

bufbomb: file format elf32-i386

Disassembly of section .init:

```
080486a8 <_init>:
80486a8: 55          push    %ebp
80486a9: 89 e5      mov     %esp,%ebp
80486ab: 83 ec 08   sub     $0x8,%esp
80486ae: e8 21 02 00 00 call    80488d4 <call_gmon_start>
80486b3: e8 a8 02 00 00 call    8048960 <frame_dummy>
80486b8: e8 73 0f 00 00 call    8049630 <__do_global_ctors_aux>
80486bd: c9        leave   %eax
80486be: c3        ret
```

Disassembly of section .plt:

```
080486c0 <sprintf@plt-0x10>:
80486c0: ff 35 e4 a0 04 08 pushl   0x804a0e4
80486c6: ff 25 e8 a0 04 08 jmp     *0x804a0e8
80486cc: 00 00     add     %al,(%eax)
...

080486d0 <sprintf@plt>:
80486d0: ff 25 ec a0 04 08 jmp     *0x804a0ec
80486d6: 68 00 00 00 00 push    $0x0
80486db: e9 e0 ff ff ff jmp     80486c0 <_init+0x18>

080486e0 <srand@plt>:
80486e0: ff 25 f0 a0 04 08 jmp     *0x804a0f0
80486e6: 68 08 00 00 00 push    $0x8
80486eb: e9 d0 ff ff ff jmp     80486c0 <_init+0x18>

080486f0 <mmap@plt>:
80486f0: ff 25 f4 a0 04 08 jmp     *0x804a0f4
80486f6: 68 10 00 00 00 push    $0x10
80486fb: e9 c0 ff ff ff jmp     80486c0 <_init+0x18>

08048700 <random@plt>:
8048700: ff 25 f8 a0 04 08 jmp     *0x804a0f8
8048706: 68 18 00 00 00 push    $0x18
804870b: e9 b0 ff ff ff jmp     80486c0 <_init+0x18>

08048710 <signal@plt>:
8048710: ff 25 fc a0 04 08 jmp     *0x804a0fc
8048716: 68 20 00 00 00 push    $0x20
804871b: e9 a0 ff ff ff jmp     80486c0 <_init+0x18>

08048720 <__gmon_start__@plt>:
8048720: ff 25 00 a1 04 08 jmp     *0x804a100
8048726: 68 28 00 00 00 push    $0x28
804872b: e9 90 ff ff ff jmp     80486c0 <_init+0x18>

08048730 <calloc@plt>:
8048730: ff 25 04 a1 04 08 jmp     *0x804a104
8048736: 68 30 00 00 00 push    $0x30
804873b: e9 80 ff ff ff jmp     80486c0 <_init+0x18>

08048740 <system@plt>:
8048740: ff 25 08 a1 04 08 jmp     *0x804a108
8048746: 68 38 00 00 00 push    $0x38
804874b: e9 70 ff ff ff jmp     80486c0 <_init+0x18>

08048750 <memset@plt>:
8048750: ff 25 0c a1 04 08 jmp     *0x804a10c
8048756: 68 40 00 00 00 push    $0x40
804875b: e9 60 ff ff ff jmp     80486c0 <_init+0x18>

08048760 <__libc_start_main@plt>:
```

```

8048760:    ff 25 10 a1 04 08    jmp    *0x804a110
8048766:    68 48 00 00 00      push   $0x48
804876b:    e9 50 ff ff ff      jmp    80486c0 <_init+0x18>

08048770 <_IO_getc@plt>:
8048770:    ff 25 14 a1 04 08    jmp    *0x804a114
8048776:    68 50 00 00 00      push   $0x50
804877b:    e9 40 ff ff ff      jmp    80486c0 <_init+0x18>

08048780 <__ctype_b_loc@plt>:
8048780:    ff 25 18 a1 04 08    jmp    *0x804a118
8048786:    68 58 00 00 00      push   $0x58
804878b:    e9 30 ff ff ff      jmp    80486c0 <_init+0x18>

08048790 <fclose@plt>:
8048790:    ff 25 1c a1 04 08    jmp    *0x804a11c
8048796:    68 60 00 00 00      push   $0x60
804879b:    e9 20 ff ff ff      jmp    80486c0 <_init+0x18>

080487a0 <getopt@plt>:
80487a0:    ff 25 20 a1 04 08    jmp    *0x804a120
80487a6:    68 68 00 00 00      push   $0x68
80487ab:    e9 10 ff ff ff      jmp    80486c0 <_init+0x18>

080487b0 <fopen@plt>:
80487b0:    ff 25 24 a1 04 08    jmp    *0x804a124
80487b6:    68 70 00 00 00      push   $0x70
80487bb:    e9 00 ff ff ff      jmp    80486c0 <_init+0x18>

080487c0 <alarm@plt>:
80487c0:    ff 25 28 a1 04 08    jmp    *0x804a128
80487c6:    68 78 00 00 00      push   $0x78
80487cb:    e9 f0 fe ff ff      jmp    80486c0 <_init+0x18>

080487d0 <strcpy@plt>:
80487d0:    ff 25 2c a1 04 08    jmp    *0x804a12c
80487d6:    68 80 00 00 00      push   $0x80
80487db:    e9 e0 fe ff ff      jmp    80486c0 <_init+0x18>

080487e0 <printf@plt>:
80487e0:    ff 25 30 a1 04 08    jmp    *0x804a130
80487e6:    68 88 00 00 00      push   $0x88
80487eb:    e9 d0 fe ff ff      jmp    80486c0 <_init+0x18>

080487f0 <random@plt>:
80487f0:    ff 25 34 a1 04 08    jmp    *0x804a134
80487f6:    68 90 00 00 00      push   $0x90
80487fb:    e9 c0 fe ff ff      jmp    80486c0 <_init+0x18>

08048800 <fwrite@plt>:
8048800:    ff 25 38 a1 04 08    jmp    *0x804a138
8048806:    68 98 00 00 00      push   $0x98
804880b:    e9 b0 fe ff ff      jmp    80486c0 <_init+0x18>

08048810 <fprintf@plt>:
8048810:    ff 25 3c a1 04 08    jmp    *0x804a13c
8048816:    68 a0 00 00 00      push   $0xa0
804881b:    e9 a0 fe ff ff      jmp    80486c0 <_init+0x18>

08048820 <remove@plt>:
8048820:    ff 25 40 a1 04 08    jmp    *0x804a140
8048826:    68 a8 00 00 00      push   $0xa8
804882b:    e9 90 fe ff ff      jmp    80486c0 <_init+0x18>

08048830 <cuserid@plt>:
8048830:    ff 25 44 a1 04 08    jmp    *0x804a144
8048836:    68 b0 00 00 00      push   $0xb0
804883b:    e9 80 fe ff ff      jmp    80486c0 <_init+0x18>

```

```

08048840 <fputc@plt>:
8048840: ff 25 48 a1 04 08    jmp     *0x804a148
8048846: 68 b8 00 00 00      push    $0xb8
804884b: e9 70 fe ff ff      jmp     80486c0 <_init+0x18>

```

```

08048850 <puts@plt>:
8048850: ff 25 4c a1 04 08    jmp     *0x804a14c
8048856: 68 c0 00 00 00      push    $0xc0
804885b: e9 60 fe ff ff      jmp     80486c0 <_init+0x18>

```

```

08048860 <rand@plt>:
8048860: ff 25 50 a1 04 08    jmp     *0x804a150
8048866: 68 c8 00 00 00      push    $0xc8
804886b: e9 50 fe ff ff      jmp     80486c0 <_init+0x18>

```

```

08048870 <munmap@plt>:
8048870: ff 25 54 a1 04 08    jmp     *0x804a154
8048876: 68 d0 00 00 00      push    $0xd0
804887b: e9 40 fe ff ff      jmp     80486c0 <_init+0x18>

```

```

08048880 <tempnam@plt>:
8048880: ff 25 58 a1 04 08    jmp     *0x804a158
8048886: 68 d8 00 00 00      push    $0xd8
804888b: e9 30 fe ff ff      jmp     80486c0 <_init+0x18>

```

```

08048890 <__strdup@plt>:
8048890: ff 25 5c a1 04 08    jmp     *0x804a15c
8048896: 68 e0 00 00 00      push    $0xe0
804889b: e9 20 fe ff ff      jmp     80486c0 <_init+0x18>

```

```

080488a0 <exit@plt>:
80488a0: ff 25 60 a1 04 08    jmp     *0x804a160
80488a6: 68 e8 00 00 00      push    $0xe8
80488ab: e9 10 fe ff ff      jmp     80486c0 <_init+0x18>

```

Disassembly of section .text:

```

080488b0 <_start>:
80488b0: 31 ed                xor     %ebp,%ebp
80488b2: 5e                   pop     %esi
80488b3: 89 e1                mov     %esp,%ecx
80488b5: 83 e4 f0             and     $0xffffffff,%esp
80488b8: 50                   push    %eax
80488b9: 54                   push    %esp
80488ba: 52                   push    %edx
80488bb: 68 b0 95 04 08      push    $0x80495b0
80488c0: 68 c0 95 04 08      push    $0x80495c0
80488c5: 51                   push    %ecx
80488c6: 56                   push    %esi
80488c7: 68 40 92 04 08      push    $0x8049240
80488cc: e8 8f fe ff ff      call    8048760 <__libc_start_main@plt>
80488d1: f4                   hlt
80488d2: 90                   nop
80488d3: 90                   nop

