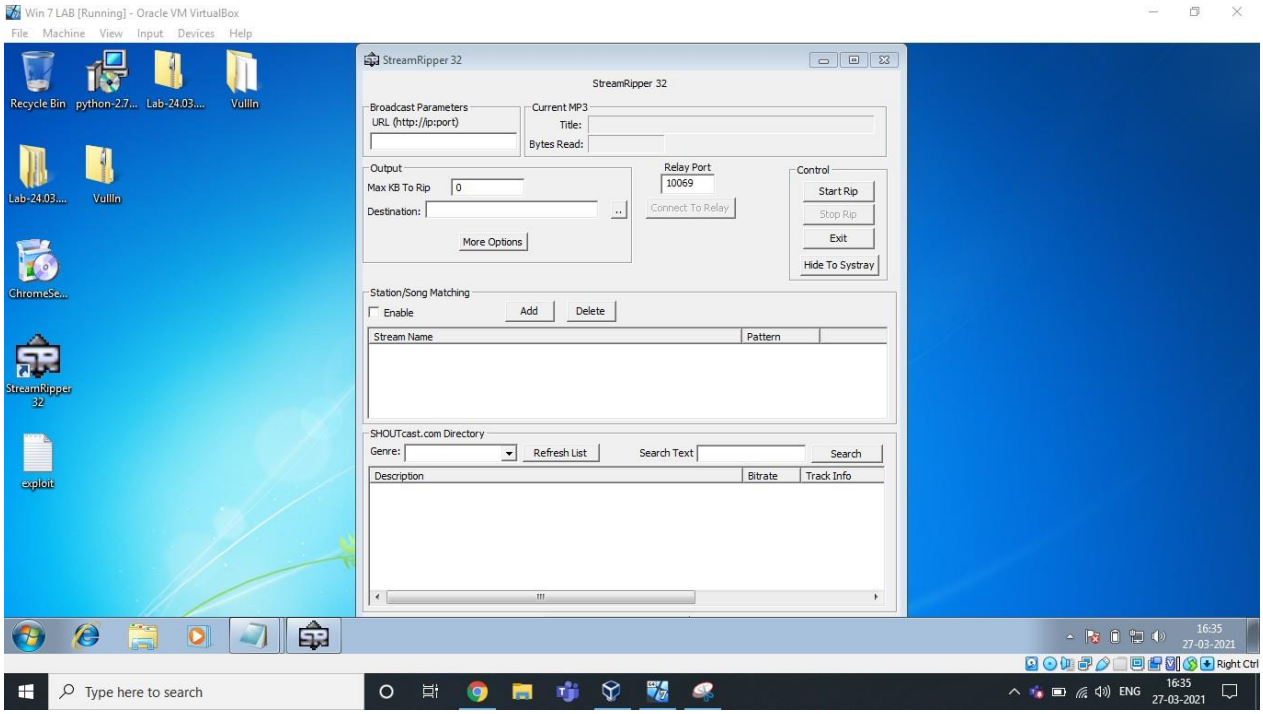
Secure Coding Lab-7

Working with the memory vulnerabilities

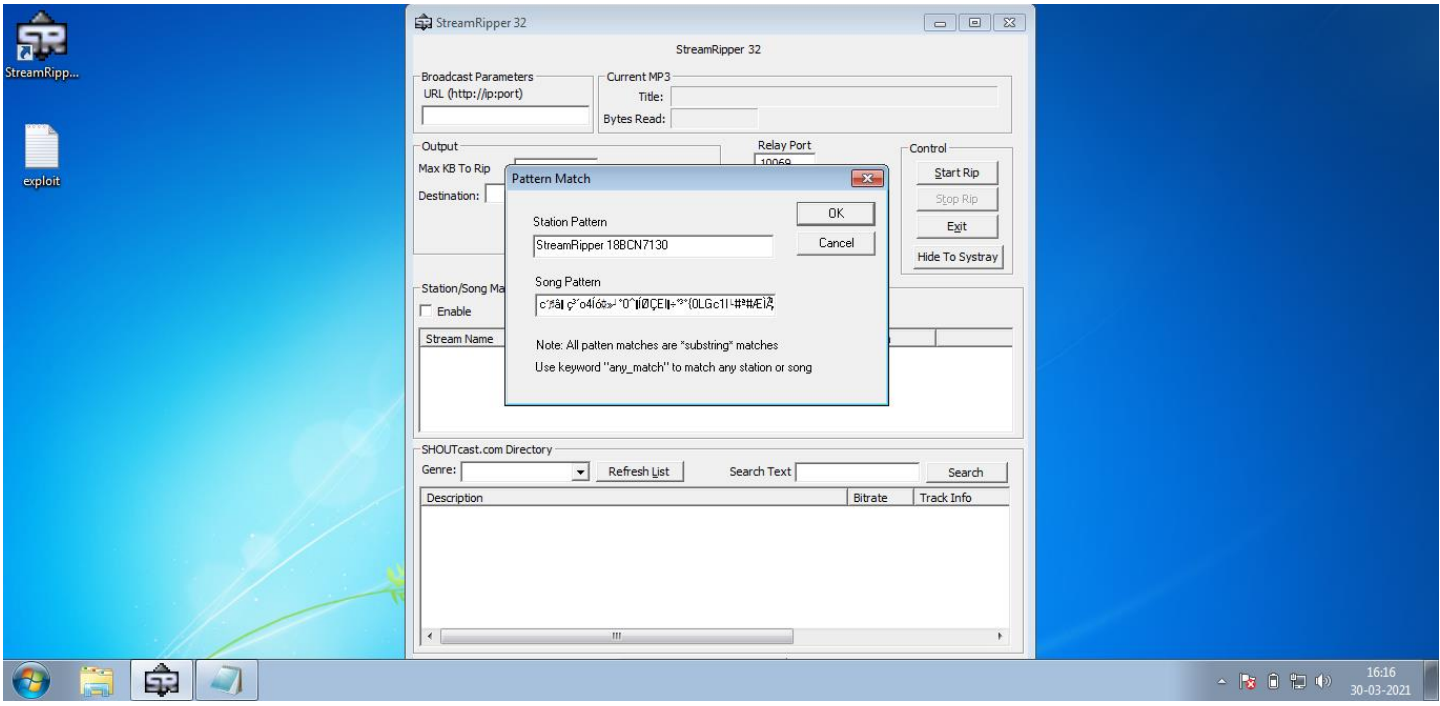
