

SECURE CODING CSE-2010

LAB-8

Name - Vishal Dung Dung
Reg - 18BCN7053
Slot - L23-L24

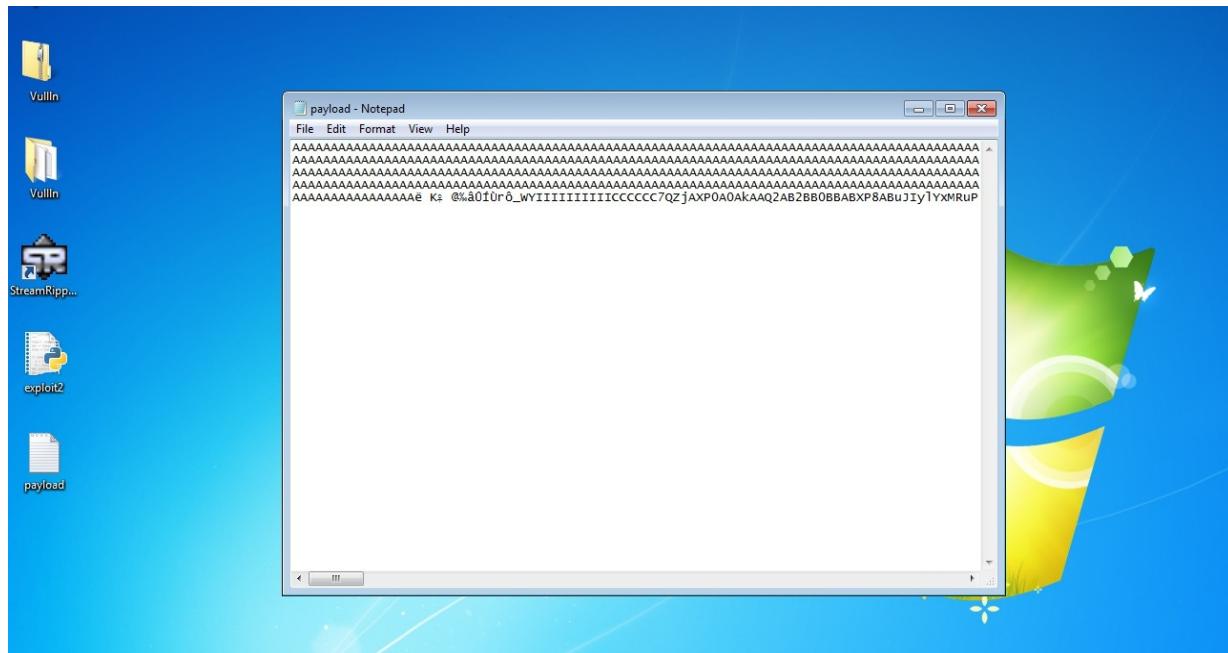
Analysis-

Try to crash the Vuln_Program_Stream program and exploitit.