```

```

080488d4 <call_gmon_start>:
80488d4: 55                   push    %ebp
80488d5: 89 e5                mov     %esp,%ebp
80488d7: 53                   push    %ebx
80488d8: 83 ec 04             sub     $0x4,%esp
80488db: e8 00 00 00 00      call    80488e0 <call_gmon_start+0xc>
80488e0: 5b                   pop     %ebx
80488e1: 81 c3 00 18 00 00    add     $0x1800,%ebx
80488e7: 8b 93 fc ff ff ff    mov     0xffffffff(%ebx),%edx
80488ed: 85 d2                test    %edx,%edx
80488ef: 74 05                je      80488f6 <call_gmon_start+0x22>
80488f1: e8 2a fe ff ff      call    8048720 <__gmon_start__@plt>
80488f6: 58                   pop     %eax

```

```

80488f7:      5b                pop    %ebx
80488f8:      c9                leave
80488f9:      c3                ret
80488fa:      90                nop
80488fb:      90                nop
80488fc:      90                nop
80488fd:      90                nop
80488fe:      90                nop
80488ff:      90                nop

08048900 <__do_global_dtors_aux>:
8048900:      55                push   %ebp
8048901:      89 e5             mov     %esp,%ebp
8048903:      53                push   %ebx
8048904:      83 ec 04          sub     $0x4,%esp
8048907:      80 3d b4 a1 04 08 00 cmpb    $0x0,0x804a1b4
804890e:      75 3f             jne     804894f <__do_global_dtors_aux+0x4f>
8048910:      b8 0c a0 04 08    mov     $0x804a00c,%eax
8048915:      2d 08 a0 04 08    sub     $0x804a008,%eax
804891a:      c1 f8 02          sar     $0x2,%eax
804891d:      8d 58 ff          lea     0xffffffff(%eax),%ebx
8048920:      a1 b0 a1 04 08    mov     0x804a1b0,%eax
8048925:      39 c3             cmp     %eax,%ebx
8048927:      76 1f             jbe     8048948 <__do_global_dtors_aux+0x48>
8048929:      8d b4 26 00 00 00 00 lea     0x0(%esi),%esi
8048930:      83 c0 01          add     $0x1,%eax
8048933:      a3 b0 a1 04 08    mov     %eax,0x804a1b0
8048938:      ff 14 85 08 a0 04 08 call    *0x804a008(,%eax,4)
804893f:      a1 b0 a1 04 08    mov     0x804a1b0,%eax
8048944:      39 c3             cmp     %eax,%ebx
8048946:      77 e8             ja      8048930 <__do_global_dtors_aux+0x30>
8048948:      c6 05 b4 a1 04 08 01 movb    $0x1,0x804a1b4
804894f:      83 c4 04          add     $0x4,%esp
8048952:      5b                pop     %ebx
8048953:      5d                pop     %ebp
8048954:      c3                ret
8048955:      8d 74 26 00       lea     0x0(%esi),%esi
8048959:      8d bc 27 00 00 00 00 lea     0x0(%edi),%edi

08048960 <frame_dummy>:
8048960:      55                push   %ebp
8048961:      89 e5             mov     %esp,%ebp
8048963:      83 ec 08          sub     $0x8,%esp
8048966:      a1 10 a0 04 08    mov     0x804a010,%eax
804896b:      85 c0             test    %eax,%eax
804896d:      74 12             je      8048981 <frame_dummy+0x21>
804896f:      b8 00 00 00 00    mov     $0x0,%eax
8048974:      85 c0             test    %eax,%eax
8048976:      74 09             je      8048981 <frame_dummy+0x21>
8048978:      c7 04 24 10 a0 04 08 movl    $0x804a010,(%esp)
804897f:      ff d0             call    *%eax
8048981:      c9                leave
8048982:      c3                ret
8048983:      90                nop
8048984:      90                nop
8048985:      90                nop
8048986:      90                nop
8048987:      90                nop
8048988:      90                nop
8048989:      90                nop
804898a:      90                nop
804898b:      90                nop
804898c:      90                nop
804898d:      90                nop
804898e:      90                nop
804898f:      90                nop

```

```

08048990 <save_char>:

```

```

8048990:      8b 0d e4 a1 04 08      mov     0x804a1e4,%ecx
8048996:      55                    push    %ebp
8048997:      89 e5                mov     %esp,%ebp
8048999:      53                    push    %ebx
804899a:      89 c3                mov     %eax,%ebx
804899c:      81 f9 ff 03 00 00      cmp     $0x3ff,%ecx
80489a2:      7f 37                jg      80489db <save_char+0x4b>
80489a4:      c0 f8 04            sar     $0x4,%al
80489a7:      83 e0 0f            and     $0xf,%eax
80489aa:      0f b6 80 4c 9c 04 08    movzbl 0x8049c4c(%eax),%eax
80489b1:      8d 14 49            lea     (%ecx,%ecx,2),%edx
80489b4:      c6 82 02 a2 04 08 20    movb    $0x20,0x804a202(%edx)
80489bb:      88 82 00 a2 04 08      mov     %al,0x804a200(%edx)
80489c1:      89 d8                mov     %ebx,%eax
80489c3:      83 e0 0f            and     $0xf,%eax
80489c6:      0f b6 80 4c 9c 04 08    movzbl 0x8049c4c(%eax),%eax
80489cd:      88 82 01 a2 04 08      mov     %al,0x804a201(%edx)
80489d3:      8d 41 01            lea     0x1(%ecx),%eax
80489d6:      a3 e4 a1 04 08      mov     %eax,0x804a1e4
80489db:      5b                    pop     %ebx
80489dc:      5d                    pop     %ebp
80489dd:      c3                    ret
80489de:      66 90                xchg    %ax,%ax

```

080489e0 <entry_check>:

```

80489e0:      55                    push    %ebp
80489e1:      89 e5                mov     %esp,%ebp
80489e3:      8b 45 08            mov     0x8(%ebp),%eax
80489e6:      5d                    pop     %ebp
80489e7:      a3 6c a1 04 08      mov     %eax,0x804a16c
80489ec:      c3                    ret
80489ed:      8d 76 00            lea     0x0(%esi),%esi

```

080489f0 <illegalhandler>:

```

80489f0:      55                    push    %ebp
80489f1:      89 e5                mov     %esp,%ebp
80489f3:      83 ec 08            sub     $0x8,%esp
80489f6:      c7 04 24 80 96 04 08    movl    $0x8049680,(%esp)
80489fd:      e8 4e fe ff ff      call    8048850 <puts@plt>
8048a02:      c7 04 24 18 9a 04 08    movl    $0x8049a18,(%esp)
8048a09:      e8 42 fe ff ff      call    8048850 <puts@plt>
8048a0e:      c7 04 24 00 00 00 00    movl    $0x0,(%esp)
8048a15:      e8 86 fe ff ff      call    80488a0 <exit@plt>
8048a1a:      8d b6 00 00 00 00      lea     0x0(%esi),%esi

```

08048a20 <alarmhandler>:

```

8048a20:      55                    push    %ebp
8048a21:      89 e5                mov     %esp,%ebp
8048a23:      83 ec 08            sub     $0x8,%esp
8048a26:      a1 70 a1 04 08      mov     0x804a170,%eax
8048a2b:      c7 04 24 ac 96 04 08    movl    $0x80496ac,(%esp)
8048a32:      89 44 24 04          mov     %eax,0x4(%esp)
8048a36:      e8 a5 fd ff ff      call    80487e0 <printf@plt>
8048a3b:      c7 04 24 18 9a 04 08    movl    $0x8049a18,(%esp)
8048a42:      e8 09 fe ff ff      call    8048850 <puts@plt>
8048a47:      c7 04 24 00 00 00 00    movl    $0x0,(%esp)
8048a4e:      e8 4d fe ff ff      call    80488a0 <exit@plt>
8048a53:      8d b6 00 00 00 00      lea     0x0(%esi),%esi
8048a59:      8d bc 27 00 00 00 00    lea     0x0(%edi),%edi

```

08048a60 <seghandler>:

```

8048a60:      55                    push    %ebp
8048a61:      89 e5                mov     %esp,%ebp
8048a63:      83 ec 08            sub     $0x8,%esp
8048a66:      c7 04 24 e0 96 04 08    movl    $0x80496e0,(%esp)
8048a6d:      e8 de fd ff ff      call    8048850 <puts@plt>
8048a72:      c7 04 24 18 9a 04 08    movl    $0x8049a18,(%esp)
8048a79:      e8 d2 fd ff ff      call    8048850 <puts@plt>

