Mark Seliternikov
picoCTF - asm3 [300 points]

לאתגר זה מקבלים קובץ אסמבלי (בסינטקס של אינטל) שנראה כך:

```
asm3:
        <+0>:   push   ebp
        <+1>:   mov    ebp,esp
        <+3>:   xor    eax,eax
        <+5>:   mov    ah,BYTE PTR [ebp+0x9]
        <+8>:   shl    ax,0x10
        <+12>:  sub    al,BYTE PTR [ebp+0xe]
        <+15>:  add    ah,BYTE PTR [ebp+0xf]
        <+18>:  xor    ax,WORD PTR [ebp+0x12]
        <+22>:  nop
        <+23>:  pop    ebp
        <+24>:  ret
```

האתגר שואל מה יהיה ה-output של asm3 אם קוראים לפונק' כך:

What does

asm3(0xd2c26416,0xe6cf51f0,0xe54409d5) return?

יש 2 דרכים לפתור את האתגר, אפשר פשוט לקמפל את האסמבלי ולראות מה יהיה ה-output (בעזרת C). או שאפשר לפתור ידנית.

למרות שאופציה א' יותר קלה, המטרה שלי באתגרים אלו היא ללמוד, לכן אעשה זאת ידנית כדי לעבוד על יכולות האסמבלי שלי. לשם כך הוספתי תגובות בקוד של האסמבלי ולמטה רשמתי את הדגל.

```
; Mark's solution
; asm3(0xd2c26416,0xe6cf51f0,0xe54409d5)
asm3:
        ; little endian
        ; ebp + 0x4 -> return adress
        ; ebp + 0x8 -> [16][64][c2][d2]
        ; ebp + 0xc -> [f0][51][cf][e6]
        ; ebp + 0x10 -> [d5][09][44][e5]
        <+0>:   push   ebp
        <+1>:   mov    ebp,esp ; (32 bit)
        <+3>:   xor    eax,eax ; equal to itself so eax = 0x00 00 00 00
        <+5>:   mov    ah,BYTE PTR [ebp+0x9] ; eax = 0x00 00 64 00
        <+8>:   shl    ax,0x10 ; eax = 0x00 00 00 00 (ax holds only 16 bits)
        <+12>:  sub    al,BYTE PTR [ebp+0xe] ; eax = 0x00 00 00 31
        <+15>:  add    ah,BYTE PTR [ebp+0xf] ; eax = 0x00 00 e6 31
        <+18>:  xor    ax,WORD PTR [ebp+0x12] ; eax = 0x00 00 03 75
        <+22>:  nop
        <+23>:  pop    ebp
        <+24>:  ret    ; flag = 0x375
```

השתמשתי במחשבון כדי לחשב את התוצאה של XOR ב-<+16>.

לאחר בדיקה, זה אכן הדגל :)

אולי התרגיל נראה קצר, אבל הוא דורש הבנה באסמבלי כדי להתמודד איתו.