buuct	f———[羊城杯 2020]log	in
原创		
<u>re3sry</u> 文章标签: 版权声明:	于 2021-09-30 18:08:05 发布 • 81 ☆ 收藏 python buctf reverse 本文为博主原创文章, 遵循 <u>CC 4.0 BY-SA</u> 版权协议,	转载请附上原文出处链接和本声明。
本文链接: 版权 1.查壳。	https://blog.csdn.net/yhfgs/article/details/120556096	

无壳,64位。(当时还不知到PyInstaller)

		Part of the	R P LATER	1991	Se. 33					
	<u>File</u> : login.exe			<i>▶</i> <u>म</u>						
	Entry Point : 00008654 00 <	EP Section :	.text	10						
2	File Offset : 00007A54	First Bytes :	48.83.EC.28.E8	0	Plug					
-	Linker Info: 14.00	SubSystem :	Win Console	PE						
	File Size : 00600E1Eh < NET	Overlay :	005BE21E	0	Ø					
	Image is 64 bit executable R	ES/OVL : 0 / 95	5 % 2020	ATA						
5	[PyInstaller v.3.6 - 2005?019 - support P	7 www.pyinstaller	Scan / t	Rip						
	Lamer Info - Help Hint - Unpack info									

2.直接丢到IDA反编译。发现啥也没有。

(连个提示性的字符串也没有,但运行是有input something。很迷。)

看了看大佬的wp,才知道这是PyInstaller打包的exe,需要解包。

3.解包,反编译。

(1) 解包;

下载PyInstaller Extractor (PyInstaller Extractor download | SourceForge.net)

把login.exe与下载得到的pyinstxtractor.py放到同一目录下。

~ ↑] >	此电周	函 〉 Windows (C:) 〉 python 〉			ٽ ~	
档	*	^	名称 ^	修改日期	类型	大小	
沜	*] python2.7	2021/9/27 14:18	文件夹		
1 java基	础精讲		🂫 pyinstxtractor.py	2021/9/29 20:32	Python File	13	КВ
uuctf			🚰 login.exe	2021/9/29 20:16	应用程序	6,148	КВ
ython							
他							CSDN @艸丛

cmd运行命令,得到一个文件夹。



Iogin.exe_extracted	2021/9/29 20:53	文件夹	
python2.7	2021/9/27 14:18	文件夹	
🚰 login.exe	2021/9/29 20:16	应用程序	6,148 KB
🏓 pyinstxtractor.py	2021/9/29 20:32	Python File	13 KB
			CODIV

在文件夹中,找到login和struct(无后缀名。)

用winhex把struct和login打开。

把login前面缺的字节补上(在struct中),

login这个是在从E3开始的,所以要把struct中E3前的字节都复制过去。

开始时:

