CSE-2010

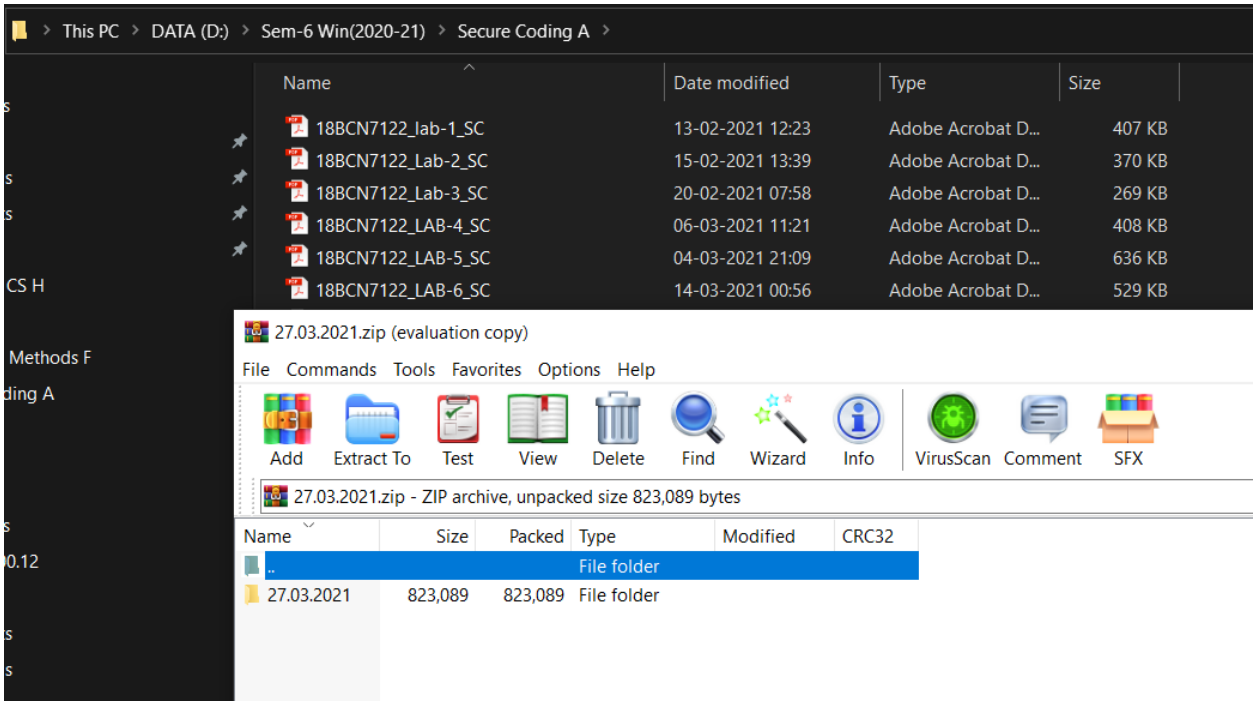
Secure Coding(L23 + L24)

