

חלק 3

בהתחלה הרצתי את הפאץ' וראיתי שהוא לא נכנס לתוך הפלאג.

לכן הפעלתי את התוכנית באמצעות הדיבגר והתחלתי לעבור שורה שורה ושמתי לב שהקוד עושה בדיקה של האם שווה ל 0 ואם כן לקפוץ לסוף הקוד.

לכן שיניתי את הקוד כך שבפקודה הזאת יהיה `jne` במקום `je`.
כך הצלחתי להיכנס לפלאג ופתור את הבעיה.

```
public main
main proc near
var_4= dword ptr -4
; __unwind {
push    rbp
mov     rbp, rsp
sub     rbp, 10h
mov     [rbp+var_4], 0
lea     rax, s          ; "Trampolines are quite fun!; I love to j"...
mov     rdi, rax        ; s
call    _puts
lea     rax, aYouShouldTryJu ; "You should try jumping too! It'll sure "...
mov     rdi, rax        ; s
call    _puts
cmp     [rbp+var_4], 0
jnz     short loc_1176
```

```
mov     eax, 0
call    give_flag
```

```
loc_1176:
mov     eax, 0
leave
retn
; } // starts at 1139
main endp
```

```
evyatar@Evyatar:~/ComputerStructure/ex3$ ./patchwork
Trampolines are quite fun!; I love to jump!
You should try jumping too! It'll sure be more fun than reversing the flag manually.
PCTF{JUmP_uP_4nd_g3t_d0wn}
```