

Ex.No: 7
Date: 24-03-2021

Name: Ganga Suresh Kumar Nair
Reg.No: 18BCN7014

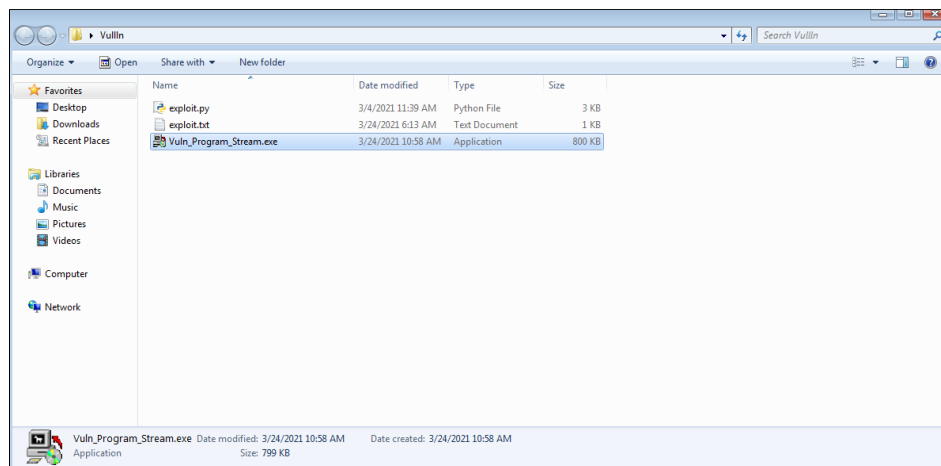
Secure Coding

Working with the memory vulnerabilities

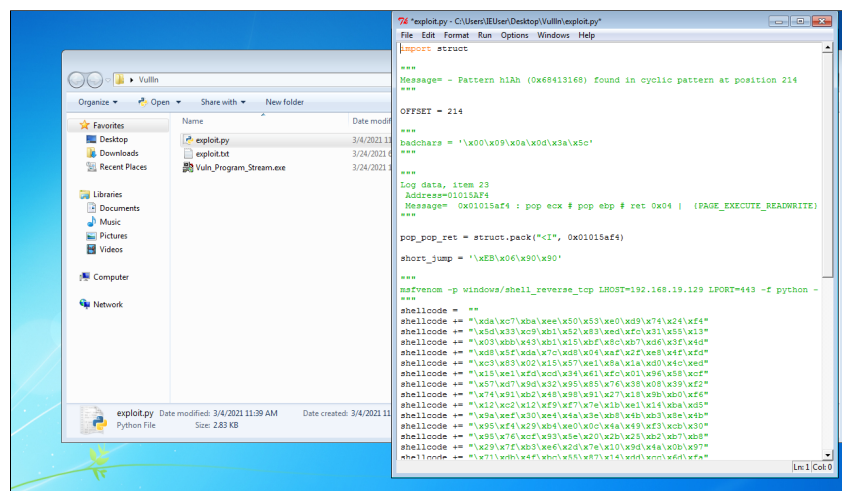
Task

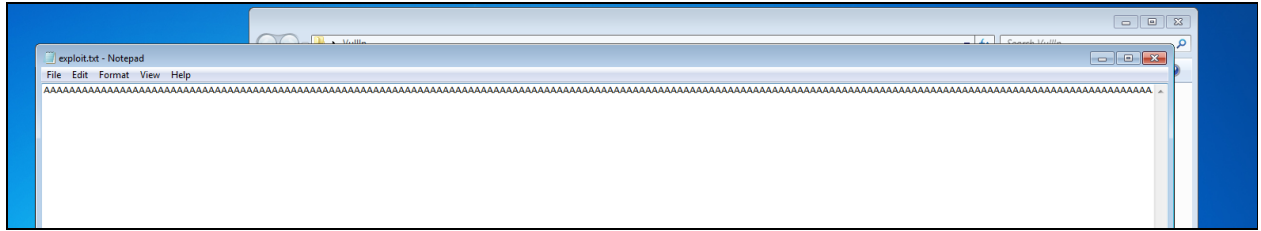
- Download Vulln.zip from teams.
- Deploy a virtual windows 7 instance and copy the Vulln.zip into it.
- Unzip the zip file. You will find two files named exploit.py and Vuln_Program_Stream.exe
- Download and install python 2.7.* or 3.5.*
- Run the exploit script to generate the payload
- Install Vuln_Program_Stream.exe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

