

# Cache Me Outside

## Description

While being super relevant with my meme references, I wrote a program to see how much you understand heap allocations. `nc mercury.picoctf.net 17612`

## Attempts

### Attempt 1: Decompiling using Ghidra

Since the compiled file is provided (`heapedit`), we can decompile it and have a look at the code.

We see that the flag is loaded from a file on the server (`flag.txt`) and then read into a variable (`char flag [72]`)

```
Decompile: main - (heapedit)
1
2 undefined8 main(void)
3
4 {
5     long in_FS_OFFSET;
6     undefined local_a9;
7     int local_a8;
8     int local_a4;
9     undefined8 *local_a0;
10    undefined8 *local_98;
11    FILE *flagfile;
12    undefined8 *local_88;
13    void *local_80;
14    undefined8 local_78;
15    undefined8 local_70;
16    undefined8 local_68;
17    undefined local_60;
18    char flag [72];
19    long local_10;
20
21    local_10 = *(long *) (in_FS_OFFSET + 0x28);
22    setbuf(stdout, (char *) 0x0);
23    flagfile = fopen("flag.txt", "r");
24    fgets(flag, 0x40, flagfile);
25    local_78 = 0x2073692073696874;
26    local_70 = 0x6d6f646e61722061;
27    local_68 = 0x2e676e6972747320;
28    local_60 = 0;
29    local_a0 = (undefined8 *) 0x0;
30    for (local_a4 = 0; local_a4 < 7; local_a4 = local_a4 + 1) {
31        local_98 = (undefined8 *) malloc(0x80);
32        if (local_a0 == (undefined8 *) 0x0) {
33            local_a0 = local_98;
34        }
35        *local_98 = 0x73746172676e6f43;
36        local_98[1] = 0x662072756f592021;
37        local_98[2] = 0x203a73692067616c;
38        *(undefined *) (local_98 + 3) = 0;
39        strcat((char *) local_98, flag);
40    }
41    local_88 = (undefined8 *) malloc(0x80);
42    *local_88 = 0x5420217972726f53;
43    local_88[1] = 0x276e6f7720736968;
44    local_88[2] = 0x7920706c65682074;
45    *(undefined4 *) (local_88 + 3) = 0x203a756f;
46    *(undefined *) ((long) local_88 + 0x1c) = 0;
47    strcat((char *) local_88, (char *) &local_78);
48    free(local_98);
49    free(local_88);
50    local_a8 = 0;
51    local_a9 = 0;
```

Figure 1: decompiled code