SECURE CODING

LAB ASSIGNMENT -7

RAKESH RANJAN

18BCE7116

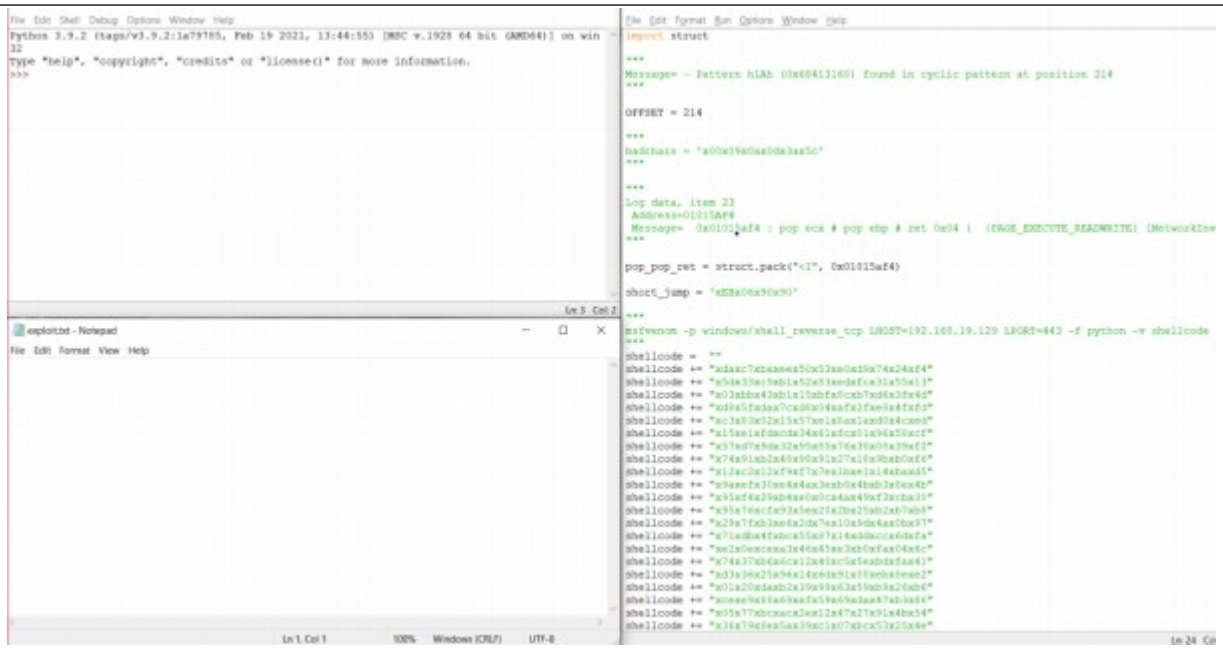
L25+26

Lab experiment - Working with the memory vulnerabilities Task

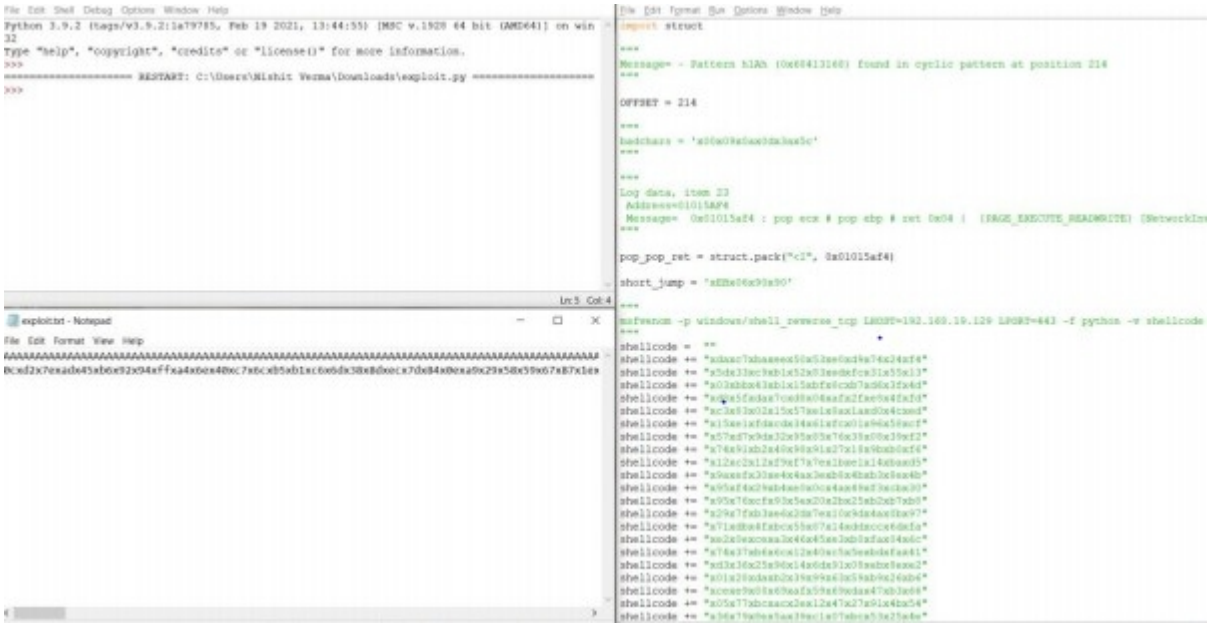
- **Download Vulln.zip from teams.**
- **Deploy a virtual windows 7 instance and copy the Vulln.zip into it.**
- **Unzip the zip file. You will find two files named exploit.py and Vuln_Program_Stream.exe**
- **Download and install python 2.7.* or 3.5.***
