SECURE CODING CSE2010

LAB-7

CH.SAI SUMEDH

REG NO:-18BCN7092

SLOT:-L39+L40

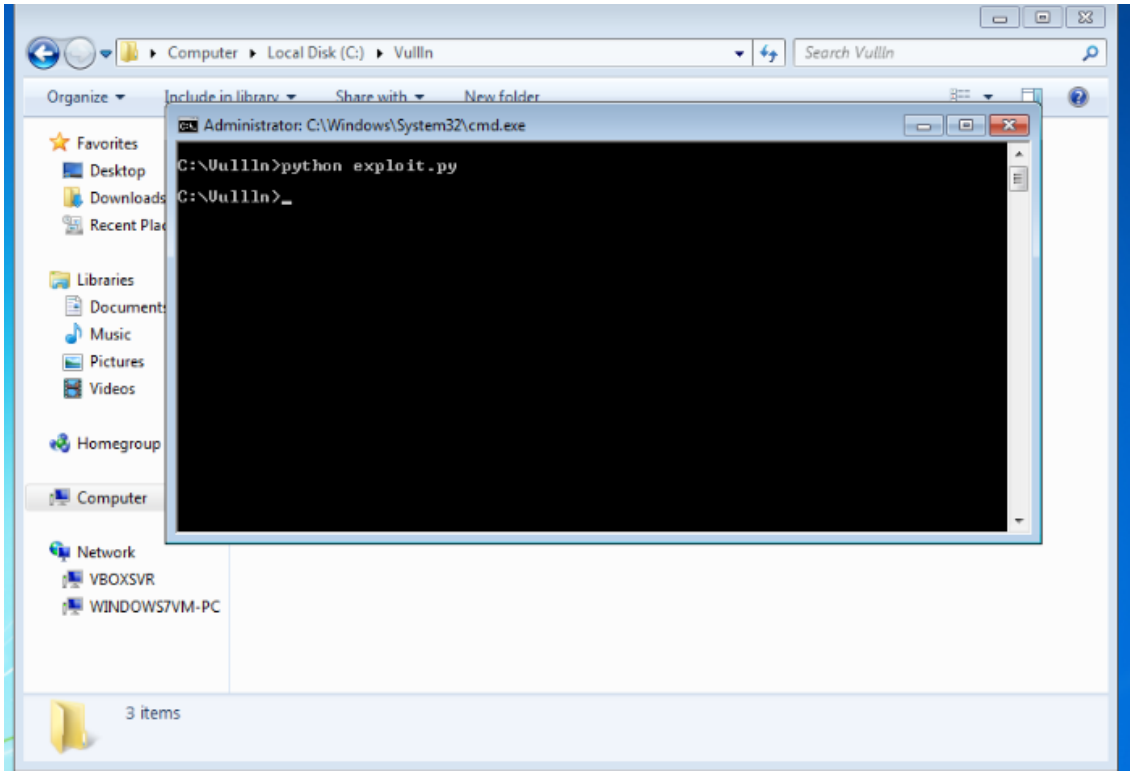
Lab experiment - Working with the memory vulnerabilities

Task

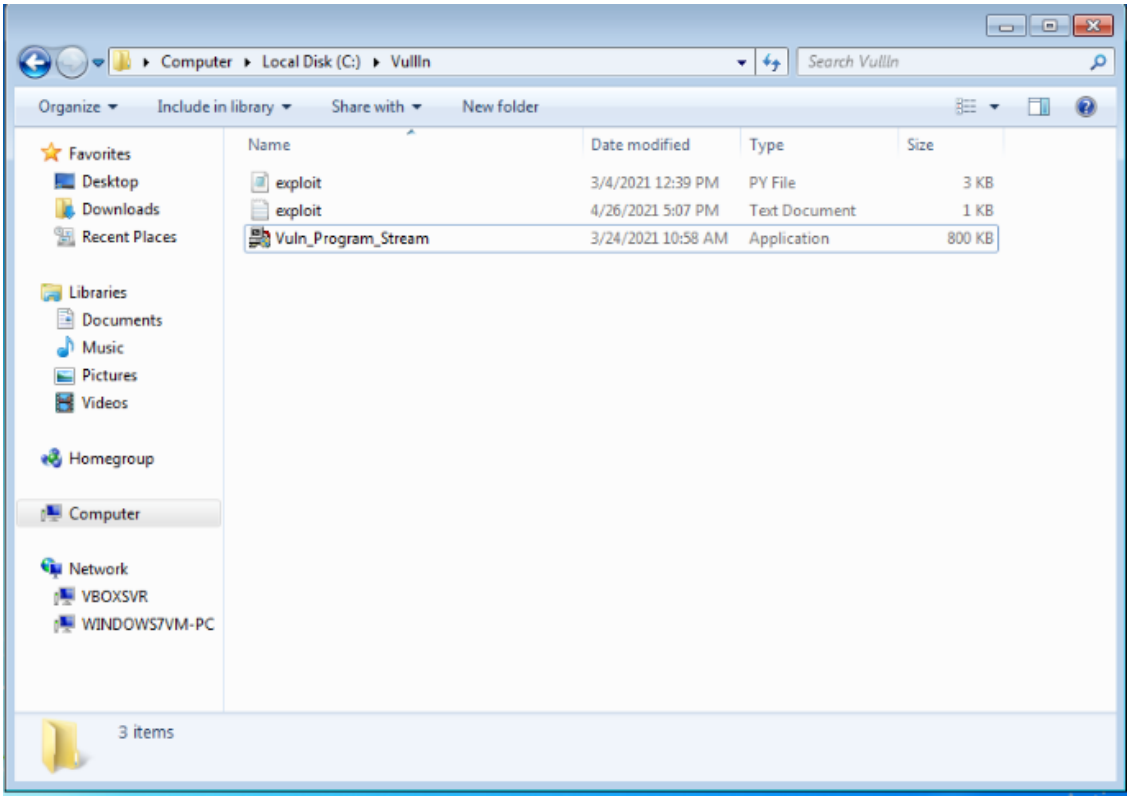
- Download Vulln.zip from teams.
- Deploy a virtual windows 7 instance and copy the Vulln.zip into it.
- Unzip the zip file. You will find two files named exploit.py and Vuln_Program_Stream.exe
- Download and install python 2.7.* or 3.5.*
- Run the exploit script to generate the payload
- Install Vuln_Program_Stream.exe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

