1. **Divide by zero**

**Steps Performed:**

Returned 0 divided result

**Bad Code:**

int x=0;

int y=1;

int z;

z = 1/0;

printk(KERN\_ALERT "Value of z : %d",z);

return\_value = z;

**Output during bzImage:**

schaud14bing@schaud14:~/Downloads/linux-4.4.4$ make bzImage

  CHK     include/config/kernel.release

  CHK     include/generated/uapi/linux/version.h

  CHK     include/generated/utsrelease.h

  CHK     include/generated/bounds.h

  CHK     include/generated/timeconst.h

  CHK     include/generated/asm-offsets.h

  CALL    scripts/checksyscalls.sh

  CHK     include/generated/compile.h

  CC      kernel/my\_xtime.o

kernel/my\_xtime.c: In function 'sys\_my\_xtime':

kernel/my\_xtime.c:17:7: warning: division by zero [-Wdiv-by-zero]

**User Space output:** Segmentation fault

**Kernel Space output:**

[  173.415569] divide error: 0000 [#2] SMP

[  173.415575] Modules linked in: bnep rfcomm bluetooth crc16 binfmt\_misc snd\_hda\_codec\_hdmi x86\_pkg\_temp\_thermal coretemp crc32c\_intel sha256\_generic hmac drbg snd\_hda\_codec\_realtek snd\_hda\_codec\_generic snd\_hda\_intel snd\_hda\_codec snd\_hwdep snd\_hda\_core snd\_pcm snd\_seq snd\_timer snd\_seq\_device aesni\_intel snd aes\_x86\_64 glue\_helper hp\_wmi lrw rfkill gf128mul iTCO\_wdt sparse\_keymap ablk\_helper iTCO\_vendor\_support cryptd psmouse evdev i2c\_i801 serio\_raw soundcore pcspkr i2c\_core parport\_pc lpc\_ich wmi parport mfd\_core button processor nfsv3 hid\_generic usbhid hid nfs lockd grace sunrpc sg sr\_mod cdrom sd\_mod ahci libahci ata\_generic ehci\_pci ehci\_hcd libata e1000e usbcore scsi\_mod ptp pps\_core usb\_common

[  173.415628] CPU: 5 PID: 2738 Comm: a.out Tainted: G      D         4.4.4 #22

[  173.415631] Hardware name: Hewlett-Packard HP Z210 Workstation/1588h, BIOS J51 v01.20 09/16/2011

[  173.415634] task: ffff8802230b8140 ti: ffff88021fb2c000 task.ti: ffff88021fb2c000

[  173.415636] RIP: 0010:[<ffffffff81097664>]  [<ffffffff81097664>] sys\_my\_xtime+0x94/0xd0

[  173.415643] RSP: 0018:ffff88021fb2ff28  EFLAGS: 00010246

[  173.415645] RAX: 0000000000000001 RBX: 00007fff7aba20b0 RCX: 0000000000000000

[  173.415647] RDX: 0000000000000000 RSI: ffff88021fb2ff38 RDI: ffffffff81728ed4

[  173.415649] RBP: 00007fff7aba20d0 R08: 00000000004dc081 R09: 0000000000000000

[  173.415651] R10: 00007f6e93466300 R11: 0000000000000202 R12: 0000000000400490

[  173.415653] R13: 00007fff7aba21b0 R14: 0000000000000000 R15: 0000000000000000

[  173.415655] FS:  00007f6e93673700(0000) GS:ffff88022dd40000(0000) knlGS:0000000000000000

[  173.415658] CS:  0010 DS: 0000 ES: 0000 CR0: 0000000080050033

[  173.415659] CR2: 00007f6e9310ff50 CR3: 000000020a861000 CR4: 00000000000406e0

[  173.415661] Stack:

[  173.415663]  0000000056e71dfd 143bcf83b6dba200 00007fff7aba21b0 0000000000000000

[  173.415667]  00007fff7aba20d0 ffffffff81574cb6 0000000000000000 0000000000000000

[  173.415670]  00007fff7aba21b0 0000000000400490 0000000000000000 0000000000000000

[  173.415673] Call Trace:

[  173.415678]  [<ffffffff81574cb6>] ? entry\_SYSCALL\_64\_fastpath+0x16/0x75

[  173.415680] Code: 5b 5d c3 48 c7 c7 a8 ed 71 81 31 c0 bd f2 ff ff ff e8 b5 54 0c 00 eb e2 b8 01 00 00 00 31 c9 48 c7 c7 d4 8e 72 81 89 c2 c1 fa 1f <f7> f9 89 c5 31 c0 e8 95 54 0c 00 48 8b 33 48 c7 c7 f0 ed 71 81

[  173.415713] RIP  [<ffffffff81097664>] sys\_my\_xtime+0x94/0xd0

[  173.415716]  RSP <ffff88021fb2ff28>

[  173.415720] ---[ end trace d11613156edfb657 ]---

1. **Dereferencing a null pointer**

**Steps Performed:**

1. Added null pointer
2. Give value of null pointer as input to another variable

**Bad Code:**

int \* in;

in = NULL;

printk(KERN\_ALERT " Value of Null Pointer : %d ",\*in );

kfree(in);

**Result:**

**User Space output:** killed

**Kernel Space output:**

32.137323] Bluetooth: BNEP socket layer initialized

[  247.089711] BUG: unable to handle kernel NULL pointer dereference at           (null)

