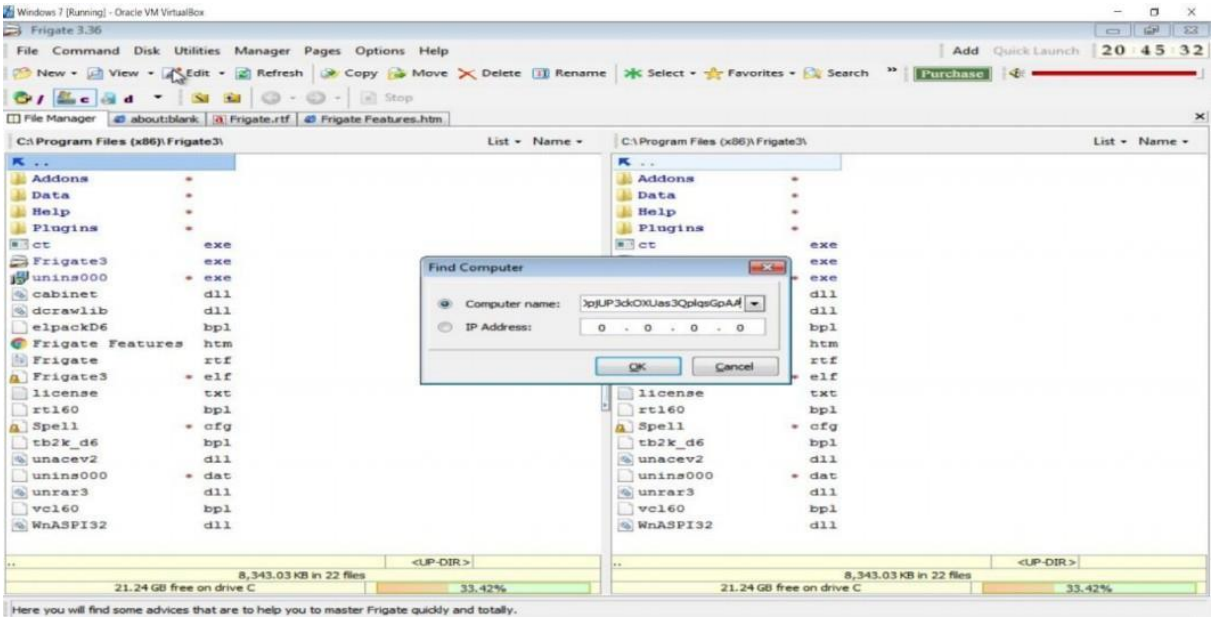
Secure coding

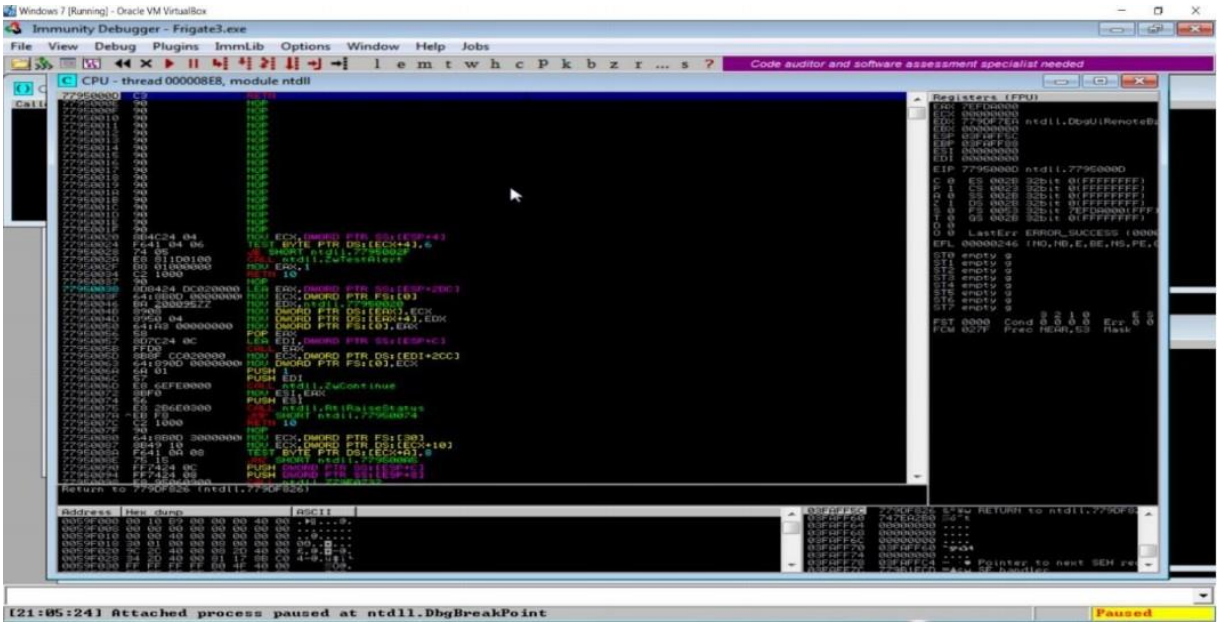
Lab-10

k.suchith reddy
18bcn7012

