

# **SECURE CODING CSE2010**

## **LAB-7**

**CH.SAI SUMEDH**

**REG NO:-18BCN7092**

**SLOT:-L39+L40**

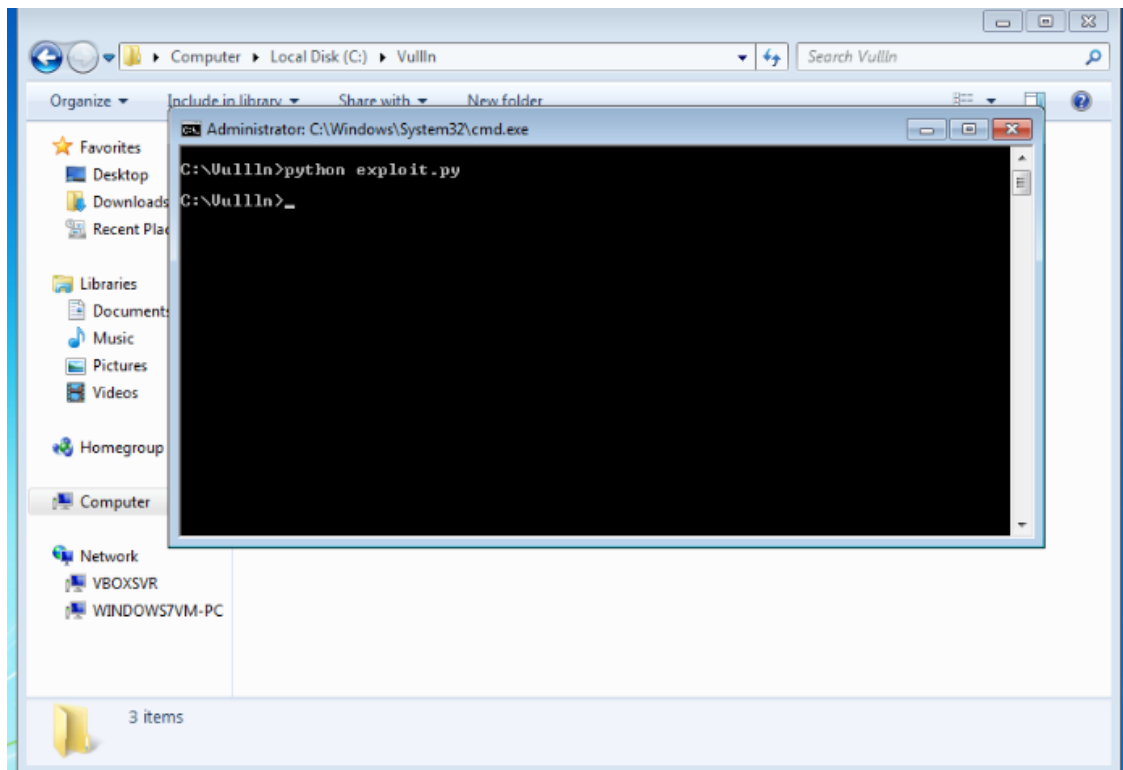
### **Lab experiment - Working with the memory vulnerabilities**

