

XCTF中hackme

原创

Most3R-03 于 2020-01-16 08:20:37 发布 281 收藏

分类专栏: [ctf安全实验室逆向](#)

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/recordliu/article/details/103998645>

版权



[ctf安全实验室逆向](#) 专栏收录该内容

3 篇文章 0 订阅

订阅专栏

总结

写代码时注意类型值的范围, 防止超出范围导致结果或者运行异常。

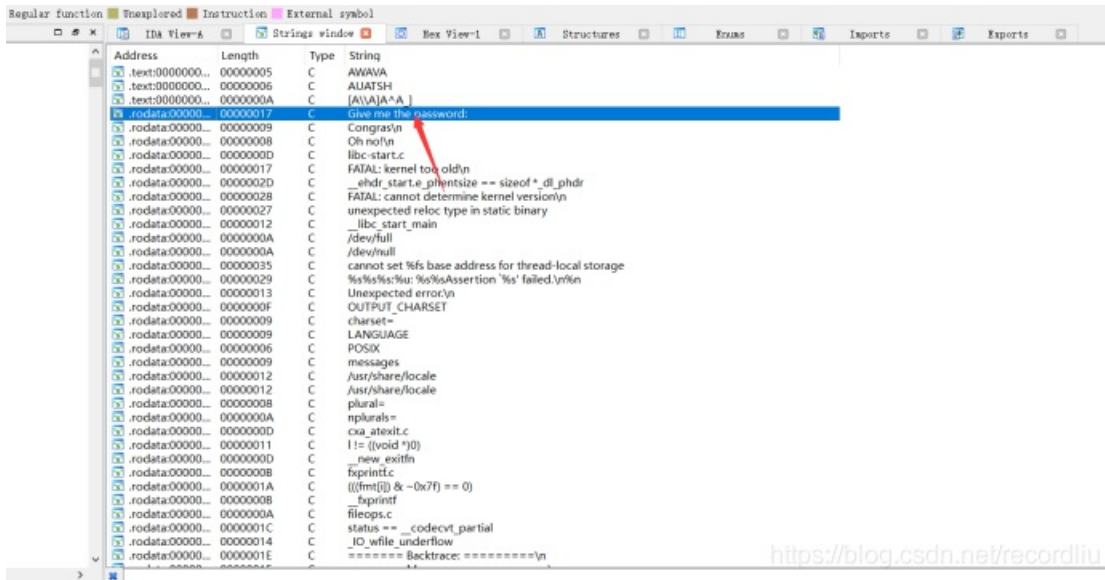
逆向开始

不是exe文件, 记事本打开一下, 发现是elf linux文件。

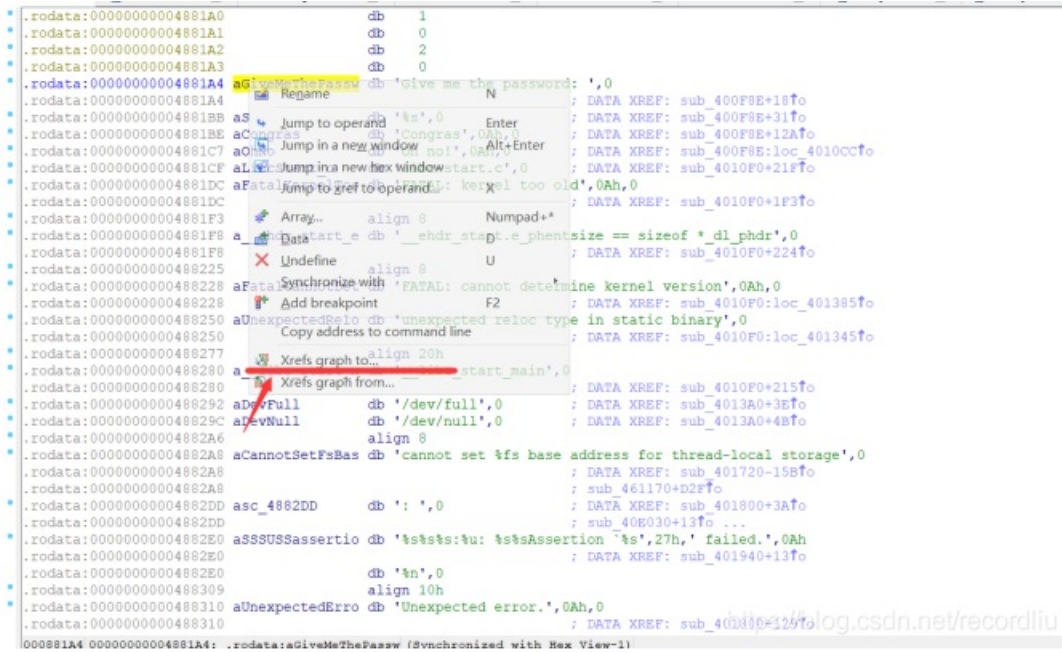
```
ctf - 记事本
文件(E) 编辑(E) 格式(O) 查看(V) 帮助(H)
|ELF 0000 > 0 n0@ @ 鏗0 @ 8 0 @ 0 0 @ @
烜0 烜0 0 0 燭0 燭k 燭k ? (@ 0 0 X0 X0@
X0@ D D 0 0 0 燭0 燭k 燭k P 0 Q鏢d
0 0 0 0 GNU 0 0 0 0 GNU 4?匱1?臺KT0破
芒? PBk % @DA HBk % 0YG @Bk % 愨A 8Bk %
€澗 0Bk % 爲A (Bk % 0嶠 Bk % €樹 0Bk % 類A
0Bk % `澗 H浚0H?m?+ H伊0鏢 H頤0? %j?+ h ?
%b?+ h ? %Z?+ h ? %R?+ h ? %J?+ h ? %B?+ h ?
%:?+ h ? %2?+ h ? %*?+ h ? ?標 @句0功 AT繼 U垚SH佸 0 H