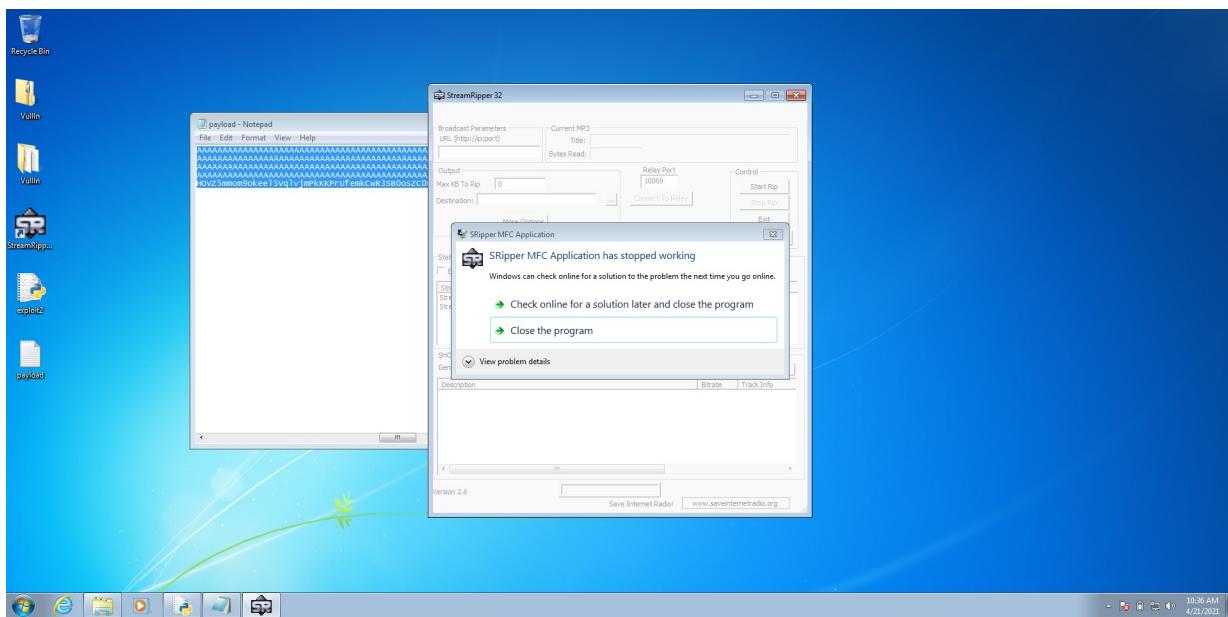
Script-

A screenshot of a Windows 7 desktop. On the left, there's a vertical taskbar with icons for File Explorer, Task View, Start, and other system icons. The desktop background is the standard Windows 7 blue gradient. In the center, there's a terminal window titled "7z exploit2.py - C:\Users\Jayadeep\Desktop\exploit2.py". The window contains Python exploit code for a ROP attack. Below the terminal window, there's a file explorer window showing a folder structure with files like "exploit2.py", "exploit3.py", and "exploit4.py". The status bar at the bottom of the terminal window shows "In 1 Col 0".

