

# SECURE CODING

## LAB-7

CH.KARTHIKEYA VARMA | 19BCD7138 | L23-24

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

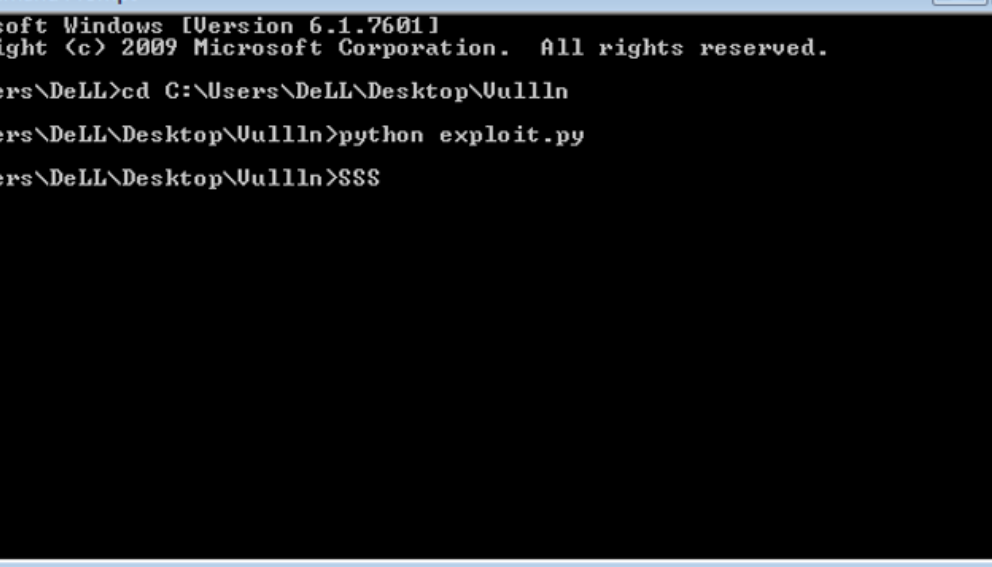
#### **Task**

- **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.



The screenshot shows a Windows desktop environment. In the foreground, a Command Prompt window is open, displaying the following text:

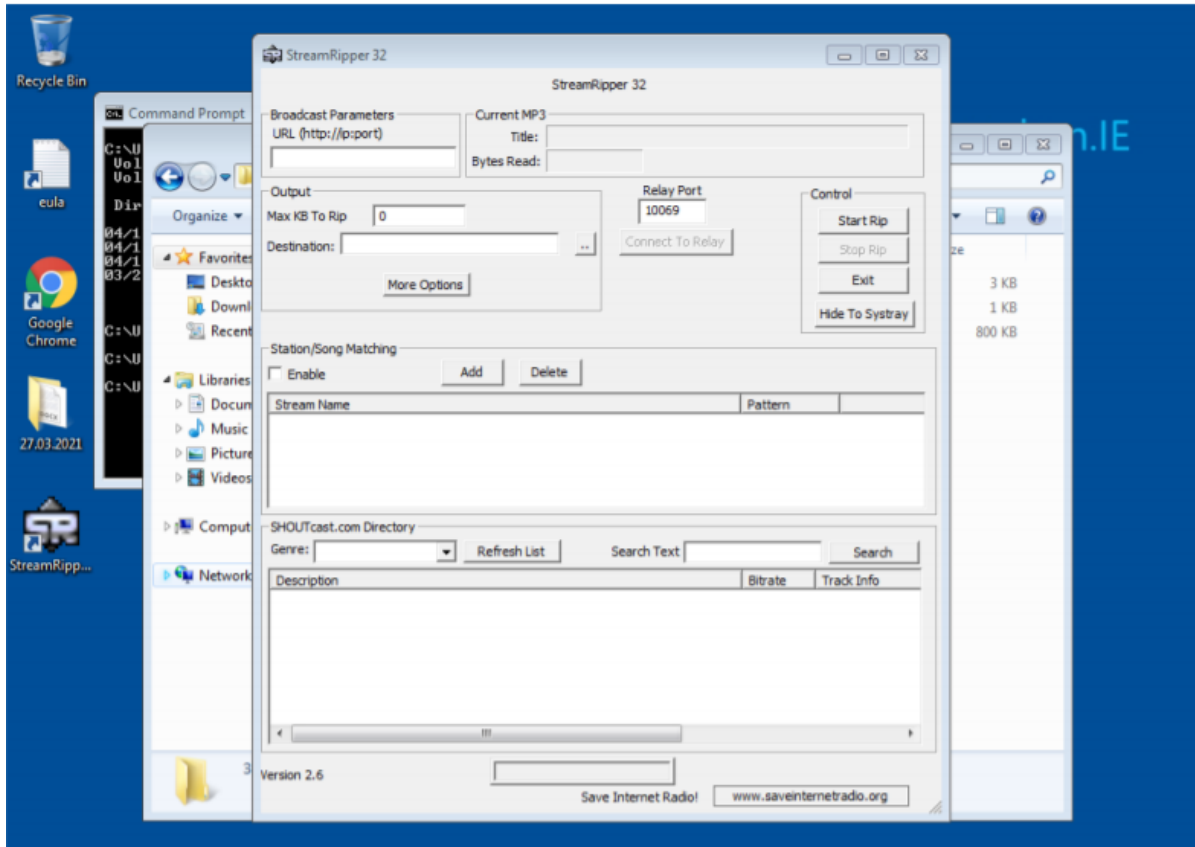
```
C:\Users\DeLL>cd C:\Users\DeLL\Desktop\Uulln
C:\Users\DeLL\Desktop\Uulln>python exploit.py
C:\Users\DeLL\Desktop\Uulln>SSS
```

