sc2_play.00A11016	
00A1100D	> 8B45 FC	mov eax,[local.1]	
00A11010	- 83C0 01	add eax,0x1	计数器加1
00A11013	- 8945 FC	mov [local.1],eax	
00A11016	> 837D FC 07	cmp [local.1],0x7	
00A1101A	- 7D 24	jge short sc2_play.00A11040	
00A1101C	- 6B4D 10 07	imul ecx,[arg.3],0x7	arg.3=0 1 2 3
00A11020	- 034D FC	add ecx,[local.1]	
00A11023	- 8B55 08	mov edx,[arg.1]	
00A11026	- 0FBE 040A	movsx eax,byte ptr ds:[edx+ecx]	清零回到相对0处
00A1102A	- 6B4D 10 07	imul ecx,[arg.3],0x7	
00A1102E	- 034D FC	add ecx,[local.1]	
00A11031	- 33C1	xor eax,ecx	与位数异或
00A11033	- 3345 10	xor eax,[arg.3]	与0 1 2 3异或
00A11036	- 8B55 0C	mov edx,[arg.2]	sc2_play.00A1103C0
00A11039	- 0355 FC	add edx,[local.1]	
00A1103C	- 8B02	mov byte ptr ds:[edx],al	
00A1103E	- EB CD	jmp short sc2_play.00A1100D	
00A11040	> 8BE5	mov esp,ebp	
00A11042	- 5D	pop ebp	sc2_play.00A1109E
00A11043	- C3	retn	
00A11044	- CC	int3	
00A11045	- 00	int0	

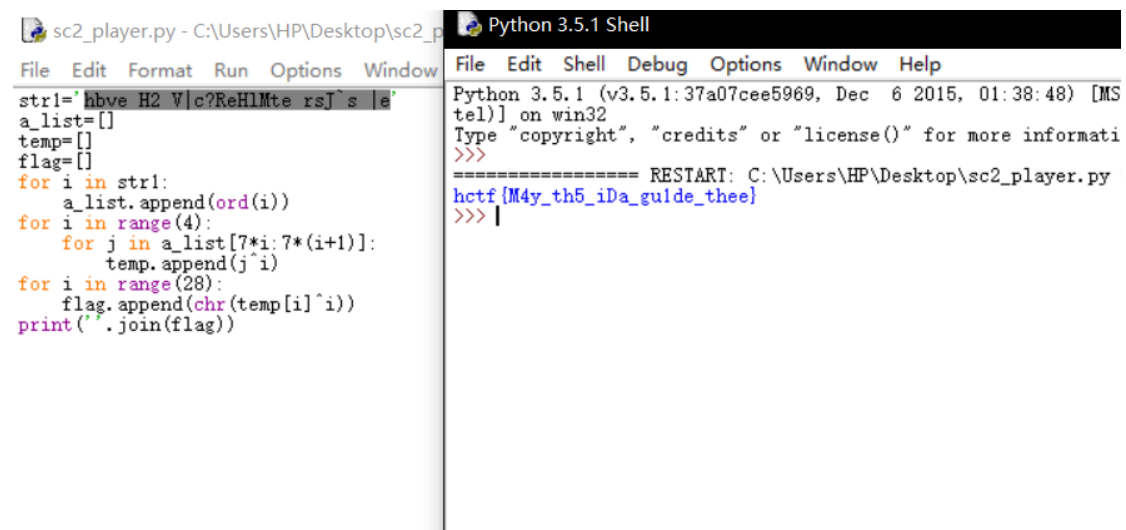
00A1110F	CC	int3	
00A11110	\$ 55	push ebp	
00A11111	- 8BEC	mov ebp,esp	
00A11113	- 51	push ecx	
00A11114	- C745 FC 0000	mov dword ptr ss:[ebp-0x4],0x0	sc2_play.00A143C0
00A11118	~ EB 09	jmp short sc2_play.00A11126	
00A1111D	> 8B45 FC	mov eax,dword ptr ss:[ebp-0x4]	
00A11120	- 83C0 01	add eax,0x1	
00A11123	- 8945 FC	mov dword ptr ss:[ebp-0x4],eax	sc2_play.00A14034
00A11126	> 837D FC 07	cmp dword ptr ss:[ebp-0x4],0x7	
00A1112A	~ 7D 20	jge short sc2_play.00A1114C	
00A1112C	- 8B4D 08	mov ecx,dword ptr ss:[ebp+0x8]	sc2_play.00A143C0
00A1112F	- 034D FC	add ecx,dword ptr ss:[ebp-0x4]	指针对应位数
00A11132	- 0FB611	movzx edx,byte ptr ds:[ecx]	输入变换后的第一段字符
00A11135	- 8B45 0C	mov eax,dword ptr ss:[ebp+0xC]	sc2_play.00A143B8
00A11138	- 0345 FC	add eax,dword ptr ss:[ebp-0x4]	指针对应位数
00A1113B	- 0FB608	movzx ecx,byte ptr ds:[eax]	内存剩下的28字符
00A1113E	- 3BD1	cmp edx,ecx	sc2_play.00A143C0
00A11140	- 75 04	jnz short sc2_play.00A11146	不等的话清零返回eax为0
00A11142	- EB D9	jmp short sc2_play.00A1111D	逐个比较
00A11144	~ EB 04	jmp short sc2_play.00A1114A	
00A11146	> 33C0	xor eax,eax	sc2_play.00A14034
00A11148	~ EB 07	jmp short sc2_play.00A11151	
00A1114A	> EB D1	jmp short sc2_play.00A1111D	
00A1114C	> B8 01000000	mov eax,0x1	
00A11151	> 8BE5	mov esp,ebp	
00A11153	- 5D	pop ebp	sc2_play.00A11172
00A11154	- C3	retn	
00A11155	CC	int3	
00A11156	CC	int3	
00A11157	CC	int3	
00A11158	CC	int3	
00A11159	CC	int3	

```
ebp=009BFE50
```