委?.0 湮 墻0配 ? 鯨岑 孛鏢00 峴 H浞$0變鏢.0? 酒岑 孛?00 1佳銃H 1黎T00 A壞
H暖$ ? 0 D委铨00 Hc鏢佞~0H暖$ H壺孛極00 Hc蠟9趨蕊c 0 00H世 0 [JA\尙
?專 L?暉 E1見0勃t5H0拘?Q0u0<_t0D岑訟€?v0<:u▲A?忘 敢G ?
</u0A 翽凜0u0D杏) 0?/H 蒞 齐碧0: ? H 瞧G /膾?尙?A? 0? 忒
0H?H啤0H?0禦0牙0凜 w$伊x?燙? 0k?D壠內 )???M碼蘆?肫肫I聯1纒空H兩
L壠H文AWAVAUATSH浚00?虎L壺H餐L峯 站 €麒0哩 L皓0H鉤I鬱L)龍壽L塔蒜
峴H宮餒)腩邛$0富餒孛桎? L葵莖c鞠膠L0鎰9鑽`H 衍0 藜帕 均 uKL9鑽F1鯨麥
7 | 蒜 蜚?F?&E映 鏢0?勳x0€?u0H 衍0| 蔑9鏢?w痞0勳0| 请0A0綺 L壠震H
姓?L壠H恹豕A\A]A^A_]肫H文AWI?? AVI壺AUATSH結H浚h柁00 ? |壠H壠鑽00 L卵
? A壞?00 M喏taH崕€H晤恂爰堆x H荅€ 鏢? H湮 媿x u0f荅? ?艱0? H
崕€H晤嫩蜚荅€ ?? H湮 u0f荅? ?艱0? L)鶉壺? H俯 0 vH壺H整x 1坭\0 H嫵
x 伊0睨€?0H峴H宮餒)腩邛$0蒜痣"H壺H整x 栲00 H伊壞H嫵x 0勳
L吞L委L晤拌4? L夠L鳥怛壠H巽 1纒 煮9?倂 A0?悞蠶€ w>H乔? 江0Hc菟
H?H?L嫵蛤H訟L畜虎H餐L屹 L)璉 莖湮 t疋?0F? 膝M喏t▲@堅幕驛€ ,t0圖 H 孰
悒?M姓H訟M0E拜輕虎H餐H 葵)滌 葵渣 0刪 A?0@?
腩勳H市u0L委H整x ?0 H嫵x ?L夫H恹豕A\A]A^A_]肫H文AWI?? AVI壺
AUATSH結H浚h柁 0 ? |壠H壠鑽00 L卵? A壞?00 M喏taH崕€H晤恂爰堆x H荅€
```

