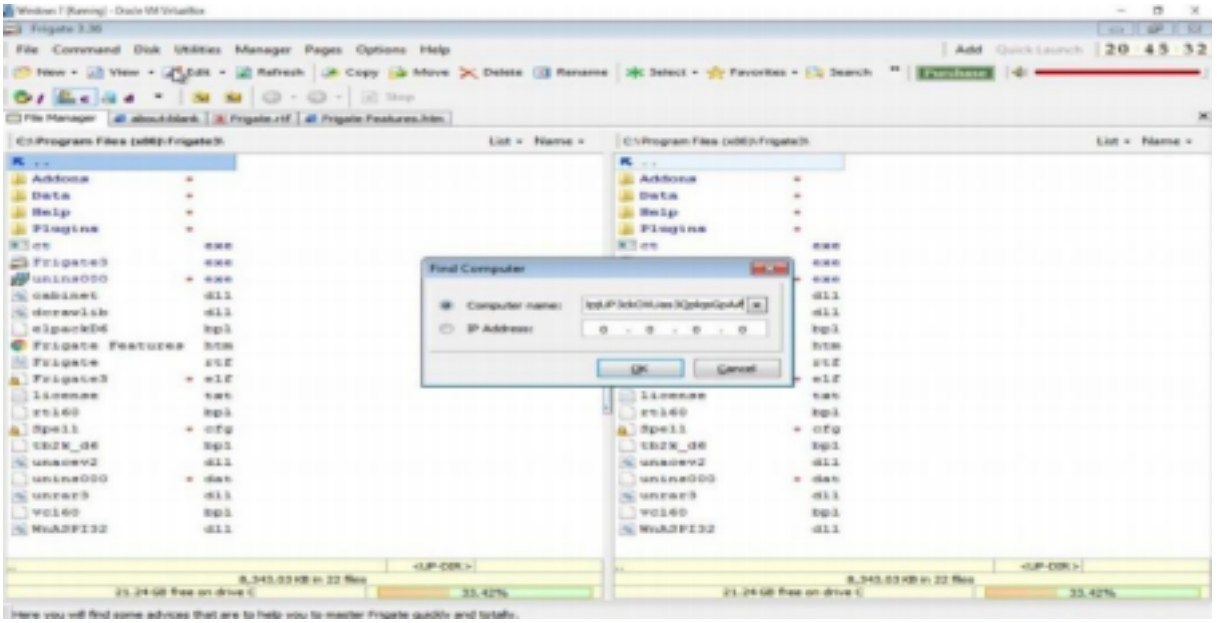
Secure coding

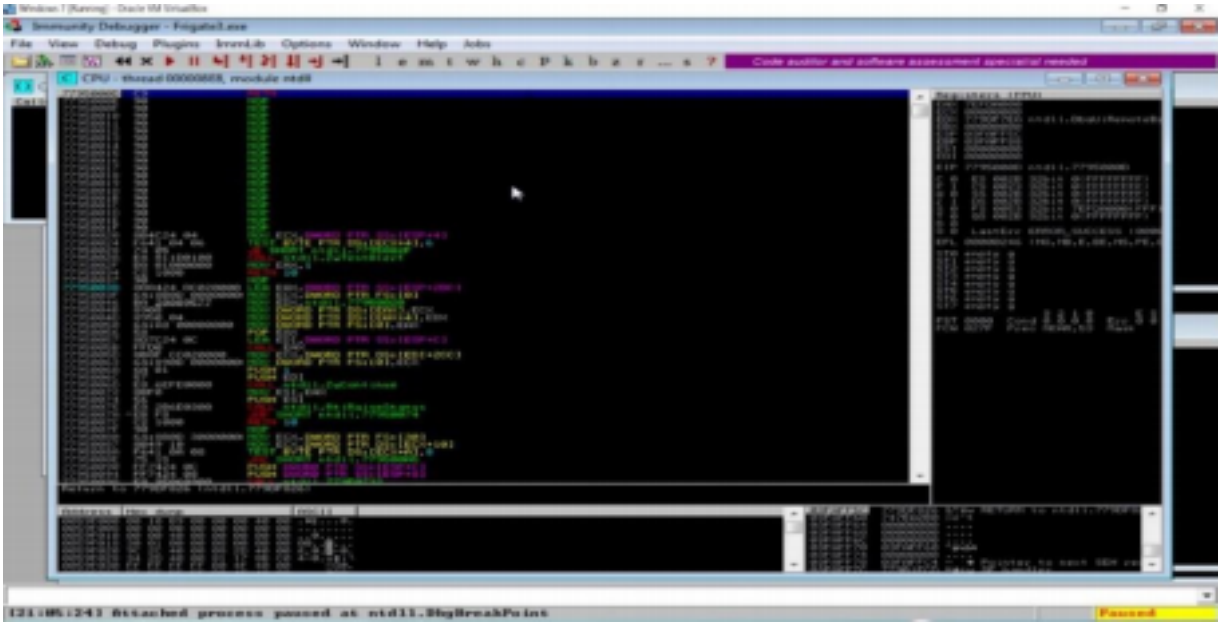
Lab-10

B.KRANTHI
18BCE7103

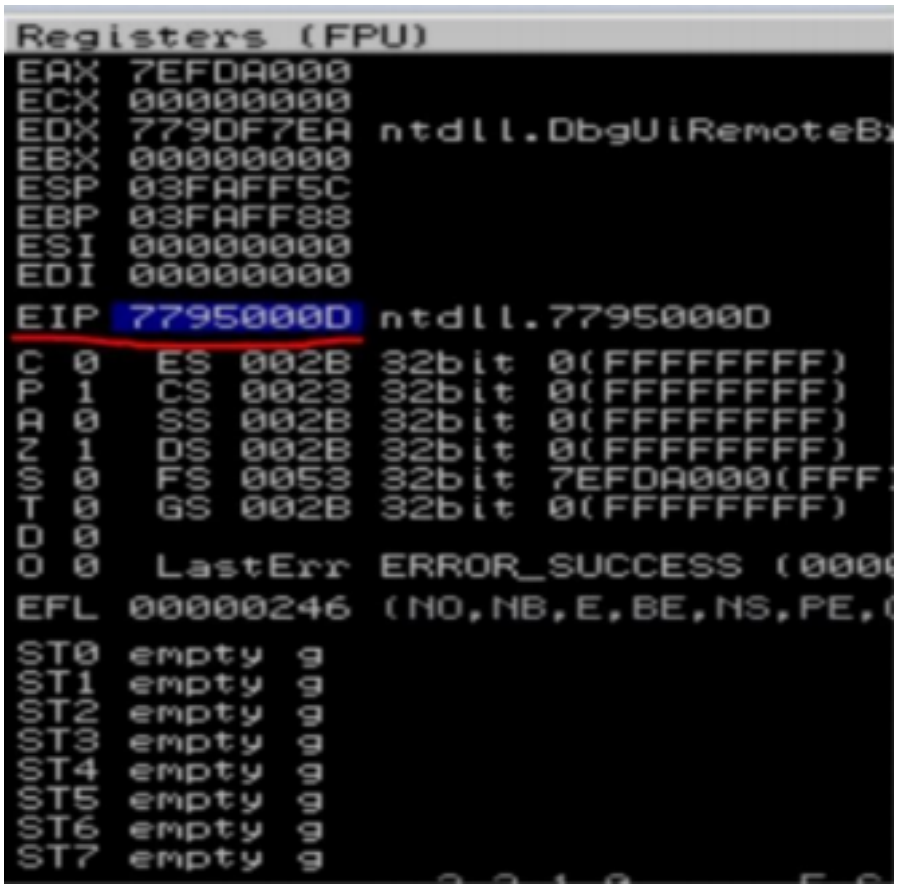
Crashing the Frigate3_Pro_v36 application and opening calc.exe (Calculator) by triggering it using the above generated payload:



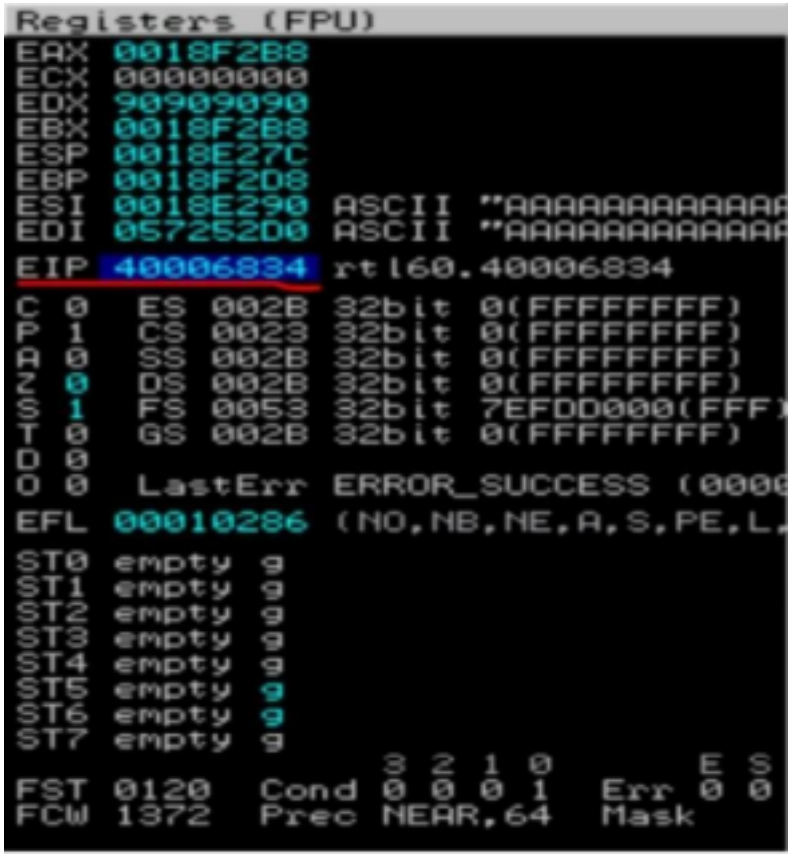
Before Execution (Exploitation): Attaching the debugger (Immunity debugger) to the application Frigate3_Pro_v36 and analysing the address of various registers:



Checking for EIP address:



Verifying the SHE chain:
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’.