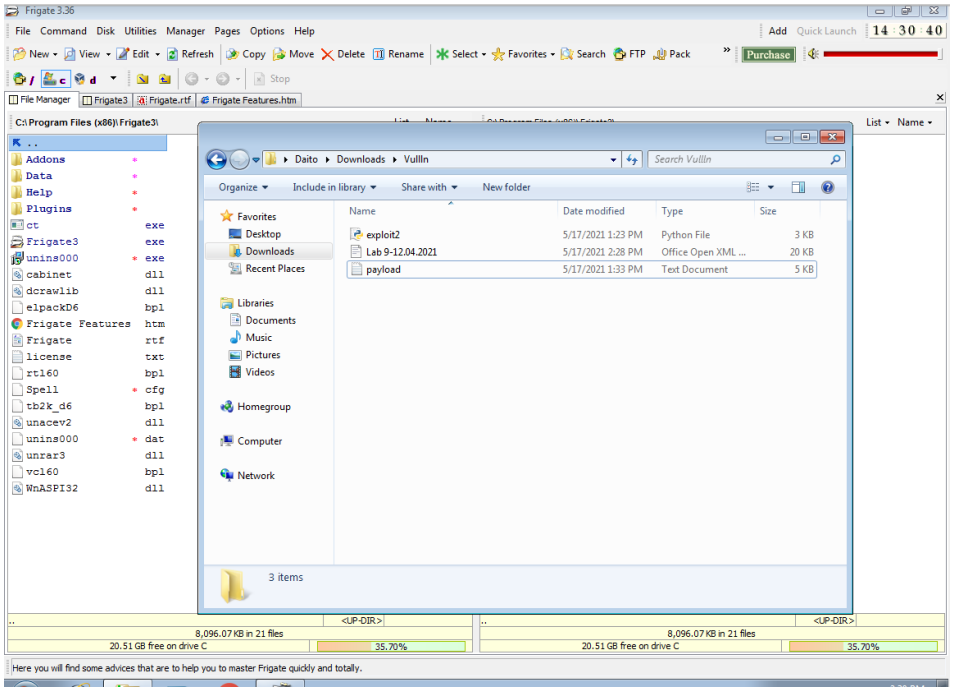
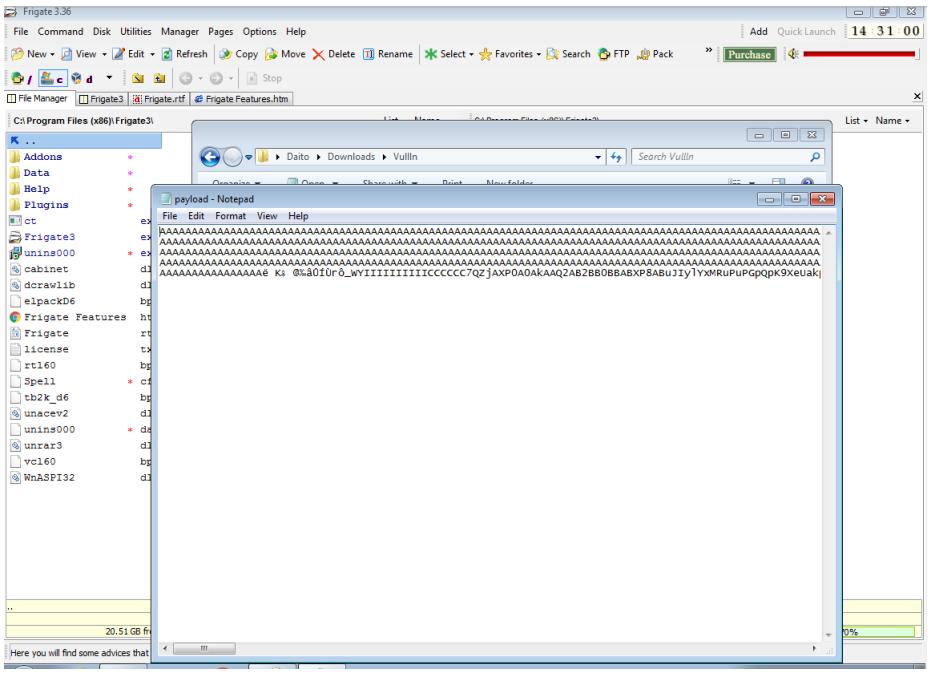
Secure coding Lab -9

