

HackTheBox HackyBird [by 0xChad]

Points: 30 Points

Description: Even Mr. Miyagi cannot seem to beat this game. Flap your wings and show him the way!

Link: <https://www.hackthebox.eu/home/challenges/Reversing>

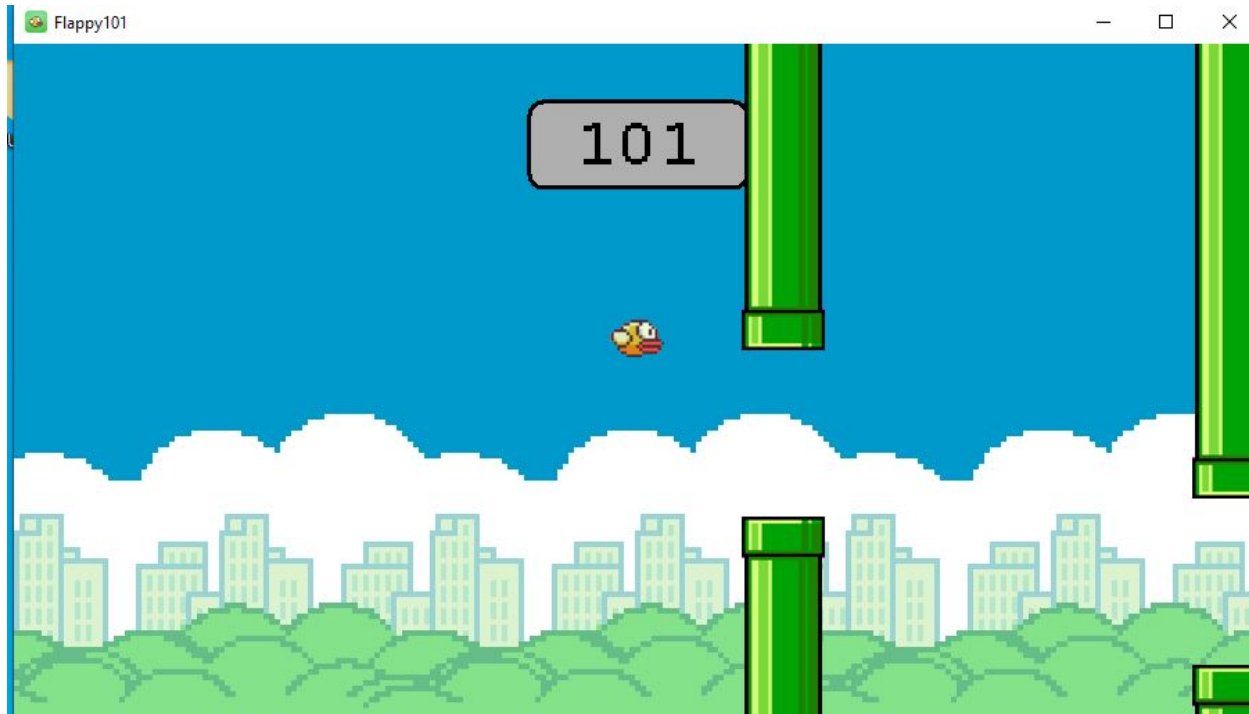
Download Link: <https://www.hackthebox.eu/home/challenges/download/192>

Zip Password: hackthebox

sha256:79d0b3c3a1b4b9dbf444224ae855b45d6b49fe34aa8ac5ef4286c98d560eb7fe



I opened Cheat Engine to try to hack my game score. I played the game and searched my memory for my current game score. Once I got the memory address for the users score I changed it to 101. However nothing occurred.



I used Cheat engine to figure out what was writing to our score memory address.

The following opcodes write to 00910FB4

Count	Instruction
1	00403404 - C7 83 94000000 00000000 - mov [ebx+00000094],00000000
1	0040312D - FF 86 94000000 - inc [esi+00000094]

```

00403127 - 7C 79 - jl HackyBird.exe+31A2
00403129 - C6 47 14 01 - mov byte ptr [edi+14],01
0040312D - FF 86 94000000 - inc [esi+00000094] <<
00403133 - 81 BE 94000000 E7030000 - cmp [esi+00000094],000003E7
0040313D - 7E 63 - jle HackyBird.exe+31A2

```

It looks like at 0x0040312D It increases the score by 1.

