

## Writeup soal\_rev1

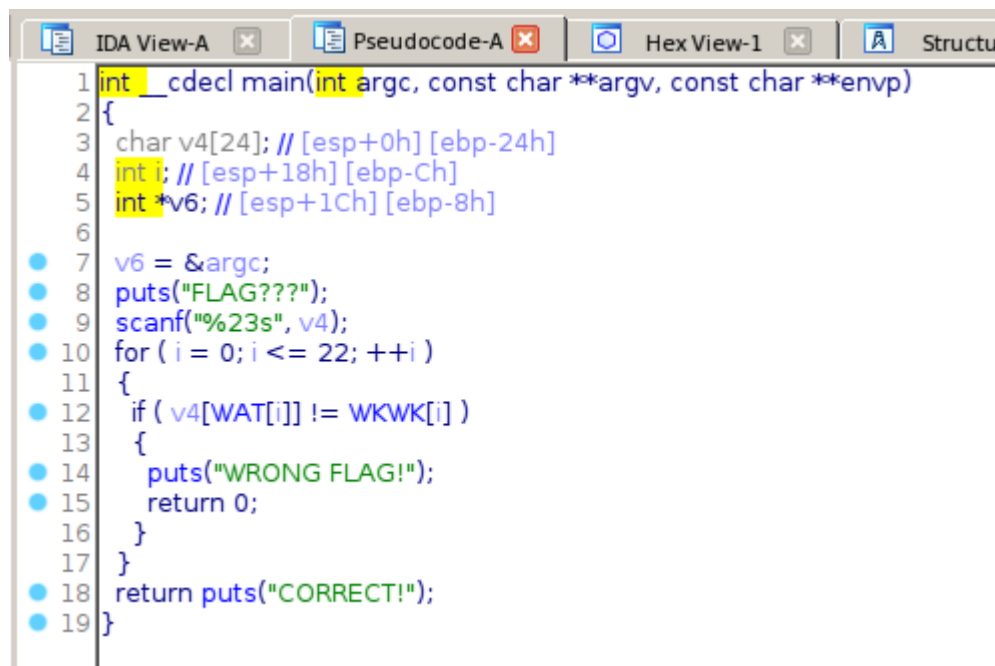
```
soal_rev1: ELF 32-bit LSB executable, Intel 80386, version 1 (SYSV), dynamically linked,
interpreter /lib/ld-linux.so.2, for GNU/Linux 3.2.0, BuildID[sha1]=cb4ec8b31200b976636935
f254e949f60d7235c0, not stripped
```

```
uS_3eNr5r_i_Ne1a_nzgdFv
FLAG???
%23s
WRONG FLAG!
CORRECT!
```

Output dari tool strings menunjukkan suatu string dengan panjang 23 karakter yang kemungkinan adalah flag, dan juga suatu format string yang memiliki arti string dengan 23 karakter, kemungkinan format string tersebut dipakai untuk fungsi scanf yang berguna untuk menerima user input.

```
mrcoffee@mrcoffee-SVF14218SGW:~/Documents$ ./soal_rev1
FLAG???
uS_3eNr5r_i_Ne1a_nzgdFv
WRONG FLAG!
```

Ternyata string yang tadi bukan flag dari soal ini.



```
1 int __cdecl main(int argc, const char **argv, const char **envp)
2 {
3     char v4[24]; // [esp+0h] [ebp-24h]
4     int i; // [esp+18h] [ebp-Ch]
5     int *v6; // [esp+1Ch] [ebp-8h]
6
7     v6 = &argc;
8     puts("FLAG???");
9     scanf("%23s", v4);
10    for ( i = 0; i <= 22; ++i )
11    {
12        if ( v4[WAT[i]] != WKWK[i] )
13        {
14            puts("WRONG FLAG!");
15            return 0;
16        }
17    }
18    return puts("CORRECT!");
19 }
```

Program dibuka di tool IDA pro dan didekompilasi. Dapat dipastikan panjang flag 23 karakter. Setelah input diterima program melakukan pemeriksaan input dengan suatu loop. Variabel v4 adalah user input, pada saat iterasi v4 indeks ke WAT[i] diperiksa apakah sama dengan WKWK[i], dengan  $0 \leq i \leq 22$ . Dapat diperkirakan bahwa WKWK adalah string dengan panjang 23 karakter, sedangkan isi WAT perlu diperiksa.

```

.data:0804A040      public WAT
.data:0804A040 ; int WAT[23]
.data:0804A040 WAT      dd 0Eh      ; DATA XREF: main+51↑r
.data:0804A044      db  5
.data:0804A045      db  0
.data:0804A046      db  0
.data:0804A047      db  0
.data:0804A048      db 14h
.data:0804A049      db  0
.data:0804A04A      db  0
.data:0804A04B      db  0
.data:0804A04C      db  1
.data:0804A04D      db  0
.data:0804A04E      db  0
.data:0804A04F      db  0
.data:0804A050      db 15h
.data:0804A051      db  0
.data:0804A052      db  0
.data:0804A053      db  0
.data:0804A054      db 0Fh
.data:0804A055      db  0
.data:0804A056      db  0
.data:0804A057      db  0
.data:0804A058      db  0
.data:0804A059      db  0
.data:0804A05A      db  0
.data:0804A05B      db  0
.data:0804A05C      db 0Bh
.data:0804A05D      db  0
.data:0804A05E      db  0
.data:0804A05F      db  0

```

Dilihat dari selisih alamat item kedua WAT dan item pertama WAT (4 byte) maka WAT adalah array yang berisi integer/bilangan bulat, dan dari pemeriksaan WAT memiliki 23 integer.

```

.rodata:08048590 aUs3eNr5r_i_Ne1a_nzgdFv,0
.rodata:08048590      ; DATA XREF: .data:WKWK↓o
.rodata:080485A8 aFlag      db 'FLAG???' ; DATA XREF: main+20↑o

```

String WKWK.

```

1 WAT = [14, 5, 20, 1, 21, 15, 0, 11, 4, 9, 10, 12, 18, 3, 6, 17, 16, 7, 22, 8, 19, 13, 2]
2 WKWK = "uS_3eNr5r_i_Ne1a_nzgdFv"
3 flag = ['=' for i in range(23)]
4 for w, c in zip(WAT, WKWK):
5     flag[w] = c
6 print ''.join(flag)

```

Sebuah script python digunakan untuk memecahkan soal ini. Pertama flag adalah list yang diisi dengan karakter '=' sebanyak 23 karakter. Kemudian untuk setiap bilangan w pada WAT dan karakter c pada WKWK flag indeks ke-w diberi nilai c. Setelah itu list yang berisi karakter tersebut diubah menjadi string dan di print

```

mrcoffee@mrcoffee-SVF14218SGW:~/Documents$ python solver_soal_rev1.py
r3verS1ng_i5_FuN_aNd_ez

```

Flagnya adalah r3verS1ng\_i5\_FuN\_aNd\_ez.

```
mrcoffee@mrcoffee-SVF14218SGW:~/Documents$ ./soal_rev1  
FLAG???  
r3verS1ng_i5_FuN_aNd_ez  
CORRECT!
```