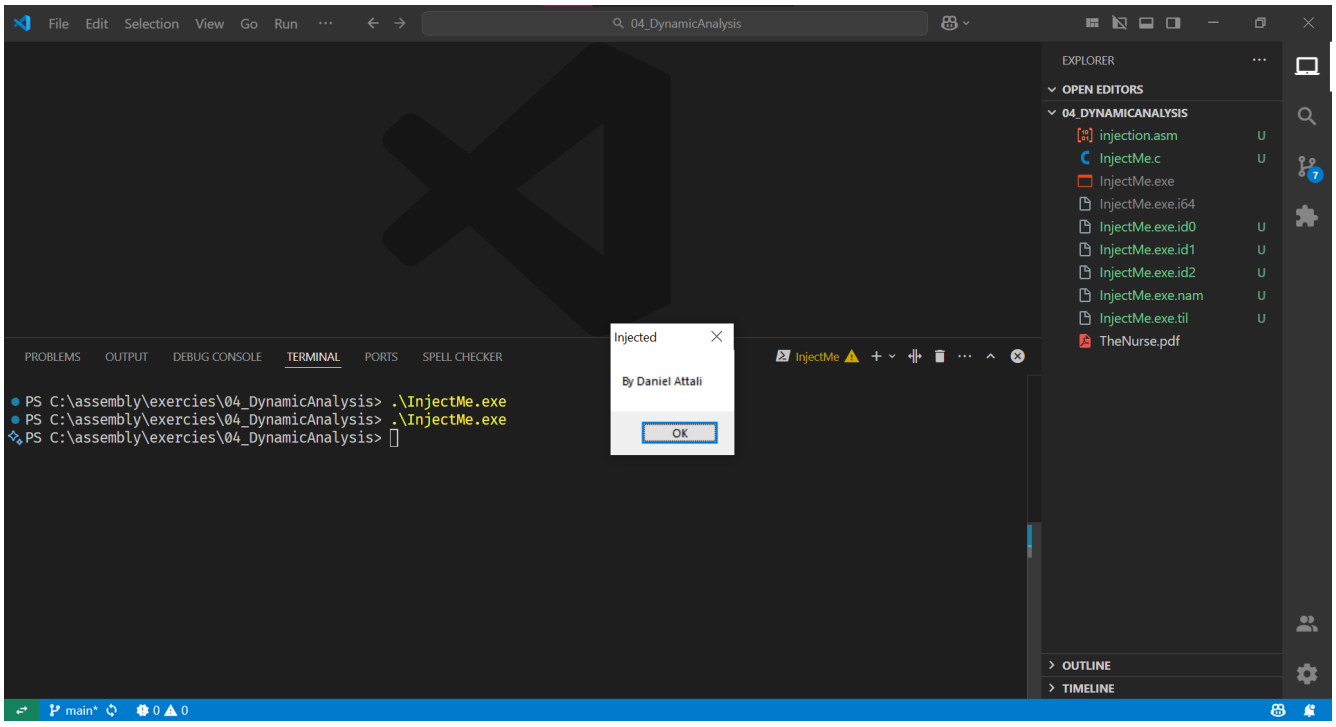
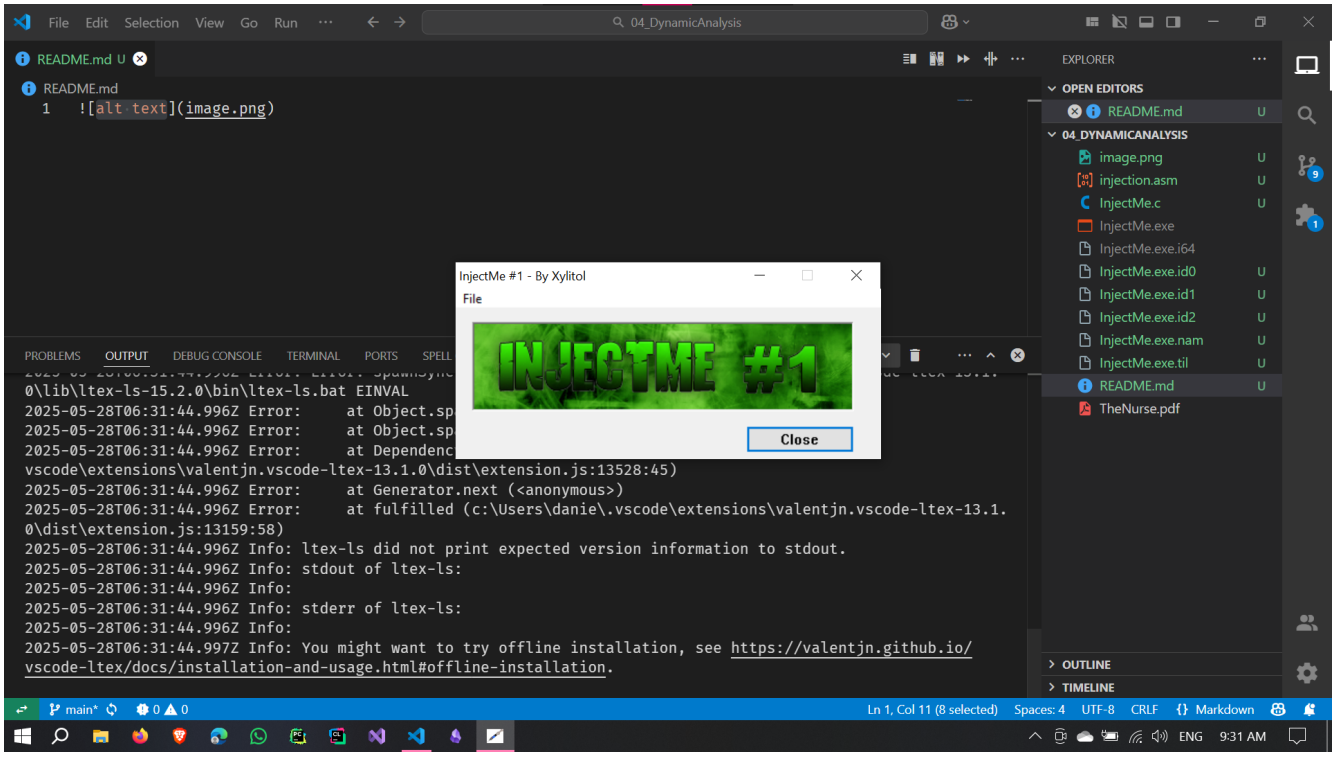
Intro-to-Reversing

Assignment 4: `InjectMe.exe`

- Submitted by: Daniel Attali
- Date: 28 May 2025
- Course: Introduction to Reversing

Final Results





Writeup

In this assignment, we are tasked with injecting and patching the provided `InjectMe.exe` executable such that the program will popup a message box with my name "Daniel Attali" when executed and then continue to run normally.

The first task is to find where the code could be injected. So when opening the exe in IDA we found a long section of `nop` instructions, which lead us to think this was the right place to inject our code.

So we started by patching the code to add two strings a caption string: `"Injected"` and a text string: `"By Daniel Attali"`.

Then we added the code to call `MessageBoxA` with the context and text strings, and finally we added a `jmp` instruction to jump over the code we injected so that the program continues to run normally.

```
push 0
push offset caption
push offset text
push 0
call MessageBoxA
```

```
.text:004010B9 ; const CHAR caption[]
.text:004010B9 caption         db 'Injected',0         ; DATA XREF: DialogFunc+A9↓o
.text:004010C2 ; ---------------------------------------------------------------------------
.text:004010C2                 nop
.text:004010C3                 nop
.text:004010C3 ; ---------------------------------------------------------------------------
.text:004010C4 ; const CHAR text[]
.text:004010C4 text            db 'By Daniel Attali',0 ; DATA XREF: DialogFunc+AE↓o
.text:004010D5 ; ---------------------------------------------------------------------------
.text:004010D5                 nop
.text:004010D6                 nop
.text:004010D7
.text:004010D7 inject:                                 ; CODE XREF: .text:start↑j
.text:004010D7                 push    0               ; uType
.text:004010D9                 push    offset caption  ; "Injected"
.text:004010DE                 push    offset text     ; "By Daniel Attali"
.text:004010E3                 push    0               ; hWnd
.text:004010E5                 call    MessageBoxA
.text:004010EA                 nop
.text:004010EB                 call    InitCommonControls
.text:004010F0                 push    0               ; lpModuleName
.text:004010F2                 call    GetModuleHandleA
.text:004010F7                 jmp     back
.text:004010FC ; ---------------------------------------------------------------------------
```

Then we got back to the start of the code at the `start` label and copy the first 3 line of assembly and put it it after the call to the message box with an addition of a `jmp` instruction to jump over the code we injected.

```
jmp back
```

and changed the first 3 lines to:

```
jmp inject
nop
...
```

```
.text:00401000 start:
.text:00401000                 jmp     inject
.text:00401005 ; ---------------------------------------------------------------------------
.text:00401005                 nop
.text:00401006                 nop
.text:00401007                 nop
.text:00401008                 nop
.text:00401009                 nop
.text:0040100A                 nop
.text:0040100B                 nop
.text:0040100C
.text:0040100C back:                                   ; CODE XREF: DialogFunc+C7↓j
```