```

```

8048a7e:      c7 04 24 00 00 00 00      movl    $0x0,(%esp)
8048a85:      e8 16 fe ff ff            call    80488a0 <exit@plt>
8048a8a:      8d b6 00 00 00 00        lea     0x0(%esi),%esi

08048a90 <bushandler>:
8048a90:      55                        push    %ebp
8048a91:      89 e5                    mov     %esp,%ebp
8048a93:      83 ec 08                sub     $0x8,%esp
8048a96:      c7 04 24 08 97 04 08    movl    $0x8049708,(%esp)
8048a9d:      e8 ae fd ff ff          call    8048850 <puts@plt>
8048aa2:      c7 04 24 18 9a 04 08    movl    $0x8049a18,(%esp)
8048aa9:      e8 a2 fd ff ff          call    8048850 <puts@plt>
8048aae:      c7 04 24 00 00 00 00    movl    $0x0,(%esp)
8048ab5:      e8 e6 fd ff ff          call    80488a0 <exit@plt>
8048aba:      8d b6 00 00 00 00        lea     0x0(%esi),%esi

08048ac0 <usage>:
8048ac0:      55                        push    %ebp
8048ac1:      89 e5                    mov     %esp,%ebp
8048ac3:      83 ec 08                sub     $0x8,%esp
8048ac6:      89 44 24 04            mov     %eax,0x4(%esp)
8048aca:      c7 04 24 28 97 04 08    movl    $0x8049728,(%esp)
8048ad1:      e8 0a fd ff ff          call    80487e0 <printf@plt>
8048ad6:      c7 04 24 2e 9a 04 08    movl    $0x8049a2e,(%esp)
8048add:      e8 6e fd ff ff          call    8048850 <puts@plt>
8048ae2:      c7 04 24 4c 9a 04 08    movl    $0x8049a4c,(%esp)
8048ae9:      e8 62 fd ff ff          call    8048850 <puts@plt>
8048aee:      c7 04 24 4c 97 04 08    movl    $0x804974c,(%esp)
8048af5:      e8 56 fd ff ff          call    8048850 <puts@plt>
8048afa:      c7 04 24 74 97 04 08    movl    $0x8049774,(%esp)
8048b01:      e8 4a fd ff ff          call    8048850 <puts@plt>
8048b06:      c7 04 24 00 00 00 00    movl    $0x0,(%esp)
8048b0d:      e8 8e fd ff ff          call    80488a0 <exit@plt>
8048b12:      8d b4 26 00 00 00 00    lea     0x0(%esi),%esi
8048b19:      8d bc 27 00 00 00 00    lea     0x0(%edi),%edi

08048b20 <validate>:
8048b20:      55                        push    %ebp
8048b21:      89 e5                    mov     %esp,%ebp
8048b23:      81 ec 48 01 00 00      sub     $0x148,%esp
8048b29:      8b 0d d4 a1 04 08      mov     0x804a1d4,%ecx
8048b2f:      89 5d f4                mov     %ebx,0xffffffff4(%ebp)
8048b32:      8b 5d 08                mov     0x8(%ebp),%ebx
8048b35:      89 75 f8                mov     %esi,0xffffffff8(%ebp)
8048b38:      89 7d fc                mov     %edi,0xfffffffffc(%ebp)
8048b3b:      85 c9                    test    %ecx,%ecx
8048b3d:      0f 84 d8 01 00 00      je      8048d1b <validate+0x1fb>
8048b43:      83 fb 04                cmp     $0x4,%ebx
8048b46:      77 58                    ja      8048ba0 <validate+0x80>
8048b48:      3b 1d 6c a1 04 08      cmp     0x804a16c,%ebx
8048b4e:      74 20                    je      8048b70 <validate+0x50>
8048b50:      c7 04 24 ec 97 04 08    movl    $0x80497ec,(%esp)
8048b57:      e8 f4 fc ff ff          call    8048850 <puts@plt>
8048b5c:      8d 74 26 00            lea     0x0(%esi),%esi
8048b60:      8b 5d f4                mov     0xffffffff4(%ebp),%ebx
8048b63:      8b 75 f8                mov     0xffffffff8(%ebp),%esi
8048b66:      8b 7d fc                mov     0xfffffffffc(%ebp),%edi
8048b69:      89 ec                    mov     %ebp,%esp
8048b6b:      5d                        pop     %ebp
8048b6c:      c3                        ret
8048b6d:      8d 76 00                lea     0x0(%esi),%esi
8048b70:      8b 04 9d 74 a1 04 08    mov     0x804a174(,%ebx,4),%eax
8048b77:      c7 05 dc a1 04 08 01    movl    $0x1,0x804a1dc
8048b7e:      00 00 00
8048b81:      83 e8 01                sub     $0x1,%eax
8048b84:      85 c0                    test    %eax,%eax
8048b86:      89 04 9d 74 a1 04 08    mov     %eax,0x804a174(,%ebx,4)
8048b8d:      7e 21                    jle     8048bb0 <validate+0x90>

```

8048b8f:	c7 04 24 63 9a 04 08	movl	\$0x8049a63, (%esp)
8048b96:	e8 b5 fc ff ff	call	8048850 <puts@plt>
8048b9b:	eb c3	jmp	8048b60 <validate+0x40>
8048b9d:	8d 76 00	lea	0x0(%esi), %esi
8048ba0:	c7 04 24 c4 97 04 08	movl	\$0x80497c4, (%esp)
8048ba7:	e8 a4 fc ff ff	call	8048850 <puts@plt>
8048bac:	eb b2	jmp	8048b60 <validate+0x40>
8048bae:	66 90	xchg	%ax, %ax
8048bb0:	8b 15 d8 a1 04 08	mov	0x804a1d8, %edx
8048bb6:	85 d2	test	%edx, %edx
8048bb8:	0f 85 7f 01 00 00	jne	8048d3d <validate+0x21d>
8048bbe:	a1 68 a1 04 08	mov	0x804a168, %eax
8048bc3:	85 c0	test	%eax, %eax
8048bc5:	0f 84 61 01 00 00	je	8048d2c <validate+0x20c>
8048bcb:	c7 44 24 04 74 9a 04	movl	\$0x8049a74, 0x4(%esp)
8048bd2:	08		
8048bd3:	c7 04 24 00 00 00 00	movl	\$0x0, (%esp)
8048bda:	e8 a1 fc ff ff	call	8048880 <tempnam@plt>
8048bdf:	c7 44 24 04 7b 9a 04	movl	\$0x8049a7b, 0x4(%esp)
8048be6:	08		
8048be7:	89 85 e0 fe ff ff	mov	%eax, 0xfffffee0(%ebp)
8048bed:	89 04 24	mov	%eax, (%esp)
8048bf0:	e8 bb fb ff ff	call	80487b0 <fopen@plt>
8048bf5:	85 c0	test	%eax, %eax
8048bf7:	89 c6	mov	%eax, %esi
8048bf9:	0f 84 76 01 00 00	je	8048d75 <validate+0x255>
8048bff:	89 44 24 0c	mov	%eax, 0xc(%esp)
8048c03:	c7 44 24 08 1b 00 00	movl	\$0x1b, 0x8(%esp)
8048c0a:	00		
8048c0b:	c7 44 24 04 01 00 00	movl	\$0x1, 0x4(%esp)
8048c12:	00		
8048c13:	c7 04 24 7d 9a 04 08	movl	\$0x8049a7d, (%esp)
8048c1a:	e8 e1 fb ff ff	call	8048800 <fwrite@plt>
8048c1f:	89 74 24 04	mov	%esi, 0x4(%esp)
8048c23:	c7 04 24 0a 00 00 00	movl	\$0xa, (%esp)
8048c2a:	e8 11 fc ff ff	call	8048840 <putc@plt>
8048c2f:	c7 04 24 00 00 00 00	movl	\$0x0, (%esp)
8048c36:	e8 f5 fb ff ff	call	8048830 <userid@plt>
8048c3b:	85 c0	test	%eax, %eax
8048c3d:	0f 84 19 01 00 00	je	8048d5c <validate+0x23c>
8048c43:	8d 7d eb	lea	0xffffffe0(%ebp), %edi
8048c46:	89 44 24 04	mov	%eax, 0x4(%esp)
8048c4a:	89 3c 24	mov	%edi, (%esp)
8048c4d:	e8 7e fb ff ff	call	80487d0 <strcpy@plt>
8048c52:	89 7c 24 08	mov	%edi, 0x8(%esp)
8048c56:	c7 44 24 04 99 9a 04	movl	\$0x8049a99, 0x4(%esp)
8048c5d:	08		
8048c5e:	89 34 24	mov	%esi, (%esp)
8048c61:	e8 aa fb ff ff	call	8048810 <fprintf@plt>
8048c66:	a1 d0 a1 04 08	mov	0x804a1d0, %eax
8048c6b:	89 5c 24 10	mov	%ebx, 0x10(%esp)
8048c6f:	8d 9d eb fe ff ff	lea	0xfffffeeb(%ebp), %ebx
8048c75:	c7 44 24 1c 00 00 00	movl	\$0x0, 0x1c(%esp)
8048c7c:	00		
8048c7d:	c7 44 24 18 00 a2 04	movl	\$0x804a200, 0x18(%esp)
8048c84:	08		
8048c85:	89 44 24 14	mov	%eax, 0x14(%esp)
8048c89:	a1 d4 a1 04 08	mov	0x804a1d4, %eax
8048c8e:	c7 44 24 08 0a 7d 00	movl	\$0x7d0a, 0x8(%esp)
8048c95:	00		
8048c96:	c7 44 24 04 5c 98 04	movl	\$0x804985c, 0x4(%esp)
8048c9d:	08		
8048c9e:	89 34 24	mov	%esi, (%esp)
8048ca1:	89 44 24 0c	mov	%eax, 0xc(%esp)
8048ca5:	e8 66 fb ff ff	call	8048810 <fprintf@plt>
8048caa:	89 34 24	mov	%esi, (%esp)
8048cad:	e8 de fa ff ff	call	8048790 <fclose@plt>
8048cb2:	8b 85 e0 fe ff ff	mov	0xfffffee0(%ebp), %eax

```

8048cb8: c7 44 24 14 a7 9a 04 movl $0x8049aa7,0x14(%esp)
8048cbf: 08
8048cc0: c7 44 24 10 b5 9a 04 movl $0x8049ab5,0x10(%esp)
8048cc7: 08
8048cc8: c7 44 24 0c bc 9a 04 movl $0x8049abc,0xc(%esp)
8048ccf: 08
8048cd0: 89 44 24 08 mov %eax,0x8(%esp)
8048cd4: c7 44 24 04 d3 9a 04 movl $0x8049ad3,0x4(%esp)
8048cdb: 08
8048cdc: 89 1c 24 mov %ebx,(%esp)
8048cdf: e8 ec f9 ff ff call 80486d0 <sprintf@plt>
8048ce4: 89 1c 24 mov %ebx,(%esp)
8048ce7: e8 54 fa ff ff call 8048740 <system@plt>
8048cec: 85 c0 test %eax,%eax
8048cee: 75 5e jne 8048d4e <validate+0x22e>
8048cf0: c7 04 24 e6 9a 04 08 movl $0x8049ae6,(%esp)
8048cf7: e8 54 fb ff ff call 8048850 <puts@plt>
8048cfc: c7 04 24 7c 98 04 08 movl $0x804987c,(%esp)
8048d03: e8 48 fb ff ff call 8048850 <puts@plt>
8048d08: 8b 85 e0 fe ff ff mov 0xffffffff0(%ebp),%eax
8048d0e: 89 04 24 mov %eax,(%esp)
8048d11: e8 0a fb ff ff call 8048820 <remove@plt>
8048d16: e9 45 fe ff ff jmp 8048b60 <validate+0x40>
8048d1b: c7 04 24 98 97 04 08 movl $0x8049798,(%esp)
8048d22: e8 29 fb ff ff call 8048850 <puts@plt>
8048d27: e9 34 fe ff ff jmp 8048b60 <validate+0x40>
8048d2c: c7 04 24 ec 98 04 08 movl $0x80498ec,(%esp)
8048d33: e8 18 fb ff ff call 8048850 <puts@plt>
8048d38: e9 23 fe ff ff jmp 8048b60 <validate+0x40>
8048d3d: c7 04 24 6e 9a 04 08 movl $0x8049a6e,(%esp)
8048d44: e8 07 fb ff ff call 8048850 <puts@plt>
8048d49: e9 12 fe ff ff jmp 8048b60 <validate+0x40>
8048d4e: c7 04 24 ac 98 04 08 movl $0x80498ac,(%esp)
8048d55: e8 f6 fa ff ff call 8048850 <puts@plt>
8048d5a: eb ac jmp 8048d08 <validate+0x1e8>
8048d5c: 8d 7d eb lea 0xffffffff0(%ebp),%edi
8048d5f: c7 45 eb 6e 6f 62 6f movl $0x6f626f6e,0xffffffff0(%ebp)
8048d66: 66 c7 45 ef 64 79 movw $0x7964,0xffffffff0(%ebp)
8048d6c: c6 45 f1 00 movb $0x0,0xffffffff1(%ebp)
8048d70: e9 dd fe ff ff jmp 8048c52 <validate+0x132>
8048d75: c7 04 24 28 98 04 08 movl $0x8049828,(%esp)
8048d7c: e8 5f fa ff ff call 80487e0 <printf@plt>
8048d81: c7 04 24 01 00 00 00 movl $0x1,(%esp)
8048d88: e8 13 fb ff ff call 80488a0 <exit@plt>
8048d8d: 8d 76 00 lea 0x0(%esi),%esi

