בס"ד

ישי לוטווק InjectMe.exe הדרך לפיתרון

```
00401000 <injectme.EntryPoint>
call <JMP.&InitCommonControls>
push 0
call <JMP.&GetModuleHandleA>
mov dword ptr ds:[406100],eax
push 0
push injectme.401030
push 0
push injectme.406000   ; 406000:"injectme"
push dword ptr ds:[406100]
call <JMP.&DialogBoxParamA>
push eax
call <JMP.&ExitProcess>
push ebp
mov ebp,esp
cmp dword ptr ss:[ebp+C],110
jne injectme.4014D9
```

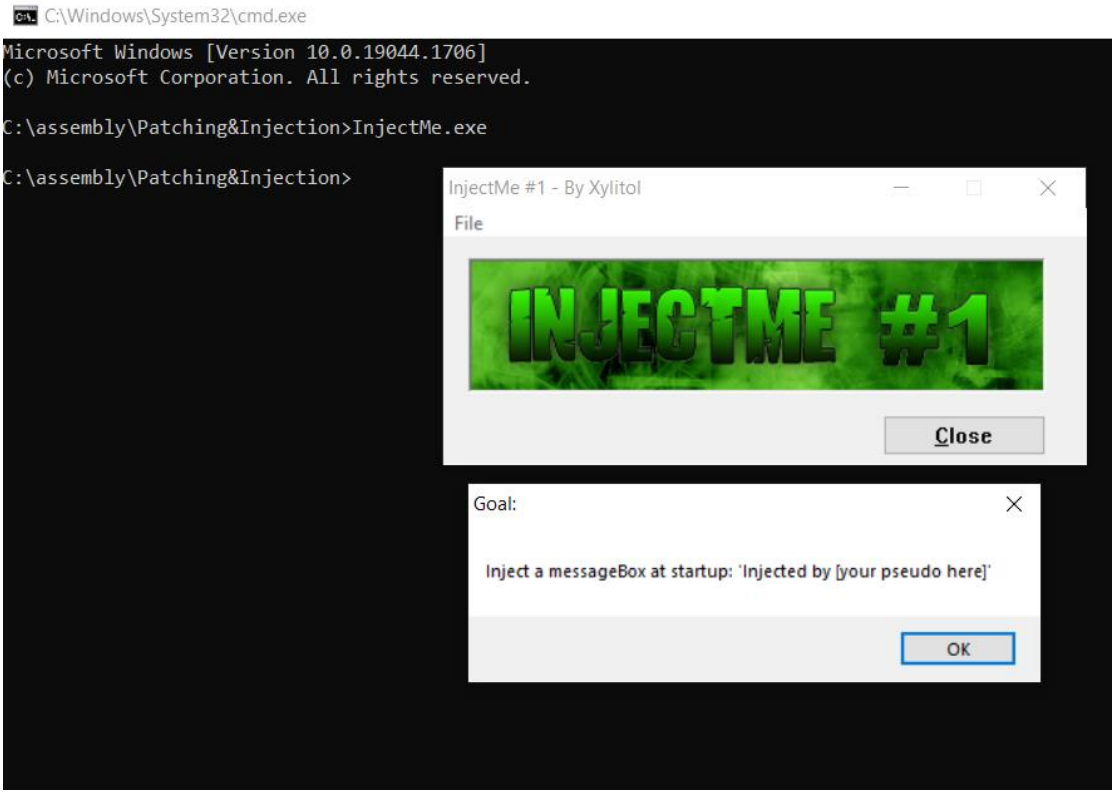
כדי לעשות את מה שנתבקשנו, נצטרך לקפוץ למקום אחר בקוד, ולחזור לפה לאחר מכן.

נבחר לפצפץ את הפקודה push 0 בשורה החמישית. כמובן שנצטרך אחר כך לשתול את הפקודה הזאת בקטע הקוד שנזריק במקום אחר, וזאת בכדי שהתוכנית תוכל להמשיך לעבוד כמצופה.