无法载入OD, 选择直接拖入ida64位

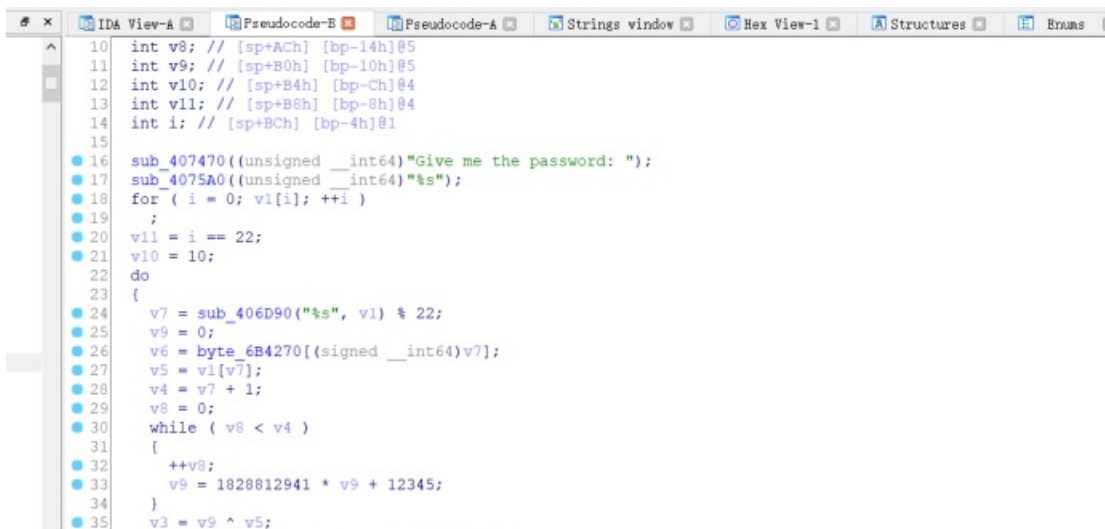
文件略大，直接按shift+f12进入字符串。



发现有关键字，双击进去看看，



右击选择交叉引用，到400f8e处直接按f5伪代码。



```
36     if ( v6 != ((unsigned __int8)v9 ^ v5) )
37         v11 = 0;
38         --v10;
39     }
40     while ( v10 )
41     if ( v11 )
42         v2 = sub_407470((unsigned __int64)"Congrats\n");
43     else
44         v2 = sub_407470((unsigned __int64)"Oh no!\n");
45     return 0LL;
46 }
```

000010B8 sub_400F8E:42 <https://blog.csdn.net/recordliu>

找到关键代码，开始分析写题解

v7只有22个数，我们可以用一个for循环，把v10都等于一遍

```
13     int v13;
14     char v9;
15     int v7;
16     int v11;
17     int zifuchuan[] = { 0x5f, 0x0f2, 0x5e, 0x8b, 0x4e,
18                       0x0e, 0x0a3, 0x0aa, 0x0c7, 0x93,
19                       0x81, 0x3d, 0x5f, 0x74, 0x0a3, 0x9
20                       , 0x91, 0x2b, 0x49, 0x28, 0x93, 0x67 };
21
22     for (int i = 0; i < 22; i++)
23     {
24         v10 = i;
25         v13 = 10;
26         do {
27             v12 = 0;
28             v7 = v10 + 1;
29             v11 = 0;
30             v9 = zifuchuan[v10];
31             while (v11 < v7)
32             {
33                 ++v11;
34                 v12= 1828812941 * v12 + 12345;
35             }
36
37             v8 = (unsigned __int8)v12^zifuchuan[v10];
38             --v13;
39         } while (v13);
```

100% <https://blog.csdn.net/recordliu>

```
16     int v11;
17     int zifuchuan[] = { 0x5f, 0x0f2, 0x5e, 0x8b, 0x4e,
18                       0x0e, 0x0a3, 0x0aa, 0x0c7, 0x93,
19                       0x81, 0x3d, 0x5f, 0x74, 0x0a3, 0x9
20                       , 0x91, 0x2b, 0x49, 0x28, 0x93, 0x67 };
21
22     for (int i = 0; i < 22; i++)
23     {
24         v10 = i;
25         v13 = 10;
26         do {
27             v12 = 0;
28             v7 = v10 + 1;
29             v11 = 0;
30             v9 = zifuchuan[v10];
31             while (v11 < v7)
32             {
33                 ++v11;
34                 v12= 1828812941 * v12 + 12345;
```

选择Microsoft Visual Studio 调试控制台
Flag {d826e6926098ef46}
C:\Users\bi_jiben\source\repos\ceshi\Debug\ceshi.exe (进程 17940) 已退出，返回代码为：0。
若要在调试停止时自动关闭控制台，请启用“工具”->“选项”->“调试”->“调试停止时自动关闭控制台”。
按任意键关闭此窗口...

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

A12应该在do里每次循环都置一次0，防止过大超出int的范围导致循环异常。