```

08048d90 <bang>:

```

8048d90: 55 push %ebp
8048d91: 89 e5 mov %esp,%ebp
8048d93: 83 ec 08 sub $0x8,%esp
8048d96: c7 04 24 02 00 00 00 movl $0x2,(%esp)
8048d9d: e8 3e fc ff ff call 80489e0 <entry_check>
8048da2: a1 e0 a1 04 08 mov 0x804a1e0,%eax
8048da7: 3b 05 d0 a1 04 08 cmp 0x804a1d0,%eax
8048dad: 74 21 je 8048dd0 <bang+0x40>
8048daf: 89 44 24 04 mov %eax,0x4(%esp)
8048db3: c7 04 24 f0 9a 04 08 movl $0x8049af0,(%esp)
8048dba: e8 21 fa ff ff call 80487e0 <printf@plt>
8048dbf: c7 04 24 00 00 00 00 movl $0x0,(%esp)
8048dc6: e8 d5 fa ff ff call 80488a0 <exit@plt>
8048dcb: 90 nop
8048dcc: 8d 74 26 00 lea 0x0(%esi),%esi
8048dd0: 89 44 24 04 mov %eax,0x4(%esp)
8048dd4: c7 04 24 38 99 04 08 movl $0x8049938,(%esp)
8048ddb: e8 00 fa ff ff call 80487e0 <printf@plt>
8048de0: c7 04 24 02 00 00 00 movl $0x2,(%esp)
8048de7: e8 34 fd ff ff call 8048b20 <validate>
8048dec: eb d1 jmp 8048dbf <bang+0x2f>

```



```

8048dee:      66 90          xchg  %ax,%ax

08048df0 <fizz>:
8048df0:      55              push  %ebp
8048df1:      89 e5          mov   %esp,%ebp
8048df3:      53              push  %ebx
8048df4:      83 ec 14       sub   $0x14,%esp
8048df7:      8b 5d 08       mov   0x8(%ebp),%ebx
8048dfa:      c7 04 24 01 00 00 00 movl  $0x1,(%esp)
8048e01:      e8 da fb ff ff call  80489e0 <entry_check>
8048e06:      3b 1d d0 a1 04 08 cmp   0x804a1d0,%ebx
8048e0c:      74 22          je    8048e30 <fizz+0x40>
8048e0e:      89 5c 24 04       mov   %ebx,0x4(%esp)
8048e12:      c7 04 24 60 99 04 08 movl  $0x8049960,(%esp)
8048e19:      e8 c2 f9 ff ff call  80487e0 <printf@plt>
8048e1e:      c7 04 24 00 00 00 00 movl  $0x0,(%esp)
8048e25:      e8 76 fa ff ff call  80488a0 <exit@plt>
8048e2a:      8d b6 00 00 00 00 lea   0x0(%esi),%esi
8048e30:      89 5c 24 04       mov   %ebx,0x4(%esp)
8048e34:      c7 04 24 0e 9b 04 08 movl  $0x8049b0e,(%esp)
8048e3b:      e8 a0 f9 ff ff call  80487e0 <printf@plt>
8048e40:      c7 04 24 01 00 00 00 movl  $0x1,(%esp)
8048e47:      e8 d4 fc ff ff call  8048b20 <validate>
8048e4c:      eb d0          jmp   8048e1e <fizz+0x2e>
8048e4e:      66 90          xchg  %ax,%ax

08048e50 <smoke>:
8048e50:      55              push  %ebp
8048e51:      89 e5          mov   %esp,%ebp
8048e53:      83 ec 08       sub   $0x8,%esp
8048e56:      c7 04 24 00 00 00 00 movl  $0x0,(%esp)
8048e5d:      e8 7e fb ff ff call  80489e0 <entry_check>
8048e62:      c7 04 24 2c 9b 04 08 movl  $0x8049b2c,(%esp)
8048e69:      e8 e2 f9 ff ff call  8048850 <puts@plt>
8048e6e:      c7 04 24 00 00 00 00 movl  $0x0,(%esp)
8048e75:      e8 a6 fc ff ff call  8048b20 <validate>
8048e7a:      c7 04 24 00 00 00 00 movl  $0x0,(%esp)
8048e81:      e8 1a fa ff ff call  80488a0 <exit@plt>
8048e86:      8d 76 00       lea   0x0(%esi),%esi
8048e89:      8d bc 27 00 00 00 00 lea   0x0(%edi),%edi

08048e90 <Gets>:
8048e90:      55              push  %ebp
8048e91:      89 e5          mov   %esp,%ebp
8048e93:      57              push  %edi
8048e94:      56              push  %esi
8048e95:      53              push  %ebx
8048e96:      83 ec 0c       sub   $0xc,%esp
8048e99:      8b 1d cc a1 04 08 mov   0x804a1cc,%ebx
8048e9f:      c7 05 e4 a1 04 08 00 movl  $0x0,0x804a1e4
8048ea6:      00 00 00
8048ea9:      8b 75 08       mov   0x8(%ebp),%esi
8048eac:      85 db          test  %ebx,%ebx
8048eae:      74 72          je    8048f22 <Gets+0x92>
8048eb0:      bf 01 00 00 00 00 mov   $0x1,%edi
8048eb5:      c7 45 f0 00 00 00 00 movl  $0x0,0xffffffff(%ebp)
8048ebc:      8d 74 26 00     lea   0x0(%esi),%esi
8048ec0:      a1 c0 a1 04 08 mov   0x804a1c0,%eax
8048ec5:      89 04 24       mov   %eax,(%esp)
8048ec8:      e8 a3 f8 ff ff call  8048770 <_IO_getc@plt>
8048ecd:      83 f8 ff       cmp   $0xffffffff,%eax
8048ed0:      89 c3          mov   %eax,%ebx
8048ed2:      74 60          je    8048f34 <Gets+0xa4>
8048ed4:      83 f8 0a       cmp   $0xa,%eax
8048ed7:      74 5b          je    8048f34 <Gets+0xa4>
8048ed9:      e8 a2 f8 ff ff call  8048780 <__ctype_b_loc@plt>
8048ede:      8b 00          mov   (%eax),%eax
8048ee0:      f6 44 58 01 10 testb $0x10,0x1(%eax,%ebx,2)

