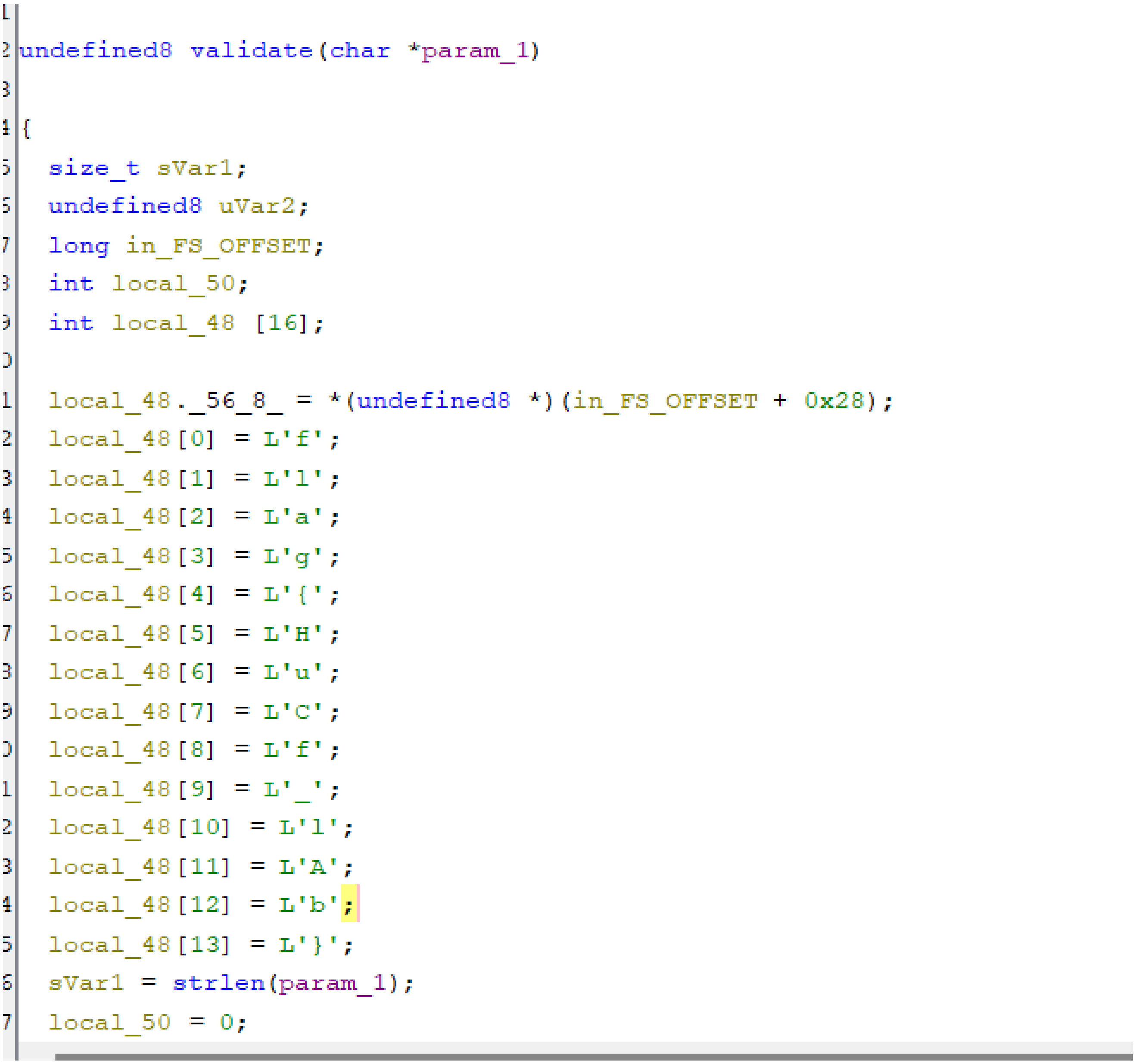
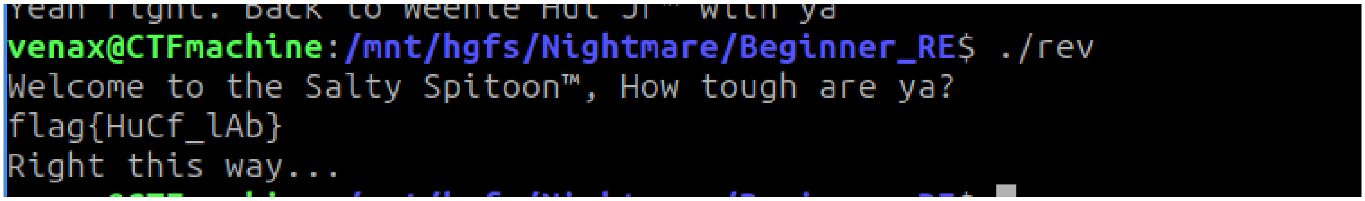
Beginner RE