🔛 WinHex ·	- [struct]										X				-								
🧱 文件(F) 🦸	编辑(E) 搜索(S) 등	/航(N) 查看((V) 工具(T) 专业	工具(I)	选项(C) 窗口(W) 帮助	📲 WinHex	- [login]												-		×
0 7 🗔 🕹	۵ 🖬 📑 👘 کې	🖼 🖪 🖻 🕅	- A #	🌢 🏥 😘	HEX	→ -€) <	-> 23/	🔛 文件(F)	编辑(E)	搜索(S)	导航(N) 査看(\	/) 工具(T) 专业	工具(I)	选项(O)	窗口(W) 帮助)(H)		20.3 SR-	2 x64	- 8 ×
Offset	0 1 2 3 4	5 6 7	8 9	A B	СD	E F	ANSI 7	0 7 🗔 🖉	🚴 💕 🛛	1 5	De 🖽 🕻	a 📭 🖏	A 👸	💏 🐴	🔬 -	+ - 🗑 🔶	→	- 3 3	. 📷 🔎 🛙	8 💦 🤞	85	II .4 🕨	* 🛛 🥔
00000000	33 0D 0D 0A 70	79 69 30	01 01	00 00 F	3 00	00 00	3 pyi0	Offset	0 1	2 3	4 5	6 7	8 9	AB	Ср	EF	J	NSI A	SCII /				
00000010	00 00 00 00 00	00 00 00	00 08	00 00 0	0 40	00 00	1	00000000	E3 00	00 00	00 00	00 00	00 00 0	0 00 0	0 07	00 00	ã						
00000020	00 73 38 00 00	/ 00 64 00	64 01	64 02 6	4 03	64 04	s8 ddd	00000010	00 40	00 00	00 73	5E 07	00 00 6	4 00 6	4 01	6C 00		d	d 1				
00000030	64 05 64 06 64	07 67 08	5A 00	64 08 C	4 09	6C 01	dddgZd	00000020	5A 00	65 01	64 02	83 01	5A 02 6	5 03 6	5 02	83 01	zedf	Ze	e f				
00000040	54 00 64 08 64	0A 6C 01	6D 02	5A 02 0	/1 00	64 08	TddlmZ	00000030	64 03	6B 03	72 2C	65 04	64 04 8	3 01 0	1 00	65 00	d k r,e	d f	e				
00000050	64 OB 6C 01 6D	/ 03 5A 03	01 00	64 OC 5	/3 00 3	29 OD	dlmZ d	00000040	6A 05	83 00	01 00	67 00	5A 06 7	8 32 6	5 07	64 05	jf g	Z x2	e d				
00000060	DA 08 63 61 6C	63 73 69	7A 65 1	DA 04 7	0 61	63 6B	Ú calcsizeÚ	00000050	83 01	44 00	5D 26	5A 08	65 06 6	A 09 6	5 0A	65 02	f D]&2	e j	e e				
00000070	DA 09 70 61 63	6B 5F 69	6E 74 (6F DA 0	6 75	6E 70	Ú pack_intoť	00000060	65 08	19 00	83 01	65 0A	65 02 6	5 08 6	4 06	17 00	e fe	ee	d				
00000080	61 63 6B DA 0B	,75 6E 70	61 63 (6B 5F 6	6 72	6F 6D	ackÚ unpack	00000070	19 00	83 01	41 00	83 01	01 00 7	1 3A 5	7 00	65 06	f A f	g:	We				
00000090	DA 0B 69 74 65	72 5F 75	6E 70 (61 63 6	BDA	06 53	Ú iter_unpac	00000080	6A 09	65 OA	65 02	64 05	19 00 8	3 01 8	3 01	01 00	jeed	I f	f				
0A00000A0	74 72 75 63 74	DA 05 65	72 72	6F 72 F	9 00	00 00	tructÚ error	00000090	65 06	64 07	19 00	5A 0B	65 06 6	4 06 1	9 00	5A 0C	ed z	e d	Z				
000000B0	00 29 01 DA 01	2A 29 01	DA OB	5F 63 6	C 65	61 72) Ú *) Ú _c	04000000	65 06	64 00	19 00	5A 0D	65 06 6	4 08 1	9 00	5A 0E	ed 2	e d	Z				
000000000	63 61 63 68 65	29 01 DA	07 5F	5F 64 6	F 63	5F 5F	cache) Ú _ ď	000000B0	65 06	64 09	19 00	5A OF	65 06 6	4 0A 1	9 00	5A 10	ed 2	e d	Z				
000000D0	4E 29 04 DA 07	5F 5F 61	6C 6C /	5F 5F D	A 07	5F 73	N) Úall	00000000	65 06	64 OB	19 00	5A 11	65 06 6	4 OC 1	9 00	5A 12	ed Z	e d	Z				
000000E0	74 72 75 63 74	, 72 OB 00	00 00 '	72 OC 0	0 00	00 A9	tructr r	000000D0	65 06	64 OD	19 00	5A 13	65 06 6	4 OE 1	9 00	5A 14	ed 2	e d	Z				
000000F0	00 72 OF 00 00	00 72 OF	00 00 /	00 FA 1	.A 64	3A 5C	r r ť	000000E0	65 06	64 OF	19 00	5A 15	65 06 6	4 10 1	9 00	5A 16	ed 2	e d	Z				
00000100	61 6E 61 63 6F	6E 64 61	33 5C /	6C 69 6	/2 5C	73 74	anaconda3\1j	000000F0	65 06	64 11	19 00	5A 17	65 06 6	4 05 1	9 00	5A 18	ed 2	e d	Z				
00000110	72 75 63 74 2E	. 70 79 DA	08 3C /	6D 6F 6	4 75	6C 65	ruct.py0 <mc< td=""><td>00000100</td><td>65 OB</td><td>64 12</td><td>14 00</td><td>65 OC</td><td>64 13 1</td><td>4 00 1</td><td>7 00</td><td>65 OD</td><td>ed e</td><td>d</td><td>e</td><td></td><td></td><td></td><td></td></mc<>	00000100	65 OB	64 12	14 00	65 OC	64 13 1	4 00 1	7 00	65 OD	ed e	d	e				
00000120	3E 03 00 00 00	73 OC 00	00 00	0A 01 0	2 03	02 03	> s	00000110	64 14	14 00	17 00	65 OE	64 0A 1	4 00 1	8 00	65 OF	d e	d	e				I
00000130	06 03 08 01 0C	: 01						00000120	64 15	14 00	17 00	65 10	64 16 1	4 00 1	7 00	65 11	d e	d	e				
								00000130	64 17	14 00	17 00	65 12	64 05 1	4 00 1	7 00	65 13	d e	d	е				I
								00000140	64 18	14 00	18 00	65 14	64 19 1	4 00 1	7 00	65 15	d e	d	e				
								00000150	64 10	14 00	17 00	65 16	64 1A 1	4 00 1	7 00	65 17	d e	d	e				
								00000160	64 1B	14 00	18 00	65 18	64 1C 1	4 00 1	7 00	64 1D	d e	d	d				
								00000170	6B 02	65 OB	64 16	14 00	65 OC 6	4 OC 1	4 00	17 00	k e d	e d					
								00000180	65 OD	64 11	14 00	17 00	65 OE 6	4 17 1	4 00	18 00	e d	e d					
								00000190	65 OF	64 1E	14 00	17 00	65 10 6	4 1F 1	4 00	17 00	e d	e d					I
								000001A0	65 11	64 20	14 00	17 00	65 12 6	4 21 1	4 00	18 00	e d	e d!					
								000001B0	65 13	64 22	14 00	17 00	65 14 6	4 OE 1	4 00	17 00	e d"	e d					
							//	000001c0	65 15	64 07	14 00	17 00	65 16 6	4 1E 1	4 00	18 00	e d	e d					
页1/1		偏移地址:		0		= 51	选块:	000001D0	65 17	64 23	14 00	18 00	65 18 6	4 24 1	4 00	17 00	e d‡	e d\$	`	·			~
narm devd	nn eve	- 1	1					页1/6			偏移的	他til:	0			= 227	先块:			无	大小: (LSDN (2月14年1