Lab - 7

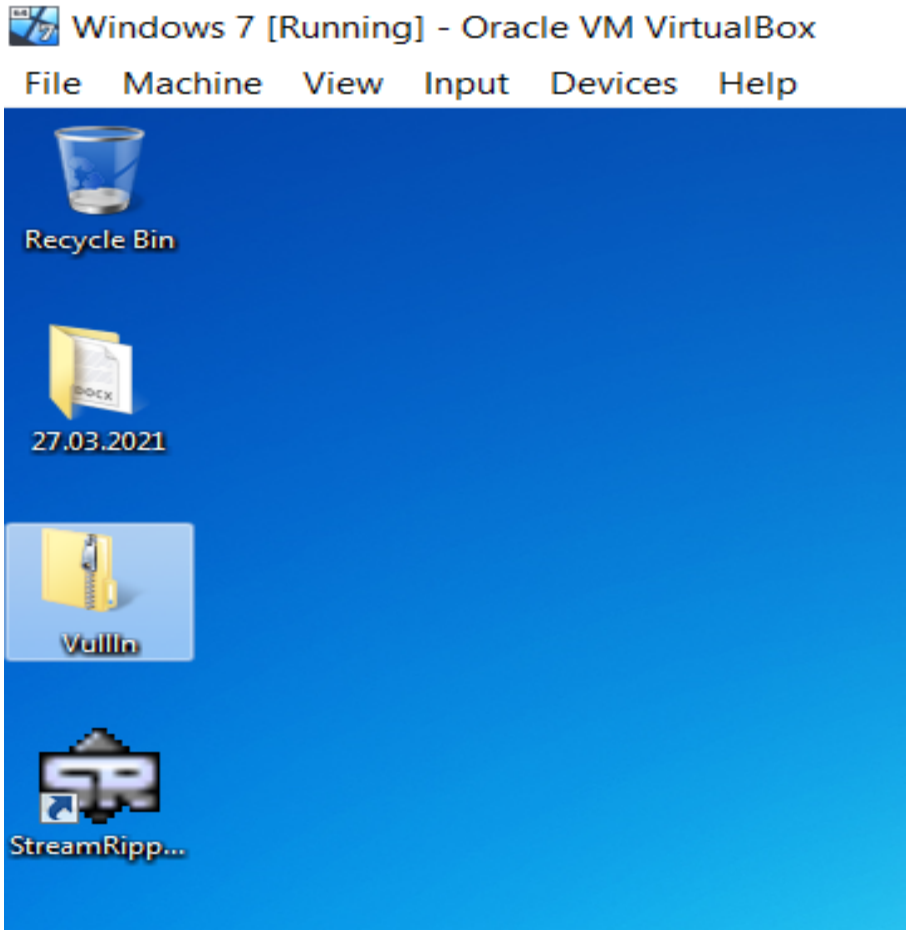
Name :- MD Shafiq Ahmed

Reg no :- 18BCN7122

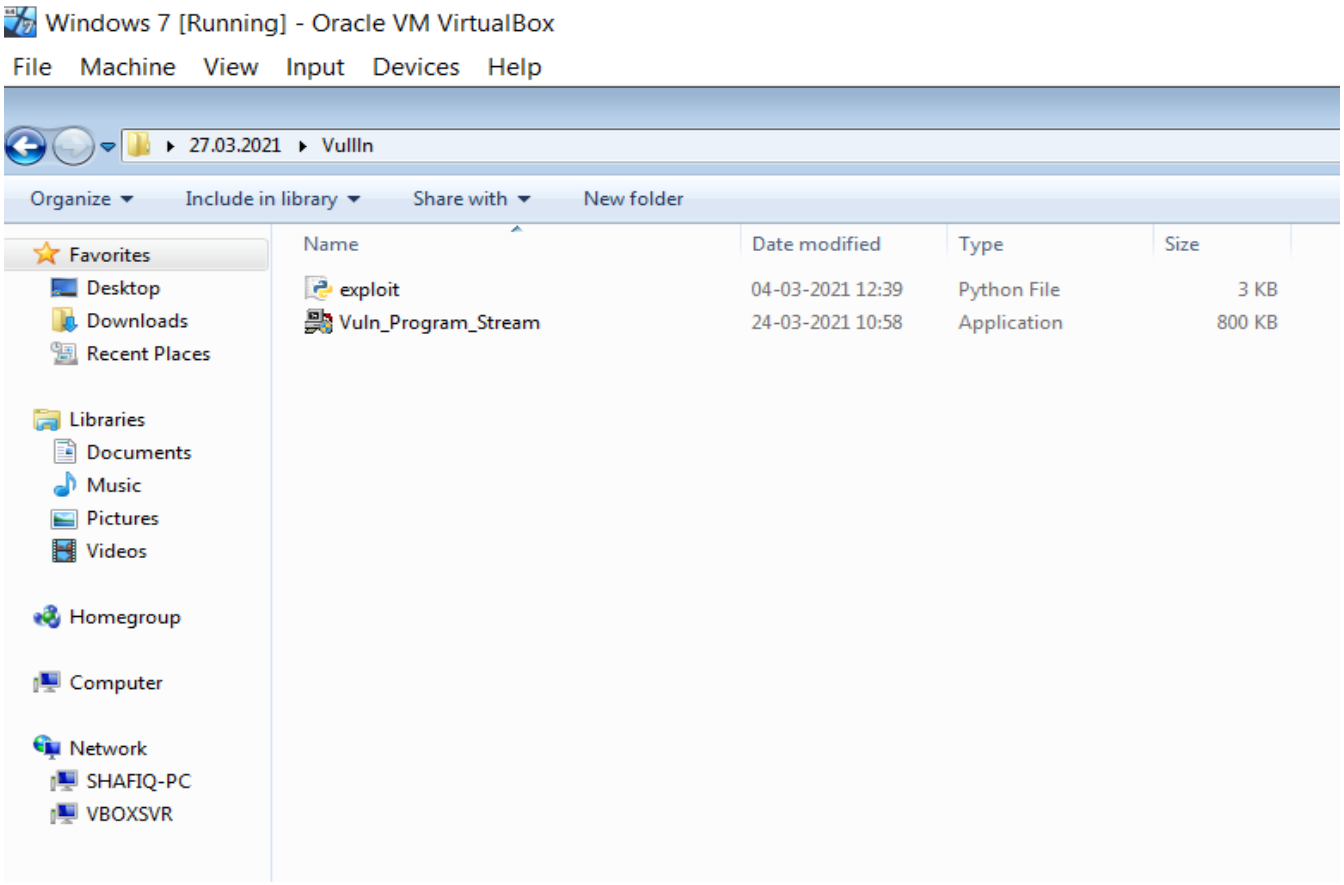