Helithumper_RE



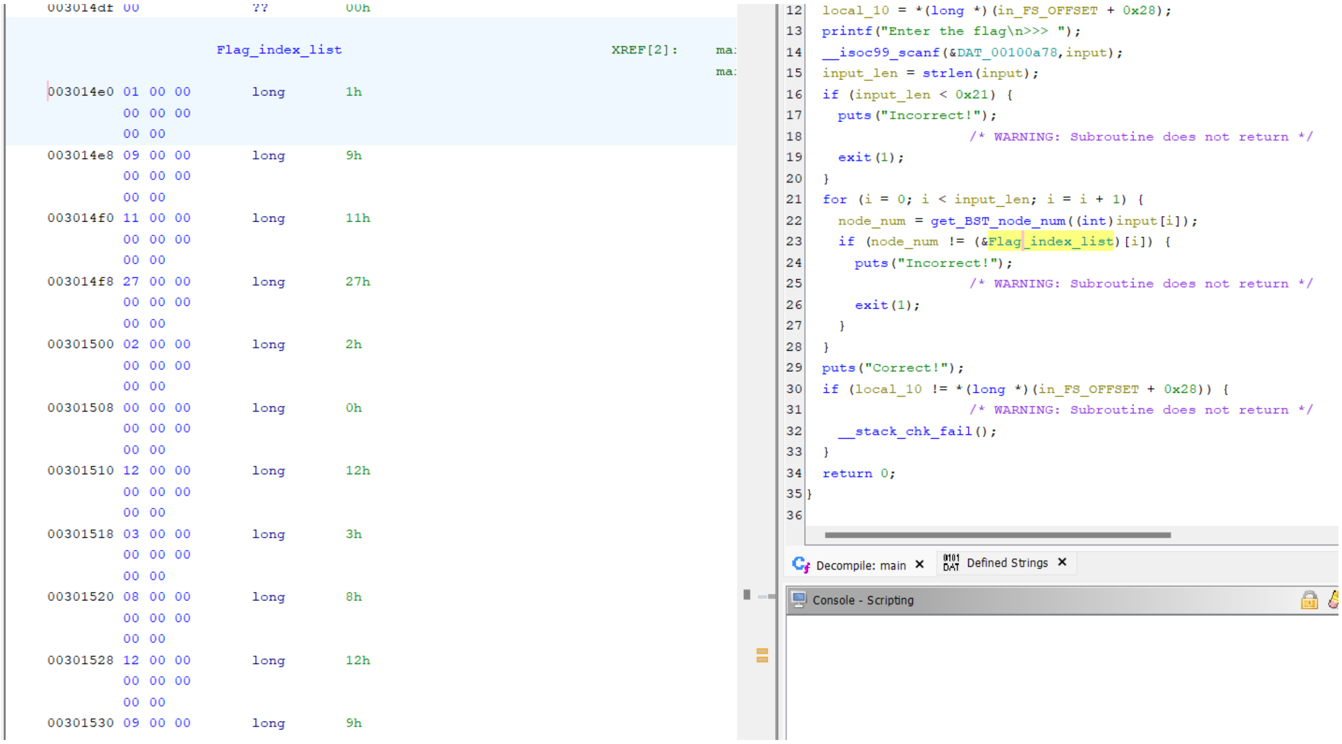
```

undefined8 validate(char *param_1)

{
  size_t sVar1;
  undefined8 uVar2;
  long in_FS_OFFSET;
  int local_50;
  int local_48 [16];

  local_48._56_8_ = *(undefined8 *)(in_FS_OFFSET + 0x28);
  local_48[0] = L'f';
  local_48[1] = L'l';
  local_48[2] = L'a';
  local_48[3] = L'g';
  local_48[4] = L'{';
  local_48[5] = L'H';
  local_48[6] = L'u';
  local_48[7] = L'C';
  local_48[8] = L'f';
  local_48[9] = L'_';
  local_48[10] = L'l';
  local_48[11] = L'A';
  local_48[12] = L'b';
  local_48[13] = L'}';
  sVar1 = strlen(param_1);
  local_50 = 0;
```



```
Yeah right. Back to Weenie Hut Jr™ with ya
venax@CTFmachine:/mnt/hgfs/Nightmare/Beginner_RE$ ./rev
Welcome to the Salty Spitoon™, How tough are ya?
flag{HuCf_lAb}
Right this way...
venax@CTFmachine:/mnt/hgfs/Nightmare/Beginner_RE$
```