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

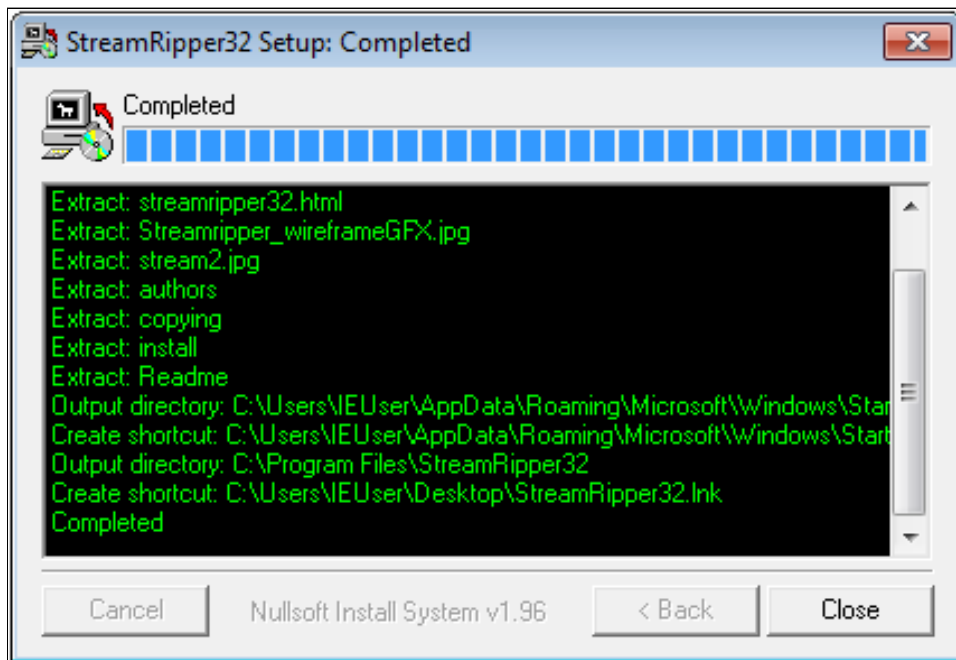
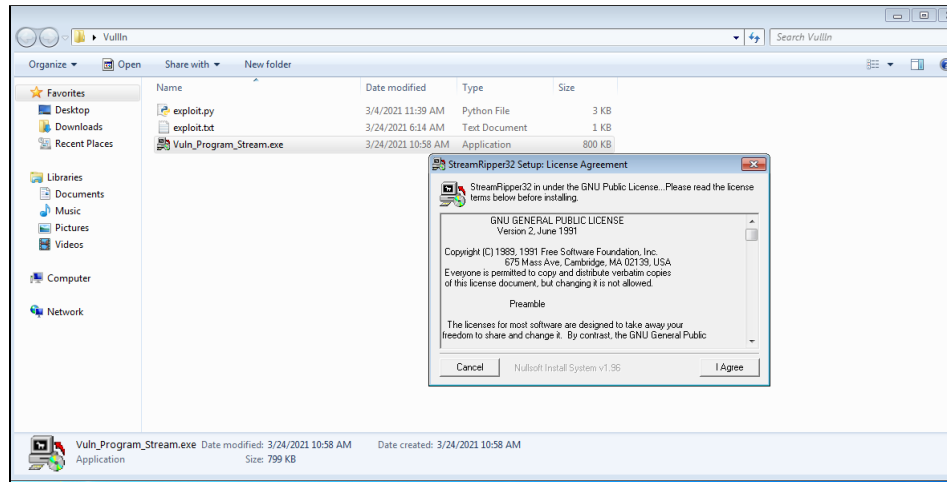