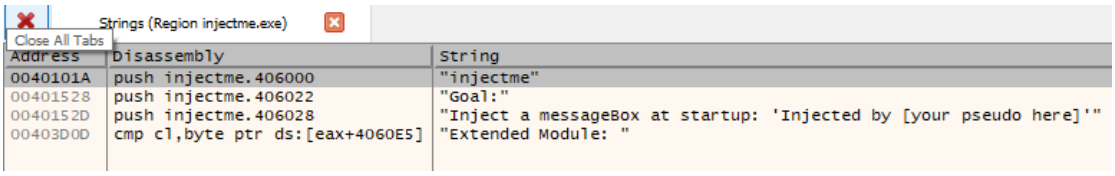
נמצא מקום ריק באזור של הקוד שבו נוכל לשתול את ההזרקה שלנו:

```
push eax
push 40
call <JMP.&GlobalAlloc>
mov dword ptr ds:[40630C],eax
mov ecx,dword ptr ds:[406308] ; ecx:EntryPoint
mov dword ptr ds:[eax],ecx ; ecx:EntryPoint
add eax,4
mov edi,eax ; edi:EntryPoint
rep movsb
pop esi ; esi:EntryPoint
push dword ptr ds:[40630C]
call injectme.401619
call injectme.4014D3
nop
nop
nop
nop
nop
nop
nop
nop
nop
nop
nop
nop
nop
nop
nop
nop
nop
nop
nop
nop
nop
nop
```

ננסה לראות איך מבוצעת הקריאה לפונקציה MessageBoxA שכבר נמצאת בקוד:

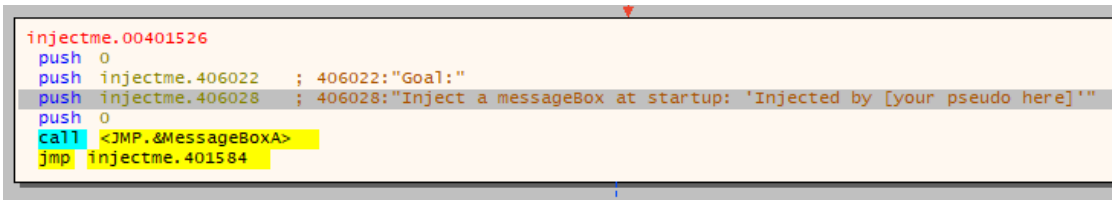


נמצא את הטקסט המודפס בהודעה:



ניתן לראות את ההודעה בשורה השלישית..

נלך לאזור הזה בקוד ונראה איך מזמנים את הפונקציה הזו:



נעשה אותו דבר רק שנשנה את הכתובות לכתובות בהן נכניס את המחרוזות שאנחנו רוצים להדפיס

(ניתן לראות בתחתית התמונה את המחרוזות אותן שתלנו באזור של datan):

Dump 1 | Dump 2 | Dump 3 | Dump 4 | Dump 5 | Watch 1 | [x=] Locals | Struct

Address	Hex	ASCII
00406022	47 6F 61 6C 3A 00 49 6E 6A 65 63 74 20 61 20 6D	Goal:.Inject a m
00406032	65 73 73 61 67 65 42 6F 78 20 61 74 20 73 74 61	essageBox at sta
00406042	72 74 75 70 3A 20 27 49 6E 6A 65 63 74 65 64 20	rtup: 'Injected
00406052	62 79 20 5B 79 6F 75 72 20 70 73 65 75 64 6F 20	by [your pseudo
00406062	68 65 72 65 5D 27 00 00 00 00 00 00 80 3F 00 00	here]'.....?..
00406072	7A 44 6F 12 83 3A CD CC CC 3E 00 00 7F 43 00 00	zDo..:ÍÌÌ>...C..
00406082	80 43 81 80 80 3B 00 00 80 3B 00 00 00 30 00 00	.C...;...;...0..
00406092	C0 59 00 00 00 00 00 00 70 40 7A 00 8B FC FA 21	ÀY.....p@z..üú!
004060A2	A9 3F 00 00 00 00 00 00 50 40 D8 0F C9 3C 00 00	©?.....P@Ø.É<..
004060B2	00 00 00 00 00 00 00 C0 2A 40 00 00 00 00 00 00	.....À*@.....
004060C2	00 40 AB AA AA 3D 00 00 00 00 00 00 00 00 80 55	.@«ªª=.....U
004060D2	C0 40 AB AA AA 3A 00 00 90 45 00 00 FF 31 E8 03	À@«ªª:...E..ÿ1è.
004060E2	00 00 01 45 78 74 65 6E 64 65 64 20 4D 6F 64 75	...Extended Modu
004060F2	6C 65 3A 20 00 00 00 00 00 00 00 00 00 00 00 00	le: .....
00406102	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
00406112	00 00 00 00 00 00 00 00 00 00 00 00 00 00 49 6E	.....In
00406122	6A 65 63 74 65 64 20 62 79 20 59 69 73 68 61 69	jected by Yishai
00406132	00 00 00 00 00 00 00 00 00 00 00 00 00 00 49 6E	.....In
00406142	6A 65 63 74 65 64 20 73 75 63 63 65 73 73 66 75	jected successfu
00406152	6C 6C 79 21 00 00 00 00 00 00 00 00 00 00 00 00	lly!.....

