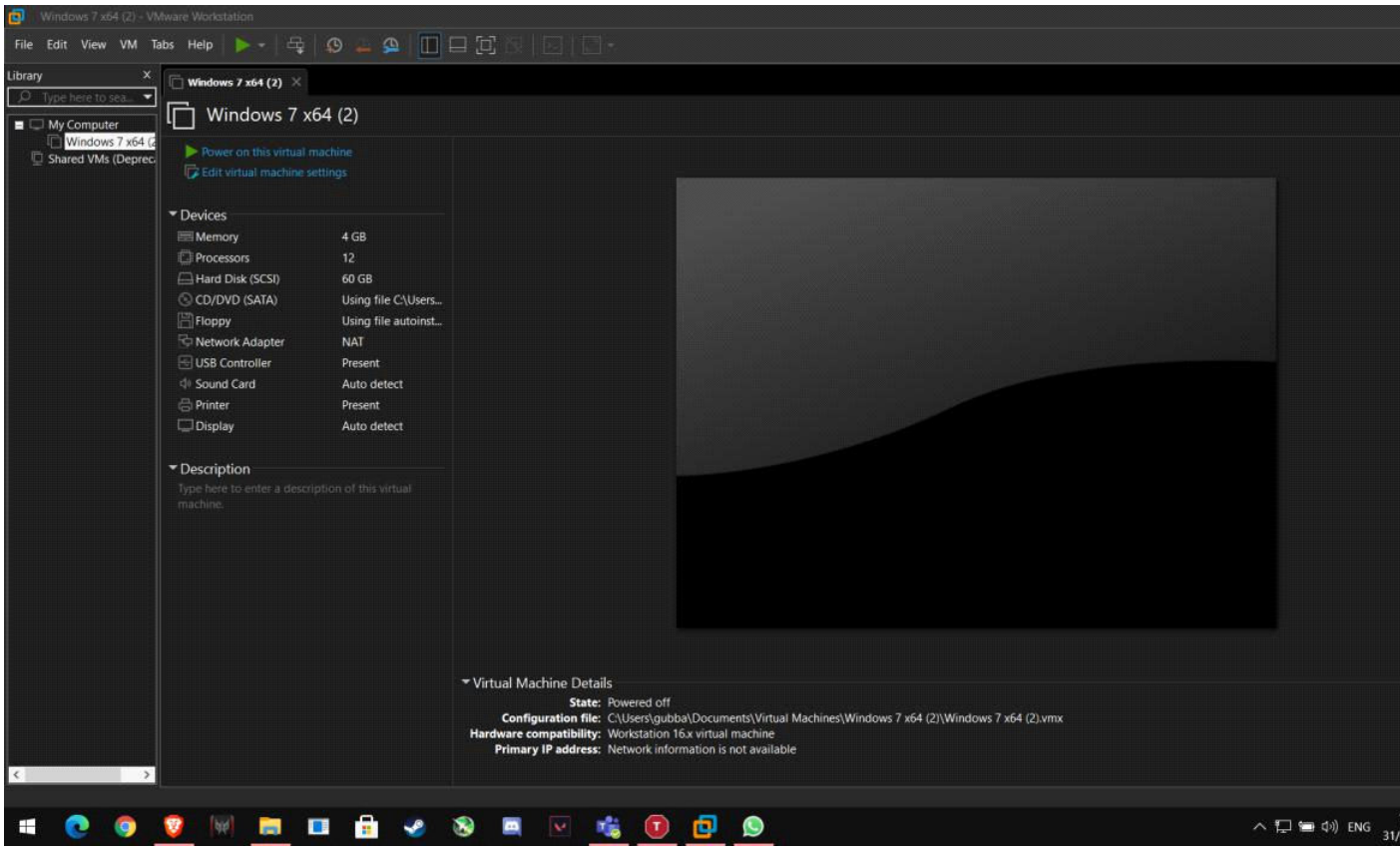
