

Name:Anumolu Anila

Reg no:18BCE7300

Lab-10:Secure coding

Step-1:

Installing the immunity debugger and running frigate3



Step-2:

Executing exploit2.py and opening the payload(exploit.txt)

Python exploit.py

Notepad exploit2.txt



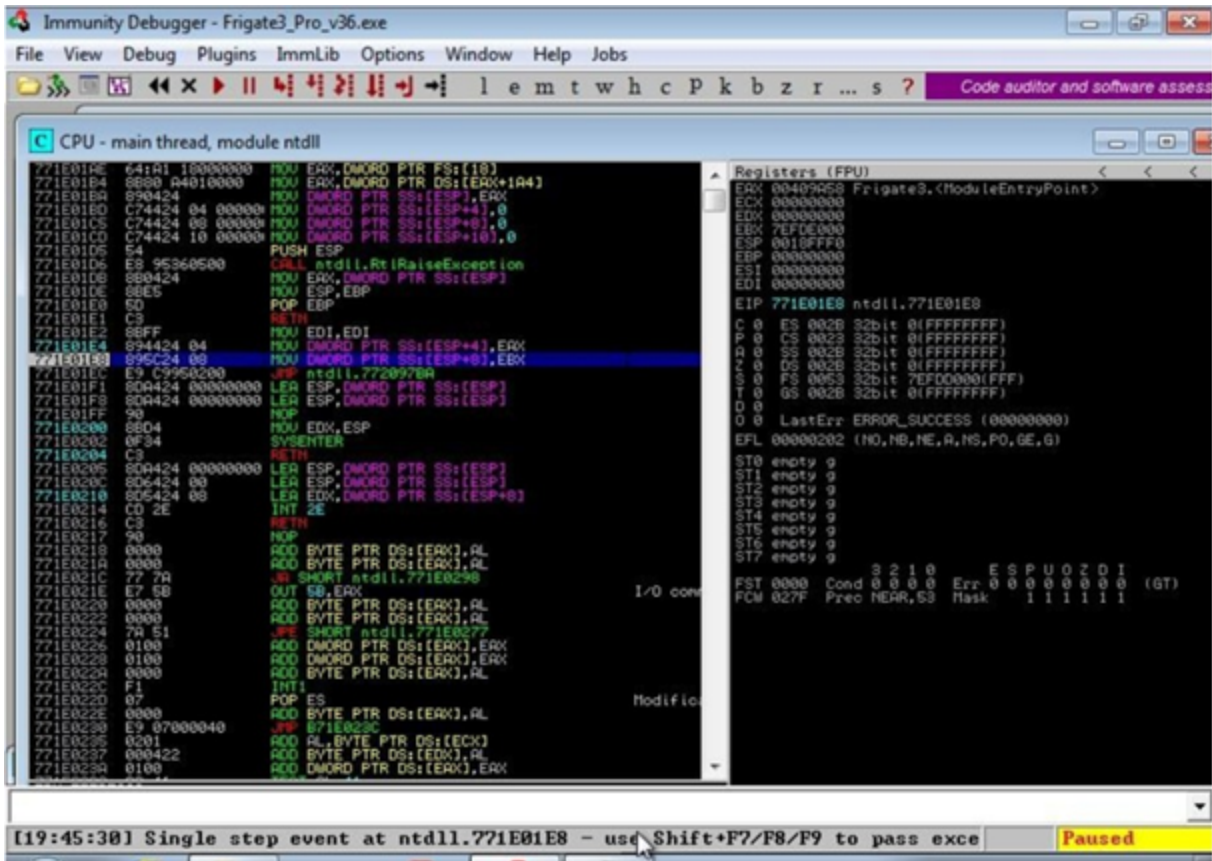
Step-4:

As we can see the default trigger changed to Calc.exe Attaching the Frigate3 to the Immunity Debugger.

After Attaching the I have got the below details from Immunity Debugger. The EIP Address is: [74FF8450](#)

The Starting and Ending of Stack Frame is: Starting address = [74FF1000](#)

Ending address = [75034FFE](#)



Step 5:

SHE Chain:

Address of dll are : [0012FFC4](#)