Got the payload exploit.txt

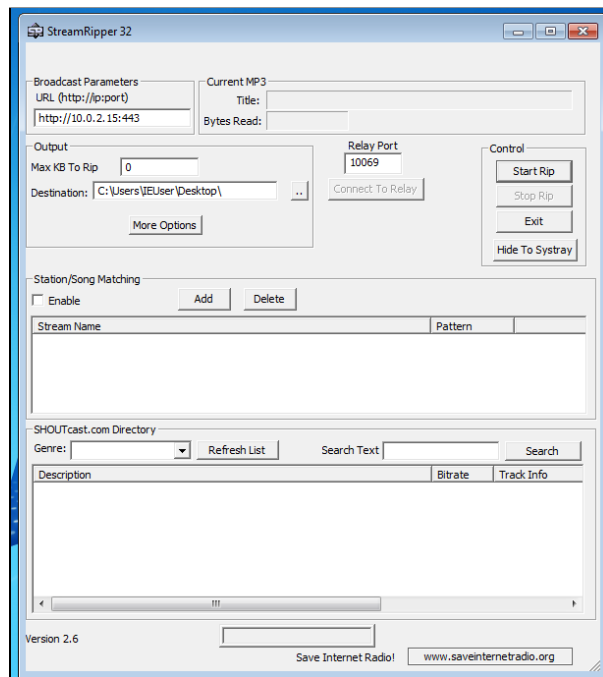




Running Vuln_Program_Stream.exe

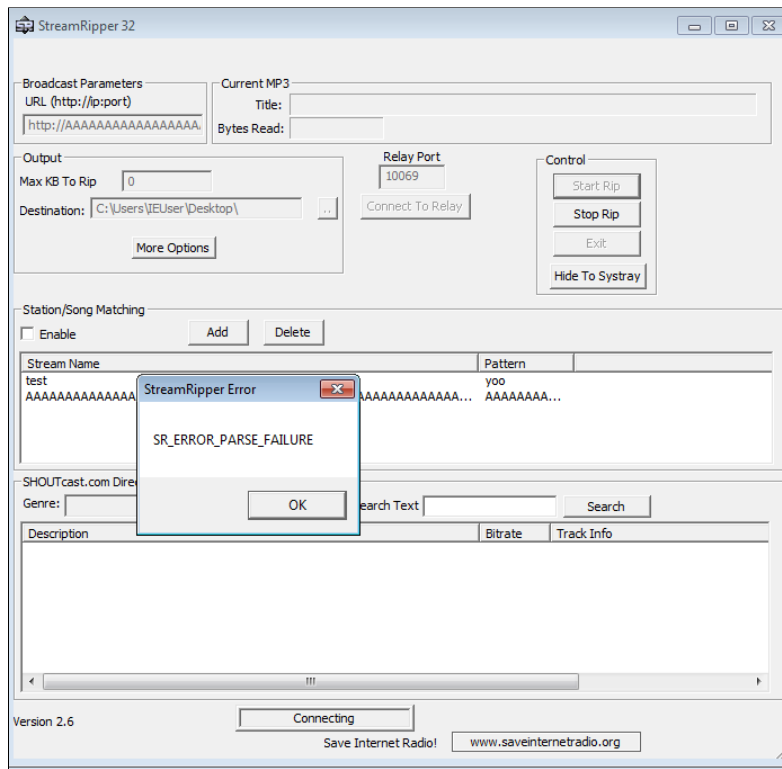


Open the application

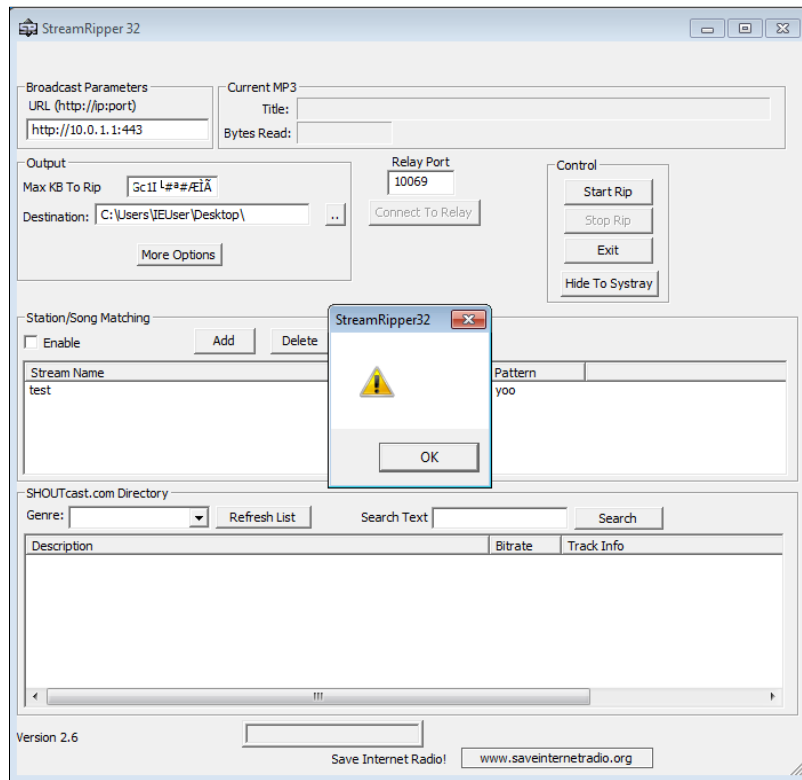


