Vietnam

发表于 2021-01-09 分类于 Challenge， 2020， CSICTF， Reverse
Challenge | 2020 | CSICTF | Reverse | Vietnam

点击此处获得更好的阅读体验

WriteUp来源

https://dunsp4rce.github.io/csictf-2020/reversing/2020/07/22/Vietnam.html

by AnandSaminathan

题目描述

> *The Viet Cong in transmitting a secret message. They built a password checker so that only a selected few can view the secret message. We've recovered the binary, we need you to find out what they're trying to say.*

题目考点

解题思路

On decompiling using Ghidra:

```
undefined8 main(void)
{
  undefined *puVar1;
  int iVar2;
  int local_18;
  int local_14;
  char *local_10;

  local_10 = (char *)malloc(0x400);
  fgets(local_10,0x400,stdin);
  setbuf(stdout,(char *)0x0);
  while (puVar1 = sa, *local_10 != '\0') {
    switch(*local_10) {
    case '!':
      tmp = sa;
      sa = sb;
      sb = sc;
      sc = puVar1;
      break;
    case '$':
      sa = sa + 1;
      *sa = 1;
      break;
    case '+':
      sa[-1] = *sa + sa[-1];
      sa = sa + -1;
      break;
    case ',':
      iVar2 = getchar();
      *sa = (char)iVar2;
      break;
    case '-':
      sa[-1] = sa[-1] - *sa;
      sa = sa + -1;
      break;
    case '.':
      puVar1 = str + 1;
      *str = *sa;
      str = puVar1;
      break;
    case '[':
      if (*sa == '\0') {
        local_14 = 1;
        while (local_14 != 0) {
          local_10 = local_10 + 1;
```

```
46          if (*local_10 == '[') {
47            local_14 = local_14 + 1;
48          }
49          else {
50            if (*local_10 == ']') {
51              local_14 = local_14 + -1;
52            }
53          }
54        }
55      }
56      break;
57    case ']':
58      if (*sa != '\0') {
59        local_18 = 1;
60        while (local_18 != 0) {
61          local_10 = local_10 + -1;
62          if (*local_10 == '[') {
63            local_18 = local_18 + -1;
64          }
65          else {
66            if (*local_10 == ']') {
67              local_18 = local_18 + 1;
68            }
69          }
70        }
71      }
72    }
73    local_10 = local_10 + 1;
74  }
75  str = STR;
76  iVar2 = strcmp(STR,"HELLO\n");
77  if (iVar2 == 0) {
78    puts(str);
79    system("cat flag.txt");
80  }
81  else {
82    puts("Failed.");
83  }
84  return 0;
85 }
```

Although there are a lot of cases, , and . looks interesting. , takes a single character input (`ivar2`) and . appends `ivar2` to the string `STR`. After all this, if `STR` is "HELLO", the flag will be printed. So the flag can be obtained using the following input:

```
1 ,.,.,.,.,.,.
2 HELLO
```

Flag

```
1 csictf{l00k_4t_th3_t0w3rs_0f_h4n01}
```

- ***本文作者：*** *CTFHub*
- ***本文链接：*** *https://writeup.ctfhub.com/Challenge/2020/CSICTF/Reverse/rKBgtqcEZLoiR4irCygF21.html*
- ***版权声明：*** *本博客所有文章除特别声明外，均采用 BY-NC-SA 许可协议。转载请注明出处！*

 # Challenge # 2020 # Reverse # CSICTF
pydis2ctf
Scrambled-Eggs