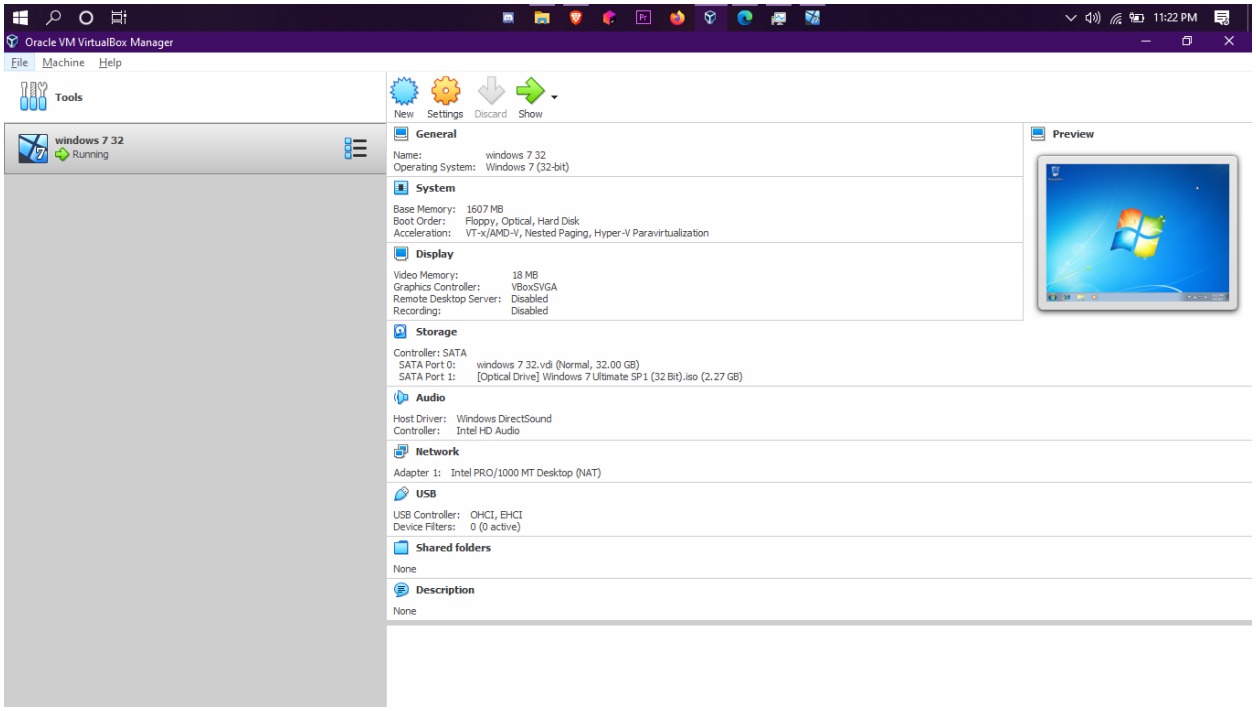
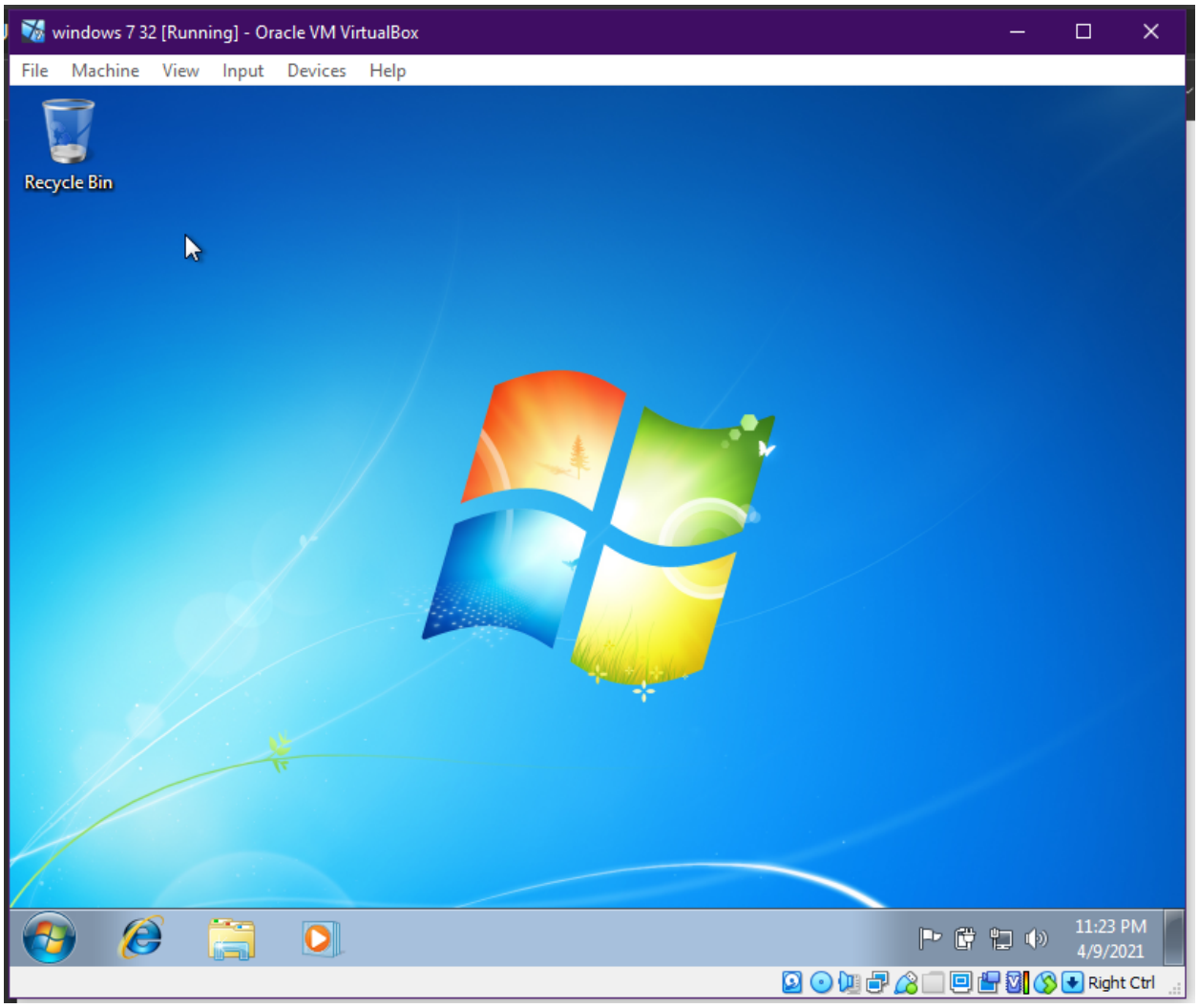
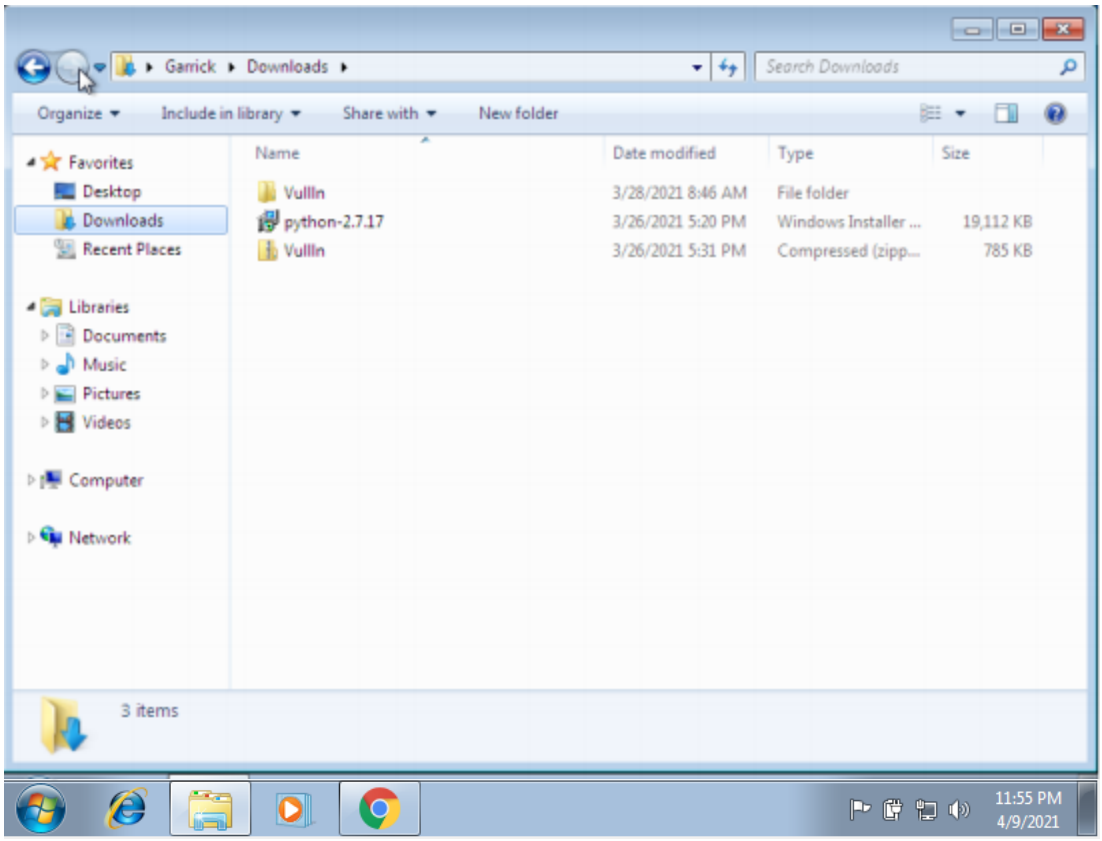
NAME: A KRISHNA AKHIL
REG NO: 18BCE7076
SECURE CODING LAB L39+L40
Guided By: Prof. Sibi Chakravarthy