Adding the payload in different input fields and testing to find any vulnerability.

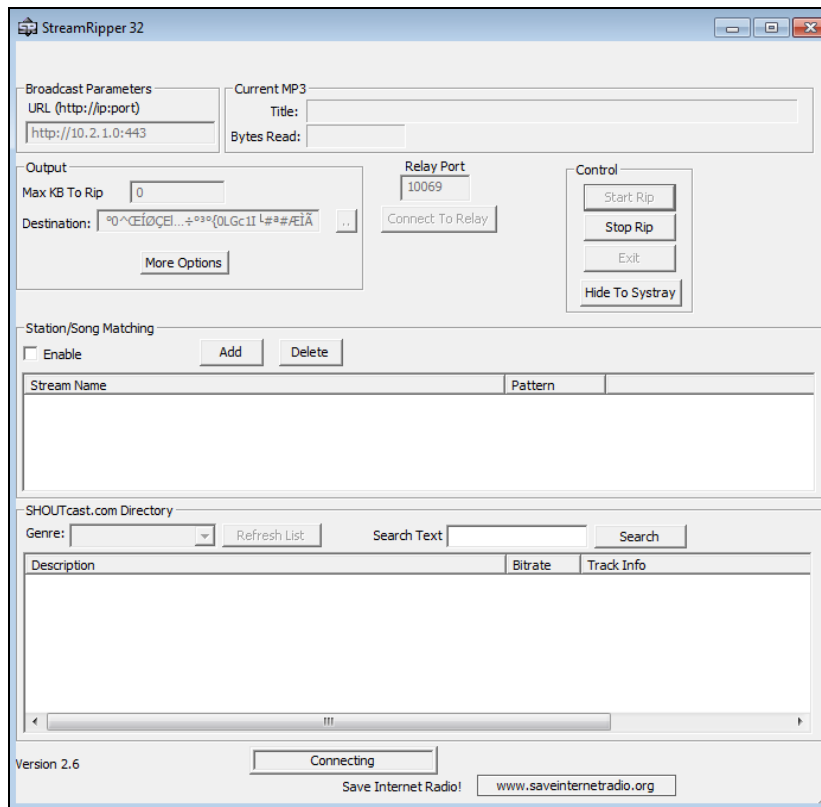
Url field works fine normally throws an error.