Payload Generated

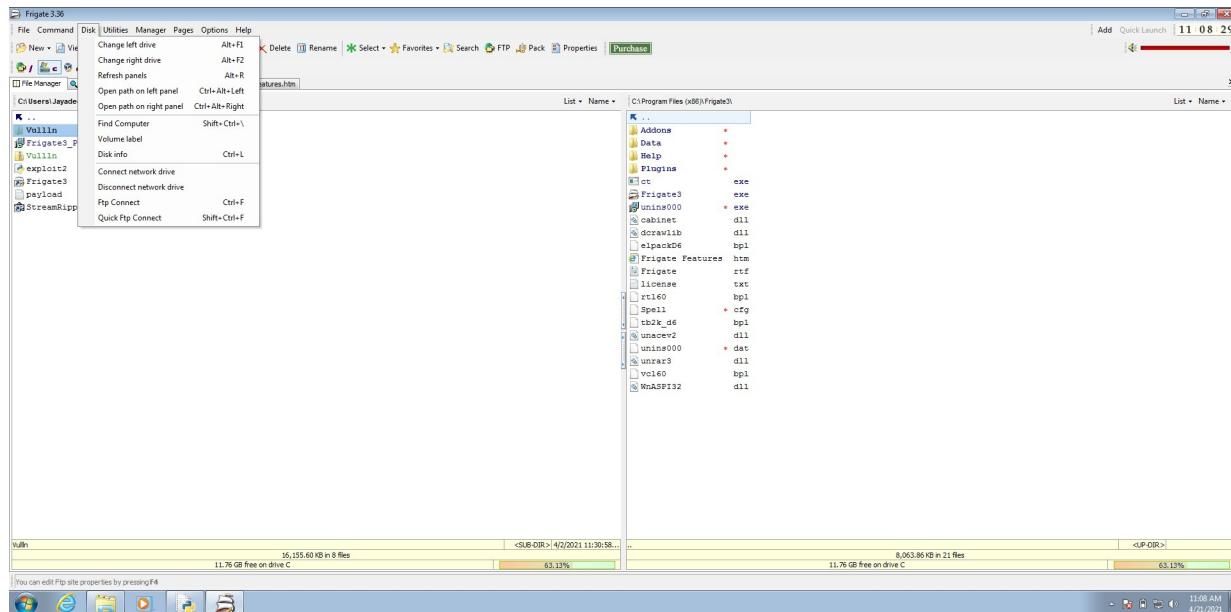


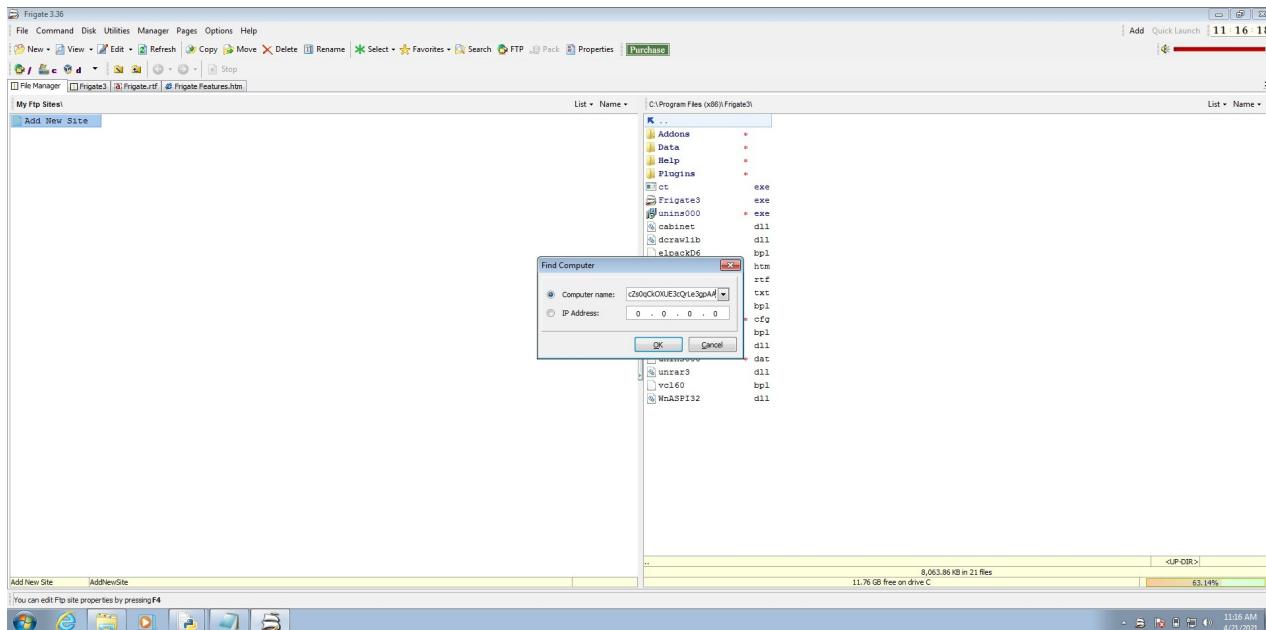
App Crashes



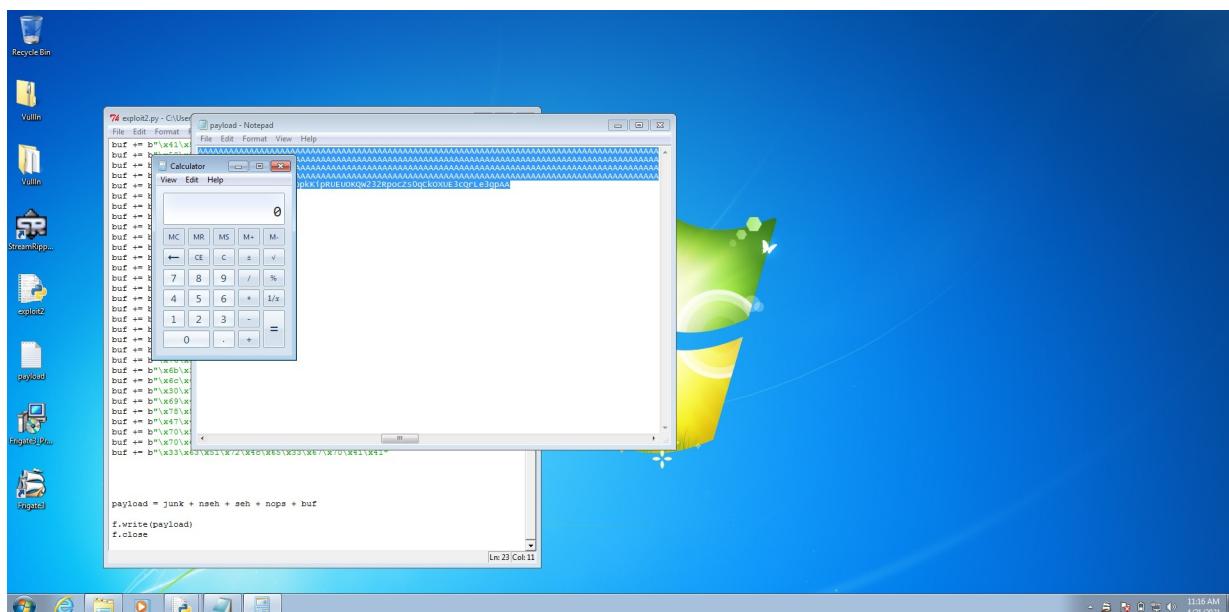
- Change the default trigger from cmd.exe to calc.exe (Use msfvenom in Kali linux).

**Copy pasting the Generated payload in exploit2.py and then
using it in frigate**

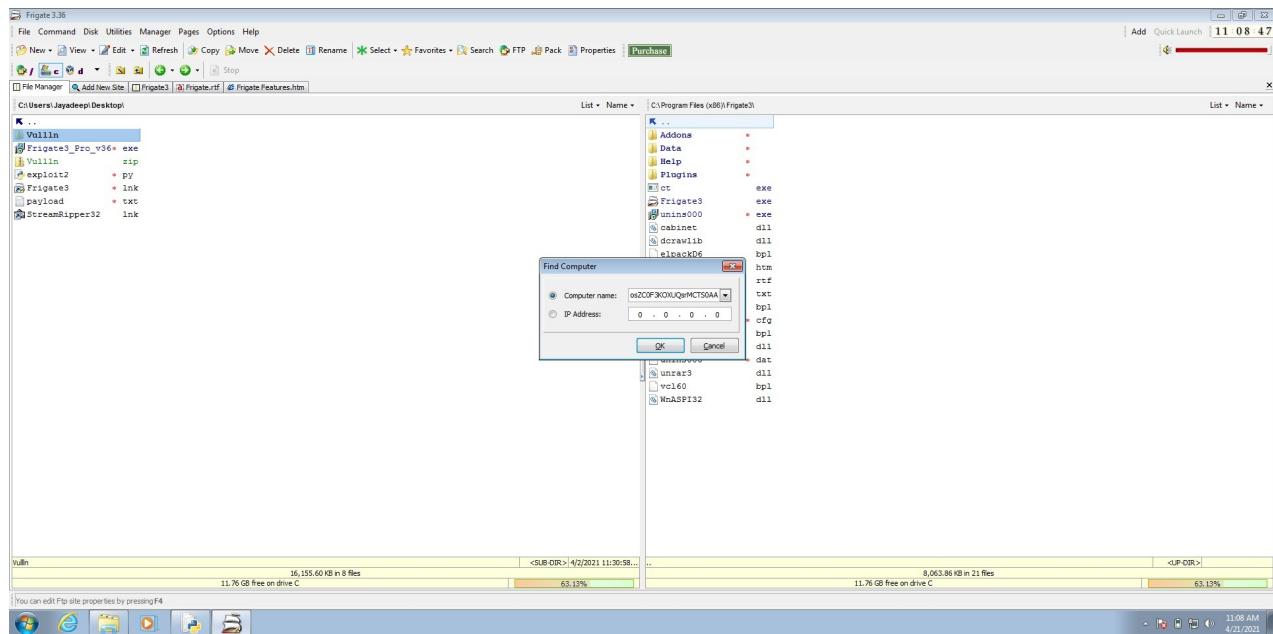




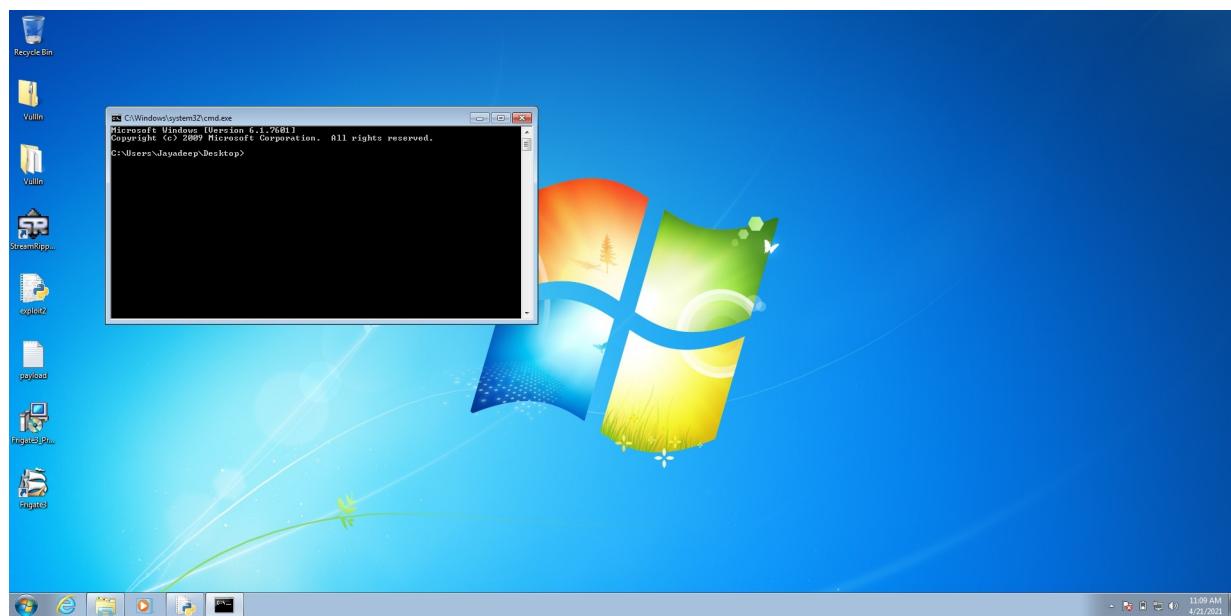
The app crashes and calculator opens



Similarly using payload for cmd

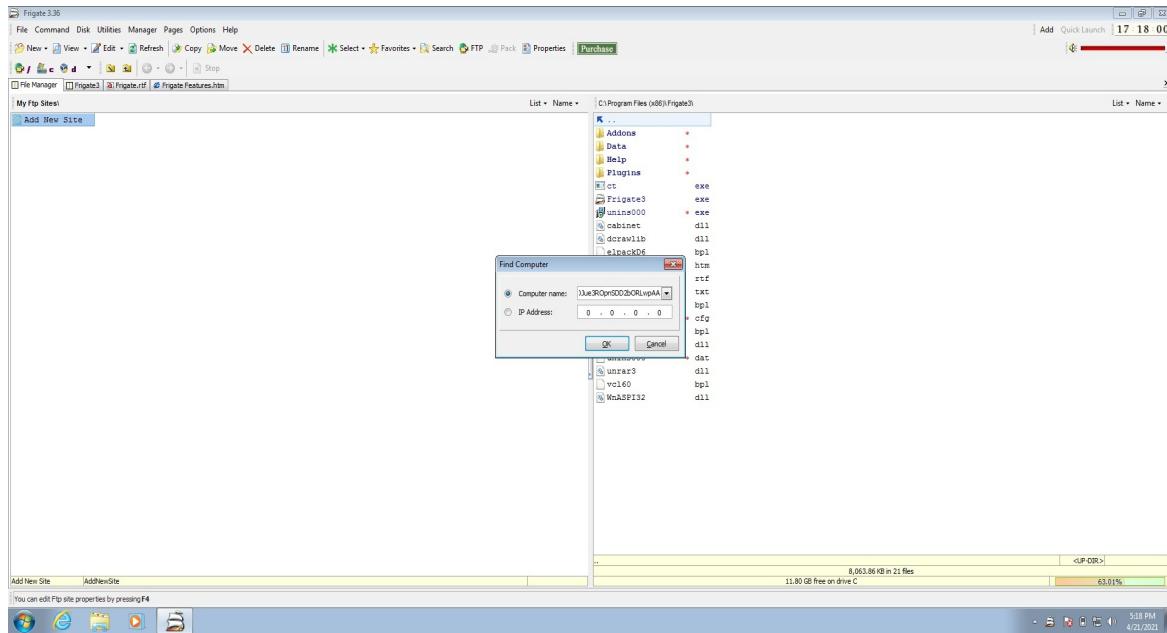