```

```

8048ee5: 74 d9      je      8048ec0 <Gets+0x30>
8048ee7: 8d 43 d0   lea     0xffffffff0(%ebx),%eax
8048eea: 83 f8 09   cmp     $0x9,%eax
8048eed: 89 c2      mov     %eax,%edx
8048eef: 76 0f      jbe     8048f00 <Gets+0x70>
8048ef1: 8d 43 bf   lea     0xffffffffbf(%ebx),%eax
8048ef4: 83 f8 05   cmp     $0x5,%eax
8048ef7: 8d 53 c9   lea     0xffffffffc9(%ebx),%edx
8048efa: 76 04      jbe     8048f00 <Gets+0x70>
8048efc: 8d 53 a9   lea     0xffffffffa9(%ebx),%edx
8048eff: 90         nop
8048f00: 85 ff      test    %edi,%edi
8048f02: 74 4c      je      8048f50 <Gets+0xc0>
8048f04: 31 ff      xor     %edi,%edi
8048f06: 89 55 f0   mov     %edx,0xffffffff0(%ebp)
8048f09: eb b5      jmp     8048ec0 <Gets+0x30>
8048f0b: 90         nop
8048f0c: 8d 74 26 00 lea     0x0(%esi),%esi
8048f10: 83 f8 0a   cmp     $0xa,%eax
8048f13: 74 1f      je      8048f34 <Gets+0xa4>
8048f15: 88 06      mov     %al,(%esi)
8048f17: 0f be c0   movsbl  %al,%eax
8048f1a: 83 c6 01   add     $0x1,%esi
8048f1d: e8 6e fa ff ff call    8048990 <save_char>
8048f22: a1 c0 a1 04 08 mov     0x804a1c0,%eax
8048f27: 89 04 24   mov     %eax,(%esp)
8048f2a: e8 41 f8 ff ff call    8048770 <_IO_getc@plt>
8048f2f: 83 f8 ff   cmp     $0xffffffff,%eax
8048f32: 75 dc      jne     8048f10 <Gets+0x80>
8048f34: c6 06 00   movb    $0x0,(%esi)
8048f37: a1 e4 a1 04 08 mov     0x804a1e4,%eax
8048f3c: c6 84 40 00 a2 04 08 movb    $0x0,0x804a200(%eax,%eax,2)
8048f43: 00
8048f44: 8b 45 08   mov     0x8(%ebp),%eax
8048f47: 83 c4 0c   add     $0xc,%esp
8048f4a: 5b        pop     %ebx
8048f4b: 5e        pop     %esi
8048f4c: 5f        pop     %edi
8048f4d: 5d        pop     %ebp
8048f4e: c3        ret
8048f4f: 90         nop
8048f50: 8b 45 f0   mov     0xffffffff0(%ebp),%eax
8048f53: bf 01 00 00 00 mov     $0x1,%edi
8048f58: c1 e0 04   shl     $0x4,%eax
8048f5b: 8d 04 02   lea     (%edx,%eax,1),%eax
8048f5e: 88 06      mov     %al,(%esi)
8048f60: 0f be c0   movsbl  %al,%eax
8048f63: 83 c6 01   add     $0x1,%esi
8048f66: e8 25 fa ff ff call    8048990 <save_char>
8048f6b: e9 50 ff ff ff jmp     8048ec0 <Gets+0x30>

```

08048f70 <getbufn>:

```

8048f70: 55        push    %ebp
8048f71: 89 e5     mov     %esp,%ebp
8048f73: 81 ec 08 02 00 00 sub     $0x208,%esp
8048f79: 8d 85 00 fe ff ff lea     0xfffffe00(%ebp),%eax
8048f7f: 89 04 24   mov     %eax,(%esp)
8048f82: e8 09 ff ff ff call    8048e90 <Gets>
8048f87: b8 01 00 00 00 mov     $0x1,%eax
8048f8c: c9        leave  %eax
8048f8d: c3        ret
8048f8e: 66 90     xchg    %ax,%ax

```

08048f90 <testn>:

```

8048f90: 55        push    %ebp
8048f91: 89 e5     mov     %esp,%ebp
8048f93: 83 ec 18   sub     $0x18,%esp
8048f96: c7 45 fc ef be ad de movl    $0xdeadbeef,0xffffffffc(%ebp)

```

```

8048f9d:    c7 04 24 04 00 00 00    movl    $0x4, (%esp)
8048fa4:    e8 37 fa ff ff          call    80489e0 <entry_check>
8048fa9:    e8 c2 ff ff ff          call    8048f70 <getbuf>
8048fae:    89 c2                   mov     %eax, %edx
8048fb0:    8b 45 fc                mov     0xffffffff(%ebp), %eax
8048fb3:    3d ef be ad de          cmp     $0xdeadbeef, %eax
8048fb8:    74 0e                   je      8048fc8 <testn+0x38>
8048fba:    c7 04 24 80 99 04 08    movl    $0x8049980, (%esp)
8048fc1:    e8 8a f8 ff ff          call    8048850 <puts@plt>
8048fc6:    c9                     leave
8048fc7:    c3                     ret
8048fc8:    3b 15 d0 a1 04 08       cmp     0x804a1d0, %edx
8048fce:    74 12                   je      8048fe2 <testn+0x52>
8048fd0:    89 54 24 04            mov     %edx, 0x4(%esp)
8048fd4:    c7 04 24 47 9b 04 08    movl    $0x8049b47, (%esp)
8048fdb:    e8 00 f8 ff ff          call    80487e0 <printf@plt>
8048fe0:    c9                     leave
8048fe1:    c3                     ret
8048fe2:    89 54 24 04            mov     %edx, 0x4(%esp)
8048fe6:    c7 04 24 ac 99 04 08    movl    $0x80499ac, (%esp)
8048fed:    e8 ee f7 ff ff          call    80487e0 <printf@plt>
8048ff2:    c7 04 24 04 00 00 00    movl    $0x4, (%esp)
8048ff9:    e8 22 fb ff ff          call    8048b20 <validate>
8048ffe:    c9                     leave
8048fff:    c3                     ret

08049000 <getbuf>:
8049000:    55                     push    %ebp
8049001:    89 e5                 mov     %esp, %ebp
8049003:    83 ec 18              sub     $0x18, %esp
8049006:    8d 45 f4              lea     0xffffffff(%ebp), %eax
8049009:    89 04 24              mov     %eax, (%esp)
804900c:    e8 7f fe ff ff          call    8048e90 <gets>
8049011:    b8 01 00 00 00        mov     $0x1, %eax
8049016:    c9                     leave
8049017:    c3                     ret
8049018:    90                     nop
8049019:    8d b4 26 00 00 00 00    lea     0x0(%esi), %esi

08049020 <test>:
8049020:    55                     push    %ebp
8049021:    89 e5                 mov     %esp, %ebp
8049023:    83 ec 18              sub     $0x18, %esp
8049026:    c7 45 fc ef be ad de    movl    $0xdeadbeef, 0xffffffff(%ebp)
804902d:    c7 04 24 03 00 00 00    movl    $0x3, (%esp)
8049034:    e8 a7 f9 ff ff          call    80489e0 <entry_check>
8049039:    e8 c2 ff ff ff          call    8049000 <getbuf>
804903e:    89 c2                   mov     %eax, %edx
8049040:    8b 45 fc                mov     0xffffffff(%ebp), %eax
8049043:    3d ef be ad de          cmp     $0xdeadbeef, %eax
8049048:    74 0e                   je      8049058 <test+0x38>
804904a:    c7 04 24 80 99 04 08    movl    $0x8049980, (%esp)
8049051:    e8 fa f7 ff ff          call    8048850 <puts@plt>
8049056:    c9                     leave
8049057:    c3                     ret
8049058:    3b 15 d0 a1 04 08       cmp     0x804a1d0, %edx
804905e:    74 12                   je      8049072 <test+0x52>
8049060:    89 54 24 04            mov     %edx, 0x4(%esp)
8049064:    c7 04 24 80 9b 04 08    movl    $0x8049b80, (%esp)
804906b:    e8 70 f7 ff ff          call    80487e0 <printf@plt>
8049070:    c9                     leave
8049071:    c3                     ret
8049072:    89 54 24 04            mov     %edx, 0x4(%esp)
8049076:    c7 04 24 63 9b 04 08    movl    $0x8049b63, (%esp)
804907d:    e8 5e f7 ff ff          call    80487e0 <printf@plt>
8049082:    c7 04 24 03 00 00 00    movl    $0x3, (%esp)
8049089:    e8 92 fa ff ff          call    8048b20 <validate>
804908e:    c9                     leave