Analysis

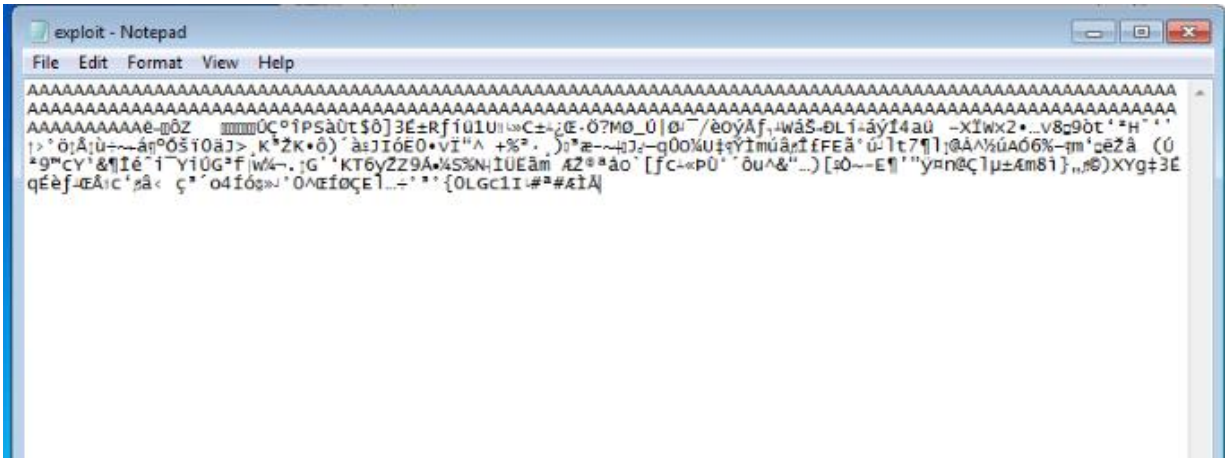
- Crash the Vuln_Program_Stream program and report the vulnerability.