- **Run the exploit script to generate the payload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

Payload Generation

- Before the execution of file ‘exploit.py’.



· After the execution of file ‘exploit.py’.



· The payload has been generated in the ‘exploit.txt’ file.

Analysis

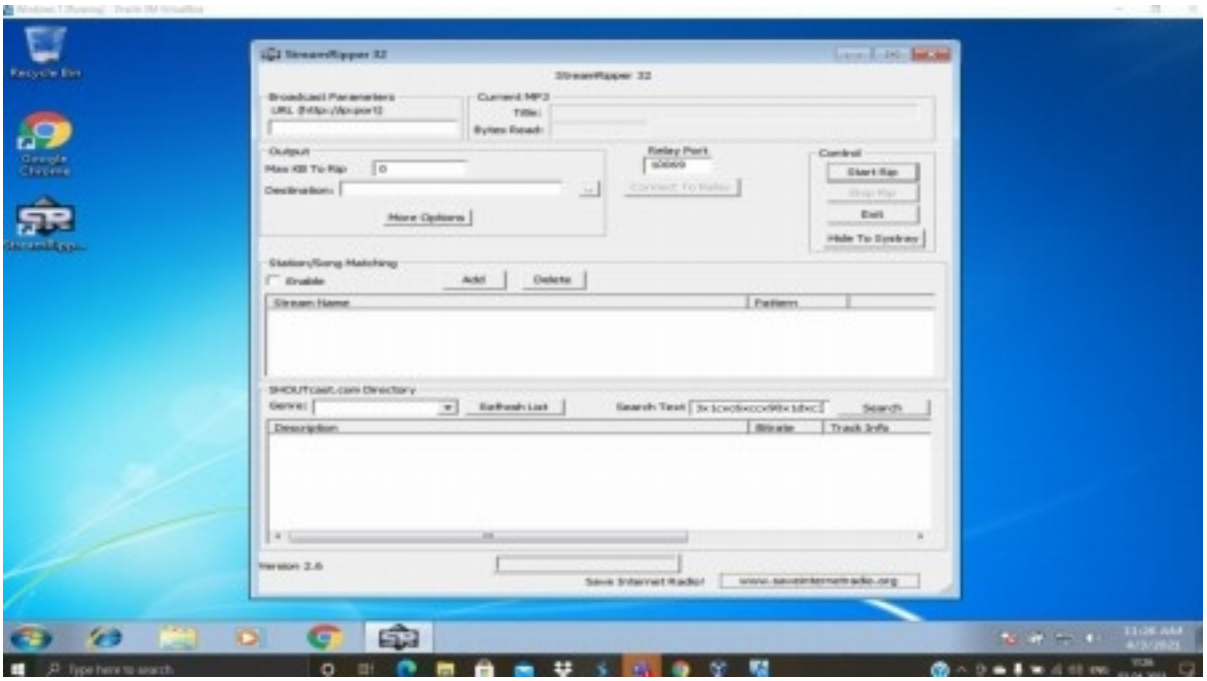
· I have generated the payload to test on the application StreamRipper32, we have to check each and every input box so that we can know which input fields are vulnerable to buffer