Ummadi. Mounika
18BCN7130
L23+L24

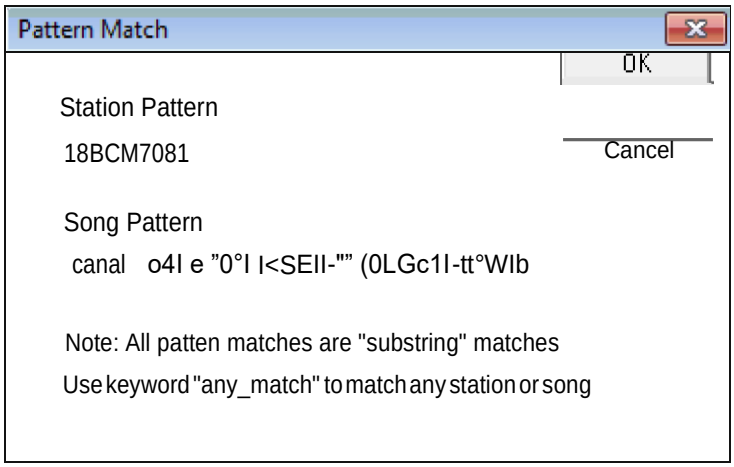
1) Crashing the StreamRipper32

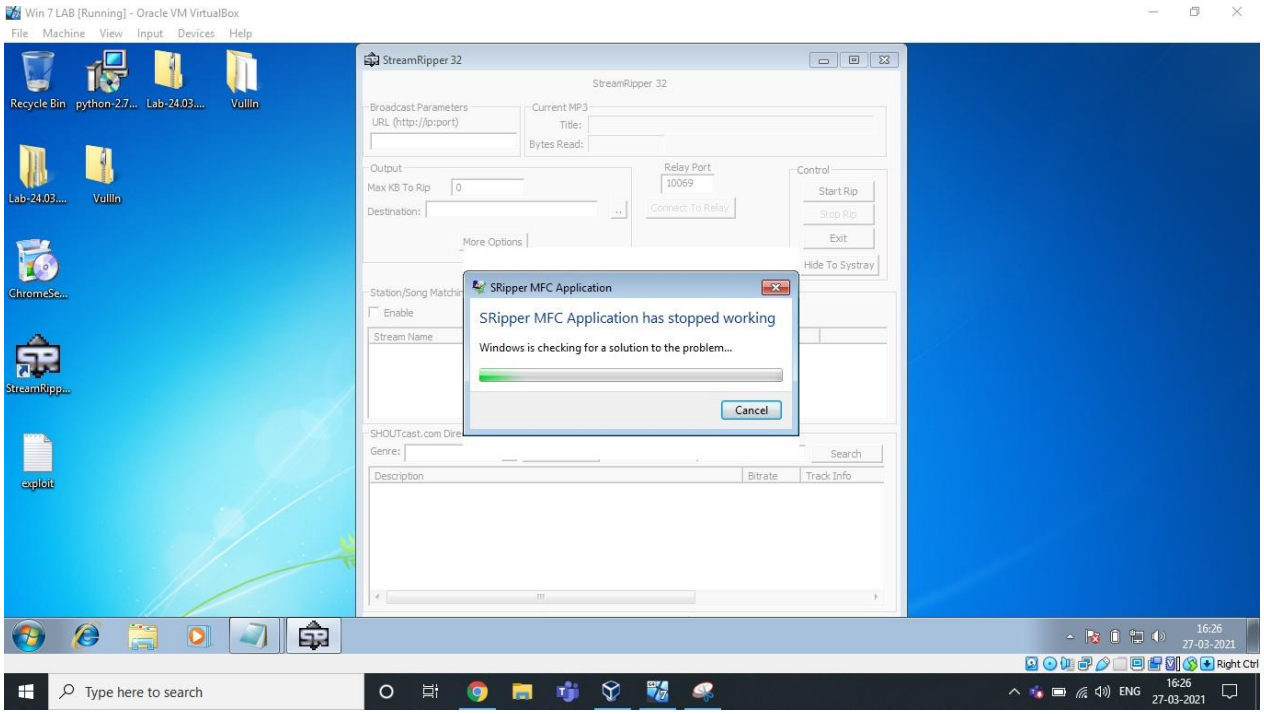


After opening the application, Click on ADD button under the Station/Song Matching Section.

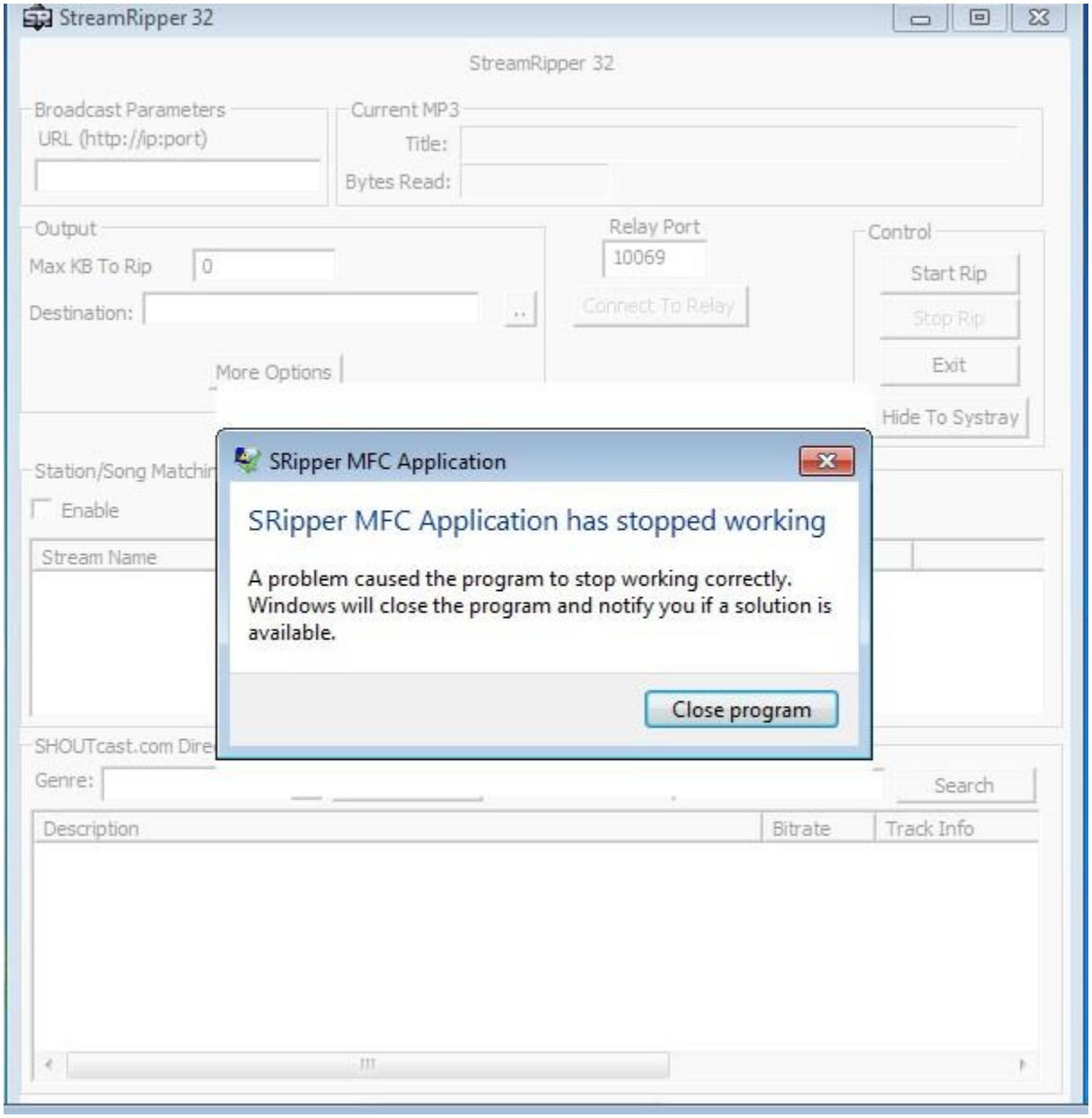
Then, Give some Name in Station Pattern as per your wish and Copy the Exploit text and Paste it in Song Pattern. Now click on Ok, as you can see below.


StreamRipp...
exploit
StreamRipper 32
StreamRipper 32
Broadcast Parameters
URL (http://ip:port)
Current MP3
Title:
Bytes Read:
Output
Max KB To Rip
Destination:
Relay Port
Control
Start Rip
Stop Rip
Exit
Hide To Systray
Pattern Match
Station Pattern
StreamRipper 18BCN7130
OK
Cancel
Song Pattern
Note: All patten matches are "substring" matches
Use keyword "any_match" to match any station or song
Station/Song Ma
Enable
Stream Name
SHOUTcast.com Directory
Genre:
Refresh List
Search Text
Search
Description
Bitrate
Track Info
16:16
30-03-2021


Pattern Match
OK
Station Pattern
18BCM7081
Cancel
Song Pattern
canal o4I e ”0°I I<SEII-"" (0LGc1I-tt°WIb
Note: All patten matches are "substring" matches
Use keyword "any_match" to match any station or song



Here is the Exploit used above.



As we can see, it’s crashed.

Analysis & Vulnerability :

Buffer Overflow is the Vulnerability in this 32 bit application. We have inserted an exploit of many characters in the field which overflowed and caused the application to crash itself. It is not capable of handling those many characters given to match/add in the song pattern. That's why it is crashed.