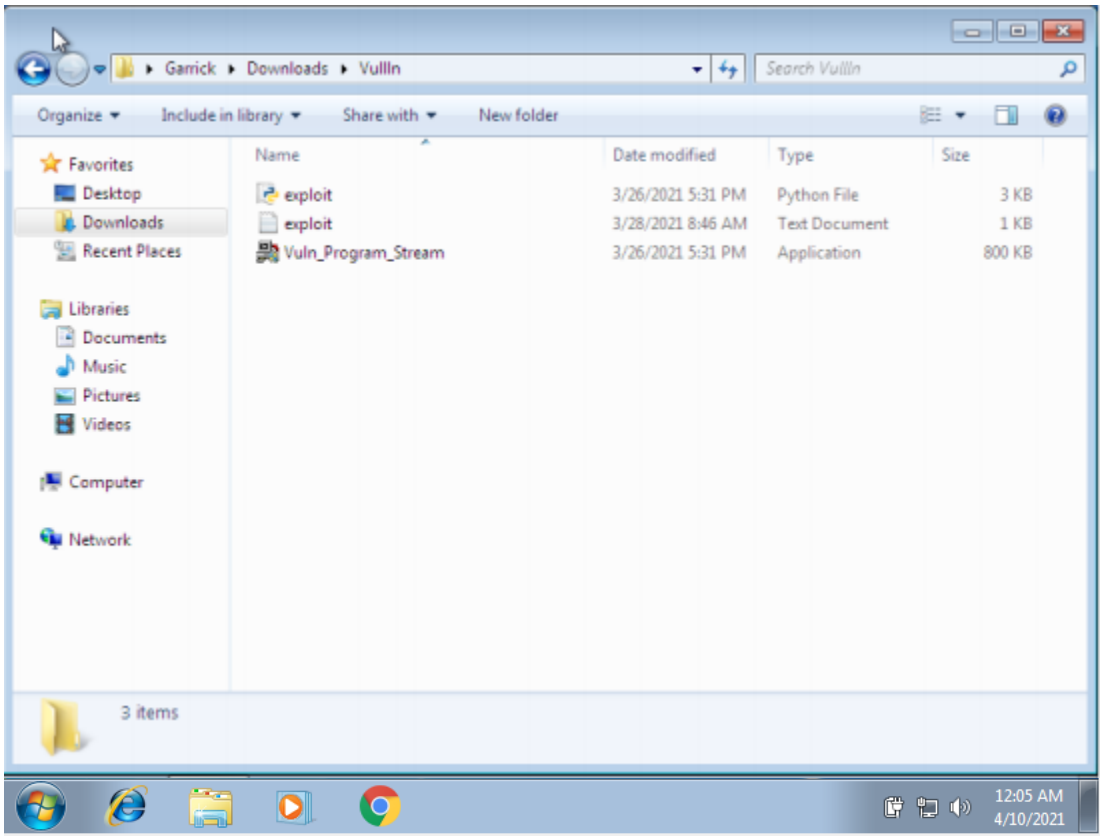
Install Windows 7 on VM:



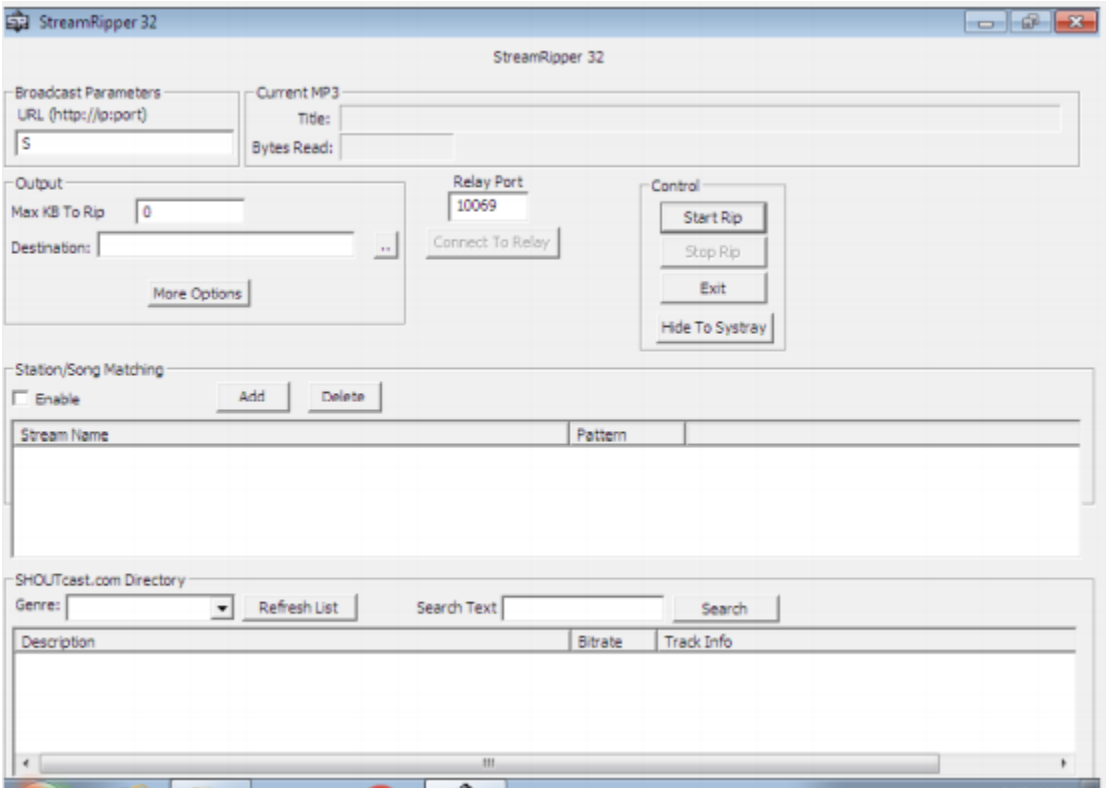


Extracting the zip file

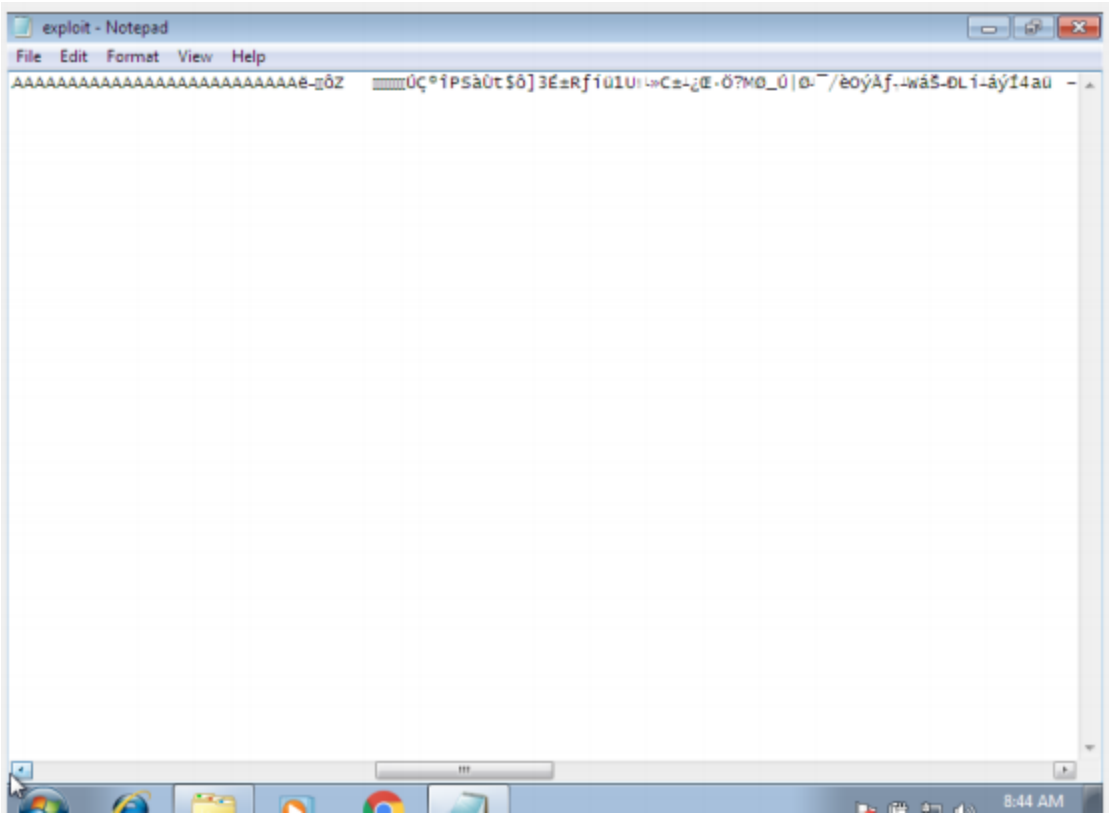

Garrick ▸ Downloads ▸
Search Downloads
Organize
Include in library
Share with
New folder
Favorites
Desktop
Downloads
Recent Places
Libraries
Documents
Music
Pictures
Videos
Computer
Network
Name
Date modified