本地调用来自 00A1116D, 00A11182, 00A11197, 00A111AC

[illegible]

于是用 Python 写个逆算法得到 flag



The image shows two windows. The left window is a text editor titled 'sc2_player.py' containing a Python script. The script takes a string 'h2v3e H2 V|c?ReHlMte rs]`s |e`' and processes it to produce a flag. The right window is a 'Python 3.5.1 Shell' showing the execution of the script, which outputs the flag 'hctf{M4y_th5_iDa_gulde_thee}'.

```
sc2_player.py - C:\Users\HP\Desktop\sc2_p
File Edit Format Run Options Window
str1='h2v3e H2 V|c?ReHlMte rs]`s |e`'
a_list=[]
temp=[]
flag=[]
for i in str1:
    a_list.append(ord(i))
for i in range(4):
    for j in a_list[7*i:7*(i+1)]:
        temp.append(j^i)
for i in range(28):
    flag.append(chr(temp[i]^i))
print(''.join(flag))

Python 3.5.1 Shell
File Edit Shell Debug Options Window Help
Python 3.5.1 (v3.5.1:37a07cee5969, Dec 6 2015, 01:38:48) [MS
tel)] on win32
Type "copyright", "credits" or "license()" for more informati
>>>
===== RESTART: C:\Users\HP\Desktop\sc2_player.py
hctf{M4y_th5_iDa_gulde_thee}
>>> |
```

Misc

白菜2 [已完成]

描述

还是我老婆hhh 知识点：初识文件结构

URL <http://p1kaloi2x.bkt.clouddn.com/misc2.jpg>

基准分数 50

当前分数 50

完成人数 136

查看 16 进制文件，看到 pk，改为 zip 文件打开，发现 flag.txt，打开得到 flag



The image shows a Notepad window titled 'flag - 记事本'. The text content is a hex string: 'hgame{af2ab981a021e3def22646407cee7bdc}'.

```
flag - 记事本
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)
hgame{af2ab981a021e3def22646407cee7bdc}
```

描述

ngc从不知道哪里抓来的流量，好像里面有一个不得了的东西呢 知识点：wireshark 初识流量包

URL <http://p1kaloi2x.bkt.clouddn.com/flag.pcap>

基准分数 50

当前分数 50

完成人数 115

用 wireshark 打开得到 flag

No.	Time	Source	Destination	Protocol	Length	Info
541	13.914139	192.168.110.1	192.168.110.128	HTTP	583	GET /p.php?act=rt&callback=jQuery11
543	14.020396	192.168.110.128	192.168.110.1	HTTP	718	HTTP/1.1 200 OK (text/html)
545	14.919810	192.168.110.1	192.168.110.128	HTTP	583	GET /p.php?act=rt&callback=jQuery11
547	15.047970	192.168.110.128	192.168.110.1	HTTP	717	HTTP/1.1 200 OK (text/html)
549	15.927748	192.168.110.1	192.168.110.128	HTTP	583	GET /p.php?act=rt&callback=jQuery11
551	16.022941	192.168.110.128	192.168.110.1	HTTP	717	HTTP/1.1 200 OK (text/html)
553	16.923226	192.168.110.1	192.168.110.128	HTTP	583	GET /p.php?act=rt&callback=jQuery11
555	17.053093	192.168.110.128	192.168.110.1	HTTP	713	HTTP/1.1 200 OK (text/html)
557	17.532392	192.168.110.1	192.168.110.128	HTTP	432	GET /flag.php HTTP/1.1
559	17.535130	192.168.110.128	192.168.110.1	HTTP	359	HTTP/1.1 200 OK (text/html)

Frame 559: 359 bytes on wire (2872 bits), 359 bytes captured (2872 bits)

Ethernet II, Src: Vmware_5e:e0:4a (00:0c:29:5e:e0:4a), Dst: Vmware_c0:00:08 (00:50:56:c0:00:08)

Internet Protocol Version 4, Src: 192.168.110.128, Dst: 192.168.110.1

Transmission Control Protocol, Src Port: 80, Dst Port: 30616, Seq: 174530, Ack: 6153, Len: 305

Hypertext Transfer Protocol

Line-based text data: text/html

hgame{bfebcf95972871907c89893aa3096ec6}