Name: DEVI JAGANNADH KOTHA

Reg no.: 18BCN7079

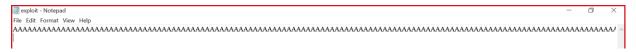
Slot: L39+40

Running the exploit2.py file to generate payload

>python2 exploit2.py

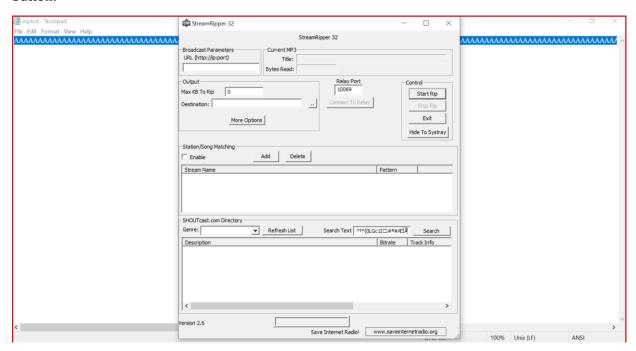
After successfully running the python file it will generate a .txt file along with the payload.

>notepad exploit2.txt

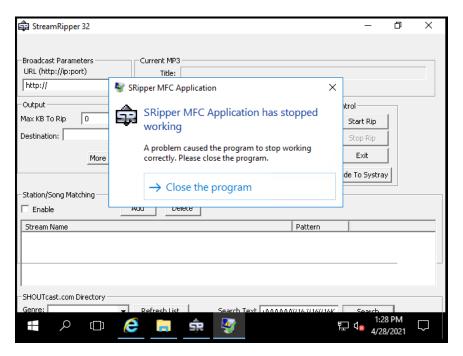


Now, install Vulnerable application (StreamRipper32).

After installing the application copy paste the payload in the search box and click on Search button.



By exploiting buffer overflow vulnerability we have crashed the application.



Trying to erase hdd

```
C:\WINDOWS\system32>diskpart
Microsoft DiskPart version 10.0.19041.964
Copyright (C) Microsoft Corporation.
On computer: DESKTOP-U6VV86T
DISKPART>
DISKPART> list disk
 Disk ###
                           Size
            Status
                                     Free
                                              Dyn
                                                   Gpt
            Online
                            476 GB
 Disk 0
                                         0 B
DISKPART> select disk 0
Disk 0 is now the selected disk.
DISKPART> clean
```