

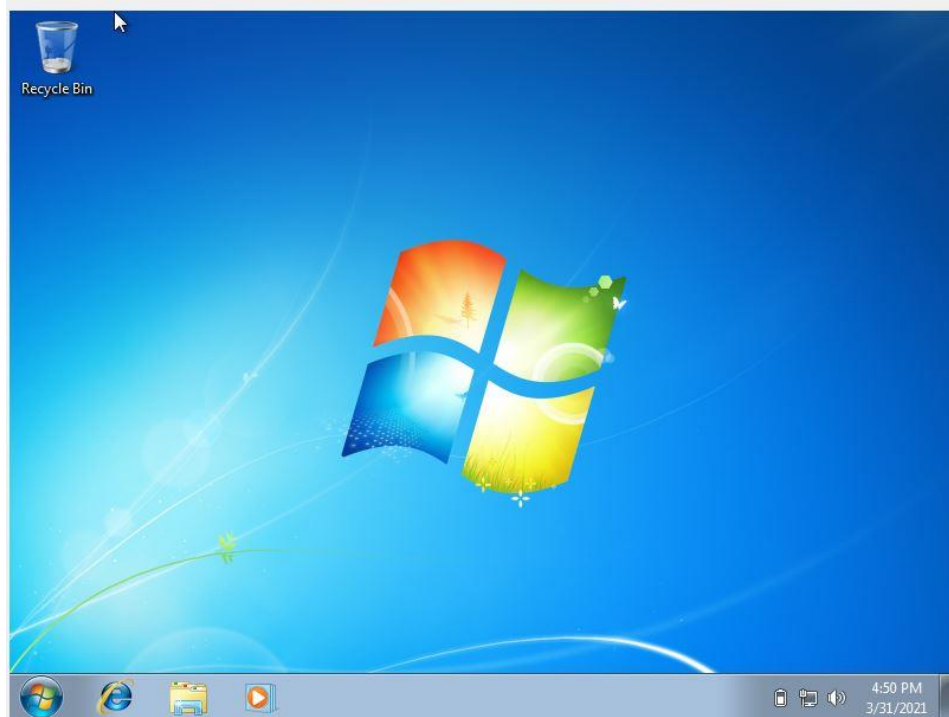
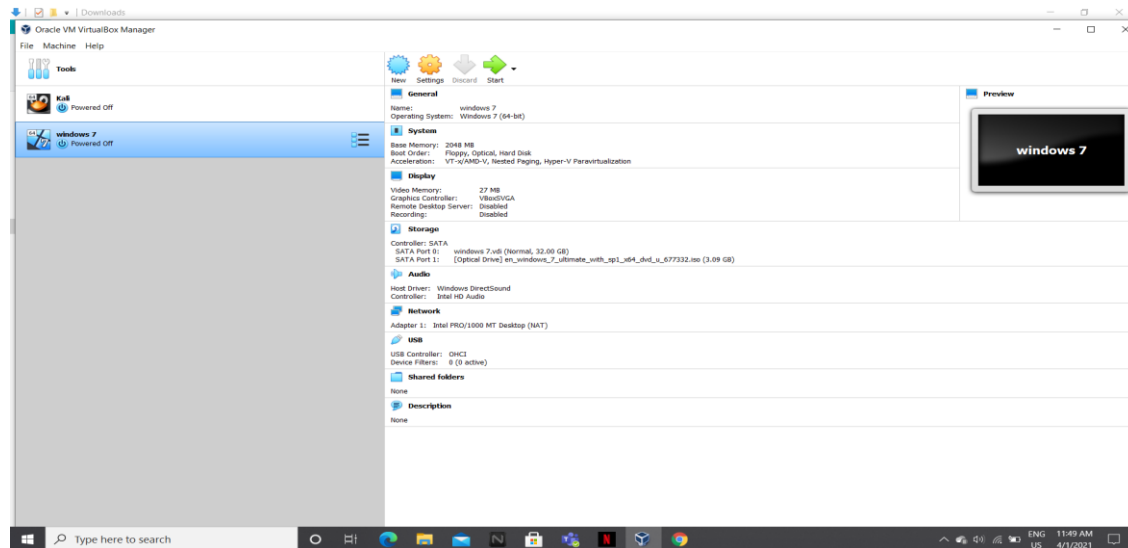
Secure Coding Lab – 7

