攻防世界Reverse进阶区-Shuffle-writeup

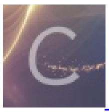
原创

y4ung 于 2020-09-19 09:20:43 发布 289 收藏

分类专栏： ctf 文章标签： ctf

本文链接：https://blog.csdn.net/qq_35056292/article/details/108676766

版权



ctf 专栏收录该内容

35 篇文章 0 订阅

订阅专栏

1. 介绍

本题是xctf攻防世界中Reverse的进阶区的题Shuffle

题目来源：SECCON-CTF-2014

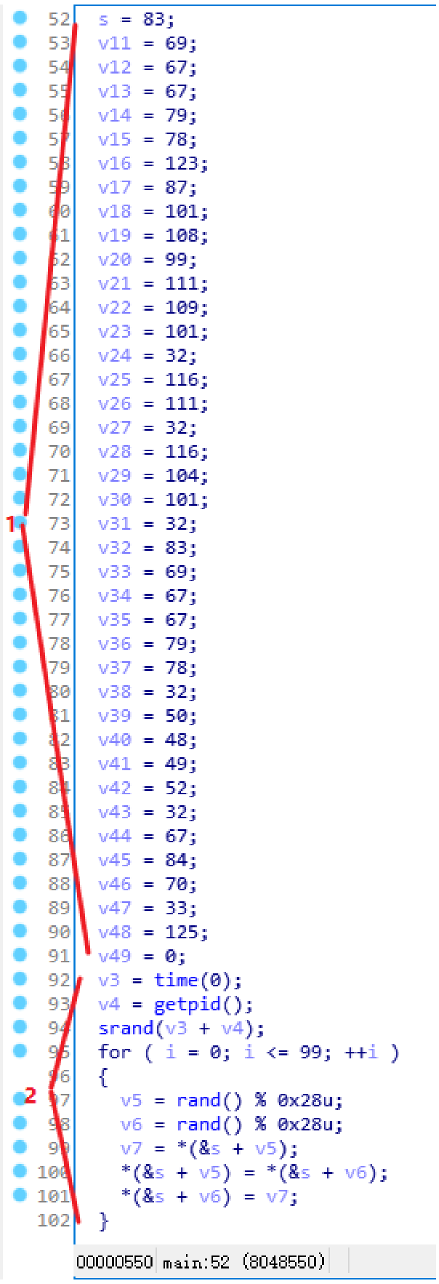
题目描述：找到字符串在随机化之前

2. 分析

Linux下的32位可执行文件

```
$ file c792c7d80be7404ca9789da97406d2ad
c792c7d80be7404ca9789da97406d2ad: ELF 32-bit LSB executable, Intel 80386, version 1 (SYSV), dynamically linked,
interpreter /lib/ld-linux.so.2, for GNU/Linux 2.6.24, BuildID[sha1]=943d2b390732673f2cfb69d12b64dc659f6779dd, no
t stripped
```

先扔进IDA里分析一下。在第1个部分中，s是某个字符串的起始，然后又定义了v11~v49这么多个字符。在第二个部分中以time和getpid的值作为种子生成随机数对s进行随机变换。那么，s应该就是flag了。



```
  s = 83;
  v11 = 69;
  v12 = 67;
  v13 = 67;
  v14 = 79;
  v15 = 78;
  v16 = 123;
  v17 = 87;
  v18 = 101;
  v19 = 108;
  v20 = 99;
  v21 = 111;
  v22 = 109;
  v23 = 101;
  v24 = 32;
  v25 = 116;
  v26 = 111;
  v27 = 32;
  v28 = 116;
  v29 = 104;
  v30 = 101;
  v31 = 32;
  v32 = 83;
  v33 = 69;
  v34 = 67;
  v35 = 67;
  v36 = 79;
  v37 = 78;
  v38 = 32;
  v39 = 50;
  v40 = 48;
  v41 = 49;
  v42 = 52;
  v43 = 32;
  v44 = 67;
  v45 = 84;
  v46 = 70;
  v47 = 33;
  v48 = 125;
  v49 = 0;
  v3 = time(0);
  v4 = getpid();
  srand(v3 + v4);
  for ( i = 0; i <= 99; ++i )
  {
    v5 = rand() % 0x28u;
    v6 = rand() % 0x28u;
    v7 = *(&s + v5);
    *(&s + v5) = *(&s + v6);
    *(&s + v6) = v7;
  }
```

```
00000550 main:52 (8048550)
```

尝试把数字转成字符（鼠标选中数字，按 `R` 键），一下子就看出flag了！
[外链图片转存失败,源站可能有防盗链机制,建议将图片保存下来直接上传(img-ppF3z7eC-1600478412108)(en-resource://database/967:1)]

最后写个脚本提取一下就拿到flag了：`SECCON{Welcome to the SECCON 2014 CTF!}`

```
target_str = """s = 'S';
  v11 = 'E';
  v12 = 'C';
  v13 = 'C';
  v14 = 'O';
  v15 = 'N';
  v16 = '{';
  v17 = 'W';
  v18 = 'e';
  v19 = 'l';
  v20 = 'c';
  v21 = 'o';
  v22 = 'm';
  v23 = 'e';
  v24 = ' ';
  v25 = 't';
  v26 = 'o';
  v27 = ' ';
  v28 = 't';
  v29 = 'h';
  v30 = 'e';
  v31 = ' ';
  v32 = 'S';
  v33 = 'E';
  v34 = 'C';
  v35 = 'C';
  v36 = 'O';
  v37 = 'N';
  v38 = ' ';
  v39 = '2';
  v40 = '0';
  v41 = '1';
  v42 = '4';
  v43 = ' ';
  v44 = 'C';
  v45 = 'T';
  v46 = 'F';
  v47 = '!';
  v48 = '}';"""

import re
res = re.findall(r".*?'(.*)'.*?", target_str)
print("flag:", "".join(res))  # SECCON{Welcome to the SECCON 2014 CTF!}
```