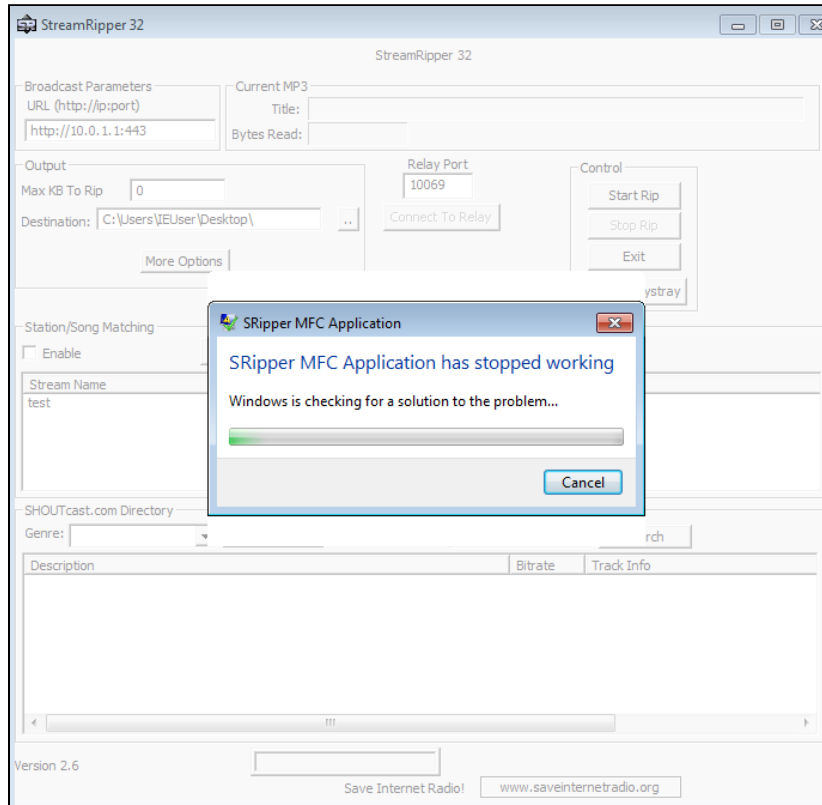
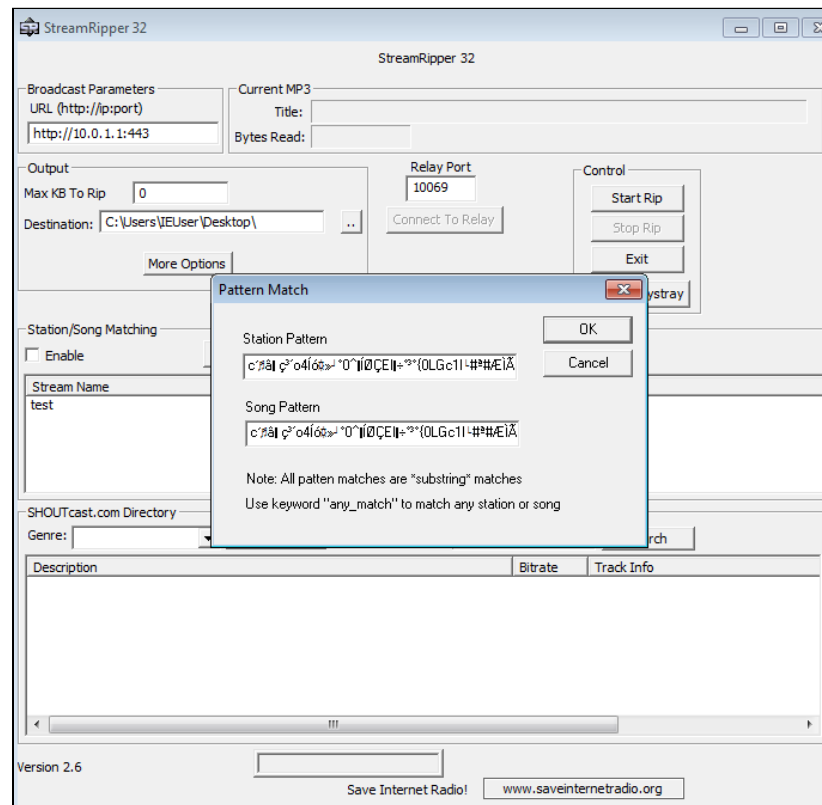
Max KB field throws an error but the application does not crash