```

```

804908f:      c3          ret

08049090 <launch>:
8049090:      55          push    %ebp
8049091:      89 e5      mov     %esp,%ebp
8049093:      83 ec 58    sub     $0x58,%esp
8049096:      89 7d fc    mov     %edi,0xffffffffc(%ebp)
8049099:      89 c7      mov     %eax,%edi
804909b:      a1 c8 a1 04 08 mov     0x804a1c8,%eax
80490a0:      89 5d f4    mov     %ebx,0xffffffff4(%ebp)
80490a3:      8d 5d b4    lea     0xffffffffb4(%ebp),%ebx
80490a6:      89 75 f8    mov     %esi,0xffffffff8(%ebp)
80490a9:      89 d6      mov     %edx,%esi
80490ab:      85 c0      test    %eax,%eax
80490ad:      0f 85 9d 00 00 00 jne     8049150 <launch+0xc0>
80490b3:      81 e3 f8 3f 00 00 and     $0x3ff8,%ebx
80490b9:      8d 04 1e    lea     (%esi,%ebx,1),%eax
80490bc:      8d 50 1e    lea     0x1e(%eax),%edx
80490bf:      83 e2 f0    and     $0xfffffffff0,%edx
80490c2:      29 d4      sub     %edx,%esp
80490c4:      8d 54 24 1b lea     0x1b(%esp),%edx
80490c8:      83 e2 f0    and     $0xfffffffff0,%edx
80490cb:      89 44 24 08 mov     %eax,0x8(%esp)
80490cf:      c7 44 24 04 f4 00 00 movl    $0xf4,0x4(%esp)
80490d6:      00
80490d7:      89 14 24    mov     %edx,(%esp)
80490da:      e8 71 f6 ff ff call    8048750 <memset@plt>
80490df:      a1 c4 a1 04 08 mov     0x804a1c4,%eax
80490e4:      85 c0      test    %eax,%eax
80490e6:      75 18      jne     8049100 <launch+0x70>
80490e8:      a1 cc a1 04 08 mov     0x804a1cc,%eax
80490ed:      85 c0      test    %eax,%eax
80490ef:      75 4f      jne     8049140 <launch+0xb0>
80490f1:      c7 04 24 bc 9b 04 08 movl    $0x8049bbc,(%esp)
80490f8:      e8 e3 f6 ff ff call    80487e0 <printf@plt>
80490fd:      8d 76 00    lea     0x0(%esi),%esi
8049100:      85 ff      test    %edi,%edi
8049102:      74 32      je      8049136 <launch+0xa6>
8049104:      e8 87 fe ff ff call    8048f90 <testn>
8049109:      8b 35 dc a1 04 08 mov     0x804a1dc,%esi
804910f:      85 f6      test    %esi,%esi
8049111:      75 16      jne     8049129 <launch+0x99>
8049113:      c7 04 24 18 9a 04 08 movl    $0x8049a18,(%esp)
804911a:      e8 31 f7 ff ff call    8048850 <puts@plt>
804911f:      c7 05 dc a1 04 08 00 movl    $0x0,0x804a1dc
8049126:      00 00 00
8049129:      8b 5d f4    mov     0xffffffff4(%ebp),%ebx
804912c:      8b 75 f8    mov     0xffffffff8(%ebp),%esi
804912f:      8b 7d fc    mov     0xffffffffc(%ebp),%edi
8049132:      89 ec      mov     %ebp,%esp
8049134:      5d        pop     %ebp
8049135:      c3        ret
8049136:      e8 e5 fe ff ff call    8049020 <test>
804913b:      eb cc      jmp     8049109 <launch+0x79>
804913d:      8d 76 00    lea     0x0(%esi),%esi
8049140:      c7 04 24 ab 9b 04 08 movl    $0x8049bab,(%esp)
8049147:      e8 94 f6 ff ff call    80487e0 <printf@plt>
804914c:      eb b2      jmp     8049100 <launch+0x70>
804914e:      66 90      xchg    %ax,%ax
8049150:      a1 a8 a1 04 08 mov     0x804a1a8,%eax
8049155:      89 5c 24 08 mov     %ebx,0x8(%esp)
8049159:      c7 44 24 04 9b 9b 04 movl    $0x8049b9b,0x4(%esp)
8049160:      08
8049161:      89 04 24    mov     %eax,(%esp)
8049164:      e8 a7 f6 ff ff call    8048810 <fprintf@plt>
8049169:      e9 45 ff ff ff jmp     80490b3 <launch+0x23>
804916e:      66 90      xchg    %ax,%ax

```

```

08049170 <launcher>:
8049170:      55                push    %ebp
8049171:      89 e5             mov     %esp,%ebp
8049173:      53                push    %ebx
8049174:      83 ec 24           sub     $0x24,%esp
8049177:      8b 45 08           mov     0x8(%ebp),%eax
804917a:      a3 e8 a1 04 08     mov     %eax,0x804a1e8
804917f:      8b 45 0c           mov     0xc(%ebp),%eax
8049182:      c7 44 24 14 00 00 00 movl    $0x0,0x14(%esp)
8049189:      00
804918a:      c7 44 24 10 00 00 00 movl    $0x0,0x10(%esp)
8049191:      00
8049192:      c7 44 24 0c 22 01 00 movl    $0x122,0xc(%esp)
8049199:      00
804919a:      a3 ec a1 04 08     mov     %eax,0x804a1ec
804919f:      c7 44 24 08 07 00 00 movl    $0x7,0x8(%esp)
80491a6:      00
80491a7:      c7 44 24 04 00 40 00 movl    $0x4000,0x4(%esp)
80491ae:      00
80491af:      c7 04 24 00 60 58 55 movl    $0x55586000,(%esp)
80491b6:      e8 35 f5 ff ff      call    80486f0 <mmap@plt>
80491bb:      83 f8 ff           cmp     $0xffffffff,%eax
80491be:      89 c3              mov     %eax,%ebx
80491c0:      74 45              je      8049207 <launcher+0x97>
80491c2:      8d 80 f8 3f 00 00   lea     0x3ff8(%eax),%eax
80491c8:      a3 04 ae 04 08     mov     %eax,0x804ae04
80491cd:      89 e2              mov     %esp,%edx
80491cf:      89 c4              mov     %eax,%esp
80491d1:      a3 08 ae 04 08     mov     %eax,0x804ae08
80491d6:      a1 e8 a1 04 08     mov     0x804a1e8,%eax
80491db:      89 15 f0 a1 04 08   mov     %edx,0x804a1f0
80491e1:      8b 15 ec a1 04 08   mov     0x804a1ec,%edx
80491e7:      e8 a4 fe ff ff      call    8049090 <launch>
80491ec:      a1 f0 a1 04 08     mov     0x804a1f0,%eax
80491f1:      89 c4              mov     %eax,%esp
80491f3:      c7 45 0c 00 40 00 00 movl    $0x4000,0xc(%ebp)
80491fa:      89 5d 08           mov     %ebx,0x8(%ebp)
80491fd:      83 c4 24           add     $0x24,%esp
8049200:      5b                pop     %ebx
8049201:      5d                pop     %ebp
8049202:      e9 69 f6 ff ff      jmp     8048870 <munmap@plt>
8049207:      a1 a0 a1 04 08     mov     0x804a1a0,%eax
804920c:      c7 44 24 08 23 00 00 movl    $0x23,0x8(%esp)
8049213:      00
8049214:      c7 44 24 04 01 00 00 movl    $0x1,0x4(%esp)
804921b:      00
804921c:      c7 04 24 cc 99 04 08 movl    $0x80499cc,(%esp)
8049223:      89 44 24 0c         mov     %eax,0xc(%esp)
8049227:      e8 d4 f5 ff ff      call    8048800 <fwrite@plt>
804922c:      c7 04 24 01 00 00 00 movl    $0x1,(%esp)
8049233:      e8 68 f6 ff ff      call    80488a0 <exit@plt>
8049238:      90                nop
8049239:      8d b4 26 00 00 00 00 lea     0x0(%esi),%esi

```

```

08049240 <main>:
8049240:      8d 4c 24 04         lea     0x4(%esp),%ecx
8049244:      83 e4 f0           and     $0xffffffff0,%esp
8049247:      ff 71 fc           pushl   0xffffffffc(%ecx)
804924a:      55                push    %ebp
804924b:      89 e5             mov     %esp,%ebp
804924d:      57                push    %edi
804924e:      56                push    %esi
804924f:      53                push    %ebx
8049250:      51                push    %ecx
8049251:      83 ec 18           sub     $0x18,%esp
8049254:      8b 31             mov     (%ecx),%esi
8049256:      8b 59 04           mov     0x4(%ecx),%ebx
8049259:      c7 44 24 04 60 8a 04 movl    $0x8048a60,0x4(%esp)

