

From the entry function we see a jump instruction that might be moving over a lot of essential instructions as when we run the binary nothing happens. So we need to replace this jump instruction with a nop operator.

```

22: entry0 ();
    0x0800004c  e9d6000000 jmp 0x8000127
    0x08000051  fec3      inc bl
    0x08000053  fec2      inc dl
    0x08000055  b98a000000 mov ecx, 0x8800008a ; '\n'
    0x0800005a  e8d0000000 call 0x800012f ;[1] ; entry0+0xe3
    0x0800005f  b988000000 mov ecx, 0x88000088 ; '\n'
    0x08000064  e8c6000000 call 0x800012f ;[1] ; entry0+0xe3
    0x08000069  b924000000 mov ecx, 0x88000024 ; '$'
    0x0800006e  e8bc000000 call 0x800012f ;[1] ; entry0+0xe3
    0x08000073  b98e000000 mov ecx, 0x8800008e ; '\x0e'
    0x08000078  e8b2000000 call 0x800012f ;[1] ; entry0+0xe3
    0x0800007d  b98e000000 mov ecx, 0x8800008e ; '\x0e'
    0x08000082  e8a8000000 call 0x800012f ;[1] ; entry0+0xe3
    0x08000087  b923000000 mov ecx, 0x88000023 ; '#'
    0x0800008c  e89e000000 call 0x800012f ;[1] ; entry0+0xe3
    0x08000091  b989000000 mov ecx, 0x88000089 ; '\n'
    0x08000096  e894000000 call 0x800012f ;[1] ; entry0+0xe3
    0x0800009b  b921000000 mov ecx, 0x88000021 ; '!'
    0x080000a0  e88e000000 call 0x800012f ;[1] ; entry0+0xe3
    0x080000a5  b98c000000 mov ecx, 0x8800008c ; '\n'
    0x080000aa  e880000000 call 0x800012f ;[1] ; entry0+0xe3
    0x080000af  b98d000000 mov ecx, 0x8800008d ; '\n'
    0x080000b4  e874000000 call 0x800012f ;[1] ; entry0+0xe3
    0x080000b9  b922000000 mov ecx, 0x88000022 ; '!'
    0x080000be  e86c000000 call 0x800012f ;[1] ; entry0+0xe3
    0x080000c3  b921000000 mov ecx, 0x88000021 ; '!'
    0x080000c8  e862000000 call 0x800012f ;[1] ; entry0+0xe3
    0x080000cd  b985000000 mov ecx, 0x88000085 ; '\n'
    0x080000d2  e858000000 call 0x800012f ;[1] ; entry0+0xe3
    0x080000d7  b921000000 mov ecx, 0x88000021 ; '!'
    0x080000dc  e84e000000 call 0x800012f ;[1] ; entry0+0xe3
    0x080000e1  b920000000 mov ecx, 0x88000020 ; '!'
    0x080000e6  e844000000 call 0x800012f ;[1] ; entry0+0xe3
    0x080000eb  b923000000 mov ecx, 0x88000023 ; '#'
    0x080000f0  e83a000000 call 0x800012f ;[1] ; entry0+0xe3
    0x080000f5  b90f000000 mov ecx, 0x8800000f ; '\x0f'
    0x080000fa  e830000000 call 0x800012f ;[1] ; entry0+0xe3
    0x080000ff  b907000000 mov ecx, 0x88000007 ; '\n'
    0x0800104  e82a000000 call 0x800012f ;[1] ; entry0+0xe3
    0x0800109  b922000000 mov ecx, 0x88000022 ; '\n'
    0x080010e  e81c000000 call 0x800012f ;[1] ; entry0+0xe3
    0x0800113  b925000000 mov ecx, 0x88000025 ; '%'
    0x0800118  e812000000 call 0x800012f ;[1] ; entry0+0xe3
    0x080011d  b905000000 mov ecx, 0x88000005 ; '\v'
    0x0800122  e801000000 call 0x800012f ;[1] ; entry0+0xe3
    ; CODE XREF from entry0 @ 0x800004c(x)
    0x0800127  30c0      xor al, al
    0x0800129  fec2      inc cl

```

The jmp address `0x0800004c` we switch to this address with `s 0x0800004c` then use `wao` to remove current opcode which is `jmp`

`o++`

`s 0x0800004c`

`wao nop`

```

;-- eip:
22: entry0 ();
0x0800004c  98      nop
0x0800004d  98      nop
0x0800004e  98      nop
0x0800004f  98      nop
0x08000050  98      nop
0x08000051  fec3    inc bl
0x08000053  fec2    inc dl
0x08000055  b78a0000 mov ecx, 0x800000a ; '\n'
0x0800005a  c8d80000 call 0x800012f ; [1] ; entry0+0xe3
0x0800005f  b7880000 mov ecx, 0x8000008
0x08000064  c8c40000 call 0x800012f ; [1] ; entry0+0xe3
0x08000069  b72d0000 mov ecx, 0x8000024 ; '$'

```

Now we see that it has been completely changed to now , now we run to test it.

And we find the flag

```

./golfer
HTB{y0U_4R3_a_g0lf3r}

```