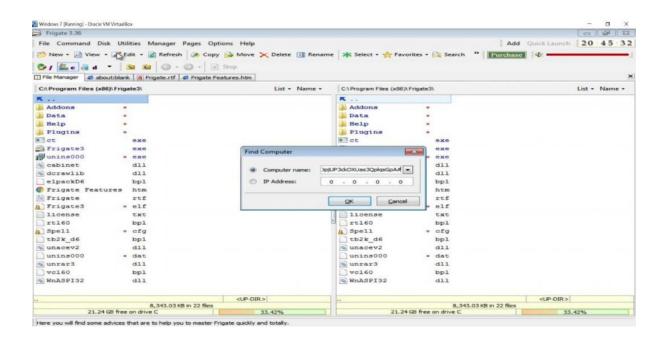
Secure coding

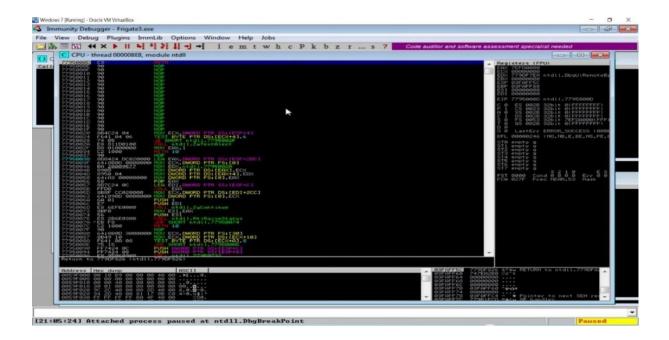
Lab-10

k.suchith reddy 18bcn7012

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



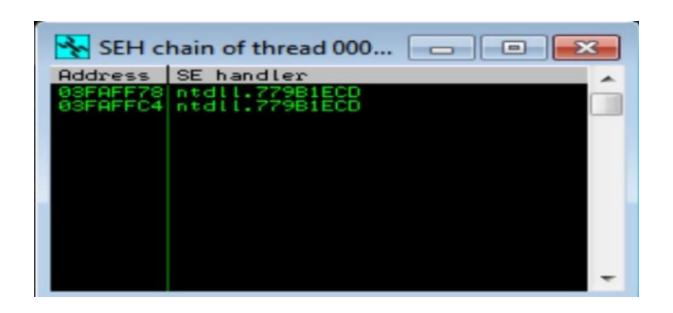
Before Execution (Exploitation): Attaching the debugger (Immunity debugger) to the application Frigate3_Pro_v36 and analysing the address of various registers:

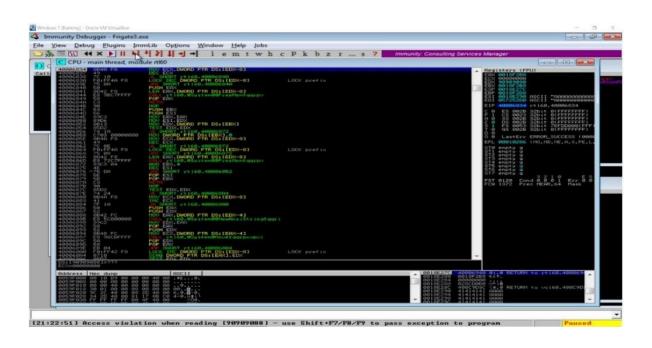


Checking for EIP address:

```
(FPU)
Registers
      7EFDA000
00000000
      779DF7EA
000000000
                    ntdll.DbgUiRemoteB:
      Ø3FAFF88
      00000000
      00000000
      7795000D
                    ntdll.7795000D
                              0(
       ČŠ
SS
            0023
0028
0028
0053
                    325 it
325 it
325 it
325 it
325 it
PANOHOO
  101000
                              0(FF
                              0(FFFFFFFF
                              Ø(FFFFFFFF)
7EFDAØØØ(FFF
        DS
                              0(FFFFFFFF)
   ø
                    ERROR_SUCCESS (0000
        LastErr
      00000246
                    (NO, NB, E, BE, NS, PE,
      empty
                g,
               0,0,0,0,0,0
      empty
```

Verifying the SHE chain:





Checkingfor EIP address:

```
Registers (FPU)

EAX 0018F288

ECX 00000000

EDX 90909090

EBX 0018F288

ESP 0018E27C

EBP 0018E290 ASCII "AAAAAAAAAAAA

EDI 057252D0 ASCII "AAAAAAAAAAAAA

EIP 40006834 rt 160.40006834

C 0 ES 0028 32bit 0(FFFFFFFF)

A 0 SS 0028 32bit 0(FFFFFFFF)

A 0 SS 0028 32bit 0(FFFFFFFF)

S 1 FS 0053 32bit 0(FFFFFFFF)

S 1 FS 0053 32bit 0(FFFFFFFF)

O 0 LastErr ERROR_SUCCESS (0006

EFL 00010286 (NO.NB.NE.A.S.PE.L.

STO empty 9

ST1 empty 9

ST2 empty 9

ST3 empty 9

ST4 empty 9

ST5 empty 9

ST6 empty 9

ST7 empty 9

ST8 empty 9

ST7 empty 9

ST8 empty 9

ST9 empty 9

ST9 empty 9

ST9 empty 9

ST9 empty 9

ST7 empty 9

ST8 empty 9

ST9 empty 9
```

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'.