```

```

8049260: 08
8049261: c7 04 24 0b 00 00 00 movl $0xb, (%esp)
8049268: e8 a3 f4 ff ff call 8048710 <signal@plt>
804926d: c7 44 24 04 90 8a 04 movl $0x8048a90, 0x4(%esp)
8049274: 08
8049275: c7 04 24 07 00 00 00 movl $0x7, (%esp)
804927c: e8 8f f4 ff ff call 8048710 <signal@plt>
8049281: c7 44 24 04 20 8a 04 movl $0x8048a20, 0x4(%esp)
8049288: 08
8049289: c7 04 24 0e 00 00 00 movl $0xe, (%esp)
8049290: e8 7b f4 ff ff call 8048710 <signal@plt>
8049295: c7 44 24 04 f0 89 04 movl $0x80489f0, 0x4(%esp)
804929c: 08
804929d: c7 04 24 04 00 00 00 movl $0x4, (%esp)
80492a4: e8 67 f4 ff ff call 8048710 <signal@plt>
80492a9: a1 a4 a1 04 08 mov 0x804a1a4, %eax
80492ae: c7 45 e8 00 00 00 00 movl $0x0, 0xffffffff8(%ebp)
80492b5: c7 45 ec 01 00 00 00 movl $0x1, 0xffffffffec(%ebp)
80492bc: a3 c0 a1 04 08 mov %eax, 0x804a1c0
80492c1: c7 44 24 08 f8 9b 04 movl $0x8049bf8, 0x8(%esp)
80492c8: 08
80492c9: 89 5c 24 04 mov %ebx, 0x4(%esp)
80492cd: 89 34 24 mov %esi, (%esp)
80492d0: e8 cb f4 ff ff call 80487a0 <getopt@plt>
80492d5: 3c ff cmp $0xff, %al
80492d7: 74 20 je 80492f9 <main+0xb9>
80492d9: 83 e8 66 sub $0x66, %eax
80492dc: 3c 12 cmp $0x12, %al
80492de: 77 10 ja 80492f0 <main+0xb0>
80492e0: 0f b6 c0 movzbl %al, %eax
80492e3: ff 24 85 00 9c 04 08 jmp *0x8049c00(, %eax, 4)
80492ea: 8d b6 00 00 00 00 lea 0x0(%esi), %esi
80492f0: 8b 03 mov (%ebx), %eax
80492f2: e8 c9 f7 ff ff call 8048ac0 <usage>
80492f7: eb c8 jmp 80492c1 <main+0x81>
80492f9: a1 d4 a1 04 08 mov 0x804a1d4, %eax
80492fe: 85 c0 test %eax, %eax
8049300: 0f 84 e5 01 00 00 je 80494eb <main+0x2ab>
8049306: a1 d0 a1 04 08 mov 0x804a1d0, %eax
804930b: 89 04 24 mov %eax, (%esp)
804930e: e8 dd f4 ff ff call 80487f0 <srandom@plt>
8049313: e8 e8 f3 ff ff call 8048700 <random@plt>
8049318: 25 f8 0f 00 00 and $0xff8, %eax
804931d: 89 45 e4 mov %eax, 0xffffffffe4(%ebp)
8049320: c7 44 24 04 04 00 00 movl $0x4, 0x4(%esp)
8049327: 00
8049328: 8b 45 ec mov 0xffffffffec(%ebp), %eax
804932b: 89 04 24 mov %eax, (%esp)
804932e: e8 fd f3 ff ff call 8048730 <calloc@plt>
8049333: 89 c7 mov %eax, %edi
8049335: 8b 45 ec mov 0xffffffffec(%ebp), %eax
8049338: 83 e8 02 sub $0x2, %eax
804933b: 85 c0 test %eax, %eax
804933d: 7e 24 jle 8049363 <main+0x123>
804933f: 8b 45 ec mov 0xffffffffec(%ebp), %eax
8049342: bb 01 00 00 00 mov $0x1, %ebx
8049347: 8d 70 ff lea 0xfffffffff(%eax), %esi
804934a: 8d b6 00 00 00 00 lea 0x0(%esi), %esi
8049350: e8 ab f3 ff ff call 8048700 <random@plt>
8049355: 83 e0 38 and $0x38, %eax
8049358: 89 44 9f fc mov %eax, 0xfffffffffc(%edi, %ebx, 4)
804935c: 83 c3 01 add $0x1, %ebx
804935f: 39 f3 cmp %esi, %ebx
8049361: 75 ed jne 8049350 <main+0x110>
8049363: 83 7d ec 01 cmpl $0x1, 0xffffffffec(%ebp)
8049367: 0f 8e 4e 01 00 00 jle 80494bb <main+0x27b>
804936d: 8b 45 ec mov 0xffffffffec(%ebp), %eax
8049370: c1 e0 02 shl $0x2, %eax

```

```

8049373: c7 44 07 f8 38 00 00 movl $0x38,0xffffffff8(%edi,%eax,1)
804937a: 00
804937b: c7 44 07 fc 00 00 00 movl $0x0,0xffffffffc(%edi,%eax,1)
8049382: 00
8049383: a1 70 a1 04 08 mov 0x804a170,%eax
8049388: 89 04 24 mov %eax,(%esp)
804938b: e8 30 f4 ff ff call 80487c0 <alarm@plt>
8049390: 31 db xor %ebx,%ebx
8049392: 8b 45 e4 mov 0xffffffffe4(%ebp),%eax
8049395: 03 04 9f add (%edi,%ebx,4),%eax
8049398: 83 c3 01 add $0x1,%ebx
804939b: 89 44 24 04 mov %eax,0x4(%esp)
804939f: 8b 45 e8 mov 0xffffffffe8(%ebp),%eax
80493a2: 89 04 24 mov %eax,(%esp)
80493a5: e8 c6 fd ff ff call 8049170 <launcher>
80493aa: 3b 5d ec cmp 0xffffffffec(%ebp),%ebx
80493ad: 7c e3 jl 8049392 <main+0x152>
80493af: 83 c4 18 add $0x18,%esp
80493b2: 31 c0 xor %eax,%eax
80493b4: 59 pop %ecx
80493b5: 5b pop %ebx
80493b6: 5e pop %esi
80493b7: 5f pop %edi
80493b8: 5d pop %ebp
80493b9: 8d 61 fc lea 0xffffffffc(%ecx),%esp
80493bc: c3 ret
80493bd: c7 05 d8 a1 04 08 01 movl $0x1,0x804a1d8
80493c4: 00 00 00
80493c7: c7 05 c4 a1 04 08 01 movl $0x1,0x804a1c4
80493ce: 00 00 00
80493d1: c7 05 70 a1 04 08 01 movl $0x1,0x804a170
80493d8: 00 00 00
80493db: e9 e1 fe ff ff jmp 80492c1 <main+0x81>
80493e0: c7 44 24 04 e1 9b 04 movl $0x8049be1,0x4(%esp)
80493e7: 08
80493e8: a1 ac a1 04 08 mov 0x804a1ac,%eax
80493ed: 89 04 24 mov %eax,(%esp)
80493f0: e8 bb f3 ff ff call 80487b0 <fopen@plt>
80493f5: 85 c0 test %eax,%eax
80493f7: a3 c0 a1 04 08 mov %eax,0x804a1c0
80493fc: 0f 85 bf fe ff ff jne 80492c1 <main+0x81>
8049402: a1 ac a1 04 08 mov 0x804a1ac,%eax
8049407: c7 04 24 e3 9b 04 08 movl $0x8049be3,(%esp)
804940e: 89 44 24 04 mov %eax,0x4(%esp)
8049412: e8 c9 f3 ff ff call 80487e0 <printf@plt>
8049417: 8b 03 mov (%ebx),%eax
8049419: e8 a2 f6 ff ff call 8048ac0 <usage>
804941e: e9 9e fe ff ff jmp 80492c1 <main+0x81>
8049423: c7 45 e8 01 00 00 00 movl $0x1,0xffffffffe8(%ebp)
804942a: c7 45 ec 05 00 00 00 movl $0x5,0xffffffffec(%ebp)
8049431: e9 8b fe ff ff jmp 80492c1 <main+0x81>
8049436: c7 05 c4 a1 04 08 01 movl $0x1,0x804a1c4
804943d: 00 00 00
8049440: e9 7c fe ff ff jmp 80492c1 <main+0x81>
8049445: c7 05 68 a1 04 08 01 movl $0x1,0x804a168
804944c: 00 00 00
804944f: e9 6d fe ff ff jmp 80492c1 <main+0x81>
8049454: a1 ac a1 04 08 mov 0x804a1ac,%eax
8049459: 89 04 24 mov %eax,(%esp)
804945c: e8 2f f4 ff ff call 8048890 <__strdup@plt>
8049461: a3 d4 a1 04 08 mov %eax,0x804a1d4
8049466: 89 44 24 04 mov %eax,0x4(%esp)
804946a: c7 04 24 c9 9b 04 08 movl $0x8049bc9,(%esp)
8049471: e8 6a f3 ff ff call 80487e0 <printf@plt>
8049476: a1 d4 a1 04 08 mov 0x804a1d4,%eax
804947b: 89 04 24 mov %eax,(%esp)
804947e: e8 ed 00 00 00 call 8049570 <gencookie>
8049483: a3 d0 a1 04 08 mov %eax,0x804a1d0

```

```

8049488: 89 44 24 04      mov    %eax,0x4(%esp)
804948c: c7 04 24 d3 9b 04 08 movl   $0x8049bd3,(%esp)
8049493: e8 48 f3 ff ff   call  80487e0 <printf@plt>
8049498: e9 24 fe ff ff   jmp   80492c1 <main+0x81>
804949d: c7 05 c8 a1 04 08 01 movl   $0x1,0x804a1c8
80494a4: 00 00 00
80494a7: e9 15 fe ff ff   jmp   80492c1 <main+0x81>
80494ac: c7 05 cc a1 04 08 01 movl   $0x1,0x804a1cc
80494b3: 00 00 00
80494b6: e9 06 fe ff ff   jmp   80492c1 <main+0x81>
80494bb: 8b 45 ec         mov    0xffffffff(%ebp),%eax
80494be: c7 44 87 fc 00 00 00 movl   $0x0,0xffffffff(%edi,%eax,4)
80494c5: 00
80494c6: a1 70 a1 04 08   mov    0x804a170,%eax
80494cb: 89 04 24         mov    %eax,(%esp)
80494ce: e8 ed f2 ff ff   call  80487c0 <alarm@plt>
80494d3: 83 7d ec 01      cmpl   $0x1,0xffffffff(%ebp)
80494d7: 0f 84 b3 fe ff ff je     8049390 <main+0x150>
80494dd: 83 c4 18         add    $0x18,%esp
80494e0: 31 c0           xor    %eax,%eax
80494e2: 59             pop    %ecx
80494e3: 5b             pop    %ebx
80494e4: 5e             pop    %esi
80494e5: 5f             pop    %edi
80494e6: 5d             pop    %ebp
80494e7: 8d 61 fc       lea    0xffffffff(%ecx),%esp
80494ea: c3             ret
80494eb: c7 04 24 f0 99 04 08 movl   $0x80499f0,(%esp)
80494f2: e8 59 f3 ff ff   call  8048850 <puts@plt>
80494f7: 8b 03          mov    (%ebx),%eax
80494f9: e8 c2 f5 ff ff   call  8048ac0 <usage>
80494fe: e9 03 fe ff ff   jmp   8049306 <main+0xc6>
8049503: 90             nop
8049504: 90             nop
8049505: 90             nop
8049506: 90             nop
8049507: 90             nop
8049508: 90             nop
8049509: 90             nop
804950a: 90             nop
804950b: 90             nop
804950c: 90             nop
804950d: 90             nop
804950e: 90             nop
804950f: 90             nop