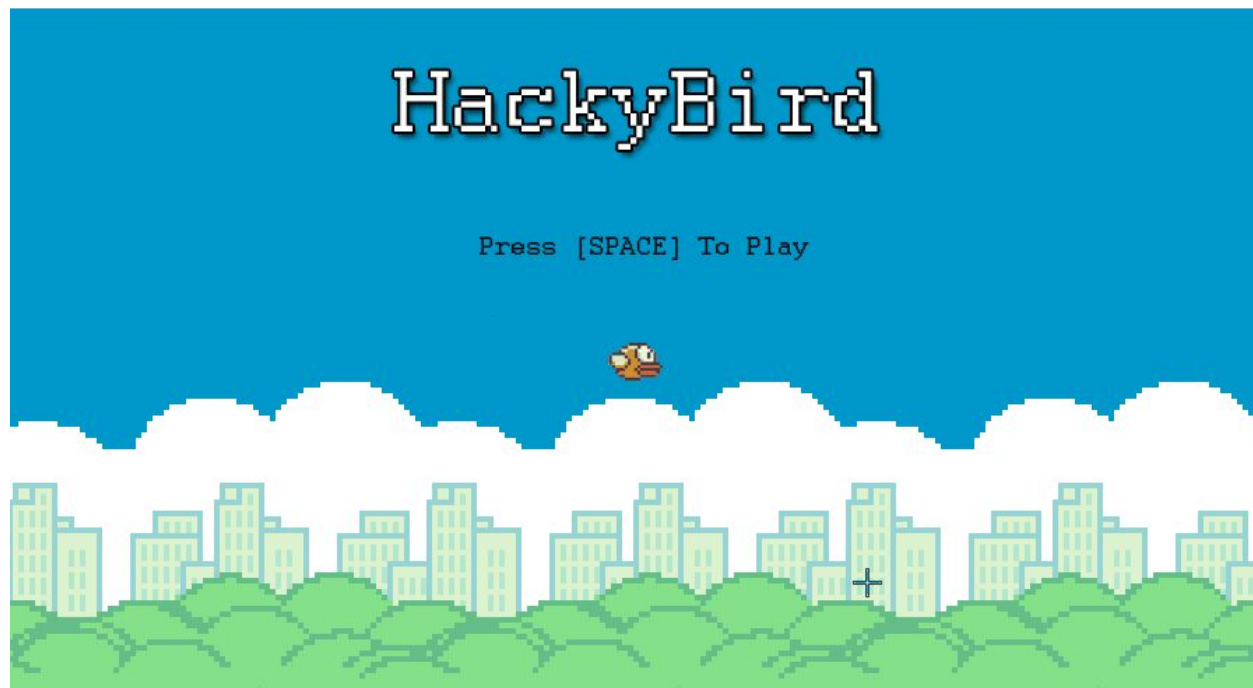
I loaded the game into Ghidra, a reverse engineering tool, so I could get a better understanding of what i'm looking for. I went to the memory address 0x0040312D

```


if ((* (char *) (piVar10 + 5) == '\\0') &&
    (piVar10[1] / 2 + piVar10[-1] <=
        *(int *) (param_1 + 0x20) / 2 + *(int *) (param_1 + 0x18))) {
    *(undefined *) (piVar10 + 5) = 1;
    *(int *) (param_1 + 0x94) = *(int *) (param_1 + 0x94) + 1;
    ppcVar6 = DAT_0041a4b4;
    if (999 < *(int *) (param_1 + 0x94)) {
        ppcVar6 = (code **) FUN_00404606(0x18);
        pcVar1 = *(code **) (param_1 + 0x94);
        *(undefined ***) ppcVar6 = &PTR_FUN_00416f68;
        ppcVar6[1] = *(code **) (param_1 + 4);
        ppcVar6[2] = *(code **) (param_1 + 8);
        ppcVar6[3] = *(code **) (param_1 + 0xc);
        ppcVar6[4] = *(code **) (param_1 + 0x10);
        *(undefined ***) ppcVar6 = &PTR_FUN_00416f58;
        ppcVar6[5] = pcVar1;
        piVar10 = piStack120;
        if (DAT_0041a4b4 != (code **) 0x0) {
            uStack20 = 4;
            ppcVar2 = (code **) *DAT_0041a4b4;
            DAT_0041a4b4 = ppcVar6;
            (**ppcVar2) (1);
            uStack20 = 0xffffffff;
            piVar10 = piStack120;

```

The line highlighted is 0x0040312D. Param_1 + 0x94 seems to be the user's score. 2 lines under this seem to be an if statement comparing the users score to 999. Let's change the score in are game to 999 and see what happens.



The challenge is not expired at the time of making this write-up so I will not be giving away the flag. When submitting the flag the game displayed on the screen I was notified that It was correct.


 [30 Points] HackyBird [by 0xChad] [223 solvers] 70  18  Difficulty: 

 First Blood: ryaagard

Even Mr. Miyagi cannot seem to beat this game. Flap your wings and show him the way!

 Download

 Zip Password: hackthebox sha256: 79d0b3c3a1b4b9dbf444224ae855b45d6b49fe34aa8ac5ef4286c98d560eb7fe

 Complete