Csaw19_Beleaf

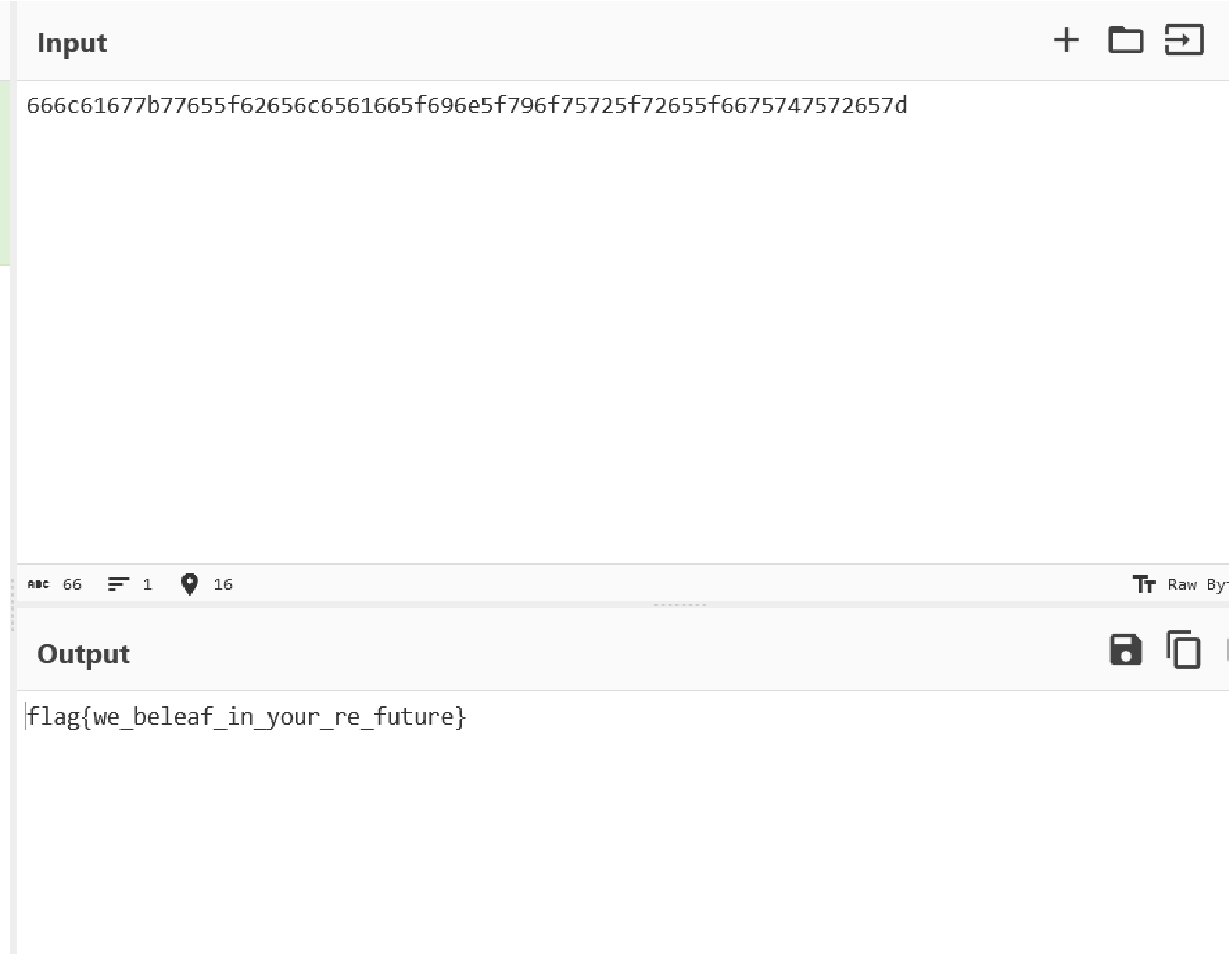
The code performs Binary Search Tree lookups in a specific order specified in the global.



```
003014df 00          ??         00h

                Flag_index_list                         XREF[2]:    ma:
                                                                    ma:
003014e0 01 00 00    long       1h
         00 00 00
         00 00
003014e8 09 00 00    long       9h
         00 00 00
         00 00
003014f0 11 00 00    long       11h
         00 00 00
         00 00
003014f8 27 00 00    long       27h
         00 00 00
         00 00
00301500 02 00 00    long       2h
         00 00 00
         00 00
00301508 00 00 00    long       0h
         00 00 00
         00 00
00301510 12 00 00    long       12h
         00 00 00
         00 00
00301518 03 00 00    long       3h
         00 00 00
         00 00
00301520 08 00 00    long       8h
         00 00 00
         00 00
00301528 12 00 00    long       12h
         00 00 00
         00 00
00301530 09 00 00    long       9h
```

```
  local_10 = *(long *)(in_FS_OFFSET + 0x28);
  printf("Enter the flag\n>>> ");
  __isoc99_scanf(&DAT_00100a78,input);
  input_len = strlen(input);
  if (input_len < 0x21) {
    puts("Incorrect!");
                    /* WARNING: Subroutine does not return */
    exit(1);
  }
  for (i = 0; i < input_len; i = i + 1) {
    node_num = get_BST_node_num((int)input[i]);
    if (node_num != (&Flag_index_list)[i]) {
      puts("Incorrect!");
                    /* WARNING: Subroutine does not return */
      exit(1);
    }
  }
  puts("Correct!");
  if (local_10 != *(long *)(in_FS_OFFSET + 0x28)) {
                    /* WARNING: Subroutine does not return */
    __stack_chk_fail();
  }
  return 0;
}
```

On doing the lookups manually by jumping to the offsets specified and copying the hex values in the BST we get the flag:



```
666c61677b77655f62656c6561665f696e5f796f75725f72655f6675747572657d
```

```
flag{we_beleaf_in_your_re_future}
```