Rishav Dhiman

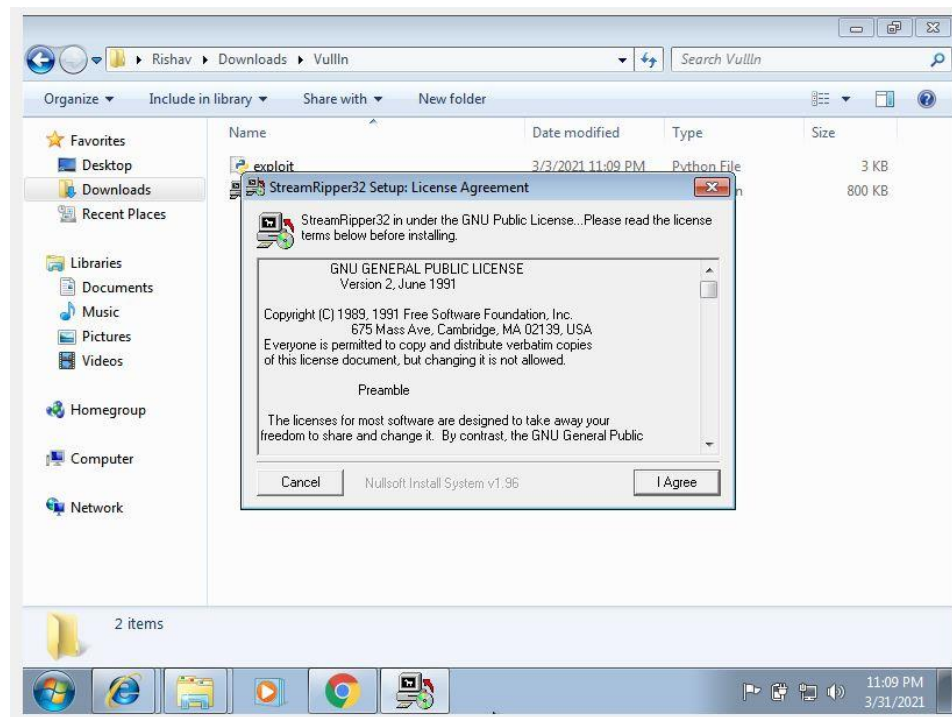
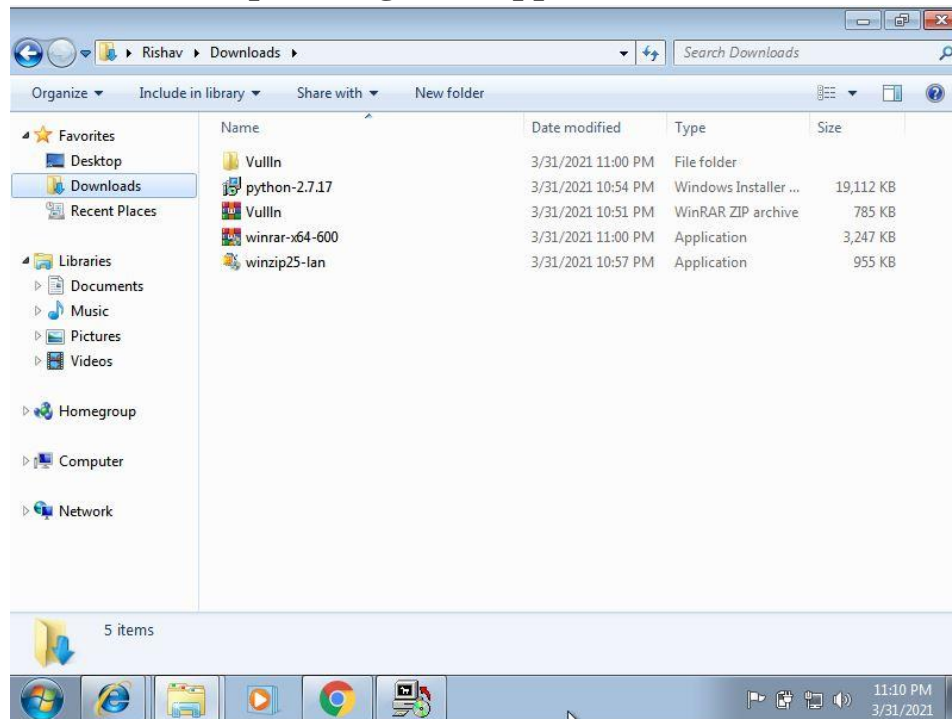
18BCN7030

