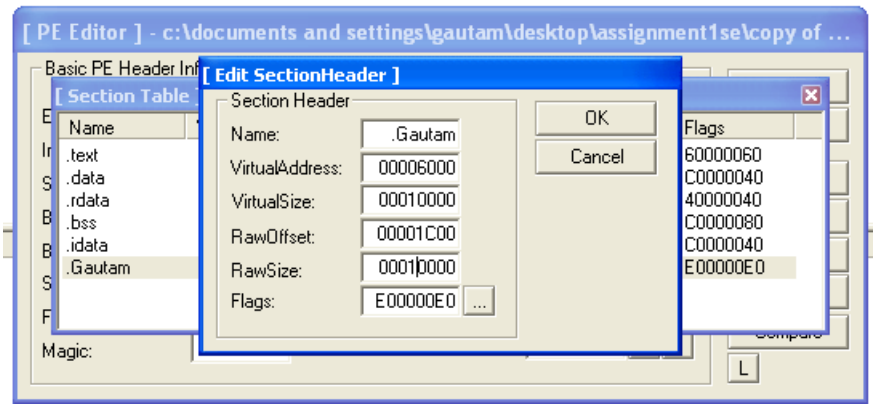
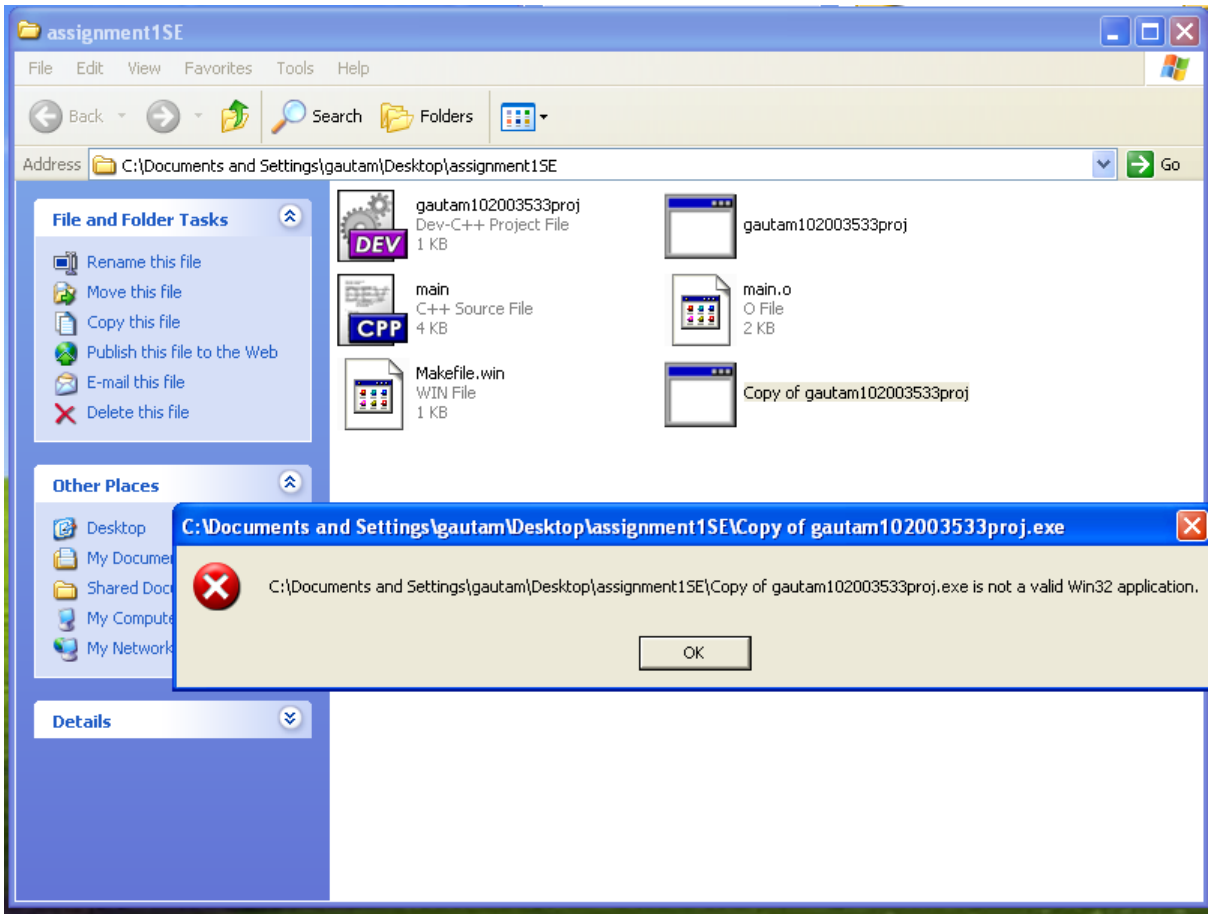
UCS638 Assignment: PE Code Injection