D.V.S MOHITH GUPTA
18BCN7072

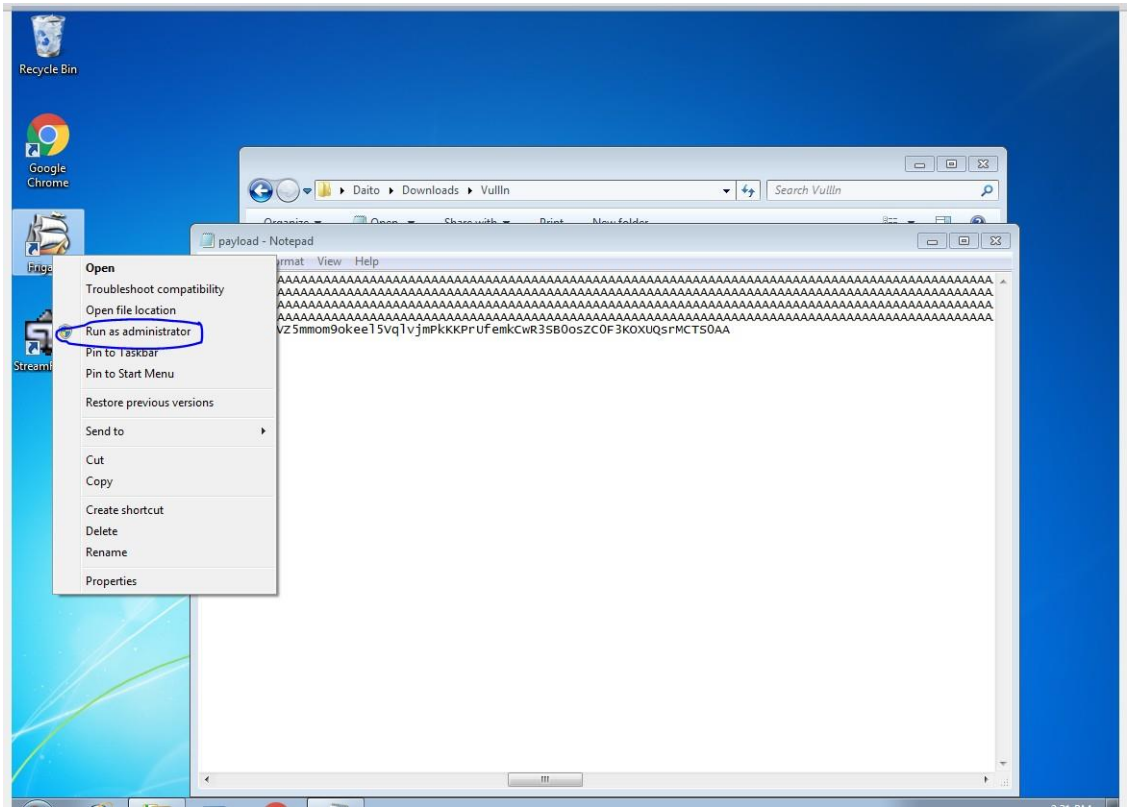
Working with the memory vulnerabilities

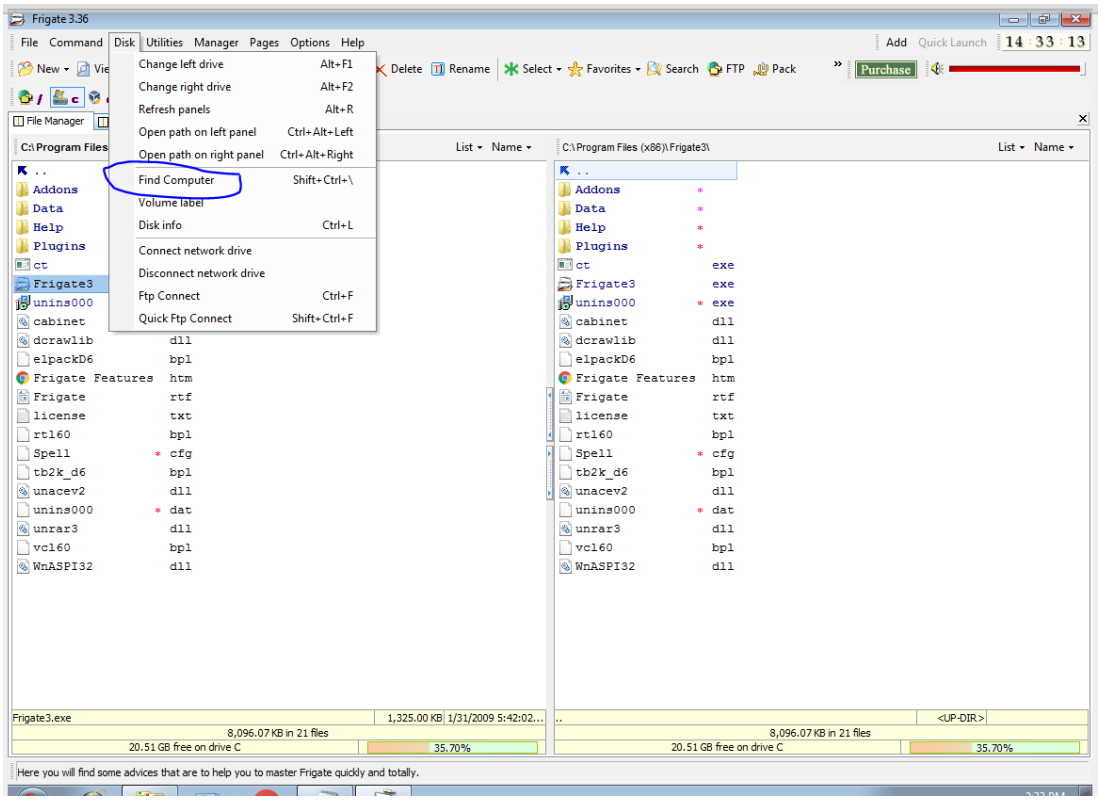
1.) Install Frigate3 on Windows 7 VM: Frigate3 UI and Execute the exploit2.py togenerate the payload_cmd.txt file.