Install windows 7 on a VM:

VM Configuration

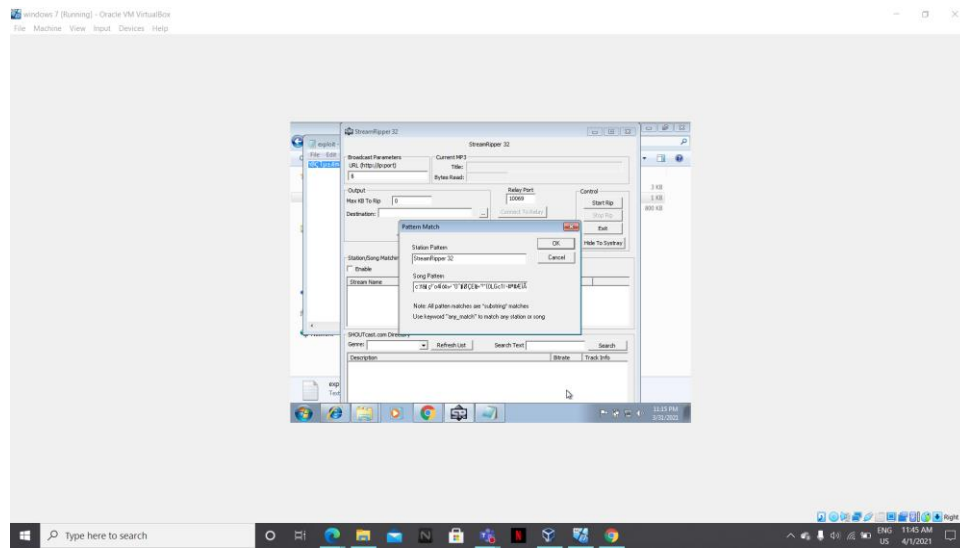


Extract the Zip file to get the application executable and a python file:

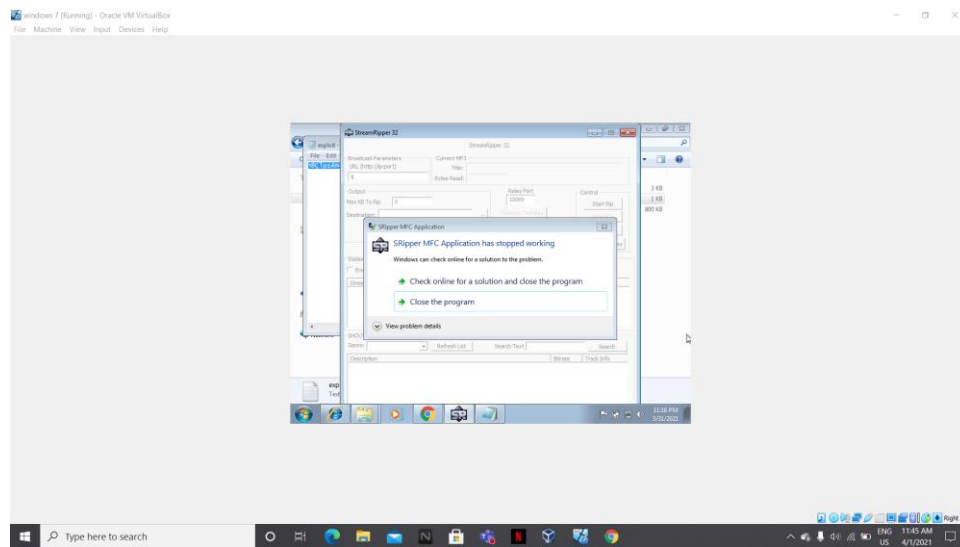


Because this is a fresh install of windows 7 and because official support for windows 7 ended a while ago, we had to install python 2.7.17 and Chrome to download the files and to execute the py file.

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.