- **Download Vulln.zip from teams.**



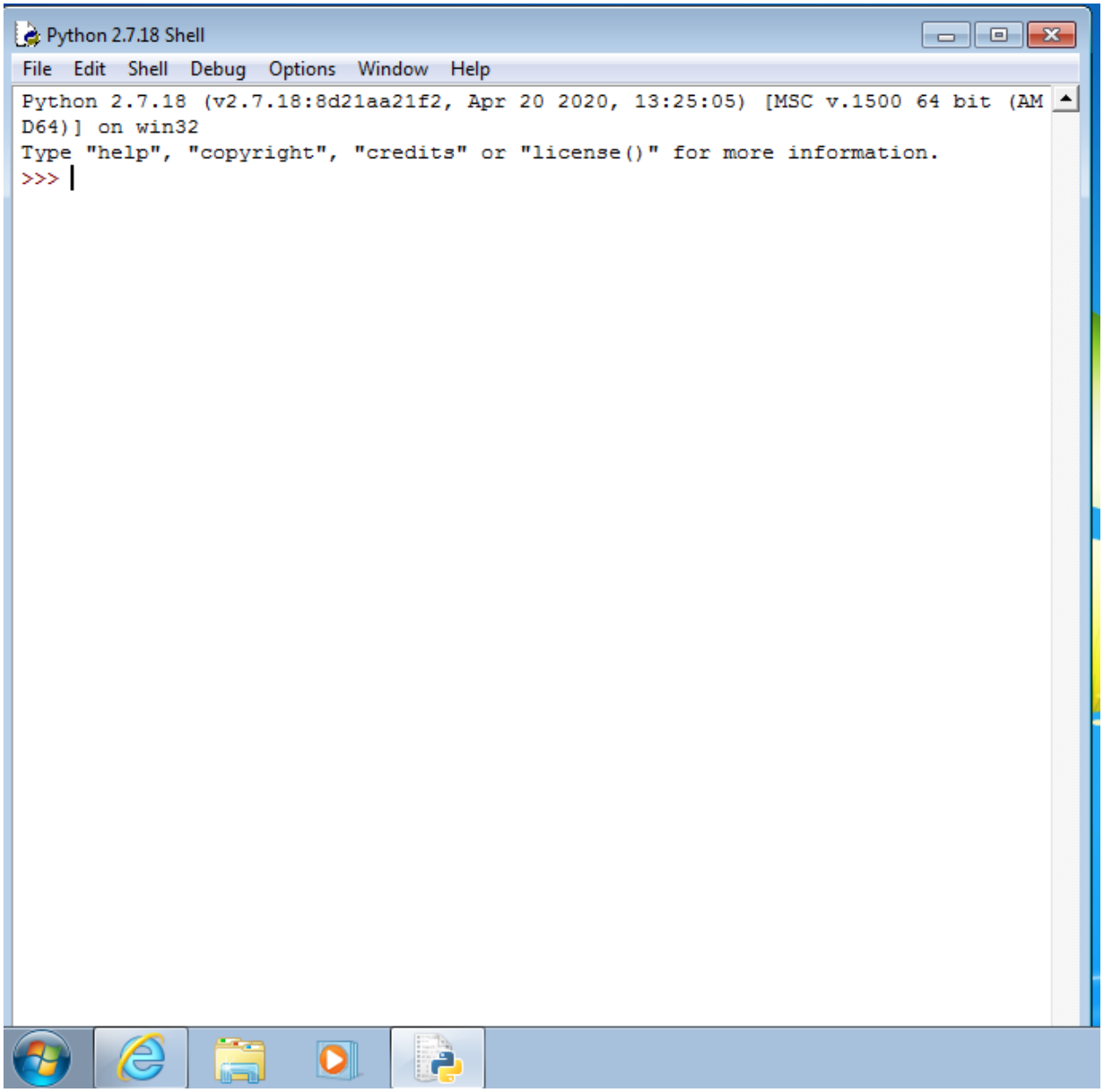
- **Deploy a virtual windows 7 instance and copy the Vulln.zip into it.**



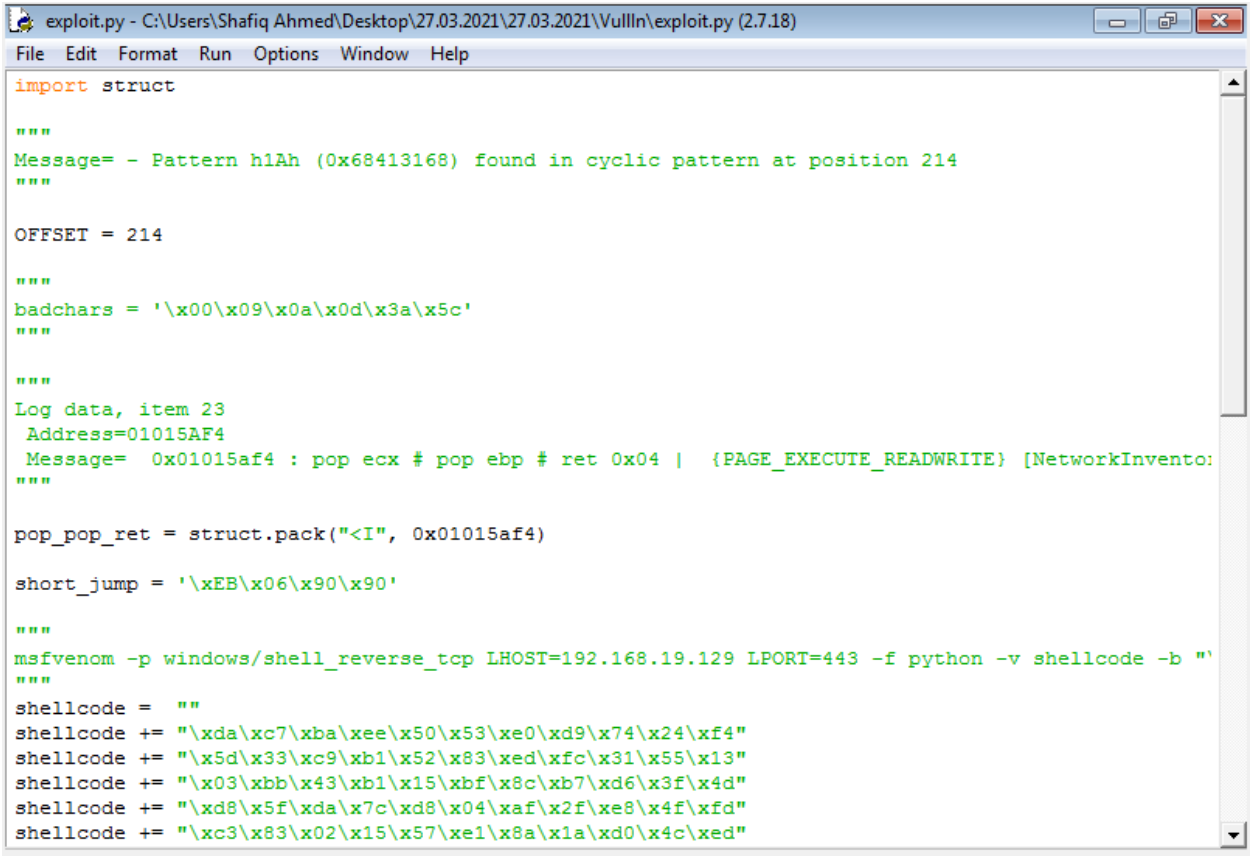
- **Unzip the zip file. You will find two files named exploit.py and Vuln_Program_Stream.exe**



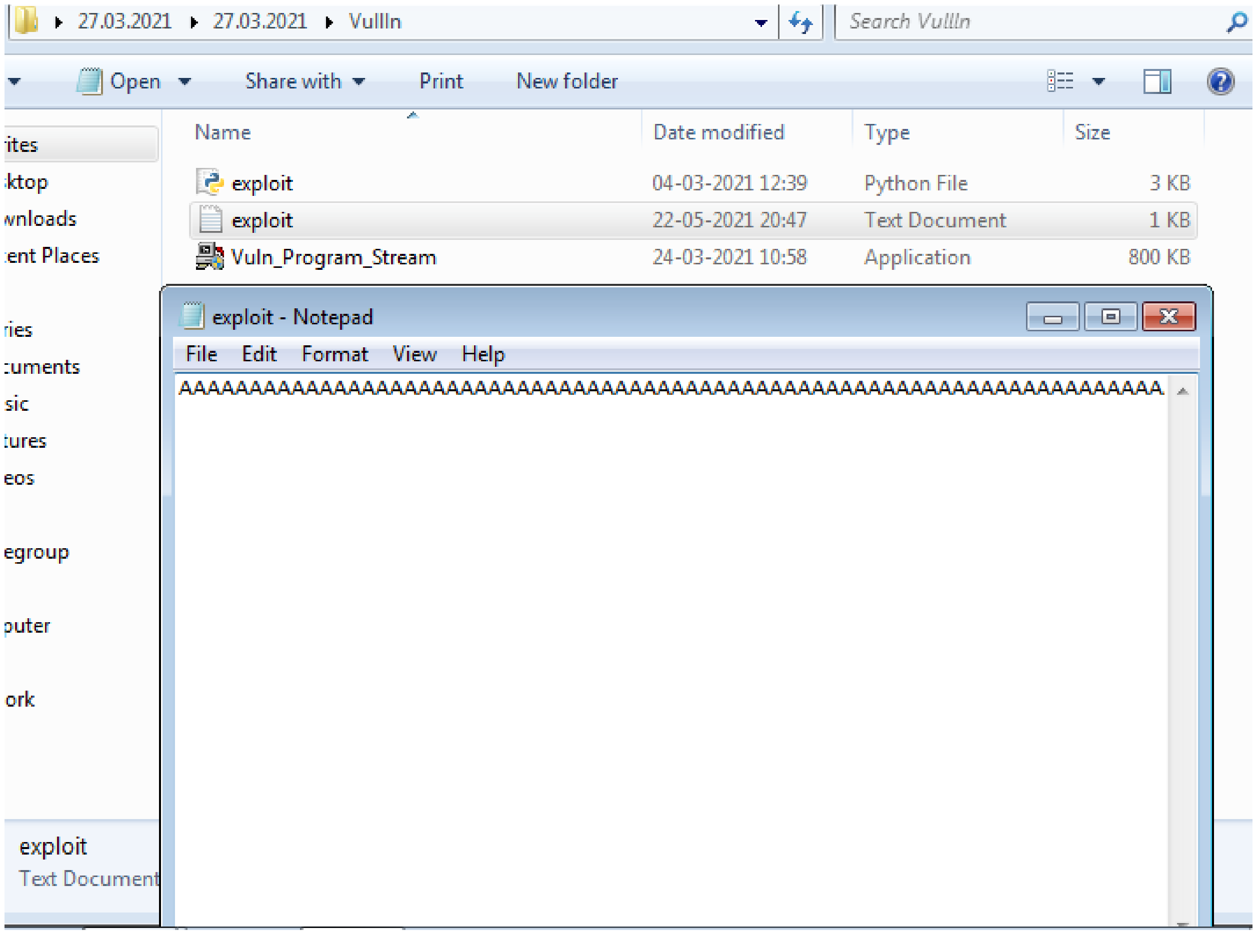
- **Download and install python 2.7.* or 3.5.***



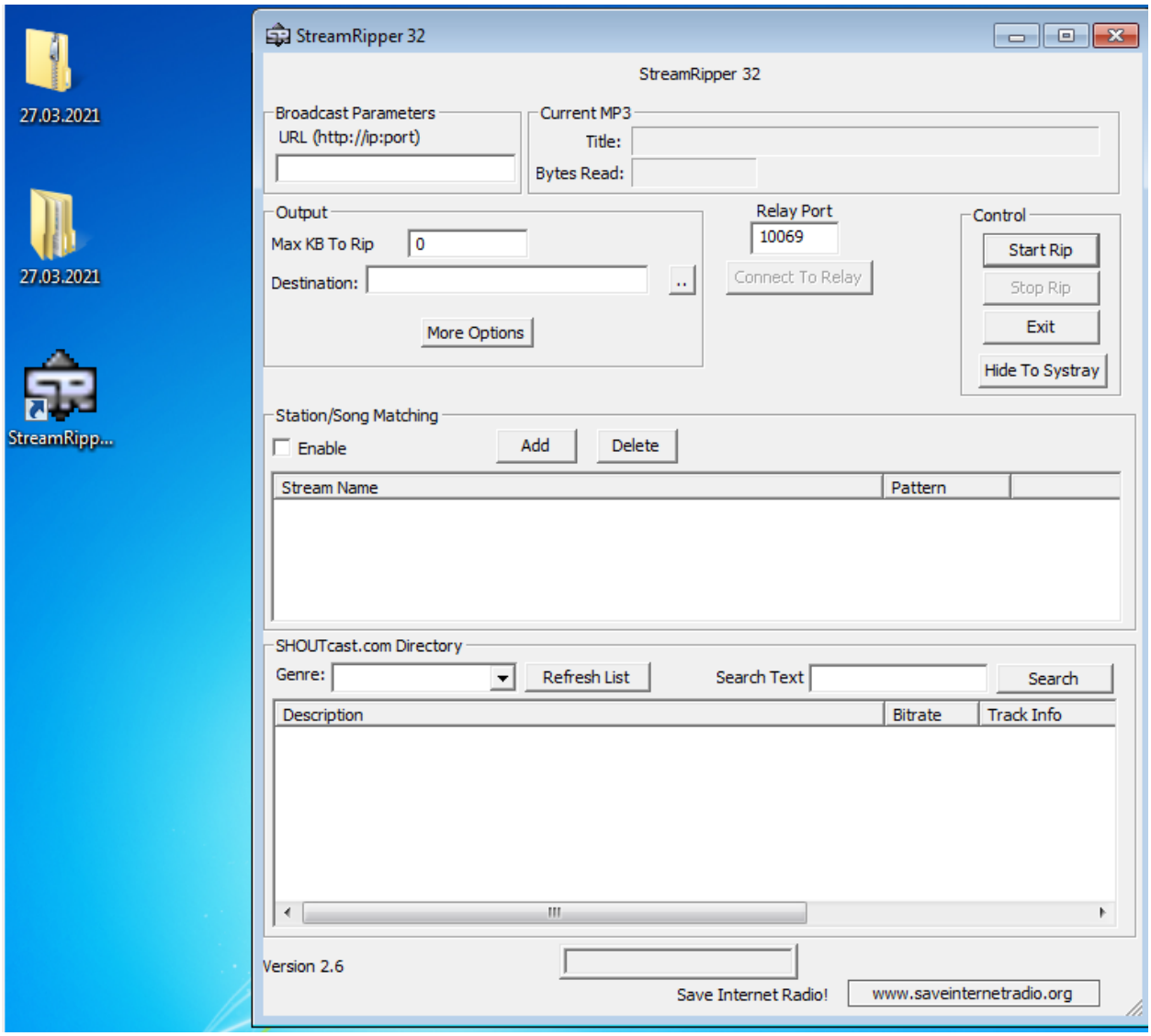
- **Run the exploit script to generate the payload**



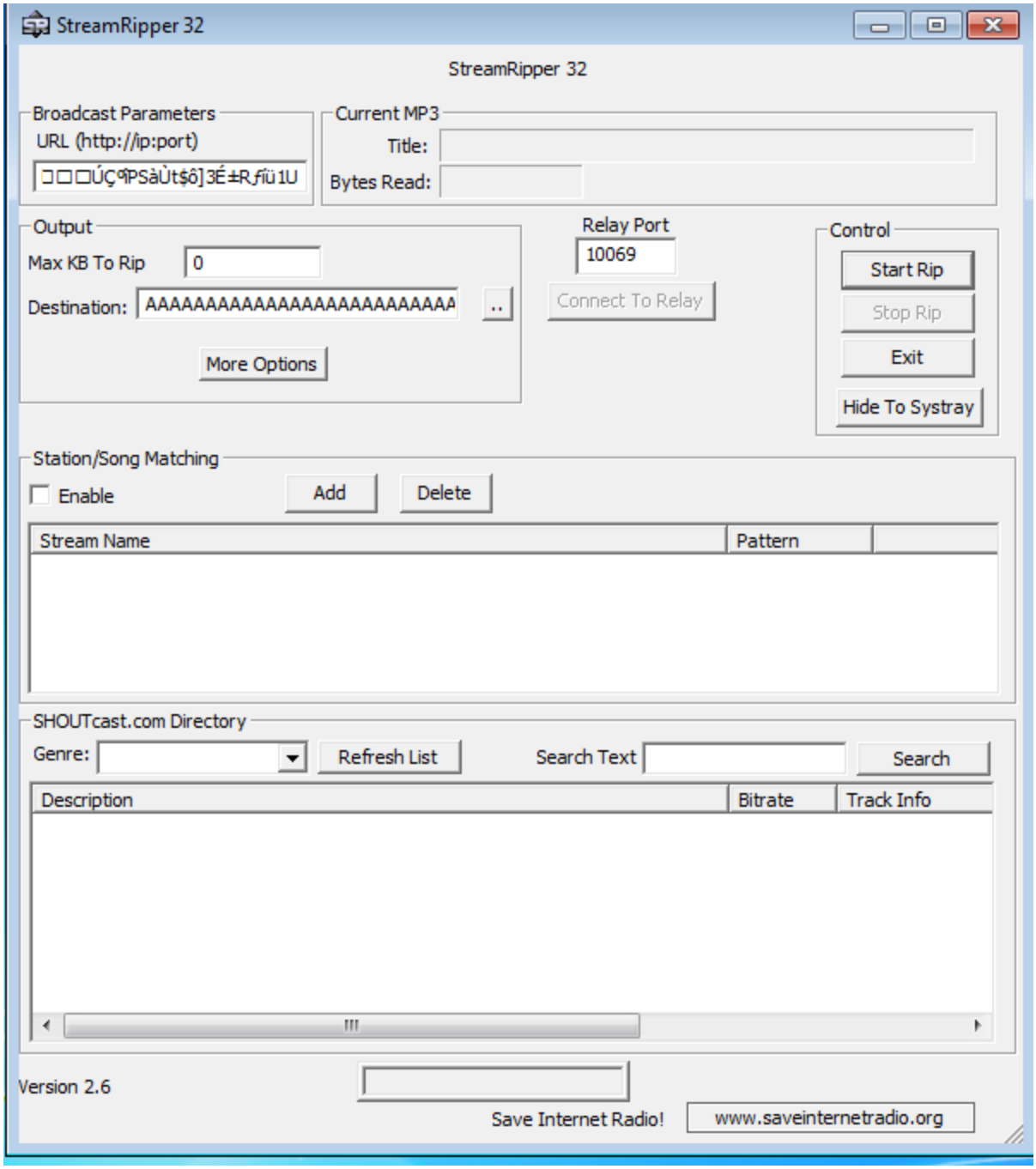
- **Generate the payload by executing exploit.py**



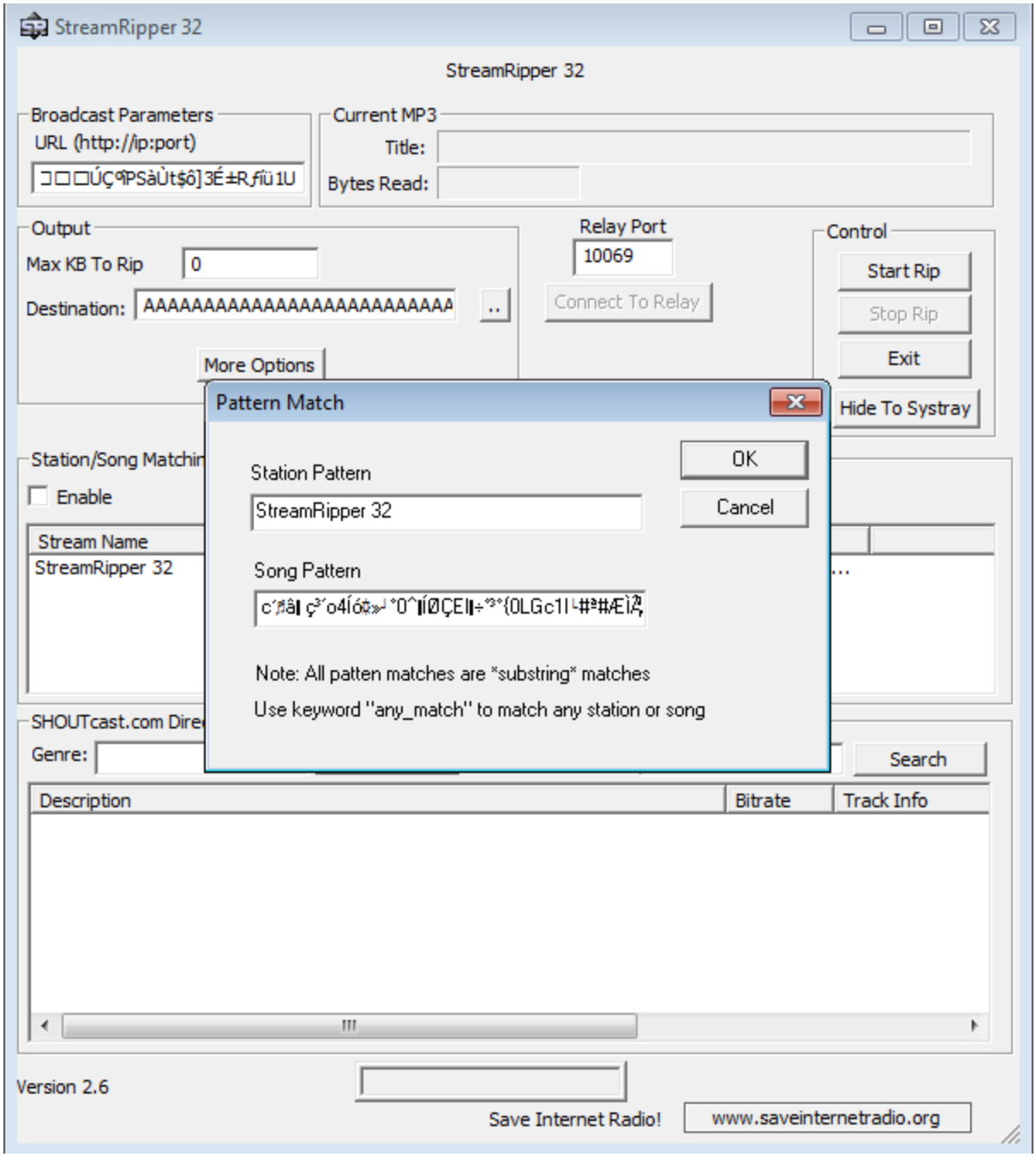
- **Install Vuln_Program_Stream.exe and Run the same**