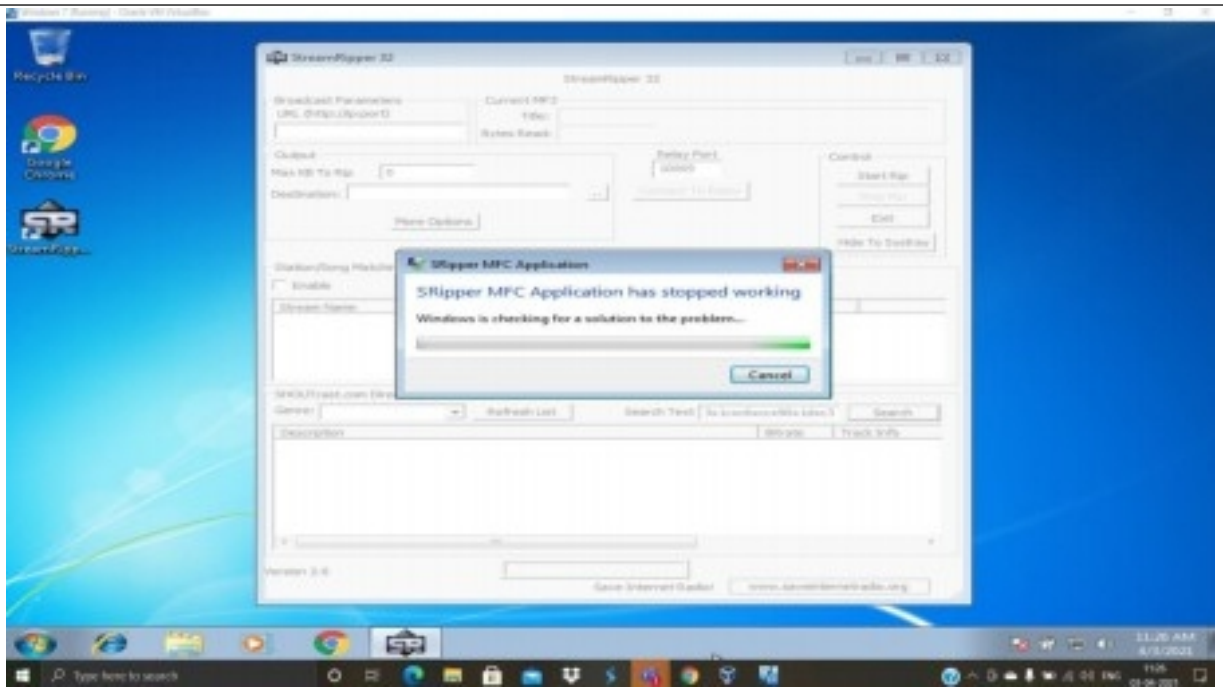
overflow.

