SECURE CODING LAB

LAB-7
SLOT-L39+L40
18BCN7128
SEGU NAIMISHA

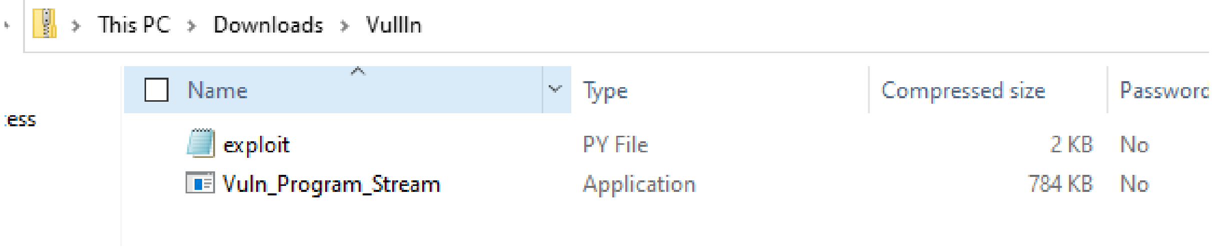
Lab experiment - Working with the memory vulnerabilities

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**

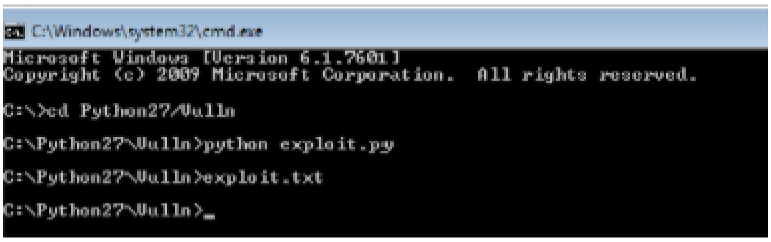
Sol:

Vuln.zip:



Name	Type	Compressed size	Passworc
exploit	PY File	2 KB	No
Vuln_Program_Stream	Application	784 KB	No

Run exploit.py python file and then open payload file.



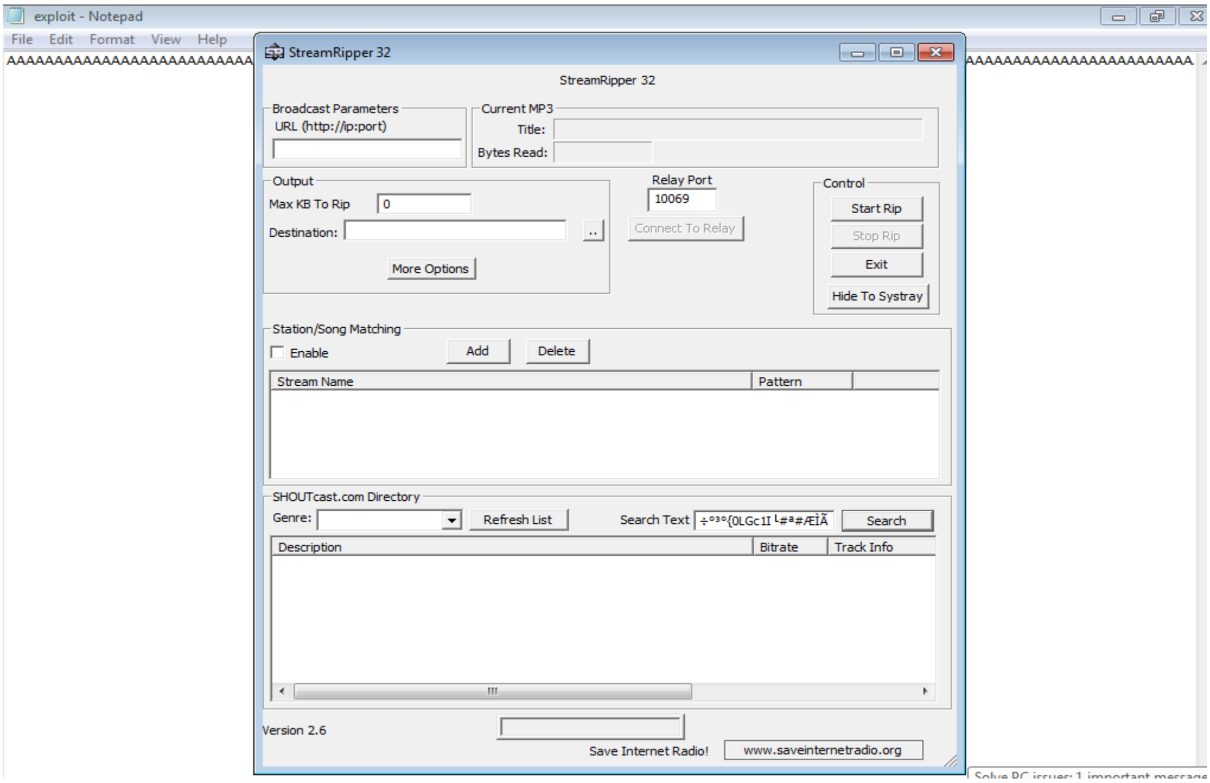
```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\>cd Python27/Vulln

C:\Python27\Vulln>python exploit.py

C:\Python27\Vulln>exploit.txt

C:\Python27\Vulln>_
```