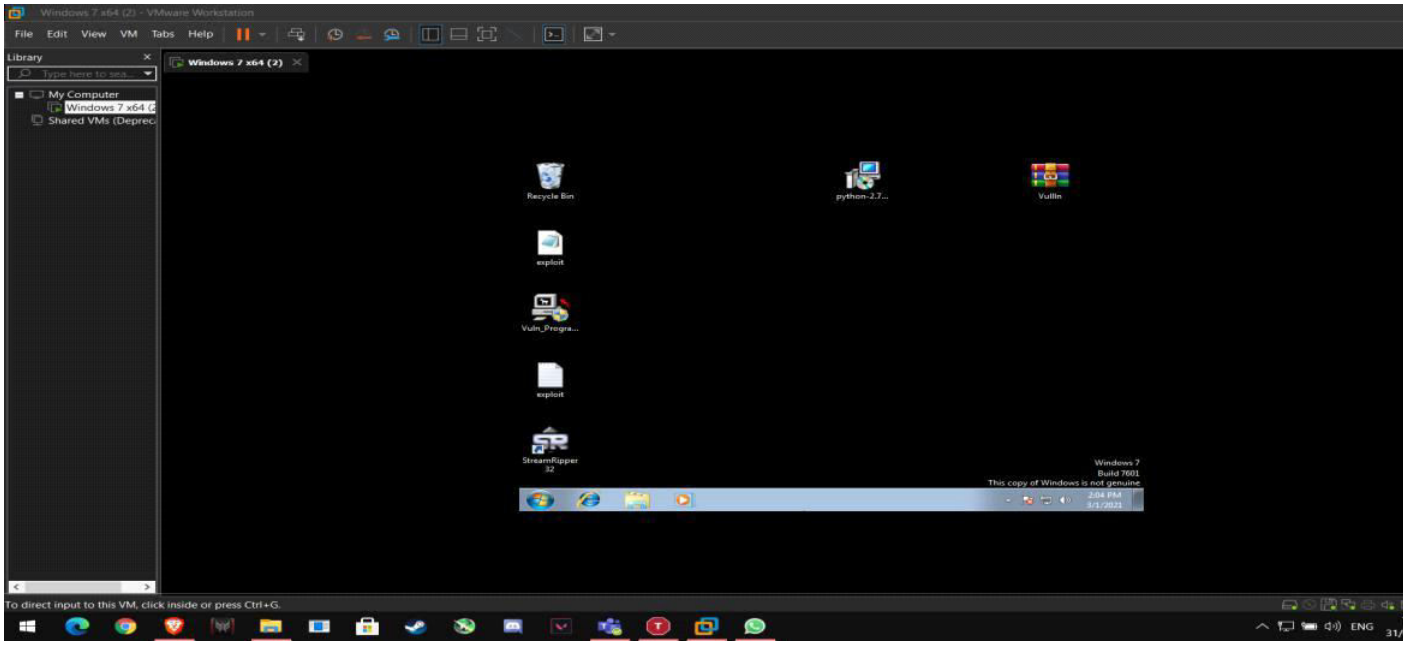
Lab – 7