#### **Task**

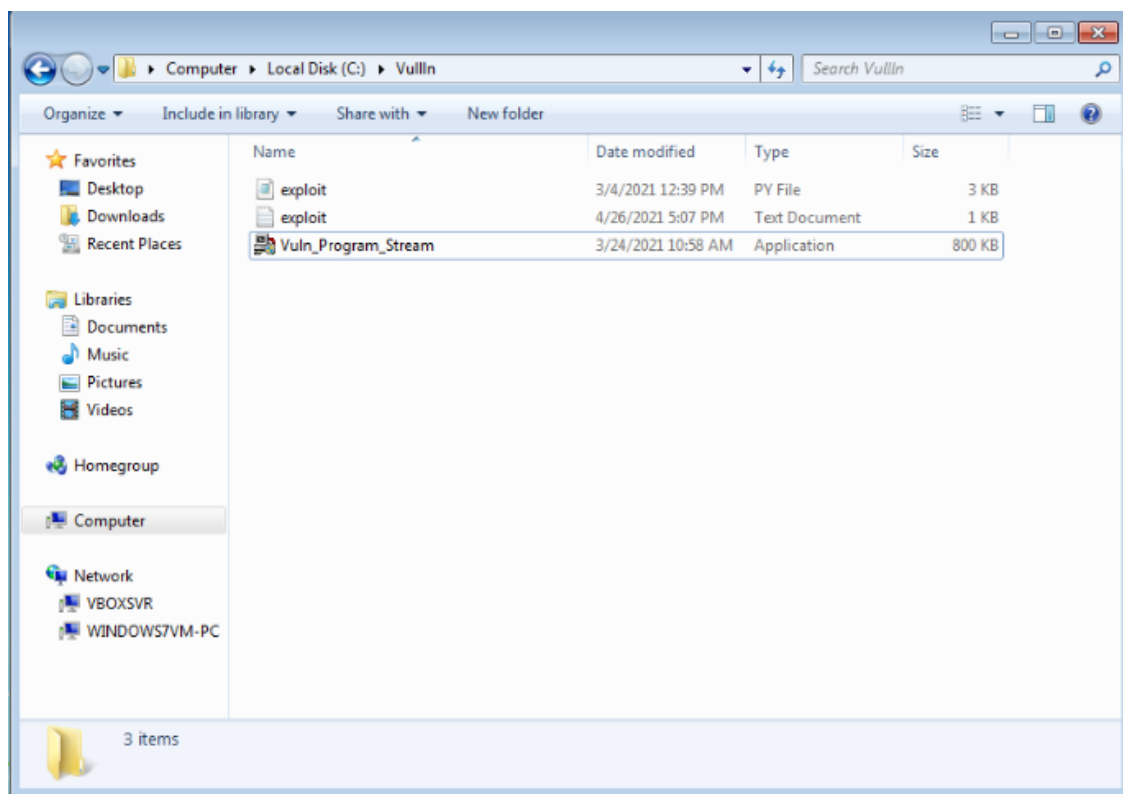
- Download Vulln.zip from teams.
- Deploy a virtual windows 7 instance and copy the Vulln.zip into it.
- Unzip the zip file. You will find two files named exploit.py and Vuln\_Program\_Stream.exe
- Download and install python 2.7.\* or 3.5.\*
- Run the exploit script to generate the payload
- Install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

#### **Analysis**

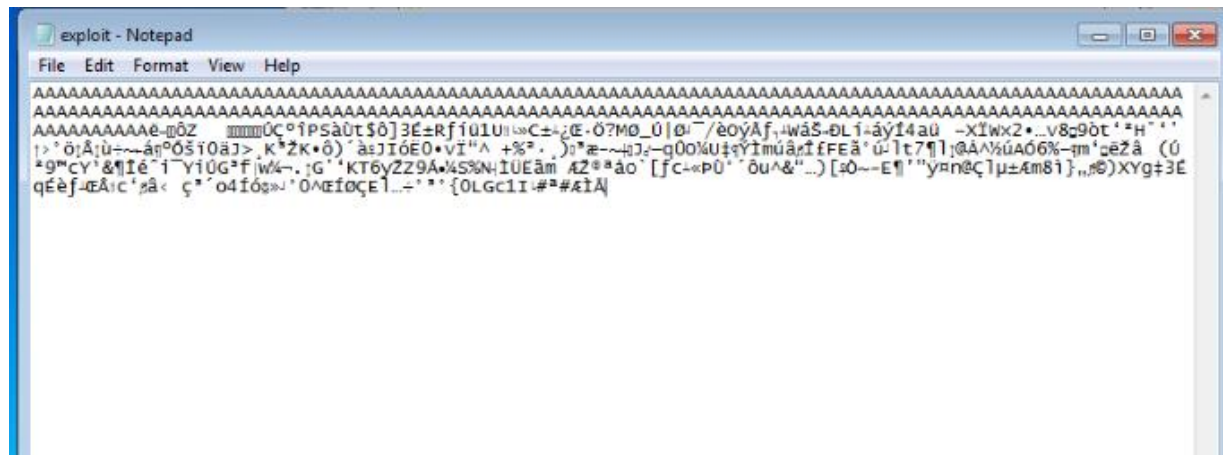
- Crash the Vuln\_Program\_Stream program and report the vulnerability.



