B05901159 邱昱禎 電機四

解題思路

一開始先 decompile main function，大致看的出來主要就是程式吃到一個字串後會丟進 dummy 做處理，最後再輸出。於是我們就到 dummy function 裡面看看。

```
1  int __cdecl main(int argc, const char **argv, const char **envp)
2  {
3    char *v3; // ST08_8
4    char s; // [rsp+10h] [rbp-410h]
5    unsigned __int64 v6; // [rsp+418h] [rbp-8h]
6
7    v6 = __readfsqword(0x28u);
8    printf("Input: ", argv, envp);
9    fgets(&s, 1024, _bss_start);
10   v3 = _dummy(&s);
11   puts(v3);
12   return 0;
13 }
```

接著看到他會先做換行字元的處理，接著建一個兩倍大的空陣列，然後跑 for 迴圈處理陣列。

Sudo code 可寫成

asca74 = ‘'~!@#$%^&*()_+=-?''

v4 = 0

for i in len(output*2):

    v1 = input[i/2]/16   if i is odd

    v4 = (init(v4) + v1) %16   // init 可視為一 int mapping 到 int 的 function

    v6[i] = asca74[v4]

所以可由下列方程式回推出答案

target_char[i] = 16x+y

output[i*2] = reverse_init(output[i*2-1]) + x

output[i*2+1] = reverse+init(output[i*2]) + y

已知 output 可得 target_char

Flag : NMLab{bA5e16_Is_muCh_Eas1er_ThAn_Base64}