Submitted by Gautam Jain, 102003533, COE21

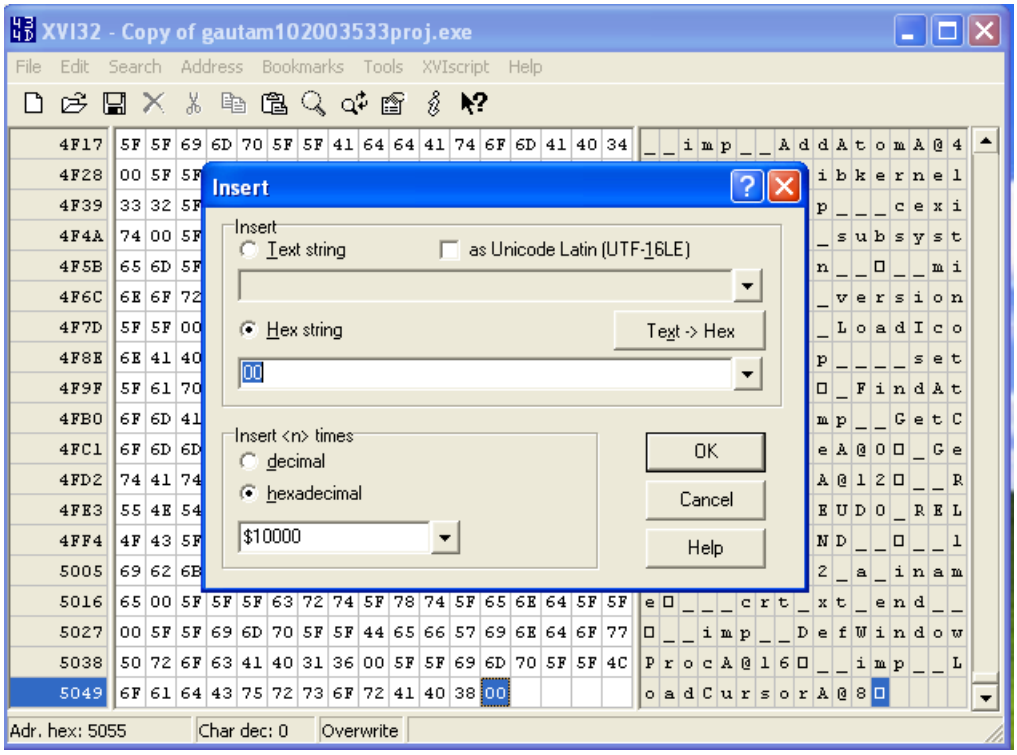
Step 1) Using LordPE to create a new section ".Gautam" to inject the code.