[  247.089718] IP: [<ffffffff810975f3>] sys\_my\_xtime+0x23/0xe0

[  247.089725] PGD 7f6f7067 PUD c91bd067 PMD 0

[  247.089730] Oops: 0000 [#1] SMP

[  247.089733] Modules linked in: bnep rfcomm bluetooth crc16 binfmt\_misc snd\_hda\_codec\_hdmi x86\_pkg\_temp\_thermal coretemp crc32c\_intel sha256\_generic hmac drbg snd\_hda\_codec\_realtek snd\_hda\_codec\_generic snd\_hda\_intel snd\_hda\_codec snd\_hwdep snd\_hda\_core snd\_pcm snd\_seq snd\_timer snd\_seq\_device snd aesni\_intel aes\_x86\_64 glue\_helper hp\_wmi lrw rfkill gf128mul iTCO\_wdt sparse\_keymap ablk\_helper iTCO\_vendor\_support cryptd psmouse evdev i2c\_i801 soundcore pcspkr serio\_raw i2c\_core parport\_pc lpc\_ich parport mfd\_core wmi button processor nfsv3 hid\_generic usbhid hid nfs lockd grace sunrpc sg sr\_mod sd\_mod cdrom ahci libahci ata\_generic ehci\_pci ehci\_hcd libata e1000e usbcore scsi\_mod ptp pps\_core usb\_common

[  247.089786] CPU: 6 PID: 2760 Comm: a.out Not tainted 4.4.4 #21

[  247.089789] Hardware name: Hewlett-Packard HP Z210 Workstation/1588h, BIOS J51 v01.20 09/16/2011

[  247.089791] task: ffff880220eb4440 ti: ffff8800b9cf4000 task.ti: ffff8800b9cf4000

[  247.089793] RIP: 0010:[<ffffffff810975f3>]  [<ffffffff810975f3>] sys\_my\_xtime+0x23/0xe0

[  247.089797] RSP: 0018:ffff8800b9cf7f38  EFLAGS: 00010296

[  247.089799] RAX: ffff88021fa4fc20 RBX: 00007ffe23e526f0 RCX: 00007faff9f9c300

[  247.089801] RDX: 0000000000000004 RSI: ffff88022dd9cd48 RDI: 0000000000000246

[  247.089803] RBP: 00007ffe23e52710 R08: 00007faff9faf2e0 R09: 0000000000000000

[  247.089805] R10: 00007faff9f9c300 R11: 0000000000000206 R12: 0000000000400490

[  247.089807] R13: 00007ffe23e527f0 R14: 0000000000000000 R15: 0000000000000000

[  247.089809] FS:  00007faffa1a9700(0000) GS:ffff88022dd80000(0000) knlGS:0000000000000000

[  247.089811] CS:  0010 DS: 0000 ES: 0000 CR0: 0000000080050033

[  247.089813] CR2: 0000000000000000 CR3: 000000007f12f000 CR4: 00000000000406e0

[  247.089815] Stack:

[  247.089817]  00007ffe23e527f0 0000000000000000 0000000000000000 ffffffff81574cf6

[  247.089820]  0000000000000000 0000000000000000 00007ffe23e527f0 0000000000400490

[  247.089823]  00007ffe23e52710 0000000000000000 0000000000000206 00007faff9f9c300

[  247.089827] Call Trace:

[  247.089832]  [<ffffffff81574cf6>] ? entry\_SYSCALL\_64\_fastpath+0x16/0x75

[  247.089834] Code: 90 90 90 90 90 90 90 90 66 66 66 66 90 53 48 89 fb ba 04 00 00 00 be c0 00 40 02 48 83 ec 10 48 8b 3d 3a 9a a4 00 e8 2d de 11 00 <8b> 34 25 00 00 00 00 48 c7 c7 d4 8e 72 81 31 c0 e8 0c 55 0c 00

[  247.089866] RIP  [<ffffffff810975f3>] sys\_my\_xtime+0x23/0xe0

[  247.089869]  RSP <ffff8800b9cf7f38>

[  247.089870] CR2: 0000000000000000

[  247.089893] ---[ end trace 86c185b21ae104d1 ]---

1. **Heap overflow**

kmalloc() function returns kernel memory of size requested. Kernel allocations always succeed, unless there is an insufficient amount of memory available.

In the system call we are allocating kernel memory to a pointer in incremental order inside the infinite loop. Hence after some allocations there will not be sufficient space left on kernel. So **this will cause the kernel to crash**.

**Bad code:**

char \* in;

int size;

size = 1;

while (1)

{

size = size \* 5;

in = kmalloc(size,GFP\_KERNEL);

printk(KERN\_ALERT "Size Allocated is : %d",size);

}

kfree(in);

1. **Stack overflow**

Called the same system call function recursively. With each function call the size of the stack will fill up. Due to this after some iterations the stack will overflow. So **this will cause the kernel to crash**.

Bad code:

int i;

while (1)

{

i = sys\_my\_xtime(current\_time,choice);

printk(KERN\_ALERT "Return value : %d",i);

}

1. **Returning incorrect value**

Given a string value to the char array of size 10. The return type of the system call is int but returned string from the function.

**Bad Code:**

char return\_str[10] = "WrongTYPE";

printk(KERN\_ALERT "Returning Wrong data type");

return return\_str;

System call returns -EFAULT.

1. **Referencing wrong data type**

Given a string value to the char array of size 10. Printed the string as an integer.

**Bad Code:**

char return\_str[10] = "WrongTYPE";

printk(KERN\_ALERT "Printing string as integer\n" );

printk(KERN\_ALERT "Printing %d", return\_str );

return\_value = 0;

System call returns -EFAULT.