

Secure Coding | Lab 7

by prof. Sibi Chakkaravarthy

Sk Saddam Hossain

18BCN7143

>_ BUFFER OVERFLOW in The Application (Stream ripper 32):

Description: A buffer overflow occurs when the volume of data exceeds the storage capacity of the memory buffer. As a result, the program attempting to write the data to the buffer overwrites adjacent memory locations.

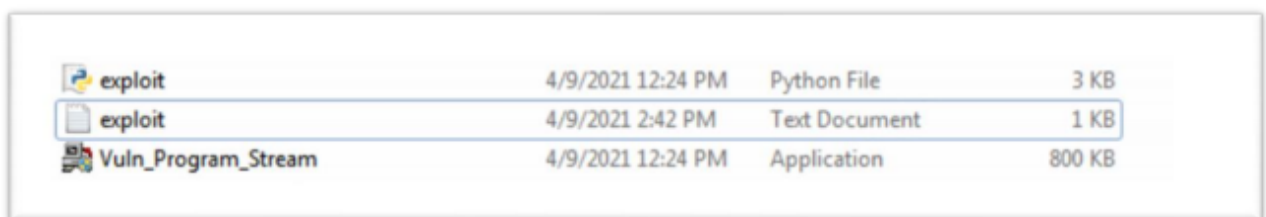
Proof-of-concept:

Step 1: download the application called stream ripper 32

Step 2: Install and open it.

Step 3: run a py(exploit.py) file which generates more than 500 characters.