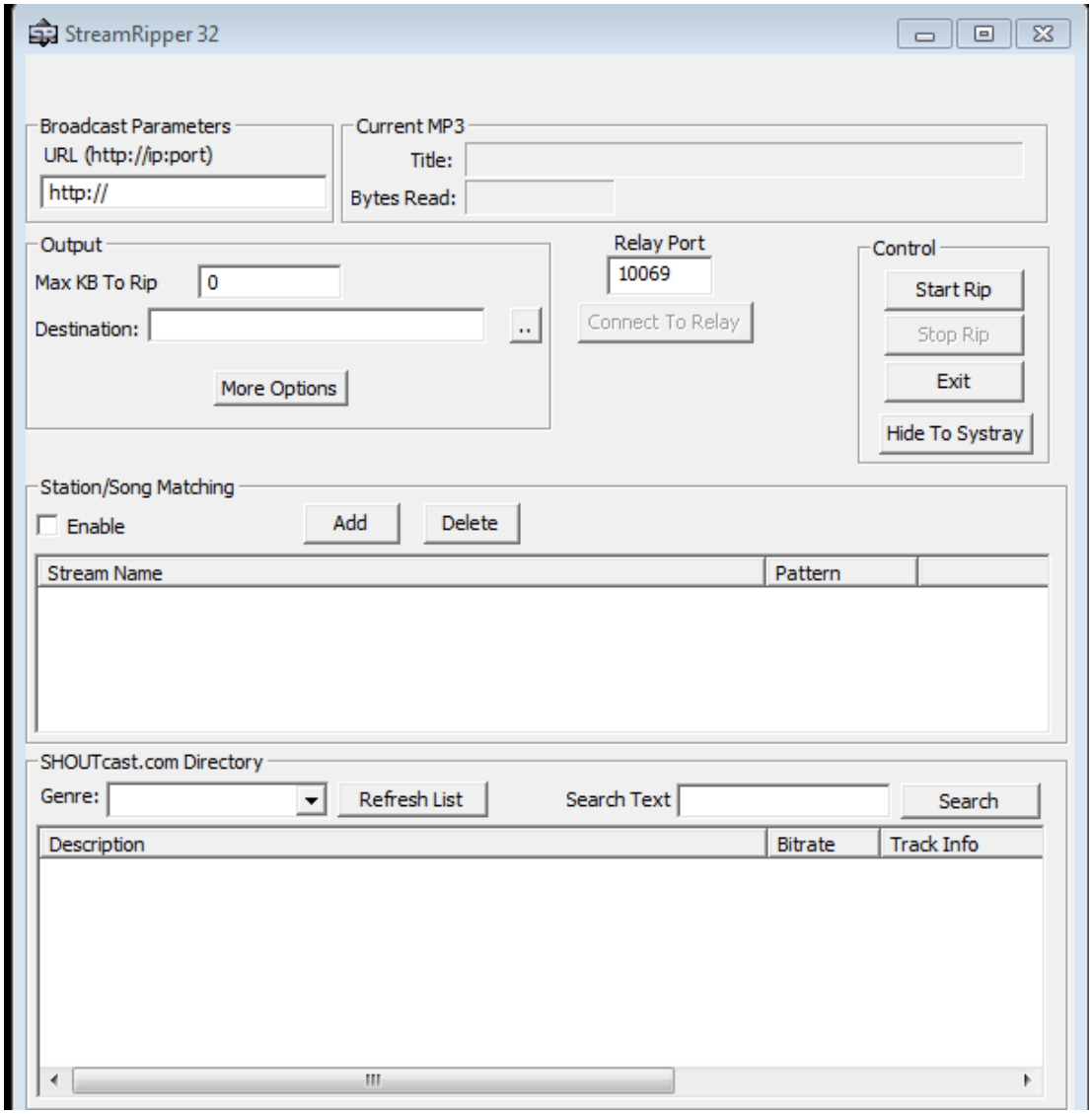
When we run this python script it will generate a text file which consists of some random text.



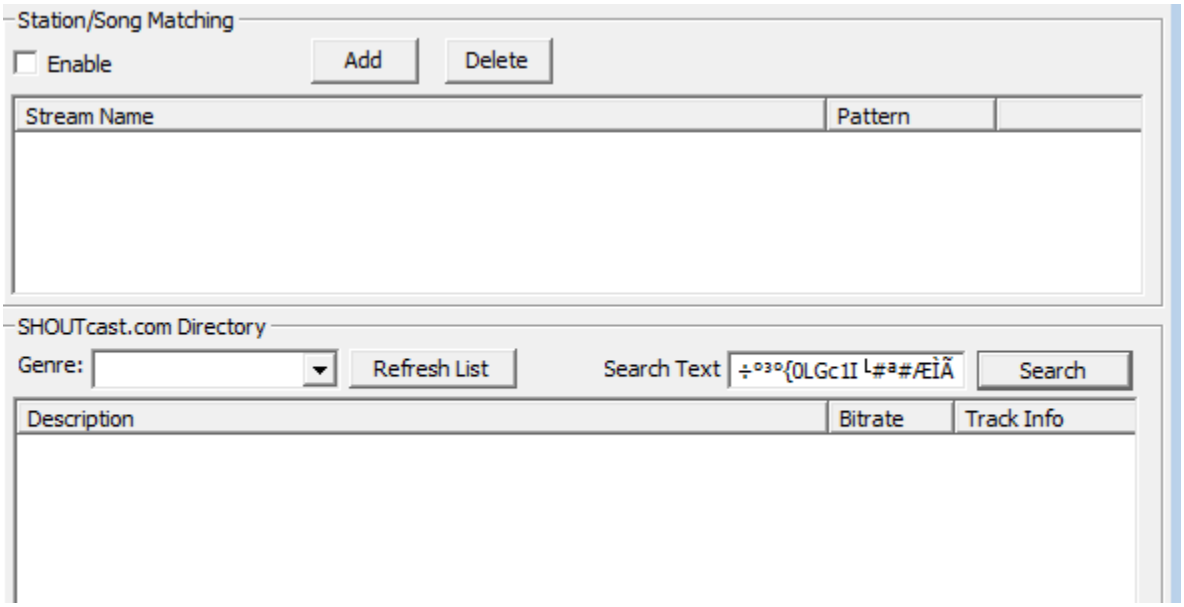
This is the exploit text file which was generated before.



This is the software which we need to crash.



Place the payload in the text field.



After when we search for that string the application will be crashed due to buffer overflow vulnerability.