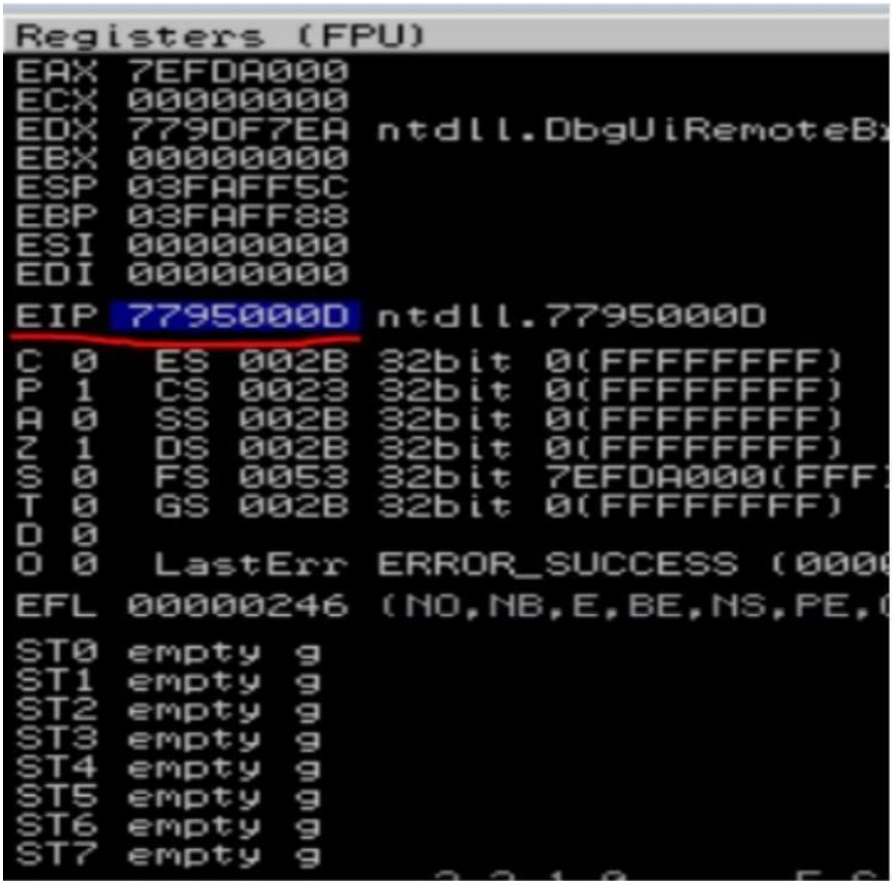
Crashing the Frigate3_Pro_v36 application and opening calc.exe (Calculator) by triggering it using the above generated payload:



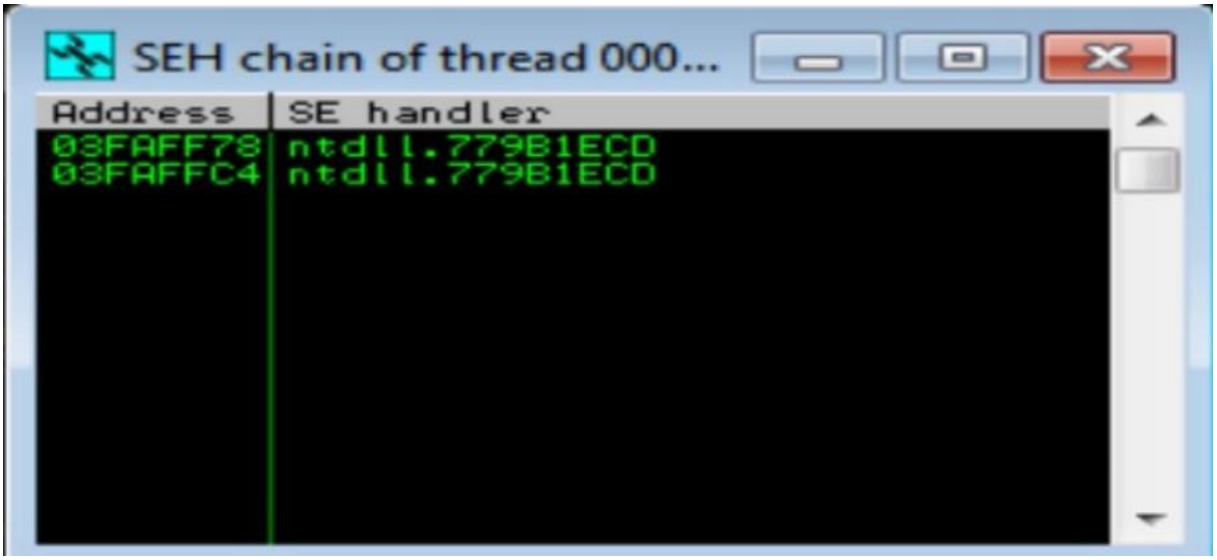
Before Execution (Exploitation): Attaching the debugger (Immunity debugger) to the application Frigate3_Pro_v36 and analysing the address of various registers:

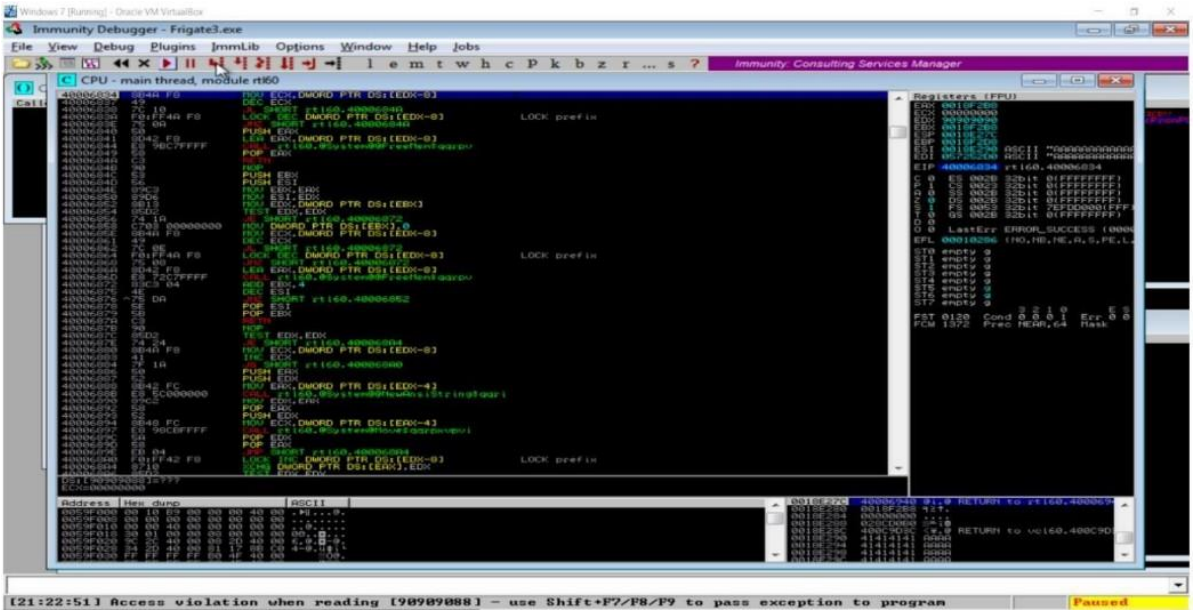


Checking for EIP address:

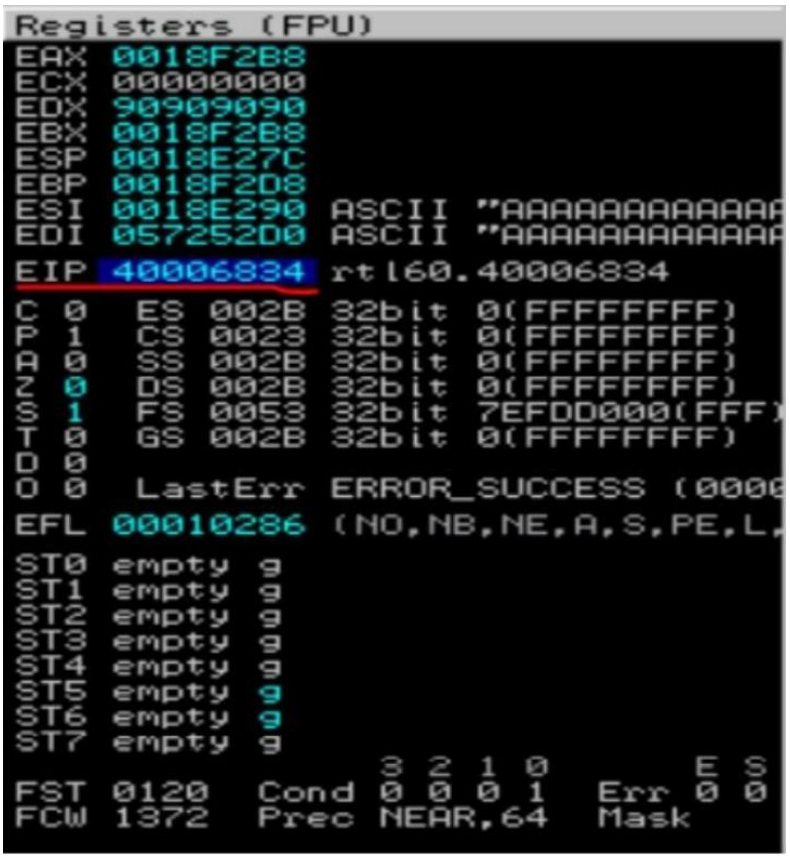


Verifying the SHE chain:


SEH chain of thread 000...
Address
SE handler
03FAFF78
ntdll.779B1ECD
03FAFFC4
ntdll.779B1ECD


Immunity Debugger - Frigate3.exe
File View Debug Plugins ImmLib Options Window Help Jobs
Immunity: Consulting Services Manager
CPU - main thread, module rt160
Registers (FPU)
[21:22:51] Access violation when reading [90909088] - use Shift+F7/F8/F9 to pass exception to program
Paused

Checkingfor EIP address:



Verifying the SHE chain and reporting the dll loaded along with the addresses:

Hence from the above analysis we found that the dll ‘rtl60.40010C4B’iscorruptedandislocatedatthe address ‘0018F2A0’.