LAB-08

NAME:AJEETH PAUL **COURSE CODE:-**CSE-2010
REG_ID:-18BCD7058 **SLOT:-**L39+L40

Working with the memory vulnerabilities

Report:

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.

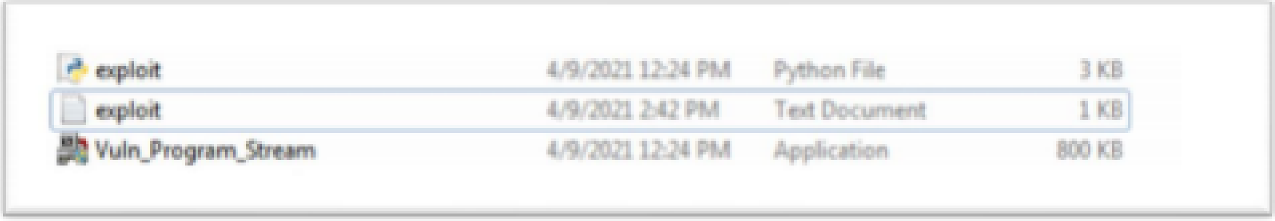
Proof-of-concept:

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.

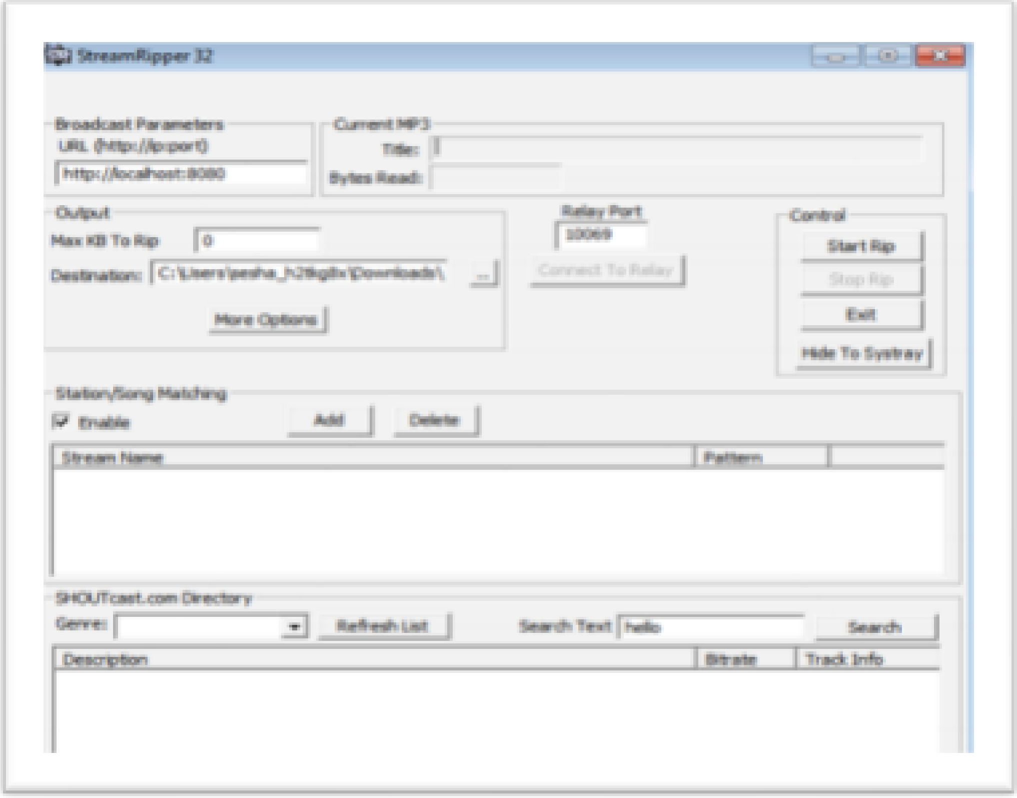
Step 4:open file called exploit.txt which will be saved where there is a py file.