Navya K
18bcn7048
L39+L40

Install windows 7 on a VM:

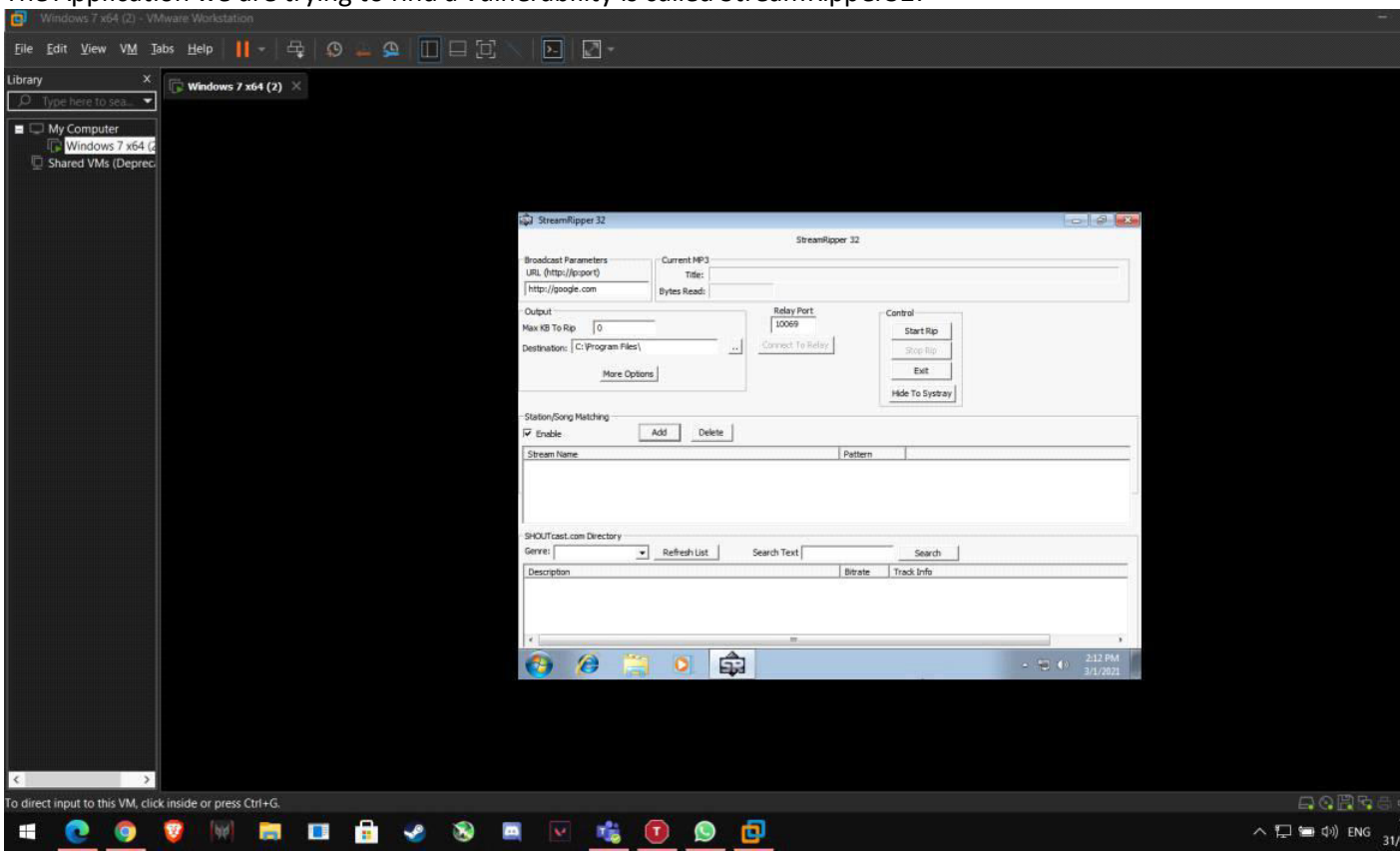


Extract the Zip file to get the application executable and a python file:

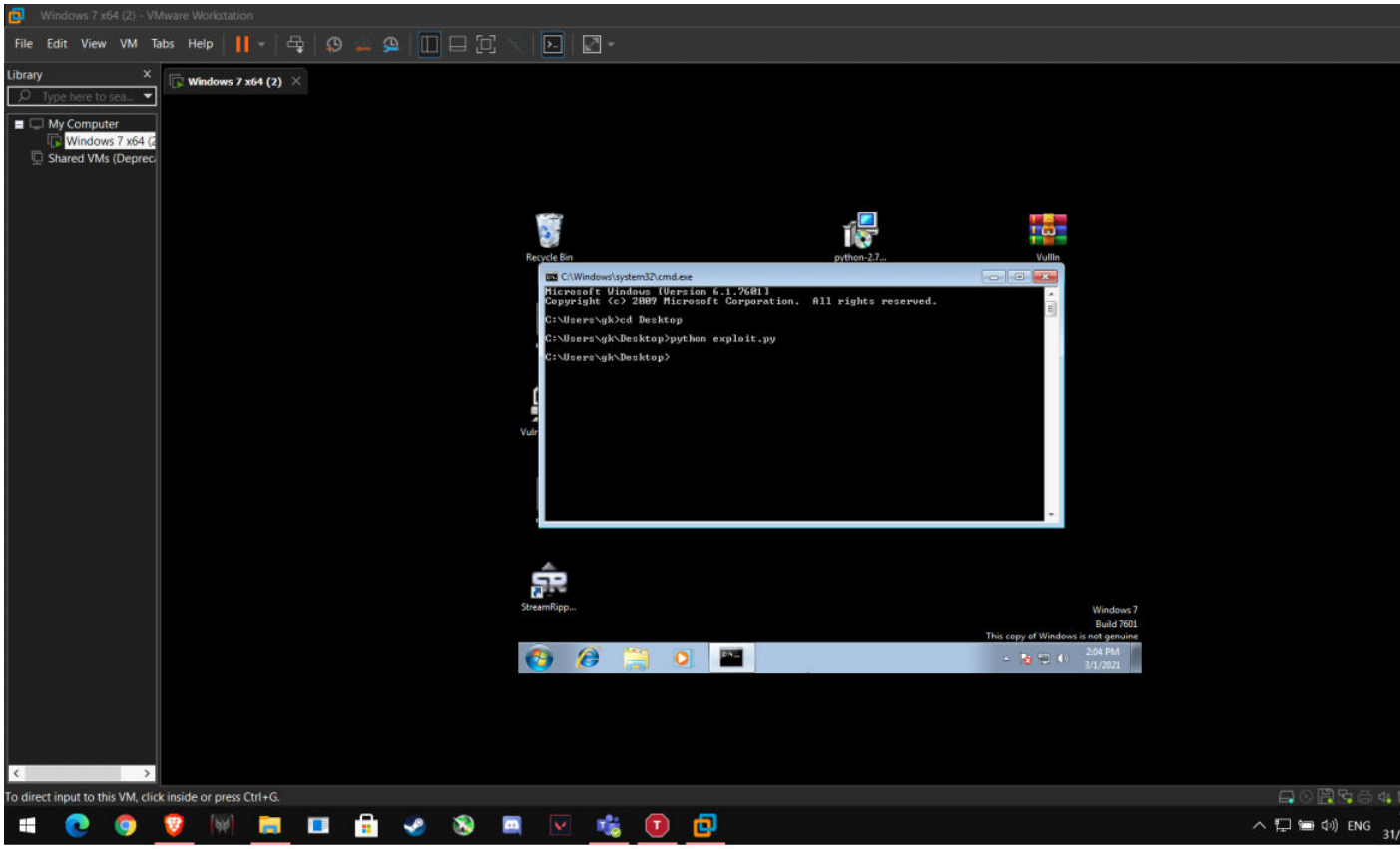


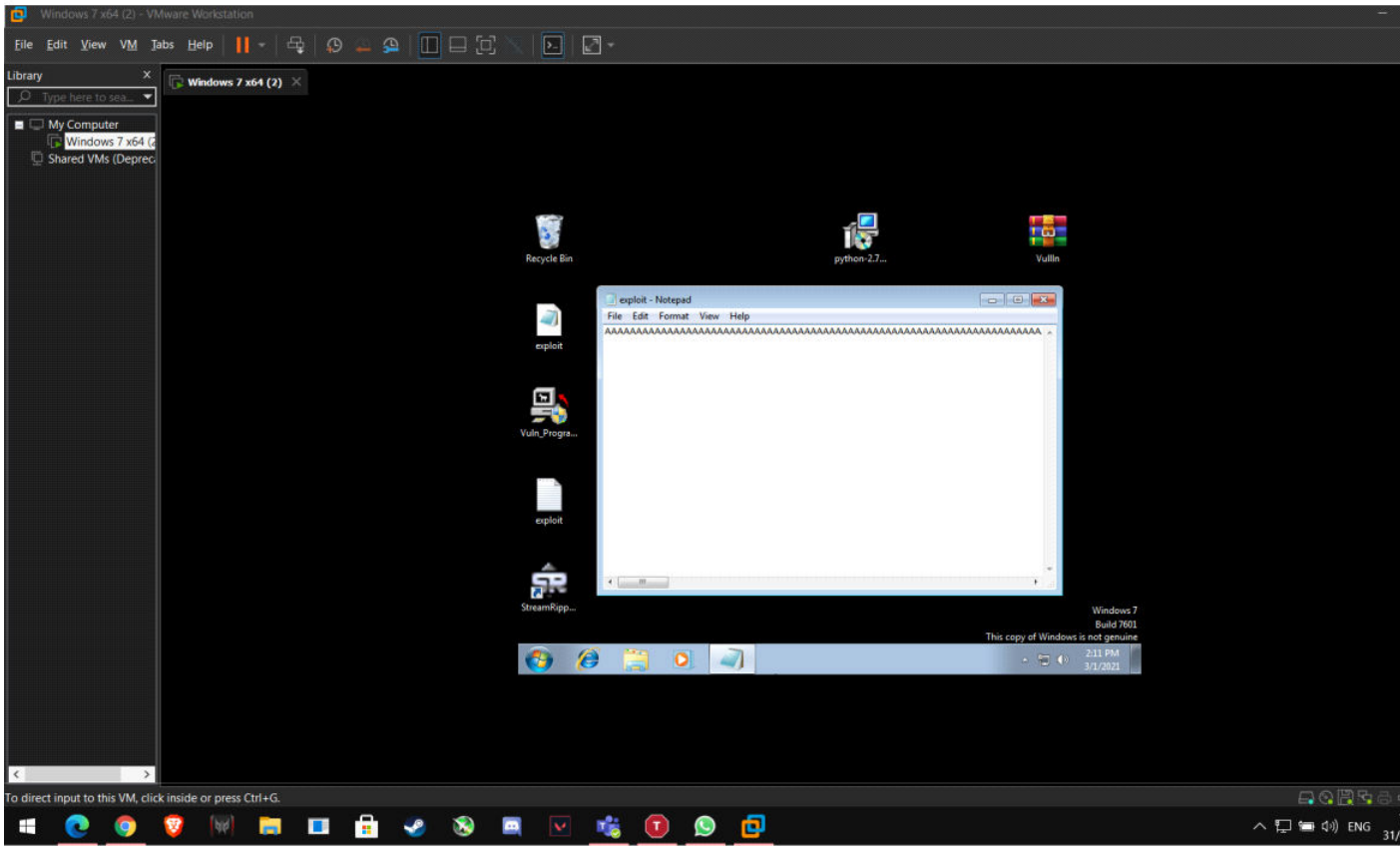
Since this is a new introduction of windows 7 and in light of the fact that official help for windows 7 finished a while prior, we needed to introduce python 2.7.17 and Chrome to download the documents and to execute the py record.