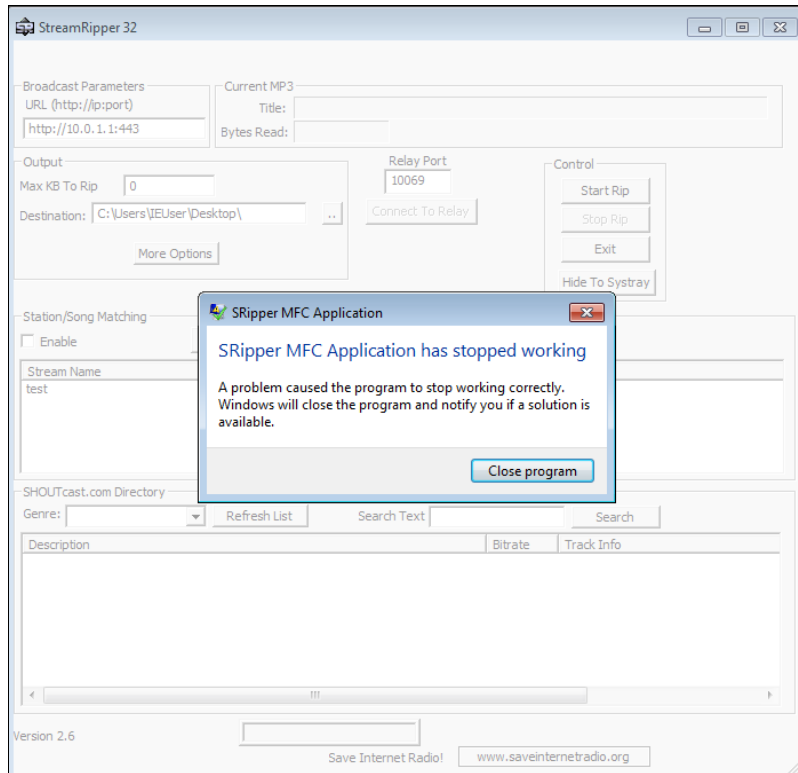


Destination and relay port field also works fine

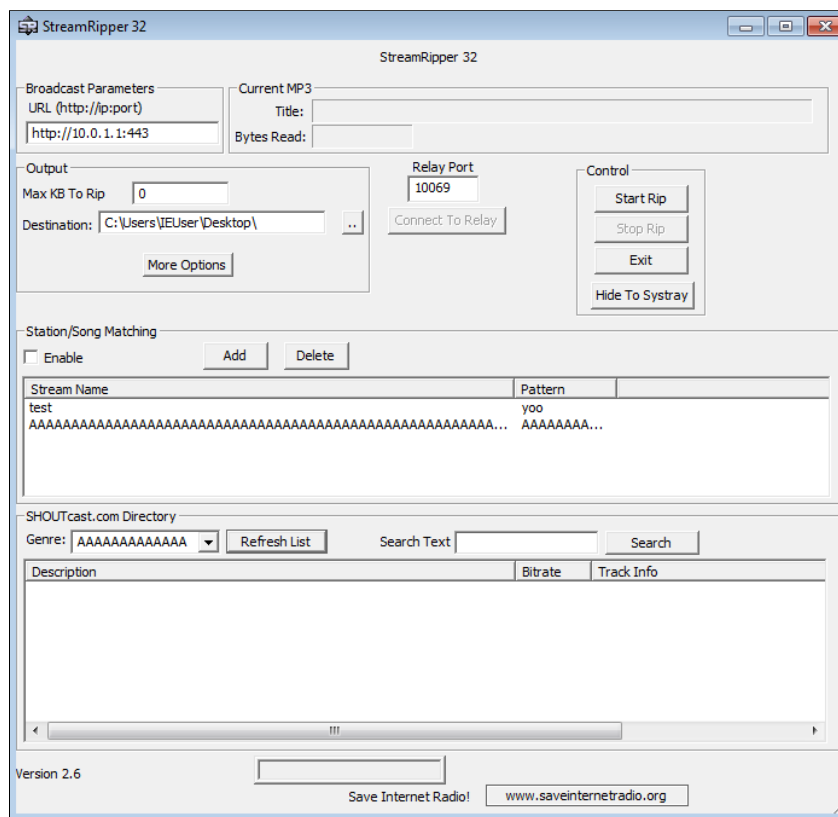


In station pattern or song pattern when we add the payload, app crashes