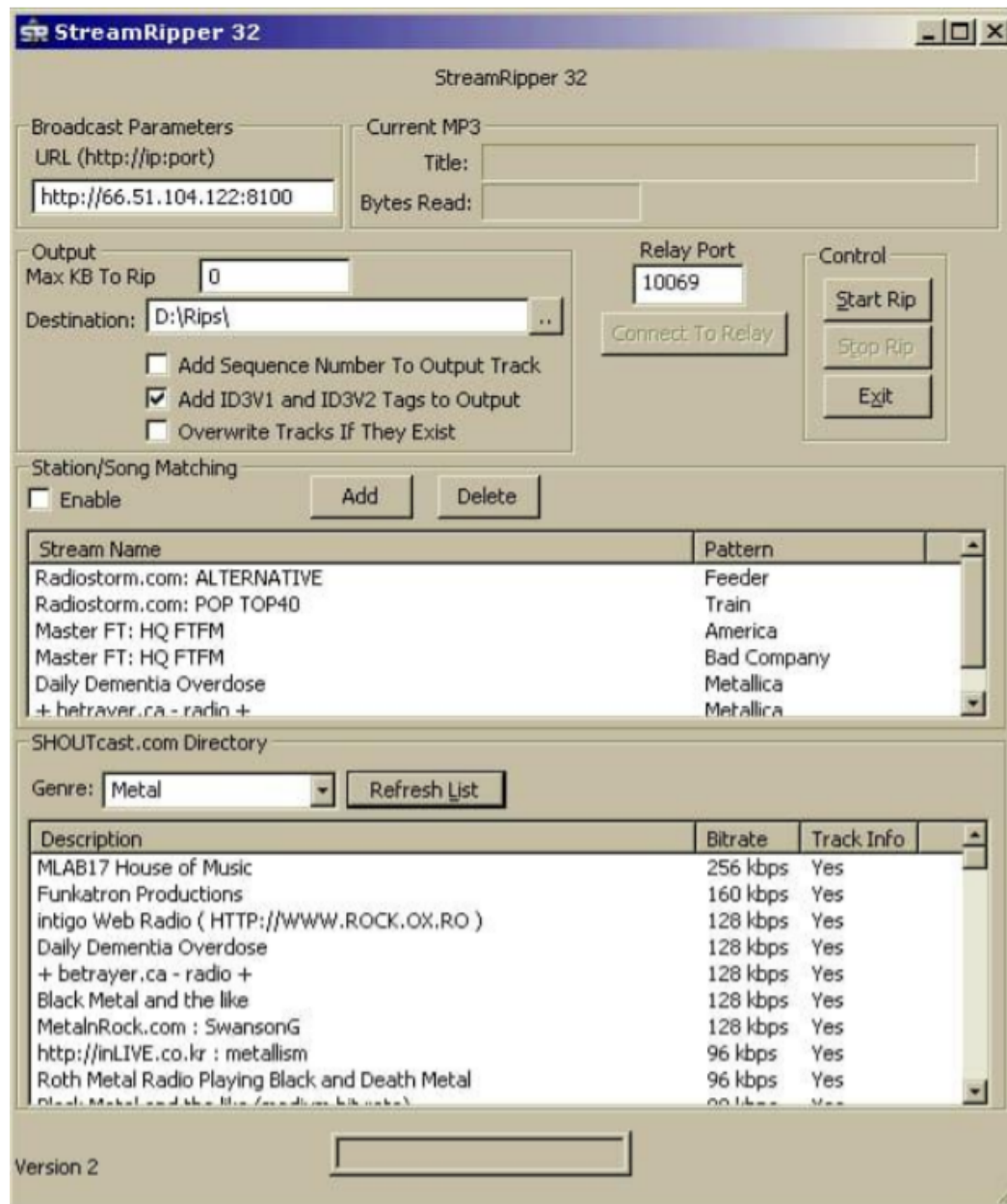
The background shows a file explorer window with the address bar set to "C:\Users\DeLL\Desktop\Uulln". The file explorer displays three items: "exploit.py", "Uulln", and "Uulln". The taskbar at the bottom shows the Start button and several open applications, including "exploit.py" and "Uulln".