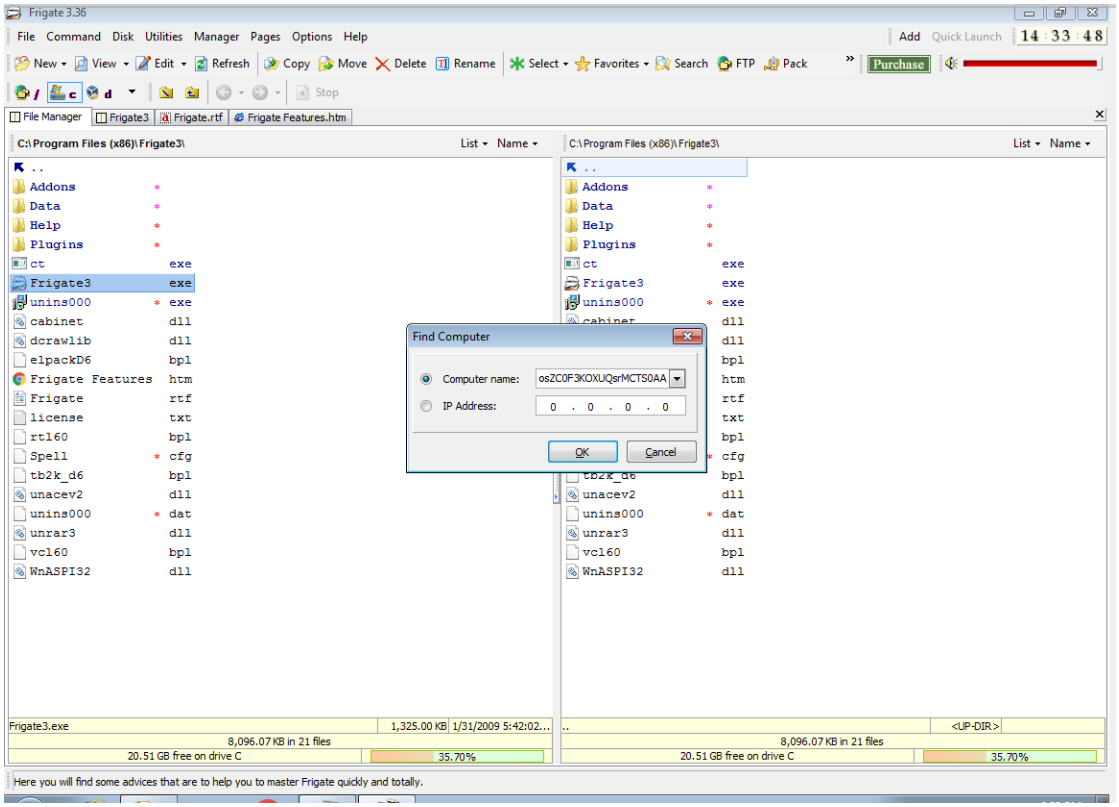




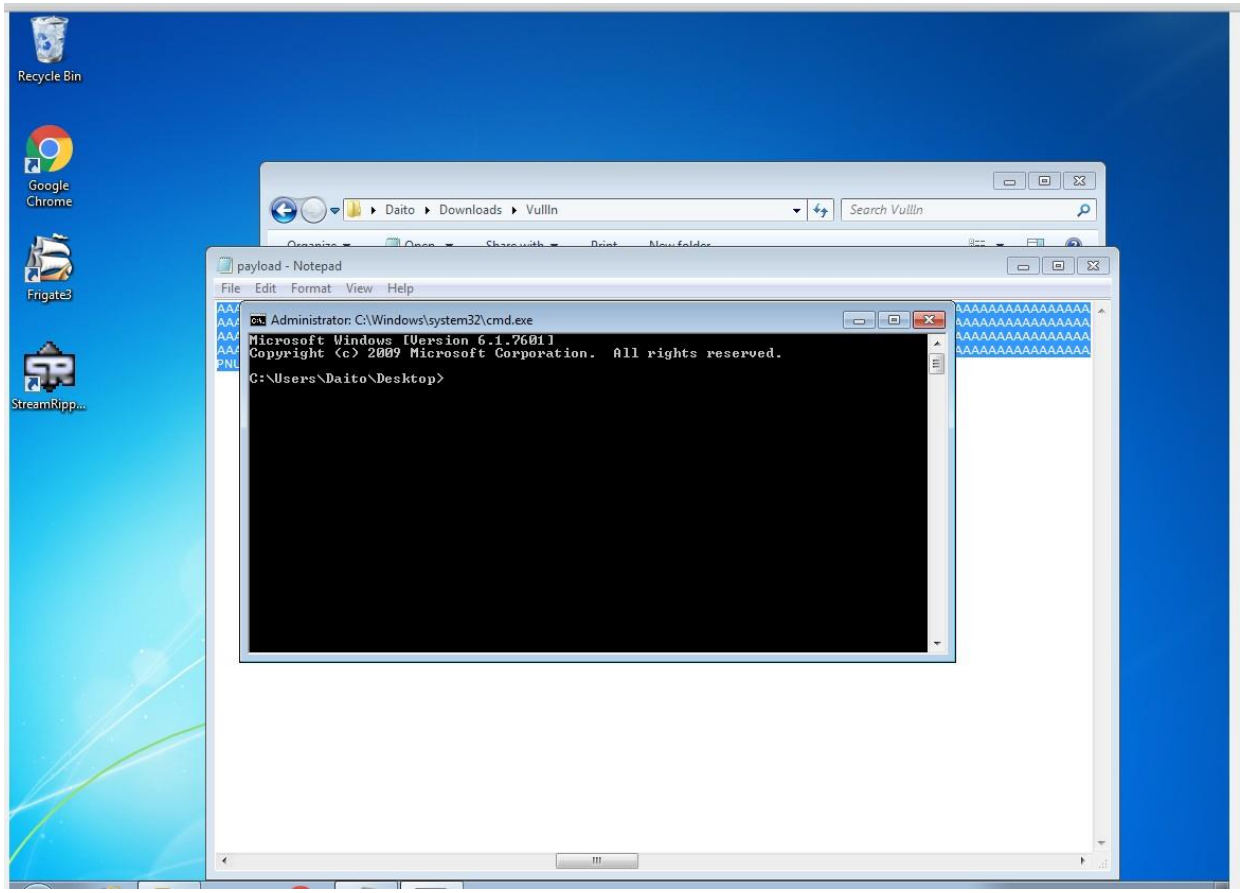
2.) Copy the payload and open the frigate software with admin privileges, Go to disksand select find computer and paste the payload in it.