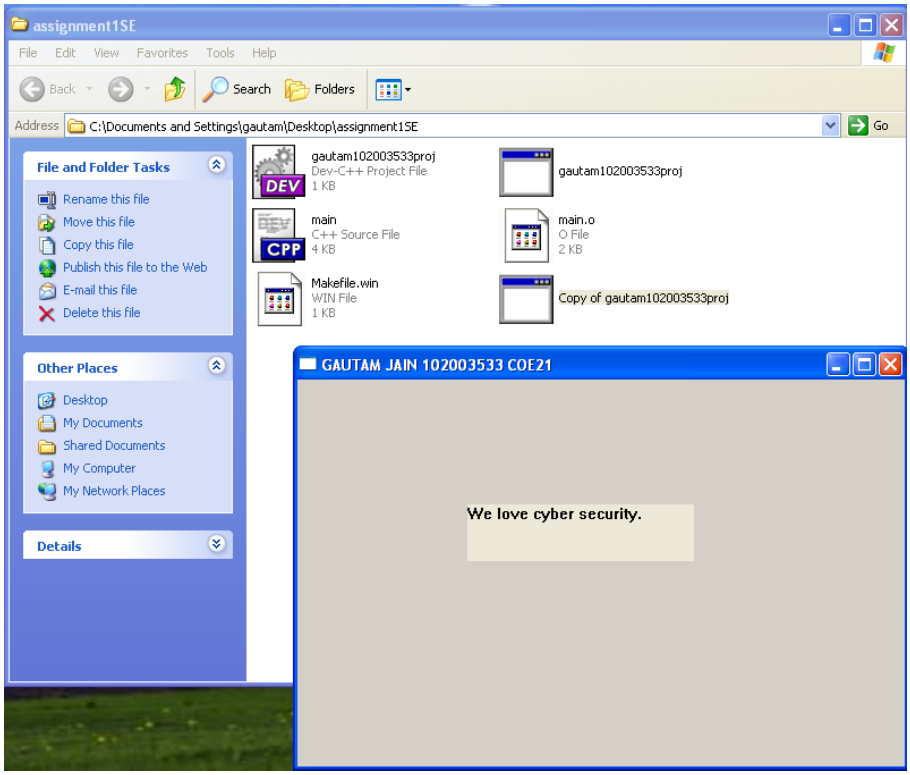
Testing the application by running it after the changes. It shows error message.



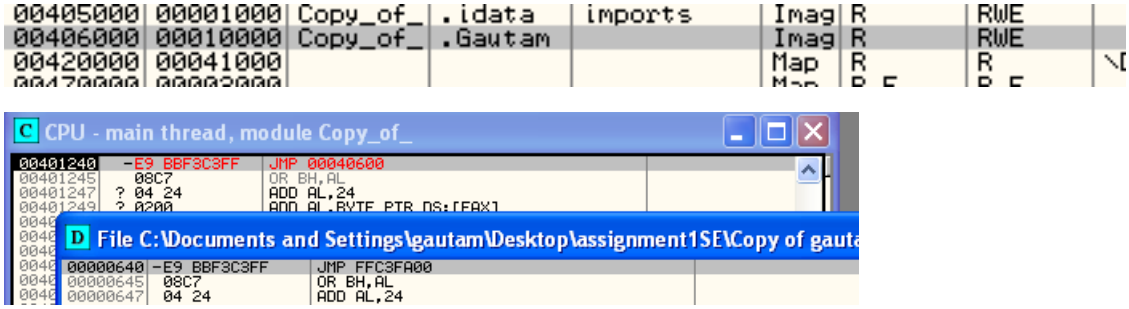
Step 2) Adding 10000 hex bytes, so that Windows accepts it as a valid win32 application.



Testing the application again.



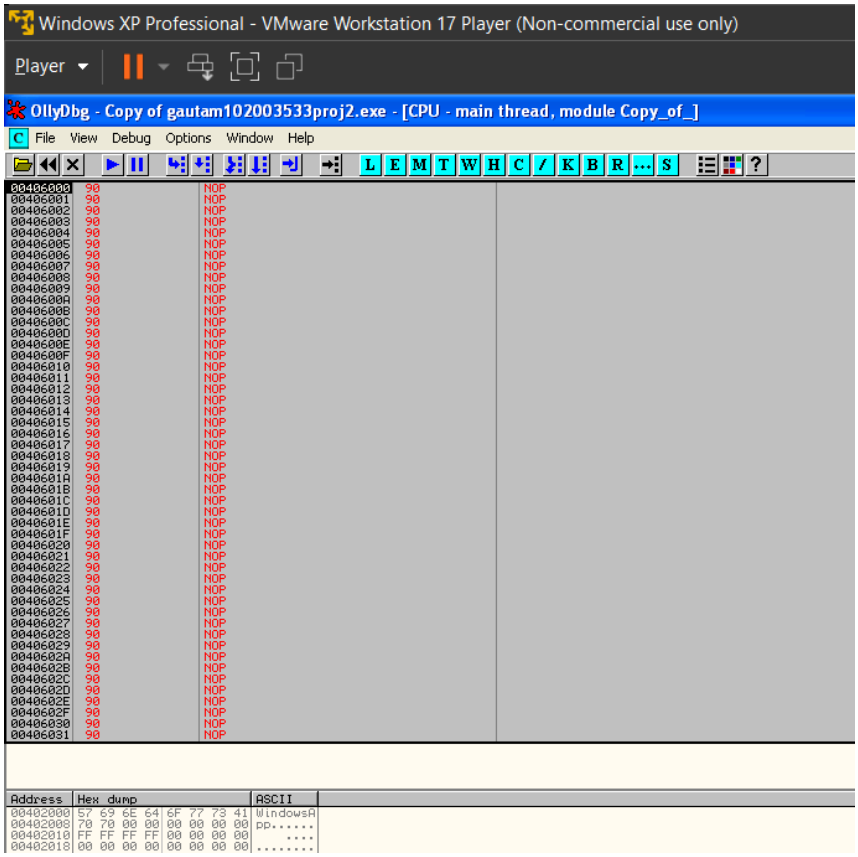
Step 3) New section is added at address 0x00406000. So, changing the application entry point to that new section.

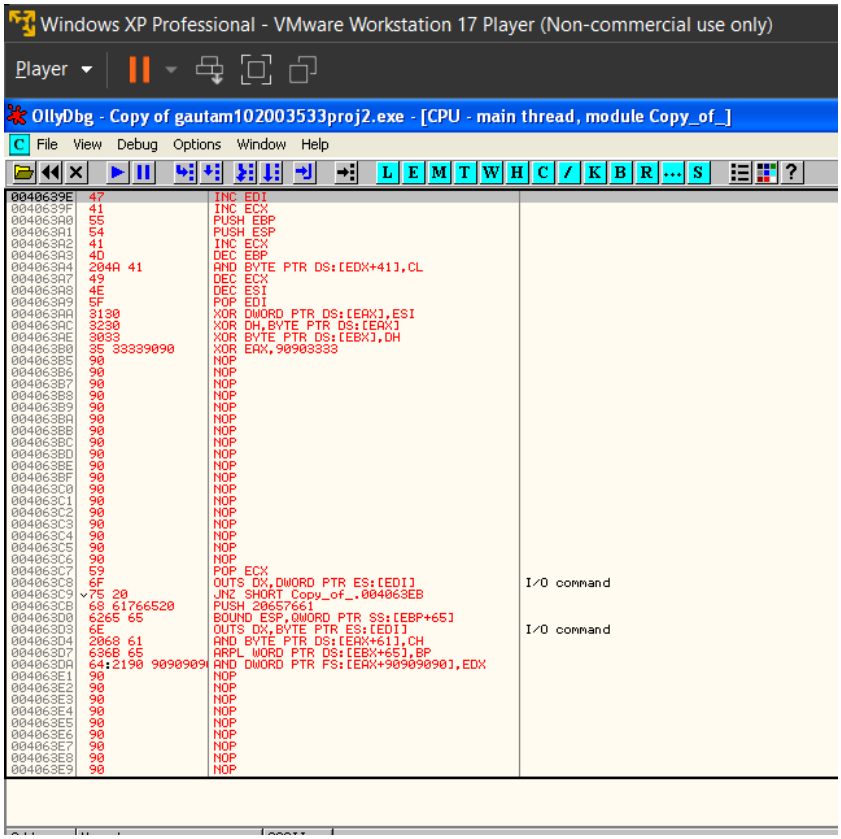


Step 4) First a particular selection in the new section is filled with NOPs. Then caption and body of the message box are added at addresses 0x0040639E and 0x004063C7 respectively.