exploit.txt - Notepad

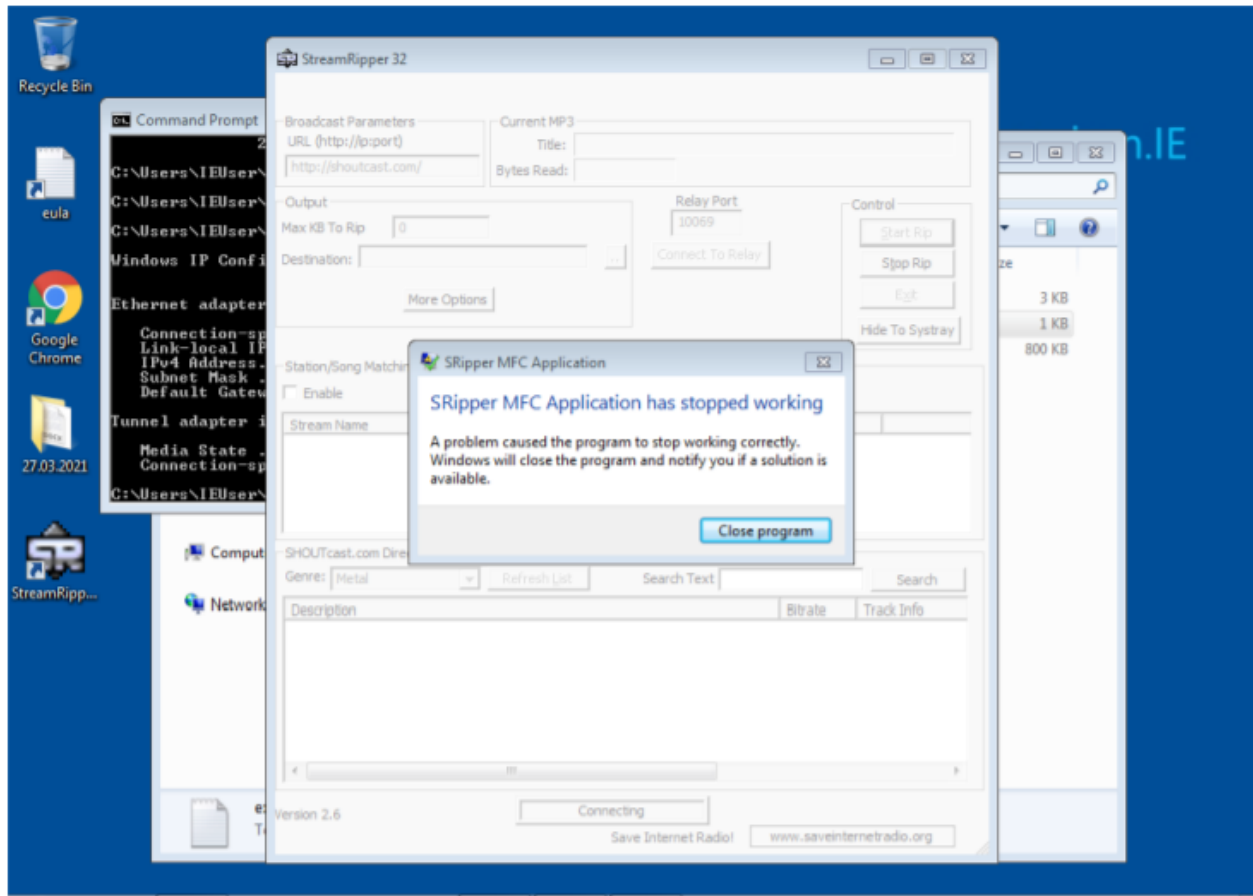
File Edit Format View Help

AA  
AA  
AAæðöZÜÇºİP  
SaÙt\$ò]3É±Rfıü1U»C±¿Æ·Ö?Mø\_Ú|ø~ /èOÿǺf WáŠĐLiíáyÍ4aü-Xİw×2•...  
v89òt‘²H˘ ‘ ¨ › ° ö Æ ü ± ~ ĩ á ¯ ° Œ š İ 0 ä J > , K³ Ž K • ô ) ´ à ♣ J I ó È Ø • v İ “ ^ + %² · . ) ¸ æ ~ ~ ª ª |—  
qÜ0%U‡ŸİmúâİİFFEä°úİt7᠑1@Å^%úAÓ6%-İm‘İēŽāİ  
(Ú²9™cY¹&᠑İéˆi`YiÚĜƒfİw%¬.İG‘KT6yŽZ9Áİ%SNİİÜÊämÆŽ®≡ăo`[fcİ«PÙ°´ôu^&“...)[♣  
Ò~·E᠑””ȳn@Çlμ±Łm8l},,İØ)XYg†3ÉqÉèfİEAİc‘İâ< ç³´o4Íóİ»İ°Ø^ÆİøÇE1...÷°³  
°{ØLGc1Iİ#≡#ÆİÄ





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



The program has crashed!!!