```

08049510 <hash>:

```

8049510: 55             push   %ebp
8049511: 31 c0          xor    %eax,%eax
8049513: 89 e5         mov    %esp,%ebp
8049515: 8b 4d 08       mov    0x8(%ebp),%ecx
8049518: 0f b6 11      movzbl (%ecx),%edx
804951b: 84 d2         test   %dl,%dl
804951d: 74 15         je     8049534 <hash+0x24>
804951f: 90             nop
8049520: 6b c0 67      imul   $0x67,%eax,%eax
8049523: 0f be d2      movsbl %dl,%edx
8049526: 8d 04 02      lea    (%edx,%eax,1),%eax
8049529: 0f b6 51 01   movzbl 0x1(%ecx),%edx
804952d: 83 c1 01      add    $0x1,%ecx
8049530: 84 d2         test   %dl,%dl
8049532: 75 ec         jne    8049520 <hash+0x10>
8049534: 5d             pop    %ebp
8049535: c3             ret
8049536: 8d 76 00      lea    0x0(%esi),%esi
8049539: 8d bc 27 00 00 00 00 lea    0x0(%edi),%edi

```

08049540 <check>:


```

8049540:      55                push    %ebp
8049541:      89 e5            mov     %esp,%ebp
8049543:      8b 55 08          mov     0x8(%ebp),%edx
8049546:      89 d0            mov     %edx,%eax
8049548:      c1 e8 1c          shr     $0x1c,%eax
804954b:      85 c0            test    %eax,%eax
804954d:      74 19            je      8049568 <check+0x28>
804954f:      31 c9            xor     %ecx,%ecx
8049551:      89 d0            mov     %edx,%eax
8049553:      d3 e8            shr     %cl,%eax
8049555:      3c 0a            cmp     $0xa,%al
8049557:      74 0f            je      8049568 <check+0x28>
8049559:      83 c1 08          add     $0x8,%ecx
804955c:      83 f9 20          cmp     $0x20,%ecx
804955f:      75 f0            jne     8049551 <check+0x11>
8049561:      5d                pop     %ebp
8049562:      b8 01 00 00 00    mov     $0x1,%eax
8049567:      c3                ret
8049568:      5d                pop     %ebp
8049569:      31 c0            xor     %eax,%eax
804956b:      c3                ret
804956c:      8d 74 26 00        lea     0x0(%esi),%esi

08049570 <gencookie>:
8049570:      55                push    %ebp
8049571:      89 e5            mov     %esp,%ebp
8049573:      53                push    %ebx
8049574:      83 ec 04          sub     $0x4,%esp
8049577:      8b 45 08          mov     0x8(%ebp),%eax
804957a:      89 04 24          mov     %eax,(%esp)
804957d:      e8 8e ff ff ff    call    8049510 <hash>
8049582:      89 04 24          mov     %eax,(%esp)
8049585:      e8 56 f1 ff ff    call    80486e0 <srand@plt>
804958a:      8d b6 00 00 00 00 lea     0x0(%esi),%esi
8049590:      e8 cb f2 ff ff    call    8048860 <rand@plt>
8049595:      89 c3            mov     %eax,%ebx
8049597:      89 04 24          mov     %eax,(%esp)
804959a:      e8 a1 ff ff ff    call    8049540 <check>
804959f:      85 c0            test    %eax,%eax
80495a1:      74 ed            je      8049590 <gencookie+0x20>
80495a3:      89 d8            mov     %ebx,%eax
80495a5:      83 c4 04          add     $0x4,%esp
80495a8:      5b                pop     %ebx
80495a9:      5d                pop     %ebp
80495aa:      c3                ret
80495ab:      90                nop
80495ac:      90                nop
80495ad:      90                nop
80495ae:      90                nop
80495af:      90                nop

080495b0 <__libc_csu_fini>:
80495b0:      55                push    %ebp
80495b1:      89 e5            mov     %esp,%ebp
80495b3:      5d                pop     %ebp
80495b4:      c3                ret
80495b5:      8d 74 26 00        lea     0x0(%esi),%esi
80495b9:      8d bc 27 00 00 00 lea     0x0(%edi),%edi

080495c0 <__libc_csu_init>:
80495c0:      55                push    %ebp
80495c1:      89 e5            mov     %esp,%ebp
80495c3:      57                push    %edi
80495c4:      56                push    %esi
80495c5:      53                push    %ebx
80495c6:      e8 5e 00 00 00    call    8049629 <__i686.get_pc_thunk.bx>
80495cb:      81 c3 15 0b 00 00 add     $0xb15,%ebx
80495d1:      83 ec 1c          sub     $0x1c,%esp

```

```

80495d4:    e8 cf f0 ff ff      call    80486a8 <_init>
80495d9:    8d 83 20 ff ff ff   lea     0xffffffff20(%ebx),%eax
80495df:    89 45 f0             mov     %eax,0xffffffff0(%ebp)
80495e2:    8d 83 20 ff ff ff   lea     0xffffffff20(%ebx),%eax
80495e8:    29 45 f0             sub     %eax,0xffffffff0(%ebp)
80495eb:    c1 7d f0 02         sarl    $0x2,0xffffffff0(%ebp)
80495ef:    8b 55 f0             mov     0xffffffff0(%ebp),%edx
80495f2:    85 d2               test    %edx,%edx
80495f4:    74 2b               je      8049621 <__libc_csu_init+0x61>
80495f6:    31 ff               xor     %edi,%edi
80495f8:    89 c6               mov     %eax,%esi
80495fa:    8d b6 00 00 00 00   lea     0x0(%esi),%esi
8049600:    8b 45 10             mov     0x10(%ebp),%eax
8049603:    83 c7 01             add     $0x1,%edi
8049606:    89 44 24 08         mov     %eax,0x8(%esp)
804960a:    8b 45 0c             mov     0xc(%ebp),%eax
804960d:    89 44 24 04         mov     %eax,0x4(%esp)
8049611:    8b 45 08             mov     0x8(%ebp),%eax
8049614:    89 04 24             mov     %eax,(%esp)
8049617:    ff 16               call    *(%esi)
8049619:    83 c6 04             add     $0x4,%esi
804961c:    39 7d f0             cmp     %edi,0xffffffff0(%ebp)
804961f:    75 df               jne     8049600 <__libc_csu_init+0x40>
8049621:    83 c4 1c             add     $0x1c,%esp
8049624:    5b                  pop     %ebx
8049625:    5e                  pop     %esi
8049626:    5f                  pop     %edi
8049627:    5d                  pop     %ebp
8049628:    c3                  ret

```

08049629 <__i686.get_pc_thunk.bx>:

```

8049629:    8b 1c 24             mov     (%esp),%ebx
804962c:    c3                  ret
804962d:    90                  nop
804962e:    90                  nop
804962f:    90                  nop

```

08049630 <__do_global_ctors_aux>:

```

8049630:    55                  push    %ebp
8049631:    89 e5               mov     %esp,%ebp
8049633:    53                  push    %ebx
8049634:    bb 00 a0 04 08     mov     $0x804a000,%ebx
8049639:    83 ec 04             sub     $0x4,%esp
804963c:    a1 00 a0 04 08     mov     0x804a000,%eax
8049641:    83 f8 ff             cmp     $0xffffffff,%eax
8049644:    74 0c               je      8049652 <__do_global_ctors_aux+0x22>
8049646:    83 eb 04             sub     $0x4,%ebx
8049649:    ff d0               call    %eax
804964b:    8b 03               mov     (%ebx),%eax
804964d:    83 f8 ff             cmp     $0xffffffff,%eax
8049650:    75 f4               jne     8049646 <__do_global_ctors_aux+0x16>
8049652:    83 c4 04             add     $0x4,%esp
8049655:    5b                  pop     %ebx
8049656:    5d                  pop     %ebp
8049657:    c3                  ret

```

Disassembly of section .fini:

08049658 <_fini>:

```

8049658:    55                  push    %ebp
8049659:    89 e5               mov     %esp,%ebp
804965b:    53                  push    %ebx
804965c:    83 ec 04             sub     $0x4,%esp
804965f:    e8 00 00 00 00     call    8049664 <_fini+0xc>
8049664:    5b                  pop     %ebx
8049665:    81 c3 7c 0a 00 00   add     $0xa7c,%ebx
804966b:    e8 90 f2 ff ff     call    8048900 <__do_global_dtors_aux>
8049670:    59                  pop     %ecx
8049671:    5b                  pop     %ebx

```

8049672:	c9	leave
8049673:	c3	ret