להלן הפיצפוץ:

לפני

```
call <JMP.&InitCommonControls>
push 0
call <JMP.&GetModuleHandleA>
mov dword ptr ds:[406100],eax
push 0
push injectme.401030
push 0
push injectme.406000
push dword ptr ds:[406100]
call <JMP.&DialogBoxParamA>
push eax
call <JMP.&ExitProcess>
push ebp
mov ebp,esp
cmp dword ptr ss:[ebp+C],110
jne injectme.4014D9
```

אחרי

```
call <JMP.&InitCommonControls>
push 0
call <JMP.&GetModuleHandleA>
mov dword ptr ds:[406100],eax
jmp injectmesolution.4010B9
nop
nop
push 0
push injectmesolution.406000
push dword ptr ds:[406100]
call <JMP.&DialogBoxParamA>
push eax
call <JMP.&ExitProcess>
push ebp
mov ebp,esp
cmp dword ptr ss:[ebp+C],110
jne injectmesolution.4014D9
```

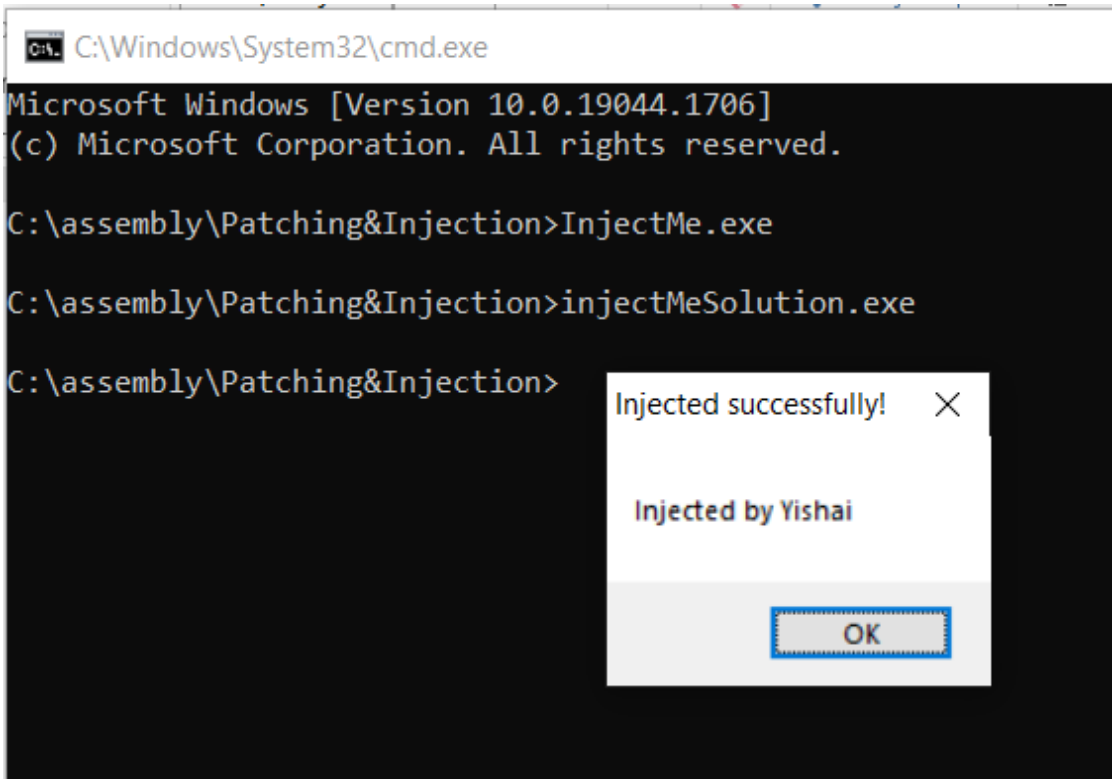
לפני

```
004010B5  90  nop
004010B6  90  nop
004010B7  90  nop
004010B8  90  nop
004010B9  90  nop
004010BA  90  nop
004010BB  90  nop
004010BC  90  nop
004010BD  90  nop
004010BE  90  nop
004010BF  90  nop
004010C0  90  nop
004010C1  90  nop
004010C2  90  nop
004010C3  90  nop
004010C4  90  nop
004010C5  90  nop
```

אחרי

```
nop
nop
nop
nop
push 0
push injectmesolution.406140
push injectmesolution.406120
push 0
call <JMP.&MessageBoxA>
push 0
push injectmesolution.401030
jmp injectmesolution.401017
nop
nop
nop
nop
nop
```

והתוצאה כמצופה:



ואחרי שלוחצים על OK