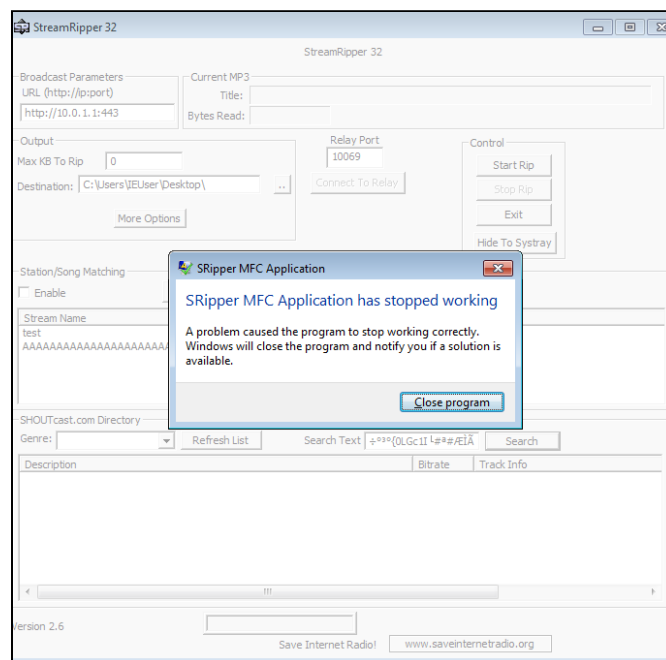
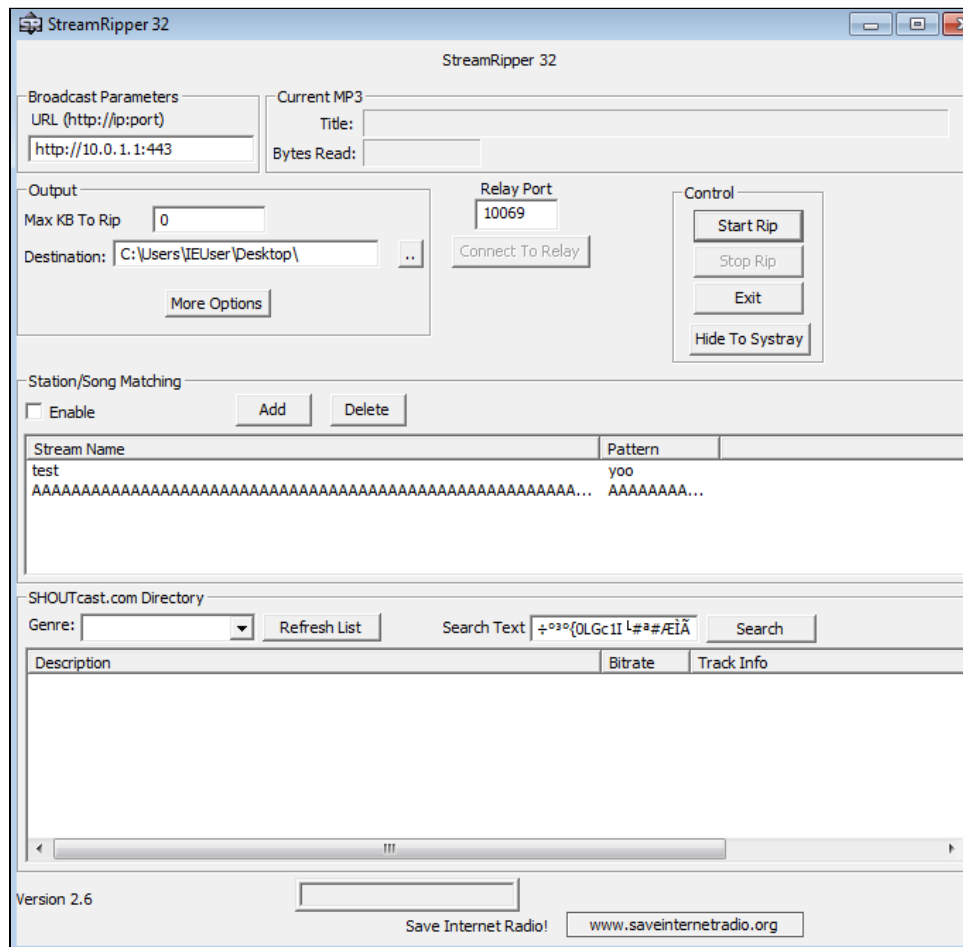




Genre field works fine



Search text field again crashes the app



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.