code cave - patching

<u>השאלה:</u>

הדגם הזרקה של show message המציג את הת.ז. שלכם למשחק שולה מוקשים

1. פתיחת האפליקציה בOdbg ומציאת מקום מלא אפסים בקוד עבור הקוד שלנו

2. הכנסת הת.ז שלנו כמחרוזת המיועדת להצגה בהזרקת הקוד

```
00423E5F    00              DB 00
00423E60  . 38 34 36 31 3   ASCII "846180",0
```

3. מעבר לתחילת הקוד המקורי,העתקת הפקודות המקוריות ושמירת הכתובת אליה נרצה לחזור לאחר הקוד המוזרק

```
004193CD    00              DB 00
004193CE    00              DB 00
004193CF    00              DB 00
004193D0  . 55              PUSH EBP
004193D1  . 8BEC            MOV EBP,ESP
004193D3  . 83C4 D8         ADD ESP,-28
004193D6  . 53              PUSH EBX
```

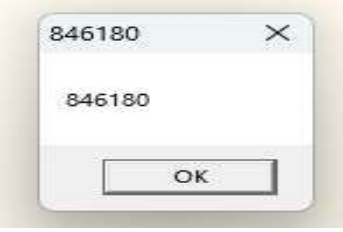
4. הכנסת הקוד שלנו הכולל את הקפצת ההודעה, לאחריה את תחילת הקוד המקורי ולבסוף קפיצה חזרה לקוד המקורי.

```
00423E68    00              DB 00
00423E69  > 6A 00           PUSH 0                    Style = MB_OK|MB_APPLMODAL
00423E6B  . 68 603E4200     PUSH hexmines.00423E60    Title = "846180"
00423E70  . 68 603E4200     PUSH hexmines.00423E60    Text = "846180"
00423E75  . 6A 00           PUSH 0                    hOwner = NULL
00423E77  . E8 349EE176     CALL USER32.MessageBoxA   MessageBoxA
00423E7C  . 55              PUSH EBP
00423E7D  . 8BEC            MOV EBP,ESP
00423E7F  . 83C4 D8         ADD ESP,-28
00423E82  .^E9 4F55FFFF     JMP hexmines.004193D6
```

5. דריסת השורות שהעתקנו לטובת קפיצה לקוד שלנו

```
004193CF    00              DB 00
004193D0  .v E9 94AA0000    JMP hexmines.00423E69
004193D5    90              NOP
004193D6  > 53              PUSH EBX
004193D7  . 56              PUSH ESI
```

6. הפעלת הקוד, הופעת ההודעה שלנו ולאחריה הרצת האפליקציה



מצורף בתקייה עם קובץ זה, סרטון הדגמה מלא של הרצת הקובץ המוגמר