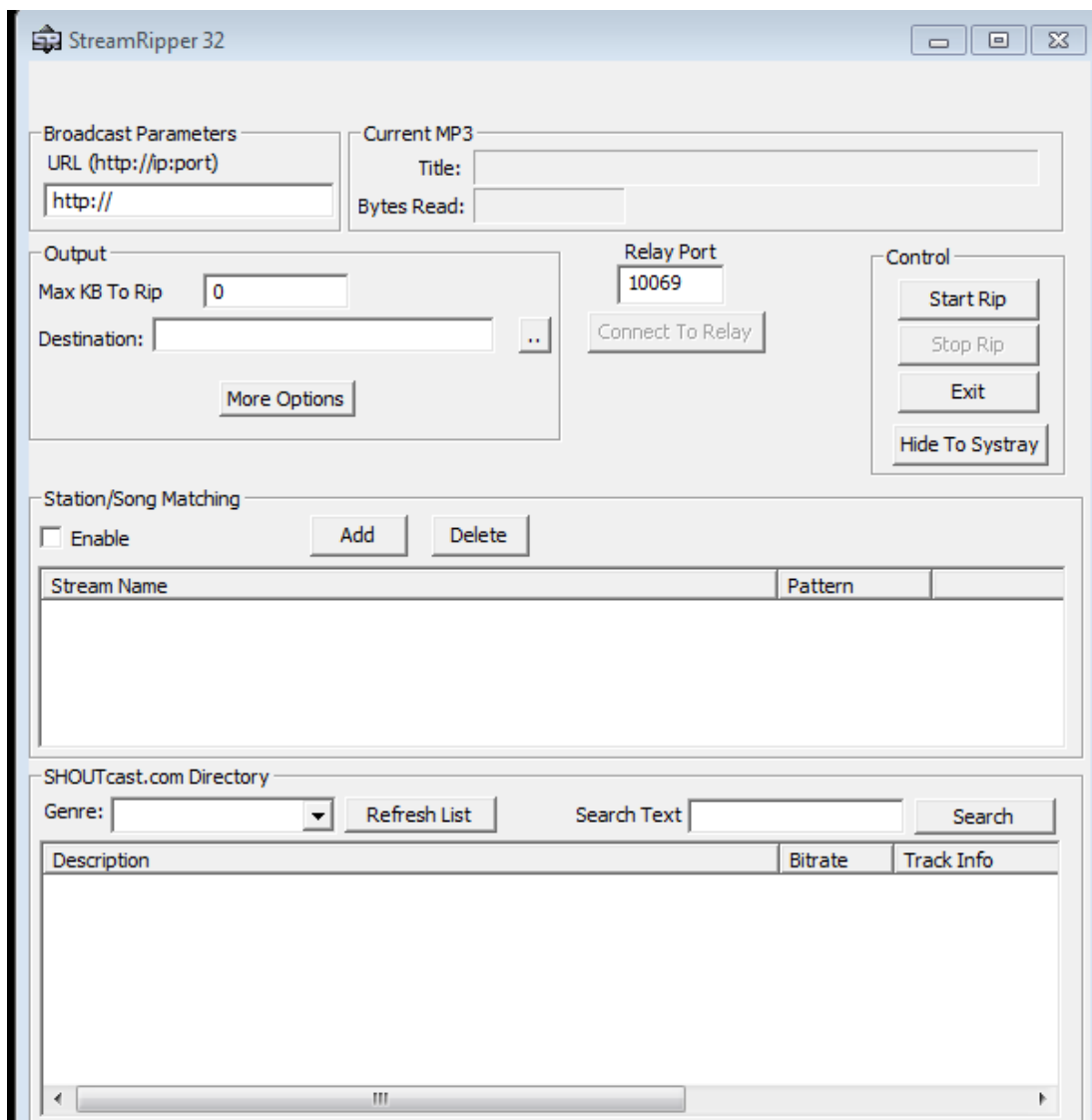
When we run this python script it will generate a text file which consists of some random text.



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.

The screenshot shows the SRipper application interface. The top section, titled "Station/Song Matching", contains an "Enable" checkbox, an "Add" button, and a "Delete" button. Below this is a table with two columns: "Stream Name" and "Pattern". The bottom section, titled "SHOUTcast.com Directory", features a "Genre:" dropdown menu, a "Refresh List" button, a "Search Text" field containing a hex string, and a "Search" button. Below the search controls is a table with three columns: "Description", "Bitrate", and "Track Info".

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

