buflab内存情况

getbuf

```
0x08049284 <+0>:     push   %ebp
0x08049285 <+1>:     mov    %esp,%ebp
0x08049287 <+3>:     sub    $0x38,%esp
0x0804928a <+6>:     lea    -0x28(%ebp),%eax
0x0804928d <+9>:     mov    %eax,(%esp)
0x08049290 <+12>:    call   0x8048d66 <Gets>
0x08049295 <+17>:    mov    $0x1,%eax
0x0804929a <+22>:    leave
0x0804929b <+23>:    ret
```

Gets

```
0x08048d66 <+0>:     push   %ebp
0x08048d67 <+1>:     mov    %esp,%ebp
0x08048d69 <+3>:     sub    $0x28,%esp
0x08048d6c <+6>:     mov    0x8(%ebp),%eax
0x08048d6f <+9>:     mov    %eax,-0x10(%ebp)
0x08048d72 <+12>:    movl   $0x0,0x804e110
0x08048d7c <+22>:    jmp    0x8048d9a <Gets+52>
0x08048d7e <+24>:    mov    -0xc(%ebp),%eax
0x08048d81 <+27>:    mov    %eax,%edx
0x08048d83 <+29>:    mov    -0x10(%ebp),%eax
0x08048d86 <+32>:    mov    %dl,(%eax)
0x08048d88 <+34>:    addl   $0x1,-0x10(%ebp)
0x08048d8c <+38>:    mov    -0xc(%ebp),%eax
0x08048d8f <+41>:    movsbl %al,%eax
0x08048d92 <+44>:    mov    %eax,(%esp)
```

```
0x08048d95 <+47>:    call   0x8048cc8 <save_char>
0x08048d9a <+52>:    mov    0x804e100,%eax
0x08048d9f <+57>:    mov    %eax,(%esp)
0x08048da2 <+60>:    call   0x8048890 <_IO_getc@plt>
0x08048da7 <+65>:    mov    %eax,-0xc(%ebp)
0x08048daa <+68>:    cmpl   $0xffffffff,-0xc(%ebp)
0x08048dae <+72>:    je     0x8048db6 <Gets+80>
```

test

```
0x08048be0 <+0>:     push   %ebp
0x08048be1 <+1>:     mov    %esp,%ebp
0x08048be3 <+3>:     sub    $0x28,%esp
0x08048be6 <+6>:     call   0x8049023 <uniqueval>
0x08048beb <+11>:    mov    %eax,-0x10(%ebp)
0x08048bee <+14>:    call   0x8049284 <getbuf>
0x08048bf3 <+19>:    mov    %eax,-0xc(%ebp)
0x08048bf6 <+22>:    call   0x8049023 <uniqueval>
0x08048bfb <+27>:    mov    -0x10(%ebp),%edx
0x08048bfe <+30>:    cmp    %edx,%eax
0x08048c00 <+32>:    je     0x8048c10 <test+48>
0x08048c02 <+34>:    movl   $0x804a650,(%esp)
0x08048c09 <+41>:    call   0x8048900 <puts@plt>
0x08048c0e <+46>:    jmp    0x8048c52 <test+114>
0x08048c10 <+48>:    mov    -0xc(%ebp),%edx
0x08048c13 <+51>:    mov    0x804e104,%eax
0x08048c18 <+56>:    cmp    %eax,%edx
0x08048c1a <+58>:    jne    0x8048c3e <test+94>
0x08048c1c <+60>:    mov    $0x804a679,%eax
0x08048c21 <+65>:    mov    -0xc(%ebp),%edx
0x08048c24 <+68>:    mov    %edx,0x4(%esp)
```

```
0x08048c28 <+72>:    mov    %eax,(%esp)
```

smoke

```
0x08048b04 <+0>:     push   %ebp
0x08048b05 <+1>:     mov    %esp,%ebp
0x08048b07 <+3>:     sub    $0x18,%esp
0x08048b0a <+6>:     movl   $0x804a5b0,(%esp)
0x08048b11 <+13>:    call   0x8048900 <puts@plt>
0x08048b16 <+18>:    movl   $0x0,(%esp)
0x08048b1d <+25>:    call   0x804942e <validate>
0x08048b22 <+30>:    movl   $0x0,(%esp)
0x08048b29 <+37>:    call   0x8048920 <exit@plt>
```

fizz

```
0x08048b2e <+0>:     push   %ebp
0x08048b2f <+1>:     mov    %esp,%ebp
0x08048b31 <+3>:     sub    $0x18,%esp
0x08048b34 <+6>:     mov    0x8(%ebp),%edx
0x08048b37 <+9>:     mov    0x804e104,%eax
0x08048b3c <+14>:    cmp    %eax,%edx
0x08048b3e <+16>:    jne    0x8048b62 <fizz+52>
0x08048b40 <+18>:    mov    $0x804a5cb,%eax
0x08048b45 <+23>:    mov    0x8(%ebp),%edx
0x08048b48 <+26>:    mov    %edx,0x4(%esp)
0x08048b4c <+30>:    mov    %eax,(%esp)
0x08048b4f <+33>:    call   0x8048830 <printf@plt>
0x08048b54 <+38>:    movl   $0x1,(%esp)
```

```
0x08048b5b <+45>:    call   0x804942e <validate>
0x08048b60 <+50>:    jmp    0x8048b76 <fizz+72>
0x08048b62 <+52>:    mov    $0x804a5ec,%eax
0x08048b67 <+57>:    mov    0x8(%ebp),%edx
0x08048b6a <+60>:    mov    %edx,0x4(%esp)
0x08048b6e <+64>:    mov    %eax,(%esp)
0x08048b71 <+67>:    call   0x8048830 <printf@plt>
0x08048b76 <+72>:    movl   $0x0,(%esp)
0x08048b7d <+79>:    call   0x8048920 <exit@plt>
```

Bang

```
0x08048b82 <+0>:     push   %ebp
0x08048b83 <+1>:     mov    %esp,%ebp
0x08048b85 <+3>:     sub    $0x18,%esp
0x08048b88 <+6>:     mov    0x804e10c,%eax
0x08048b8d <+11>:    mov    %eax,%edx
0x08048b8f <+13>:    mov    0x804e104,%eax
0x08048b94 <+18>:    cmp    %eax,%edx
0x08048b96 <+20>:    jne    0x8048bbd <bang+59>
0x08048b98 <+22>:    mov    0x804e10c,%edx
0x08048b9e <+28>:    mov    $0x804a60c,%eax
0x08048ba3 <+33>:    mov    %edx,0x4(%esp)
0x08048ba7 <+37>:    mov    %eax,(%esp)
0x08048baa <+40>:    call   0x8048830 <printf@plt>
0x08048baf <+45>:    movl   $0x2,(%esp)
0x08048bb6 <+52>:    call   0x804942e <validate>
```

```
0x08048bbb <+57>:    jmp    0x8048bd4 <bang+82>
0x08048bbd <+59>:    mov    0x804e10c,%edx
0x08048bc3 <+65>:    mov    $0x804a631,%eax
0x08048bc8 <+70>:    mov    %edx,0x4(%esp)
0x08048bcc <+74>:    mov    %eax,(%esp)
0x08048bcf <+77>:    call   0x8048830 <printf@plt>
0x08048bd4 <+82>:    movl   $0x0,(%esp)
```

Getbufn

```
0x0804929c <+0>:     push   %ebp
0x0804929d <+1>:     mov    %esp,%ebp
0x0804929f <+3>:     sub    $0x218,%esp
0x080492a5 <+9>:     lea    -0x208(%ebp),%eax
0x080492ab <+15>:    mov    %eax,(%esp)
0x080492ae <+18>:    call   0x8048d66 <Gets>
0x080492b3 <+23>:    mov    $0x1,%eax
0x080492b8 <+28>:    leave
0x080492b9 <+29>:    ret
```

Testn

```
0x08048c54 <+0>:     push   %ebp
0x08048c55 <+1>:     mov    %esp,%ebp
0x08048c57 <+3>:     sub    $0x28,%esp
0x08048c5a <+6>:     call   0x8049023 <uniqueval>
0x08048c5f <+11>:    mov    %eax,-0x10(%ebp)
0x08048c62 <+14>:    call   0x804929c <getbufn>
0x08048c67 <+19>:    mov    %eax,-0xc(%ebp)
```

```
0x08048c6a <+22>:    call   0x8049023 <uniqueval>
0x08048c6f <+27>:    mov    -0x10(%ebp),%edx
0x08048c72 <+30>:    cmp    %edx,%eax
0x08048c74 <+32>:    je     0x8048c84 <testn+48>
0x08048c76 <+34>:    movl   $0x804a650,(%esp)
0x08048c7d <+41>:    call   0x8048900 <puts@plt>
0x08048c82 <+46>:    jmp    0x8048cc6 <testn+114>
0x08048c84 <+48>:    mov    -0xc(%ebp),%edx
0x08048c87 <+51>:    mov    0x804e104,%eax
0x08048c8c <+56>:    cmp    %eax,%edx
0x08048c8e <+58>:    jne    0x8048cb2 <testn+94>
0x08048c90 <+60>:    mov    $0x804a6b4,%eax
0x08048c95 <+65>:    mov    -0xc(%ebp),%edx
0x08048c98 <+68>:    mov    %edx,0x4(%esp)
0x08048c9c <+72>:    mov    %eax,(%esp)
0x08048c9f <+75>:    call   0x8048830 <printf@plt>
0x08048ca4 <+80>:    movl   $0x4,(%esp)
0x08048cab <+87>:    call   0x804942e <validate>
0x08048cb0 <+92>:    jmp    0x8048cc6 <testn+114>
0x08048cb2 <+94>:    mov    $0x804a6d4,%eax
0x08048cb7 <+99>:    mov    -0xc(%ebp),%edx
0x08048cba <+102>:   mov    %edx,0x4(%esp)
0x08048cbe <+106>:   mov    %eax,(%esp)
0x08048cc1 <+109>:   call   0x8048830 <printf@plt>
0x08048cc6 <+114>:   leave
0x08048cc7 <+115>:   ret
```

Test()	ebp:0x55683be0	eip:0x55683be4
getbuf()	ebp:0x55683bb0	eip:0x55683bb4
Gets()	ebp:0x55683b70	tip:0x55683b74

字符缓冲区输入入口：0x55683b88