复制后:

```
🚟 WinHex - [login]
🇱 文件(F) 编辑(E) 搜索(S) 导航(N) 查看(V) 工具(T) 专业工具(I) 选项(O) 窗口(W) 帮助(H)
| ] 7 7 🖬 😃 📚 😰 📑 | 🔊 🐚 强 🖻 🐘 | 🗛 🗛 🙏 🎎 | → 🕀 🔶 | 3 4 3 4 🖗 📾 🗩 🖉 🔬
                        56
                                                  E F
          0
                2
                   3
                     4
                             7
                                  8 9 A
                                          B C
                                               D
                                                             ANSI ASCII
 Offset
             1
                                                                        \sim
         33 0D 0D 0A 70 79 69 30
                                                       3 pyi0
                                01 01 00 00 E3 00 00 00
                                                                ã
00000000
         00 00 00 00 00 00 00 00
00000010
                                00 07 00 00 00 40 00 00
                                                                   0
                                                        s^
         00 73 5E 07 00 00 64 00 64 01 6C 00 5A 00 65 01
                                                             ddl Ze
00000020
00000030 64 02 83 01 5A 02 65 03 65 02 83 01 64 03 6B 03 d f z e e (FSD) A @ ∰ <u>M</u>
```

并以.pyc为后缀名保存。

(2) 用uncompyle反编译。(uncompyle6安装使用方法 - pcat - 博客园)