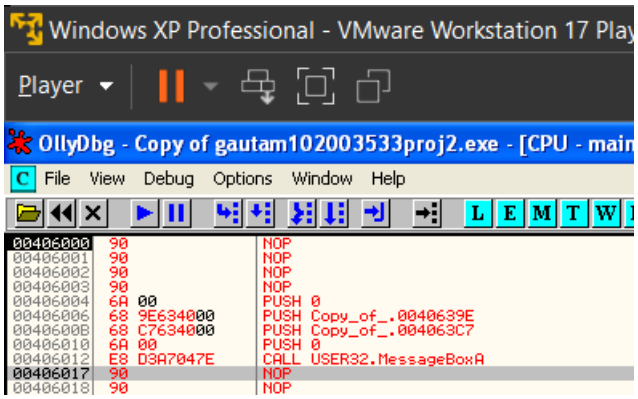
Caption: Gautam Jain_102003533

Body: You have been hacked!



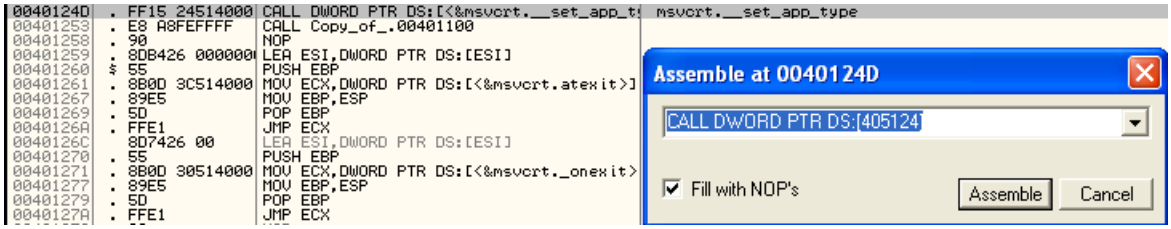


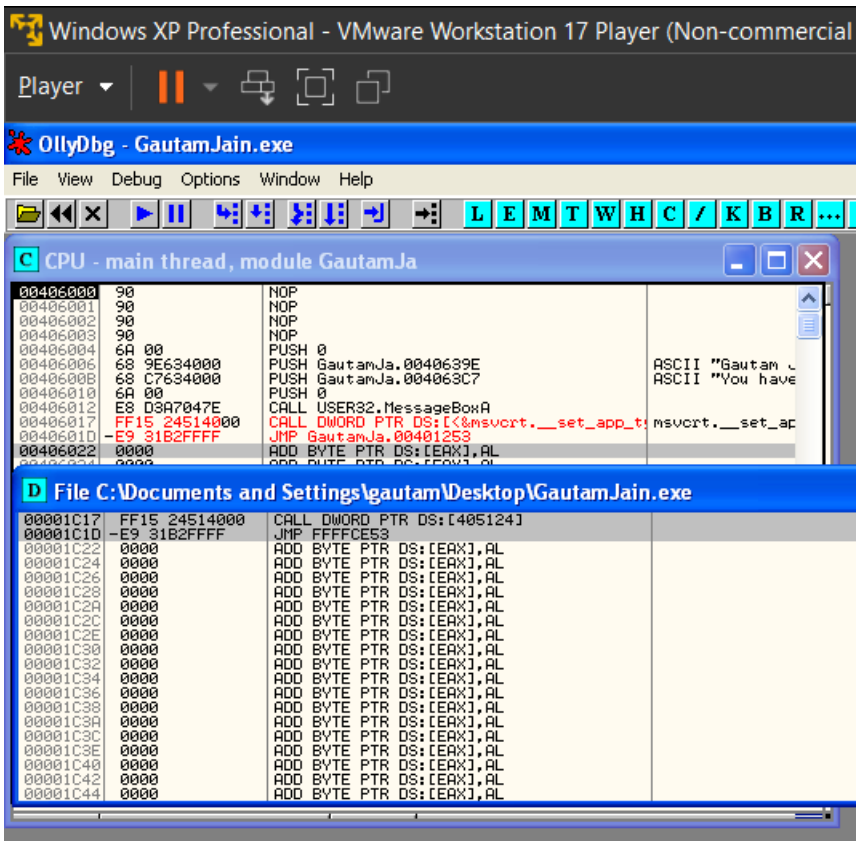
Step 5) MessageBoxA is called by defining the parameters.



Only a Message Box is displayed on opening the application.

Step 6) Calling back the original application after message box is exited.





The output when application is just called.

The output after the message box is closed.