The App crashes and CMD opens

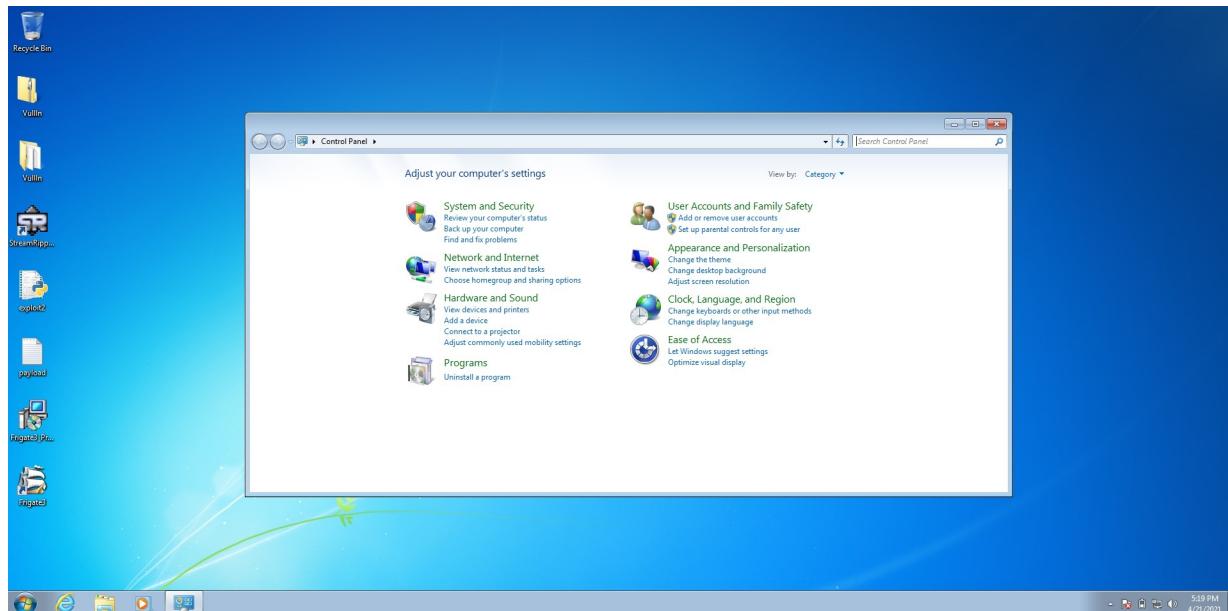


- Change the default trigger to open the control panel.

Copy pasting the Generated payload in exploit2.py and then using it in frigate



The app crashes and the control



panel opens