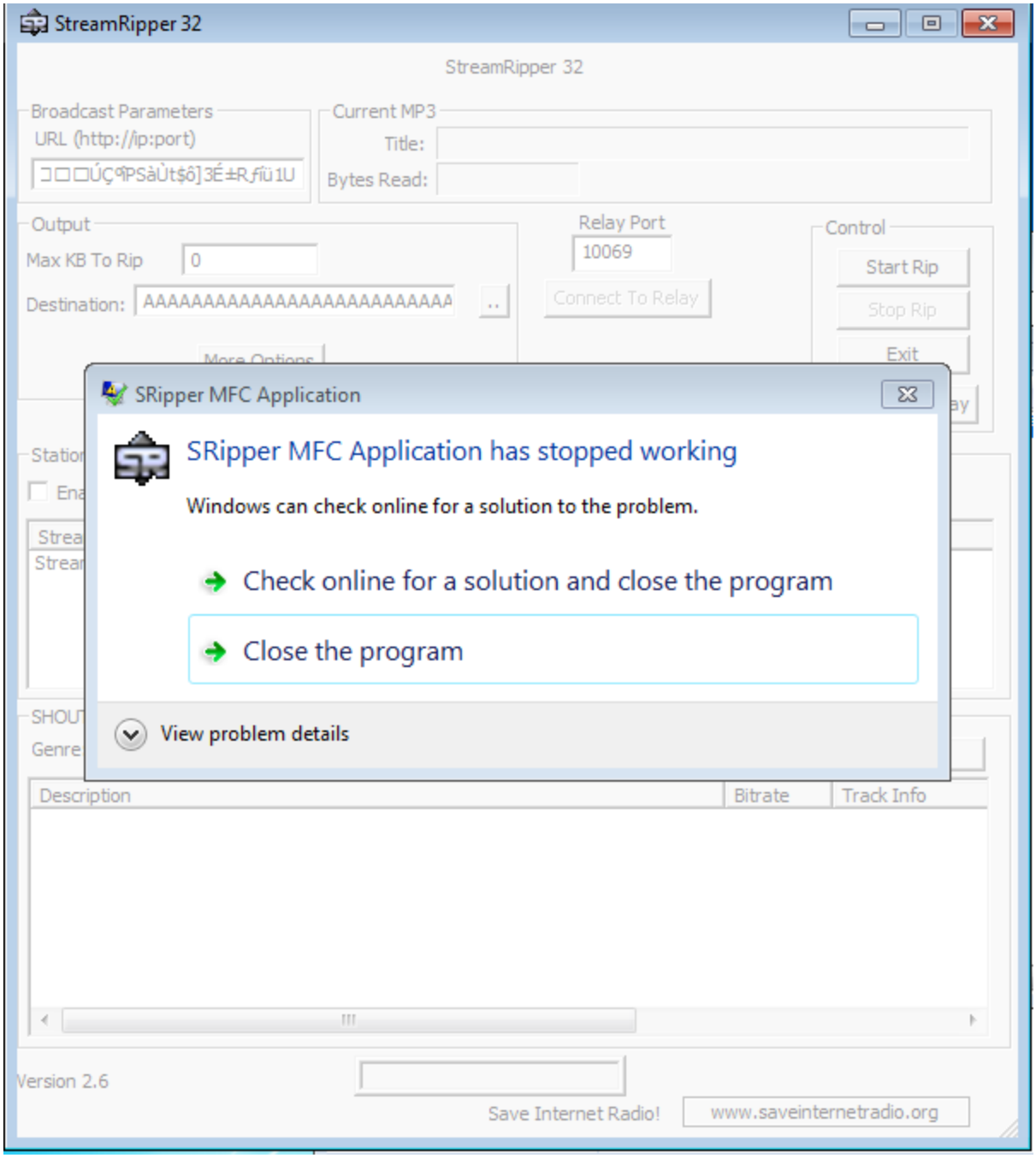


- **Testing for vulnerability by copy pasting generated payloads in different fields.**



- **Vulnerability found by generating payload at the pattern match field**


StreamRipper 32
StreamRipper 32
Broadcast Parameters
URL (http://ip:port)
Current MP3
Title:
Bytes Read:
Output
Max KB To Rip
0
Destination:
Relay Port
10069
Connect To Relay
Control
Start Rip
Stop Rip
Exit
Hide To Systray
More Options
Pattern Match
OK
Cancel
Station Pattern
StreamRipper 32
Song Pattern
Note: All patten matches are *substring* matches
Use keyword "any_match" to match any station or song
Station/Song Matchin
Enable
Stream Name
StreamRipper 32
SHOUTcast.com Dire
Genre:
Search
Description
Bitrate
Track Info
Version 2.6
Save Internet Radio!
www.saveinternetradio.org


StreamRipper 32
StreamRipper 32
Broadcast Parameters
URL (http://ip:port)
Current MP3
Title:
Bytes Read:
Output
Max KB To Rip
0
Destination:
Relay Port
10069
Connect To Relay
Control
Start Rip
Stop Rip
Exit
SRipper MFC Application
SRipper MFC Application has stopped working
Windows can check online for a solution to the problem.
Check online for a solution and close the program
Close the program
View problem details
Description
Bitrate
Track Info
Version 2.6
Save Internet Radio!
www.saveinternetradio.org