Type
Size
VulIIn
3/28/2021 8:46 AM
File folder
python-2.7.17
3/26/2021 5:20 PM
Windows Installer ...
19,112 KB
VulIIn
3/26/2021 5:31 PM
Compressed (zipp...
785 KB
3 items
11:55 PM
4/9/2021



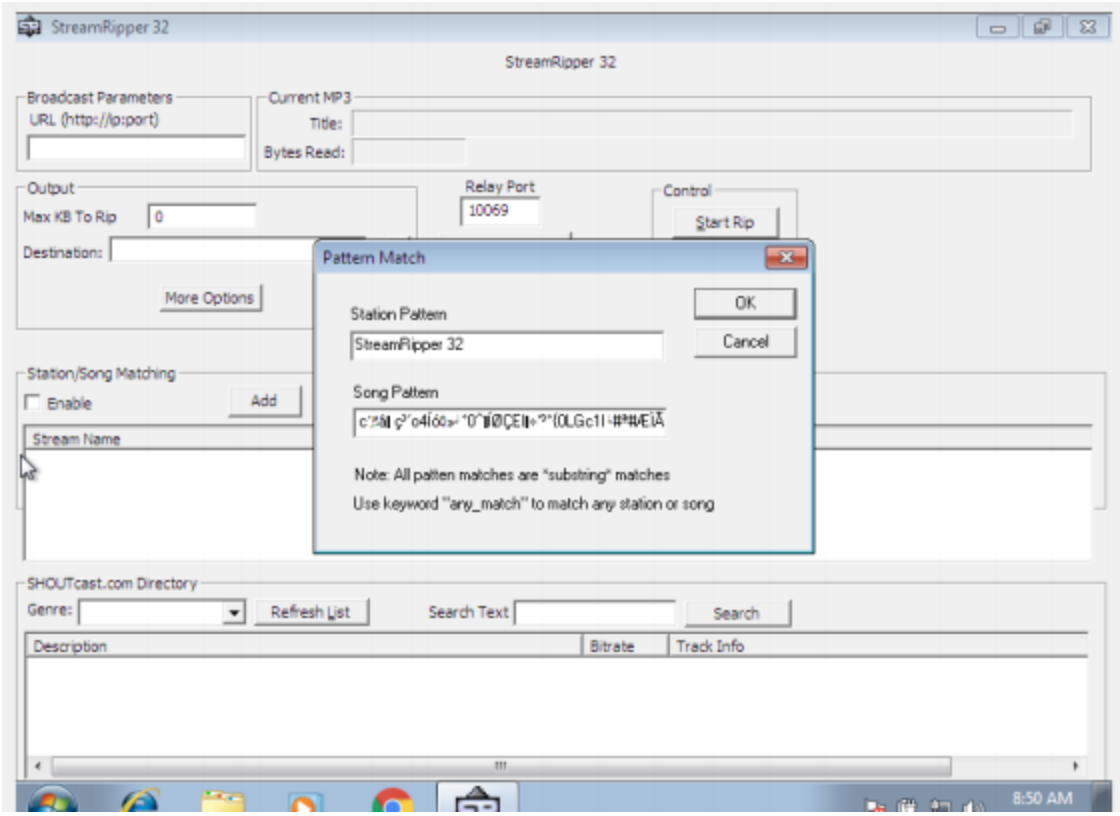
The Application we are trying to find a vulnerability is called StreamRipper32:



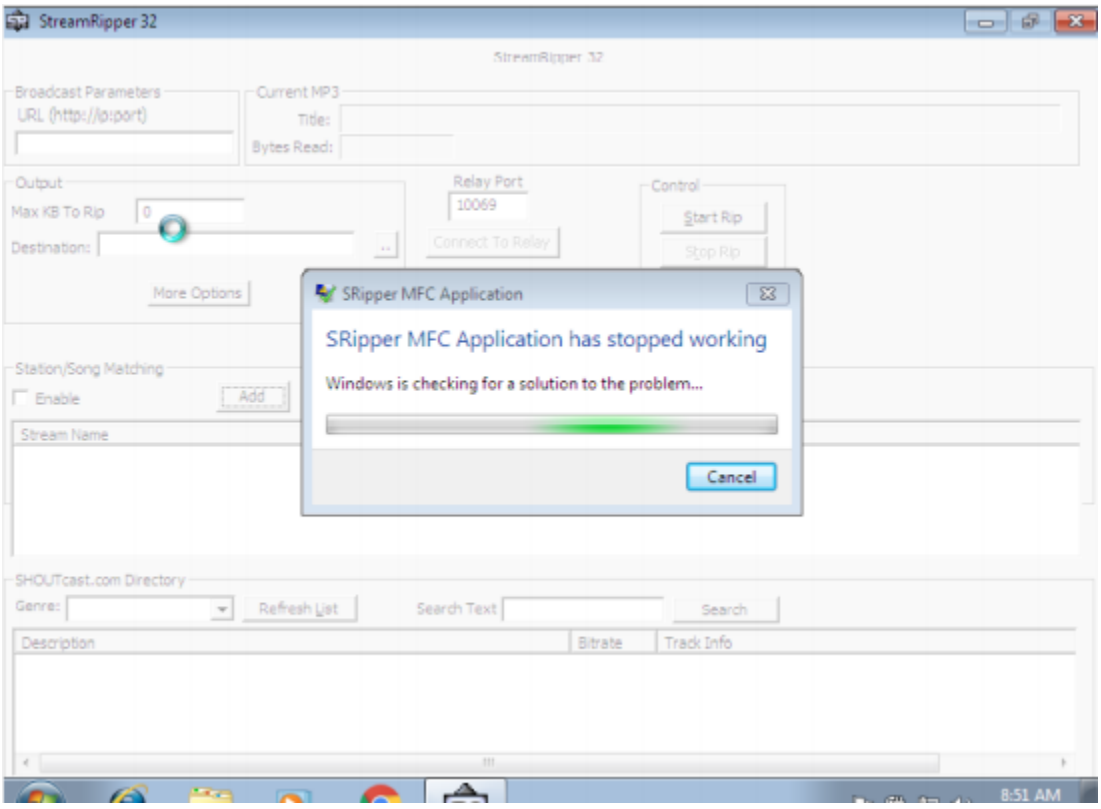
After executing the python file, we get a new exploit.exe file which has the required payload for the exploit:



Copy Paste the payload onto the Station/Song matching, Add:



And the Application crashes:



Why the Application crashes:

So when the input in that text field exceeds 256 characters, Buffer Overflow happens and that causes the application to crash, because it is not being handled properly. This vulnerability can be easily fixed by limiting the number of characters that specific field takes or just taking the first 256 characters from that field