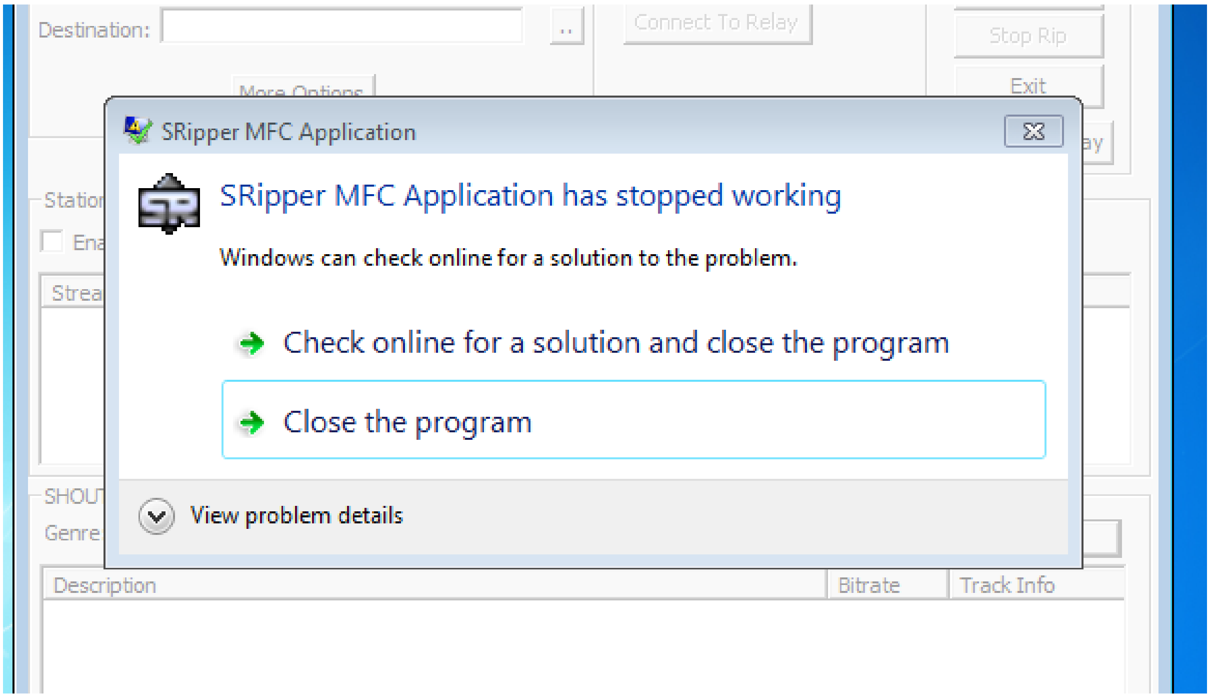
AAAAAAAAAAAAAAAAAAAAAAAAAA

Max KB To Rip: 0

Relay Port: 10069

Search Text: ÷º³º{0LGc1I └#ª#ÆÌÃ

Now copy paste the text in the search box and Finding a malicious Vulnerability file in ripper stream.



SRipper MFC Application

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

View problem details

We can see that the application crashed due to the payload and the application closes/crashes.