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



URL (http://ip:port): http://localhost:8080

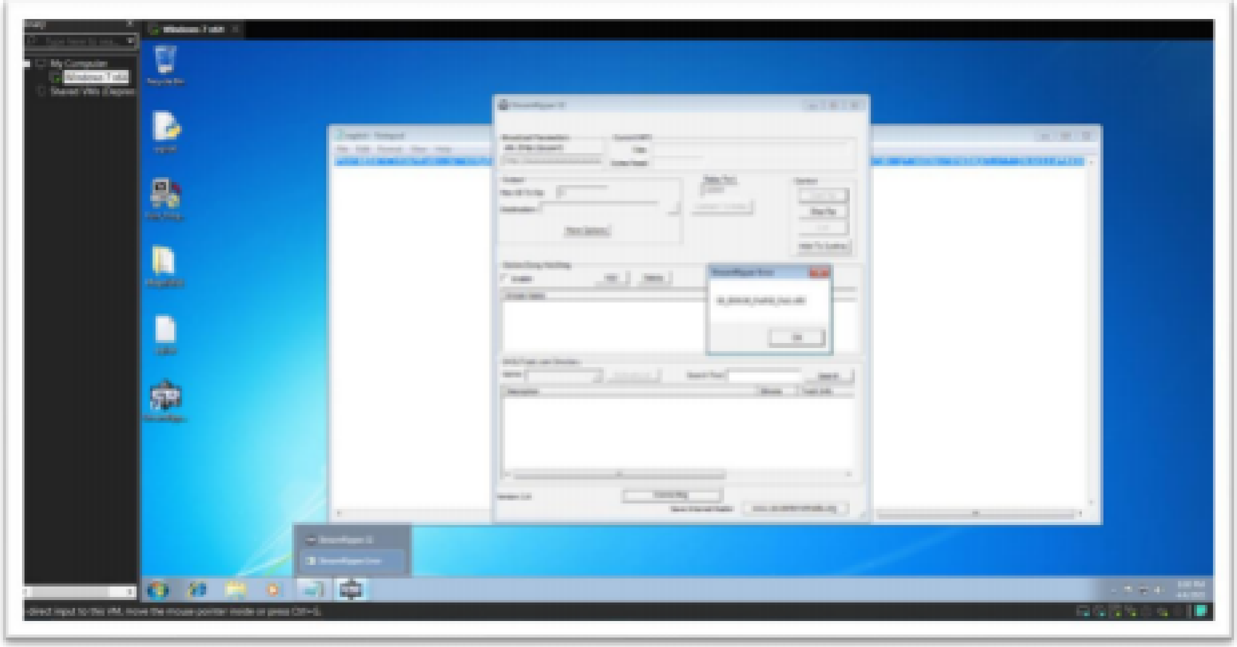
Max KB To Rip: 0

Destination: C:\Users\pesha_h2tkg8x\Downloads\

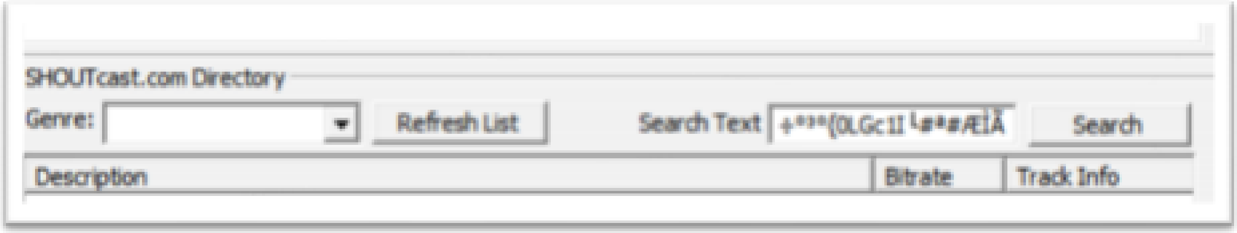
Relay Port: 10069

☑ Enable

Search Text: hello



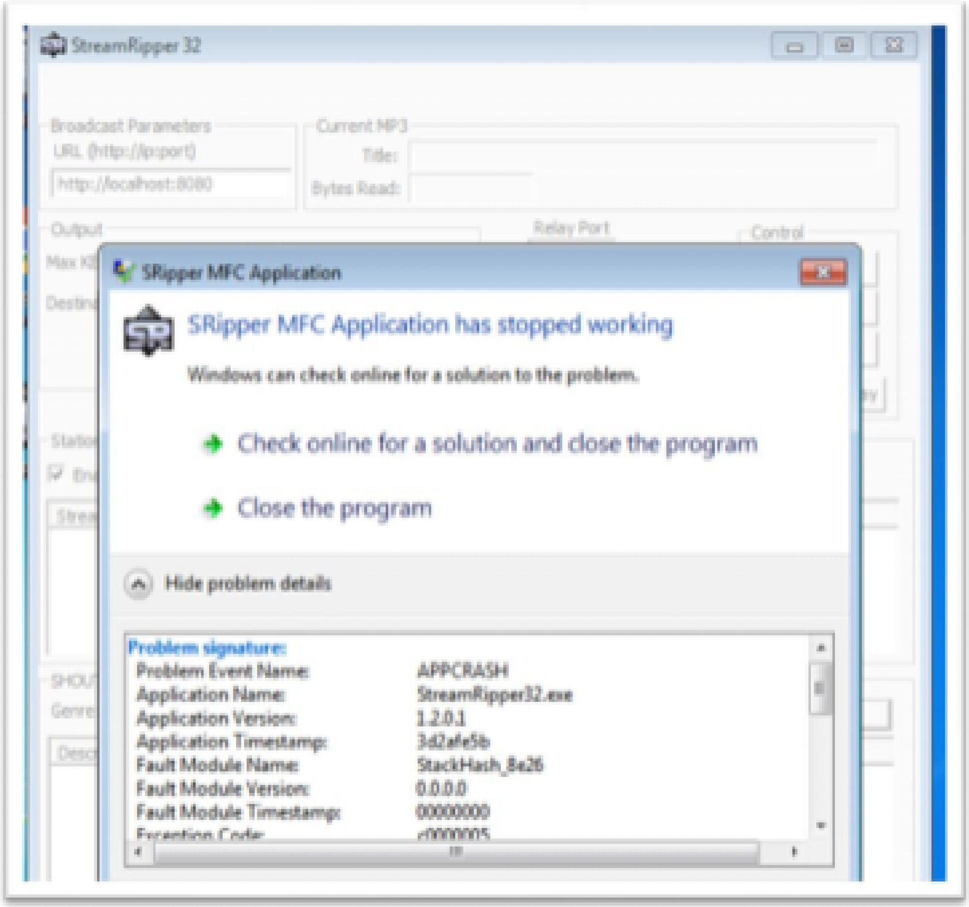
Step7: pastethetext inSearchTextboxfromcopyentiretextfrom exploit.txt



Step8:click on Search button.

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

DUE TO BUFFER OVERFLOW



URL (http://ip:port) http://localhost:8080

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

```
Problem signature:
  Problem Event Name:          APPCRASH
  Application Name:            StreamRipper32.exe
  Application Version:         1.2.0.1
  Application Timestamp:       3d2afe5b
  Fault Module Name:           StackHash_8e26
  Fault Module Version:        0.0.0.0
  Fault Module Timestamp:      00000000
  Exception Code:              c0000005
```

Solution: To fix this vulnerability we can use common protections like: • Address space randomization (ASLR) • Data execution prevention • Structured exception handler overwrite protection (SEHOP)