· Buffer Overflow is an anomaly where a program, while writing data to a buffer, overruns the buffer's boundary and overwrites adjacent memory locations thus making the application vulnerable to data leaks, unauthorized access and also results in crashes

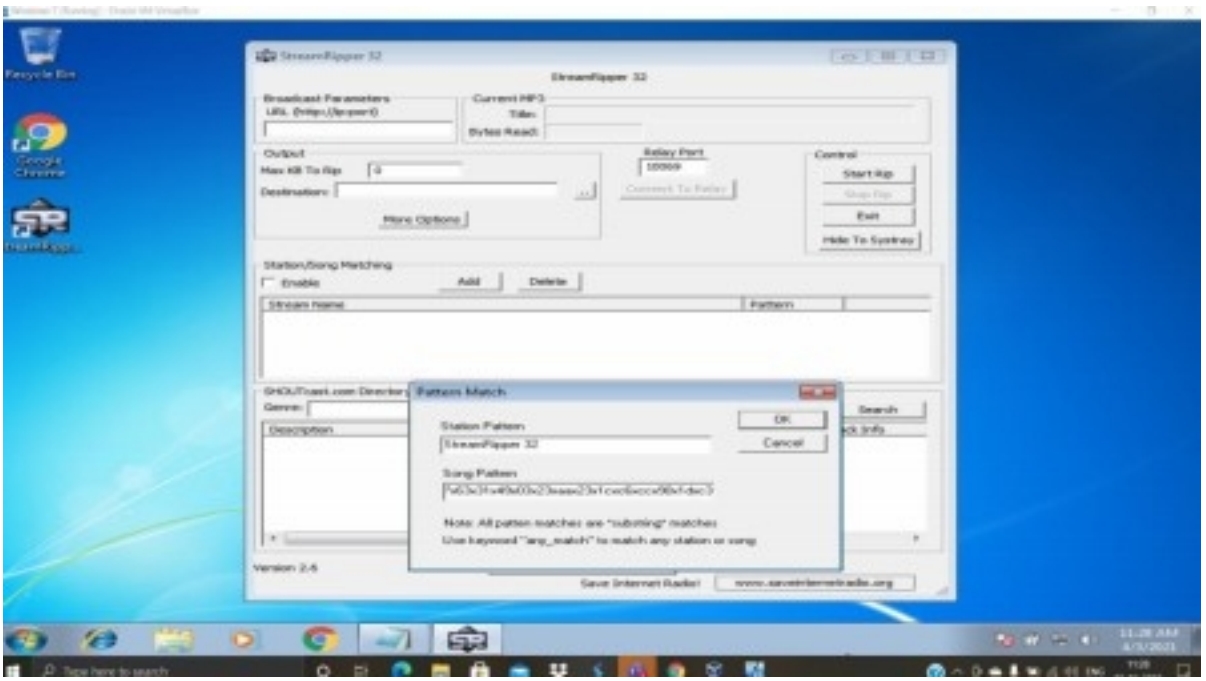
.

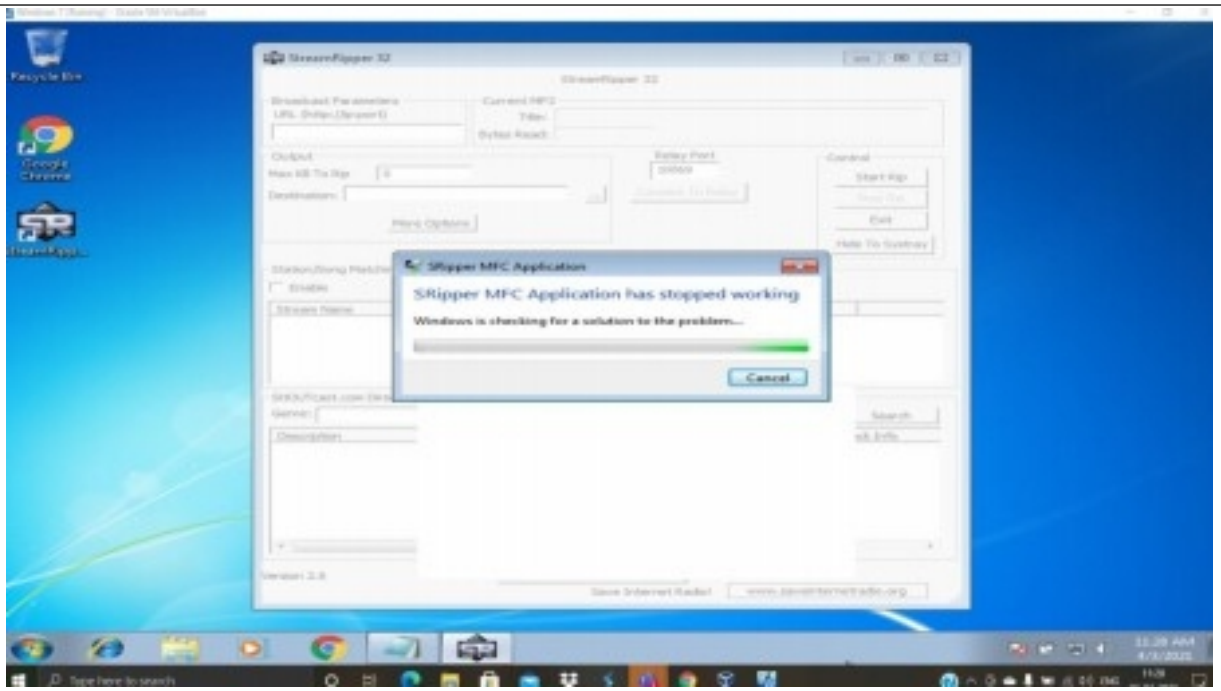
1. 1st instance of Buffer Overflow occurs from the Search Text Box when we enter the payload inside the search text box and click on Search.