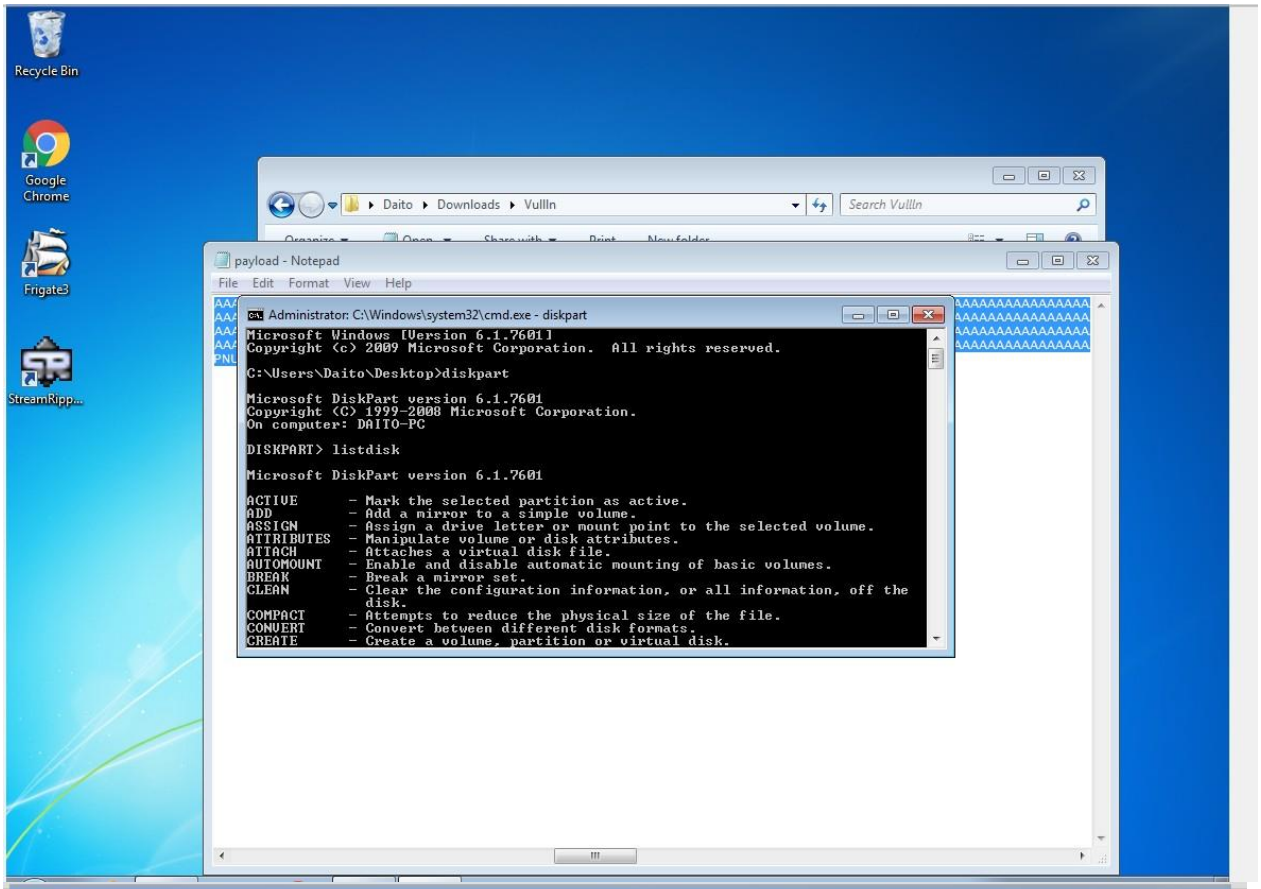


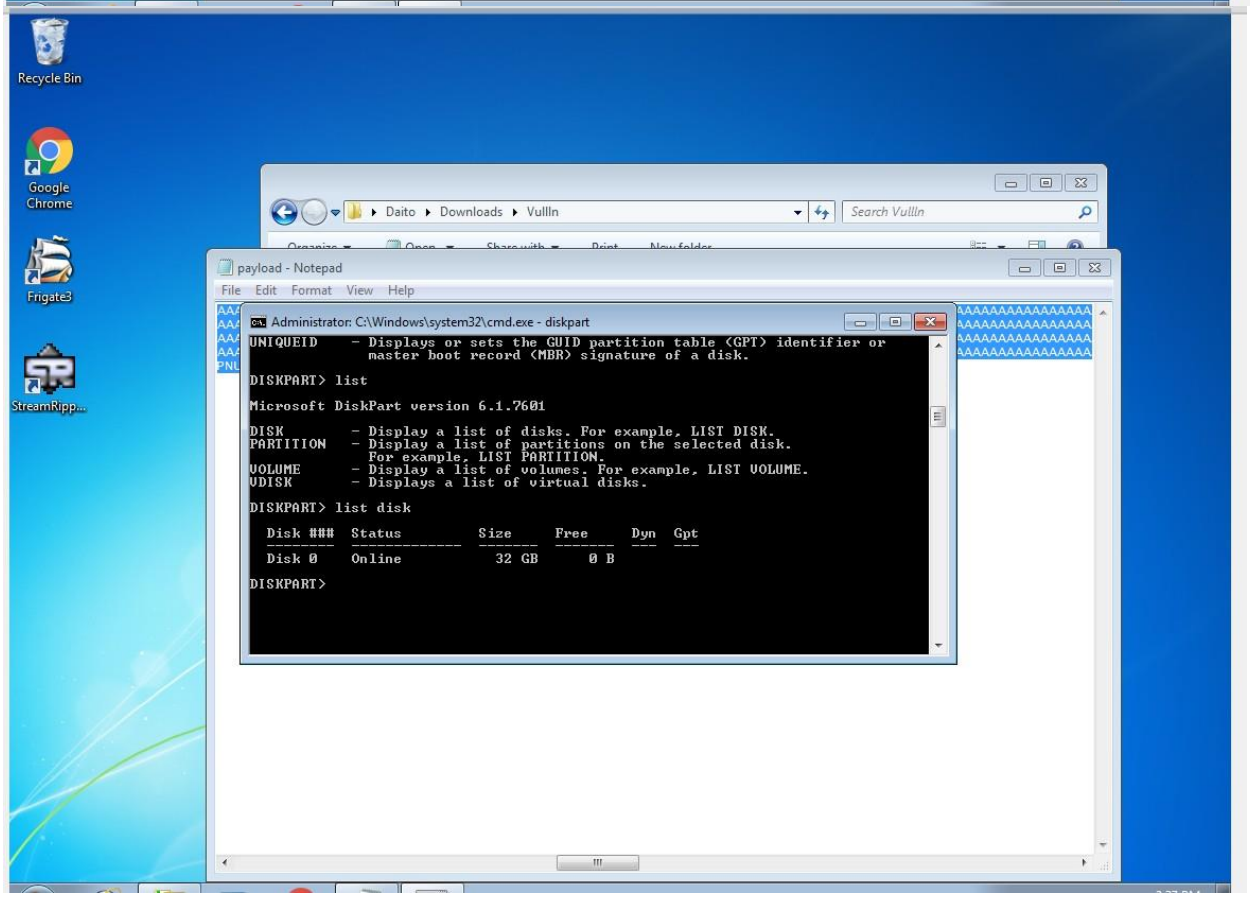


3.) The CMD that opens after crashing the application is opened with elevatedprivileges.



4.) Type diskpart and follow the screenshots





5.) From the diskpart prompt, type clean and press Enter. The drive's partition, data, and signature is now removed. You will return to the diskpart prompt. Warning: Once you type clean and hit enter the drive will be erased.

Check the drive in Device management: