Mark Seliternikov
picoCTF - asm2 [250 points]

האתגר הזה היה יחסית קל אז הפתרון קצר בתוכן.
מקבלים אסמבלי, והמטרה היא למצוא מה יהיה הפלט עם
המשתנים אשר מקבלים.

יכולתי פשוט לקמפל את הקוד ולעשות printf כדי למצוא מה
יהיה הפלט, אבל המטרה שלי היא ללמוד אסמבלי בנוסף לשאר
הנושאים אז פתרתי ידנית כתרגול לאסמבלי

הנה הפתרון כתוב כתגובות מסביב לקוד המקורי

```
; Mark's solution
; asm2(0x4,0x21)
asm2:
    <+0>:   push   ebp
    <+1>:   mov    ebp,esp ; (32 bit)
    ; ebp+0x4 -> return adress
    ; ebp+0x8 -> 0x00 00 00 04  (c int is 4 bytes)
    ; ebp+0xc -> 0x00 00 00 21
    <+3>:   sub    esp,0x10
    <+6>:   mov    eax,DWORD PTR [ebp+0xc] ; eax = 0x... 21
    <+9>:   mov    DWORD PTR [ebp-0x4],eax ; ebp-0x4 -> 0x... 21
    <+12>:  mov    eax,DWORD PTR [ebp+0x8] ; eax = 0x... 04
    <+15>:  mov    DWORD PTR [ebp-0x8],eax ; ebp-0x8 -> 0x... 04
    <+18>:  jmp    0x509 <asm2+28> ; jumped once
    <+20>:  add    DWORD PTR [ebp-0x4],0x1 ; caculated below
    <+24>:  add    DWORD PTR [ebp-0x8],0x74 ; ebp-0x8 + 0x74 * 22b > 0xfb46
    <+28>:  cmp    DWORD PTR [ebp-0x8],0xfb46
    <+35>:  jle    0x501 <asm2+20> ; loops til ebp-0x8 is equal or more to 0xfb46
    <+37>:  mov    eax,DWORD PTR [ebp-0x4] ; eax = 21 + 22b = 0x24c
    <+40>:  leave
    <+41>:  ret    ; the solution is 0x24c
~
```

(השתמשתי ב-vim עם molokai theme למי שמעוניין)