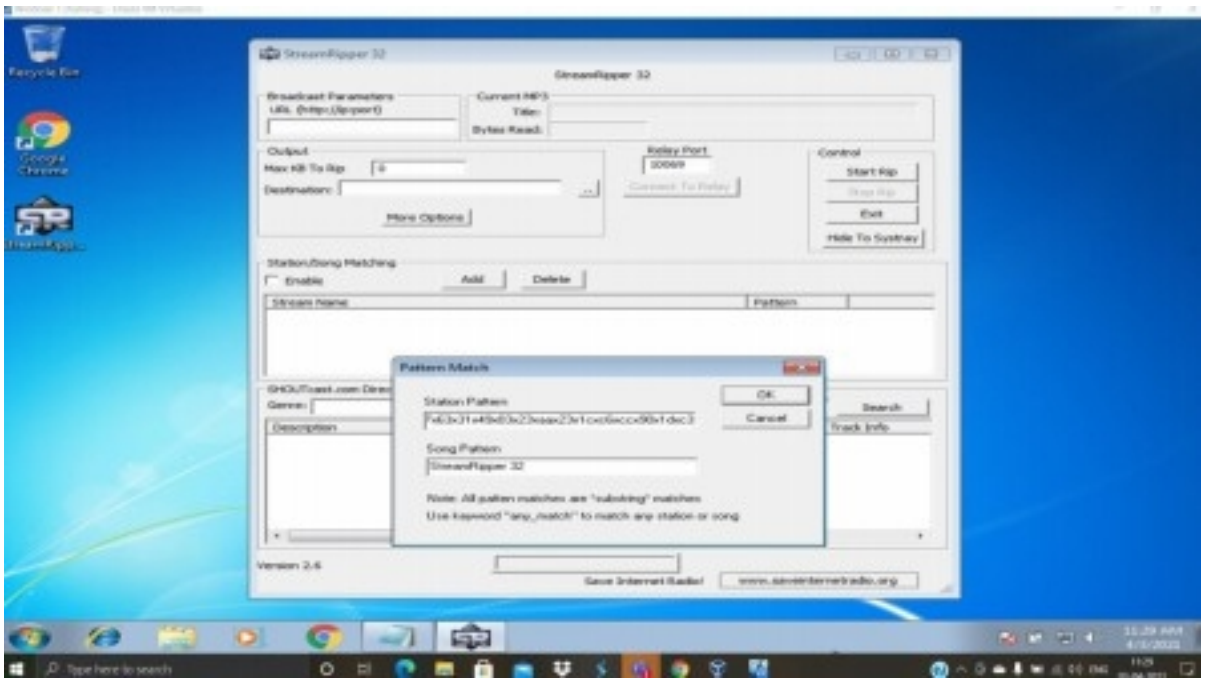


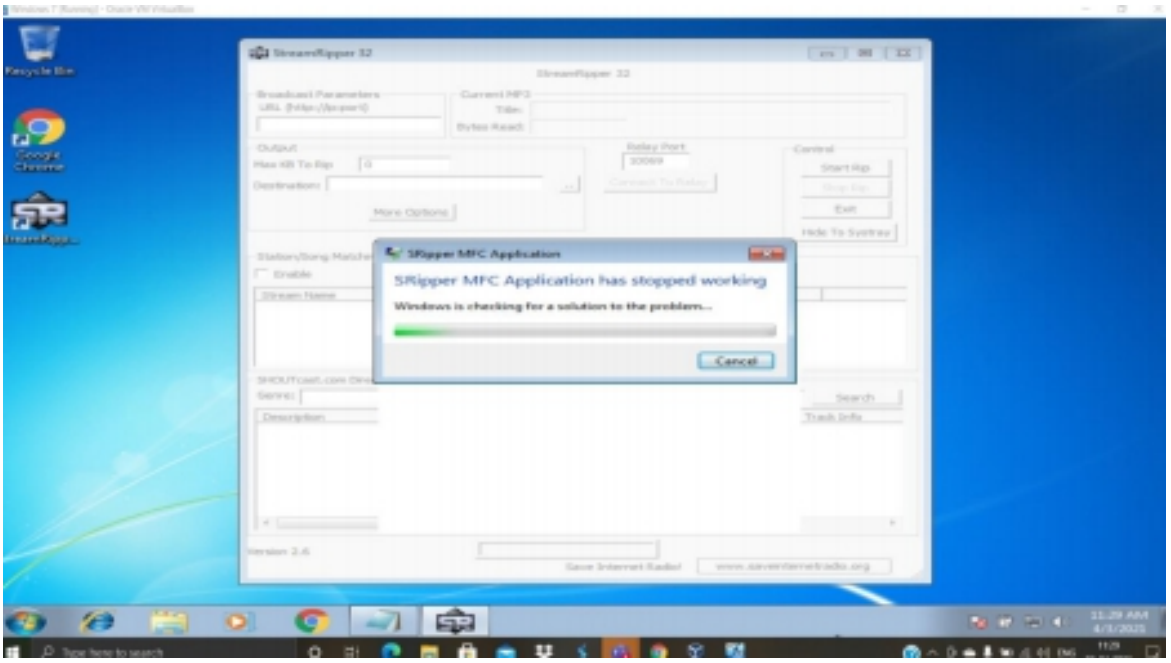
2. 2nd instance of Buffer Overflow occurs from the Song Pattern text box (which appears when we click on the add button) when we enter the payload inside the song pattern text box and click on Ok.





3. 3rd instance of Buffer Overflow occurs from the Station Pattern text box (which appears when we click on the add button) when we enter the payload inside the station pattern text box and click on Ok.





Conclusion

· The application StreamRipper32 crashes as we enter the payload inside the aforementioned input text boxes.
· So, the application StreamRipper32 is vulnerable to Buffer Overflow from 3 different input fields. They are
1. Search Box
2. Song pattern
3. Station Pattern