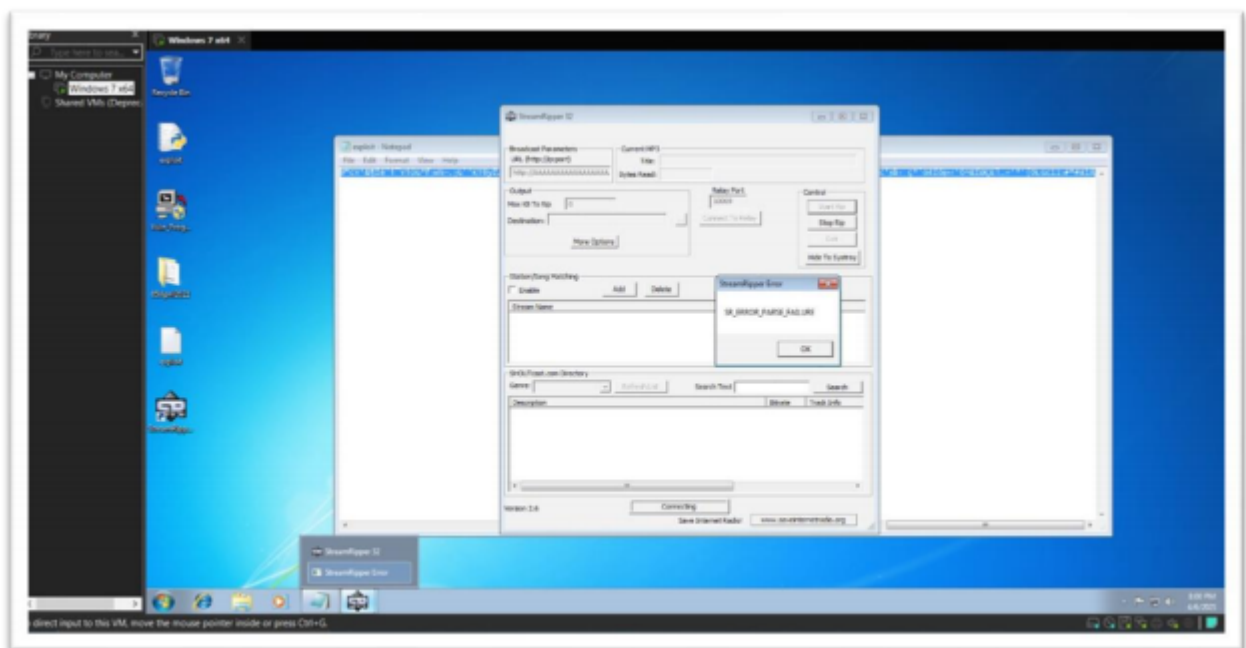
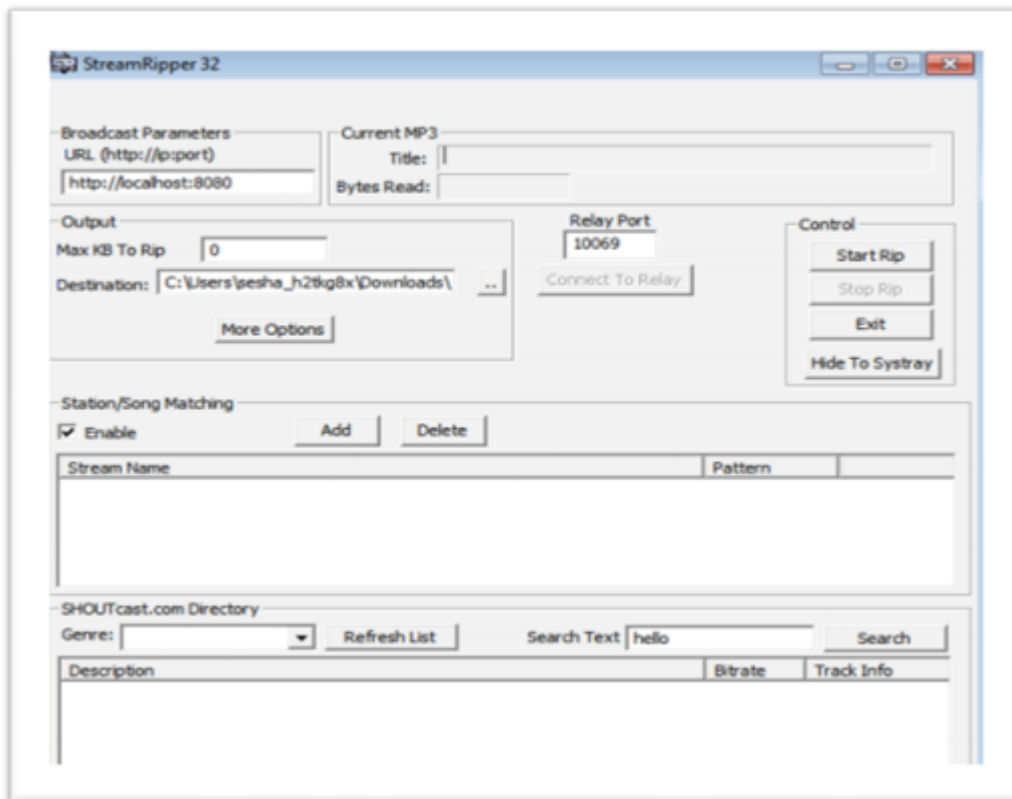
Step 4: open file called exploit.txt which will be saved where there is a py file.



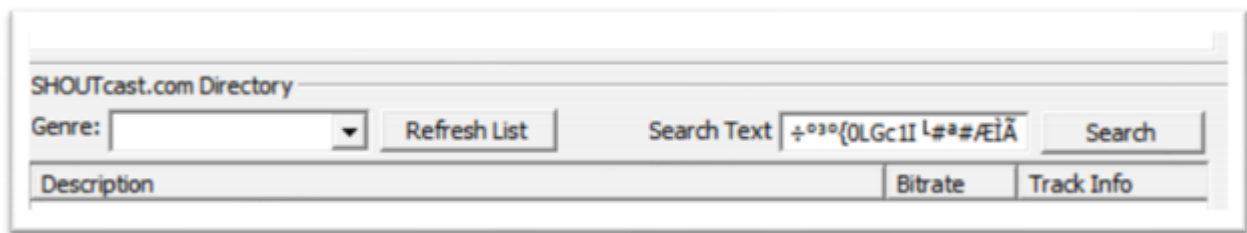
exploit	4/9/2021 12:24 PM	Python File	3 KB
exploit	4/9/2021 2:42 PM	Text Document	1 KB
Vuln_Program_Stream	4/9/2021 12:24 PM	Application	800 KB