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

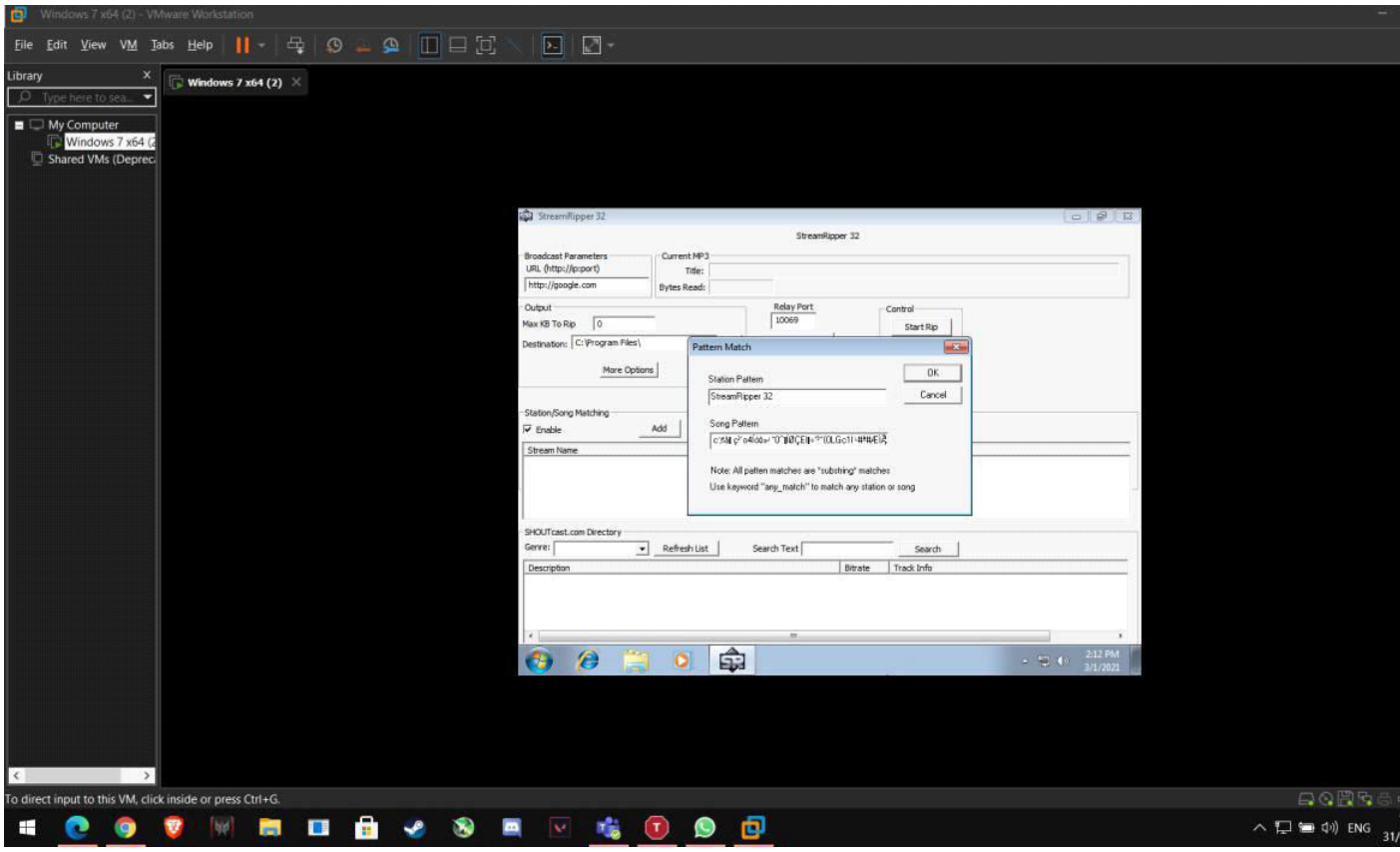


After executing the python file, we get a new exploit.exe file which has the required payload for the exploit:

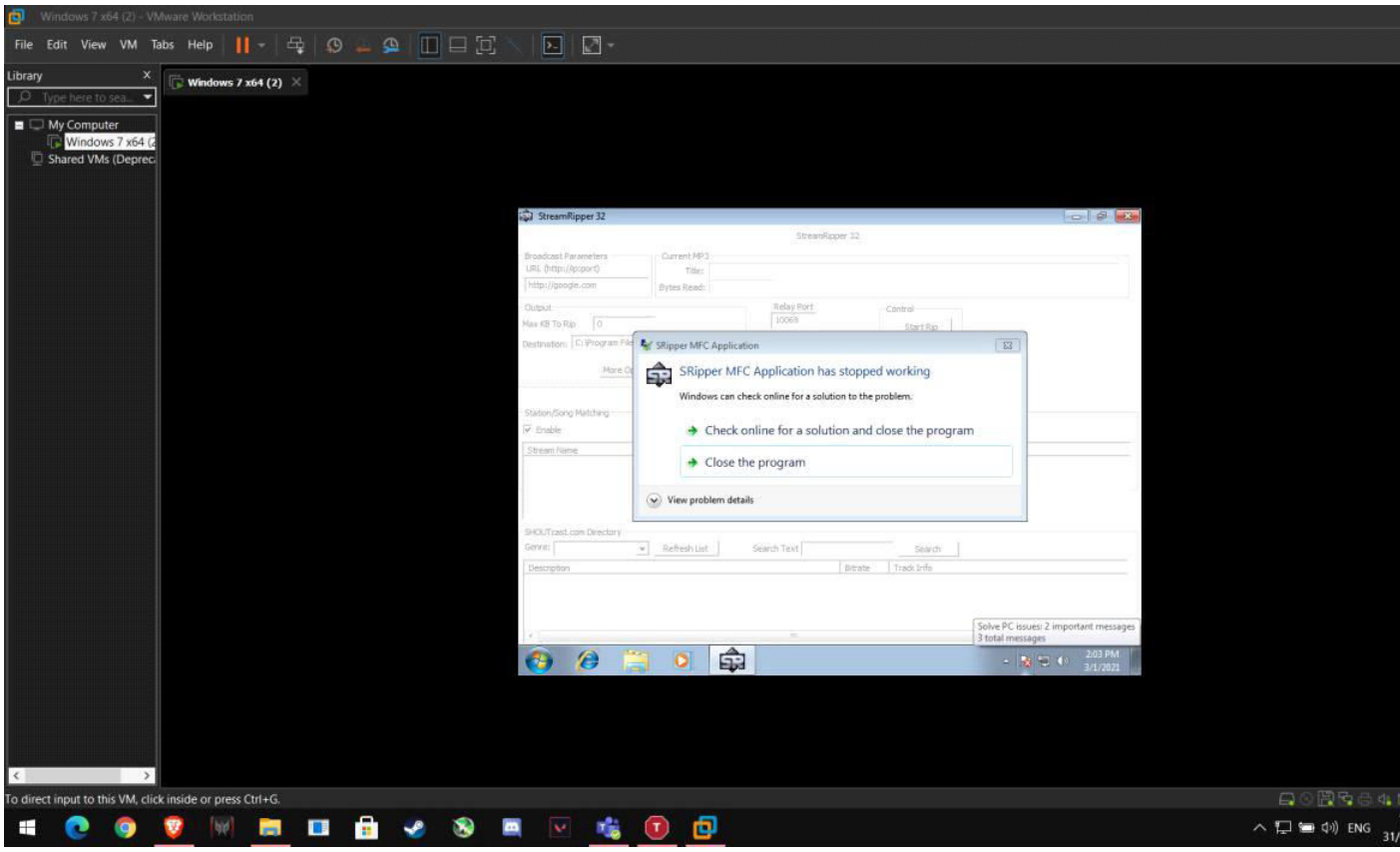




Copy Paste the payload onto the Station/Song matching, Add:



And the Application crashes:



Why the Application crashes:

So when the contribution to that text field surpasses 256 characters, Buffer Overflow occurs and that makes the application crash, since it isn't being dealt with appropriately. This weakness can be handily fixed by restricting the quantity of characters that particular field takes or simply taking the initial 256 characters from that field.