得到.py文件。



4.打开py文件进行分析。

```
login.py - C:\Users\86150\Desktop\login.py (2.7.18)
                                                                          ×
<u>File Edit Format Run Options Window Help</u>
input1 = input('input something:')
                                                                                    ٠
if len(input1) != 14:
    print ('Wrong length!')
    sys.exit()
else:
    code = []
    for i in range(13):
        code.append(ord(input1[i]) ^ ord(input1[(i + 1)]))
    code.append(ord(input1[13]))
    a1 = code[2]
    a2 = code[1]
    a3 = code[0]
    a4 = code[3]
    a5 = code[4]
    a6 = code[5]
    a7 = code[6]
    a8 = code[7]
    a9 = code[9]
    a10 = code[8]
    all = code[10]
    a12 = code[11]
    a13 = code[12]
    a14 = code[13]
      (a1 * 88 + a2 * 67 + a3 * 65 - a4 * 5 + a5 * 43 + a6 * 89 + a7 * 25 + a8
    if
    & (a1 * 89 + a2 * 7 + a3 * 12 - a4 * 25 + a5 * 41 + a6 * 23 + a7 * 20 - a8 *
    (a1 * 28 + a2 * 35 + a3 * 16 - a4 * 65 + a5 * 53 + a6 * 39 + a7 * 27 + a8 *
    (a1 * 23 + a2 * 34 + a3 * 35 - a4 * 59 + a5 * 49 + a6 * 81 + a7 * 25 + a8 *
    (a1 * 38 + a2 * 97 + a3 * 35 - a4 * 52 + a5 * 42 + a6 * 79 + a7 * 90 + a8 *
    (a1 * 22 + a2 * 27 + a3 * 35 - a4 * 45 + a5 * 47 + a6 * 49 + a7 * 29 + a8 *
    (a1 * 12 + a2 * 45 + a3 * 35 - a4 * 9 - a5 * 42 + a6 * 86 + a7 * 23 + a8 * 8
    (a1 * 79 + a2 * 62 + a3 * 35 - a4 * 85 + a5 * 33 + a6 * 79 + a7 * 86 + a8 *
    (a1 * 8 + a2 * 6 + a3 * 64 - a4 * 85 + a5 * 73 + a6 * 29 + a7 * 2 + a8 * 23
    (a1 * 67 - a2 * 68 + a3 * 68 - a4 * 51 - a5 * 43 + a6 * 81 + a7 * 22 - a8 *
    (a1 * 85 + a2 * 63 + a3 * 5 - a4 * 51 + a5 * 44 + a6 * 36 + a7 * 28 + a8 * 1
    (a1 * 47 + a2 * 64 + a3 * 66 - a4 * 5 + a5 * 43 + a6 * 112 + a7 * 25 + a8 *
    (a1 * 89 + a2 * 67 + a3 * 85 - a4 * 25 + a5 * 49 + a6 * 89 + a7 * 23 + a8 *
    (a1 * 95 + a2 * 34 + a3 * 62 - a4 * 9 - a5 * 43 + a6 * 83 + a7 * 25 + a8 * 1
        print('flag is GWHT{md5(your_input)}')
        print ('Congratulations and have fun!
                                                                       CSDA: @Hotel 0
```

一个简单异或加解方程(z3)最后MD5加密。

上脚本:

impor #解方	tł 程	hashlib
from	z3	import*

a1, a2, a3, a4, a5, a6, a7, a8, a9, a10, a11, a12, a13, a14 = Ints('a1 a2 a3 a4 a5 a6 a7 a8 a9 a10 a11 a12 a13 a14') $x=Solver() \\ x: add(a1 * 88 + a2 * 67 + a3 * 65 - a4 * 5 + a5 * 43 + a6 * 89 + a7 * 25 + a8 * 13 - a9 * 36 + a10 * 15 + a11 * 11 + a12 * 47 - a13 * 60 + a14 * 29 == 22748) \\ x: add(a1 * 89 + a2 * 7 + a3 * 12 - a4 * 25 + a5 * 41 + a6 * 23 + a7 * 20 - a8 * 66 + a9 * 31 + a10 * 8 + a11 * 2 - a12 * 41 - a13 * 39 + a14 * 17 == 7258) \\ x: add(a1 * 28 + a2 * 35 + a3 * 16 - a4 * 65 + a5 * 53 + a6 * 39 + a7 * 27 + a8 * 15 - a9 * 33 + a10 * 15 + a11 * 11 + a12 * 47 - a13 * 60 + a14 * 29 == 22748) \\ x: add(a1 * 23 + a2 * 34 + a3 * 35 - a4 * 59 + a5 * 49 + a6 * 81 + a7 * 27 + a8 * 15 - a9 * 33 + a10 * 13 + a11 * 10 + 12 * 90 - a13 * 34 + a14 * 23 == 26190) \\ x: add(a1 * 22 + a2 * 34 + a3 * 35 - a4 * 59 + a5 * 49 + a6 * 81 + a7 * 25 + a8 * 128 - a9 * 32 + a10 * 75 + a11 * 81 + a12 * 47 - a13 * 60 + a14 * 29 == 37136) \\ x: add(a1 * 22 + a2 * 97 + a3 * 35 - a4 * 52 + a5 * 47 + a6 * 49 + a7 * 29 + a8 * 18 - a9 * 26 + a10 * 57 + a11 * 81 + a12 * 47 - a13 * 60 + a14 * 29 == 37136) \\ x: add(a1 * 12 + a2 * 45 + a3 * 35 - a4 * 59 + a5 * 47 + a6 * 49 + a7 * 29 + a8 * 18 - a9 * 26 + a10 * 35 + a11 * 41 + a12 * 40 - a13 * 61 + a14 * 28 == 17298) \\ x: add(a1 * 12 + a2 * 45 + a3 * 35 - a4 * 85 + a5 * 37 + a6 * 49 + a7 * 29 + a8 * 14 - a9 * 30 + a10 * 25 + a11 * 11 + a12 * 57 - a13 * 50 - a44 * 9 = = 22764) \\ x: add(a1 * 8 + a2 * 6 + a3 * 64 - a4 * 85 + a5 * 37 + a6 * 29 + a7 * 2 + a8 * 23 - a9 * 30 + a10 * 25 + a11 * 11 + a12 * 57 - a13 * 50 - a14 * 9 = 22784) \\ x: add(a1 * 8 + a2 * 6 + a3 * 64 - a4 * 85 + a5 * 73 + a6 * 29 + a7 * 2 + a8 * 12 - a9 * 30 + a10 * 25 + a11 * 11 + a12 * 57 - a13 * 60 - a14 * 9 = = 22784) \\ x: add(a1 * 8 + a2 * 6 + a3 * 64 - a4 * 85 + a5 * 73 + a6 * 29 + a7 * 2 + a8 * 12 - a9 * 30 + a10 * 25 + a11 * 11 + a12 * 57 - a13 * 64 + a14 * 27 = = 9710) \\ x: add(a1 * 85 + a2 * 63 + a3 * 56 - a4 * 51 + a5 * 44 + a6 * 36 + a7 * 22 + a8 * 12 - a9 * 36 + a10 * 75 + a11 * 31 + a12 * 47 - a13 * 64 + a14 * 27 = = 9710) \\ x: add(a1 * 89 + a2 * 67 + a3 * 86 - a4 * 51 + a5 * 44 + a6 * 36 + a7 * 22 + a8 * 15 - a9 * 36 + a10 *$ check = x.check() 🌛 Python 2.7.18 Shell П \times print(x.model()) <u>File Edit Shell Debug Options Window H</u>elp #异或 Python 2.7.18 (v2.7.18:8d21aa21f2, Apr 20 2020, 13:25:05) [MSC v.1500 64 bit (AM A D64)] on win32 Type "help", "copyright", "credits" or "license()" for more information. model=[119, 24, 10, 7, 104, 43, 28, 91, 52, 108, 88, 74, 88, 33]
new=[10, 24, 119, 7, 104, 43, 28, 91, 108, 52, 88, 74, 88, 33]
flag=' RESTART: C:\Users'
[a13 = 88,
 a3 = 10,
 a4 = 7,
 a10 = 108,
 a12 = 74,
 a1 = 119,
 a7 = 28,
 a6 = 43,
 a9 = 52,
 a14 = 33,
 a5 = 104,
 a8 = 91,
 a2 = 24,
 a11 = 88]
flag[56964088b637e50d3a22b9510c1d1ef8]
>>> ====== RESTART: C:\Users\86150\Desktop\1.py ===== for i in range(12,-1,-1):
 new[i] = new[i] ^new[i+1]
for i in range(len(new)):
 flag += chr(new[i]) #105110寥 mmbashib.md5()
m.update(flag.encode('utf-8'))
print('flag{'+m.hexdigest()+'}') CSDN @艸丛

5.get flag

flag{58964088b637e50d3a22b9510c1d1ef8}