Step 5: copy entire text from exploit.txt (got it from exploit.py file)

Step 6: open stream ripper 32 application in VM WARE



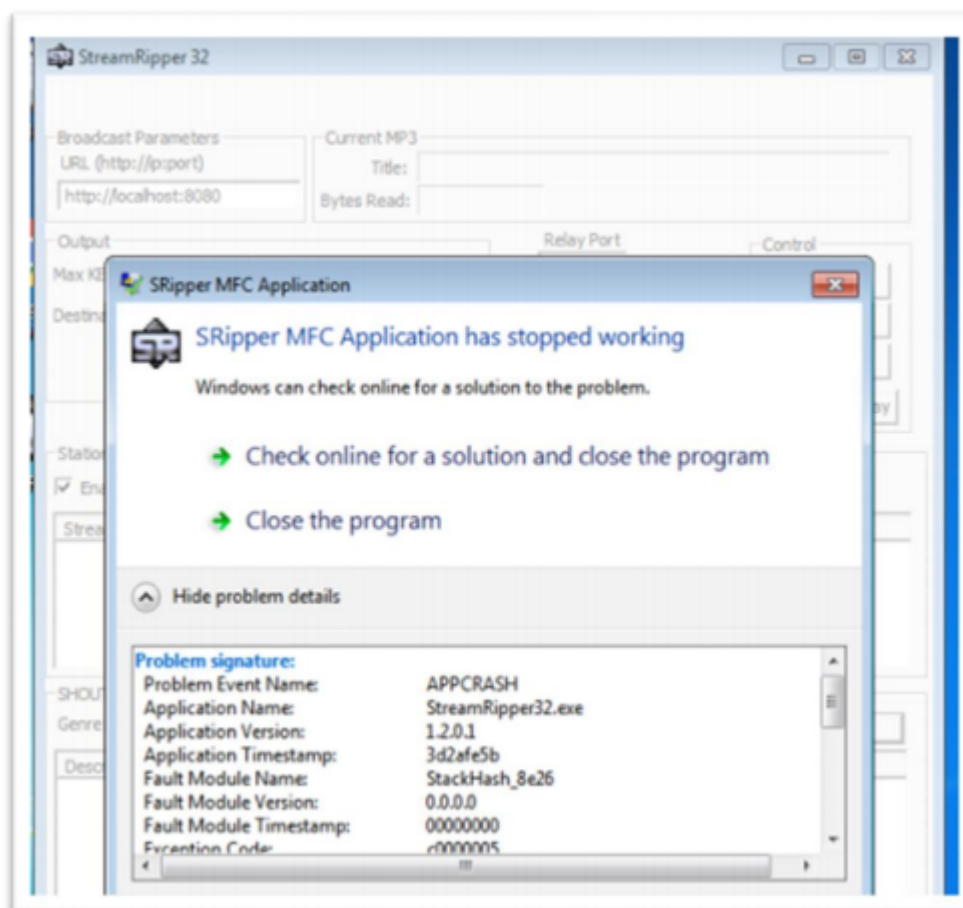
Step 7: paste the text in the Search Text box from copy entire text from exploit.txt



Step8: click on the Search button.

RESULT - When you click on the Search button, streamRipper32 applications get crashed/it stops working.

DUE TO BUFFER OVERFLOW



Solution: To fix this vulnerability we can use common protections like

- Address space randomization (ASLR)
- Data execution prevention
- Structured exception handler overwrite protection (SEHOP)