Muhammed Nifal V

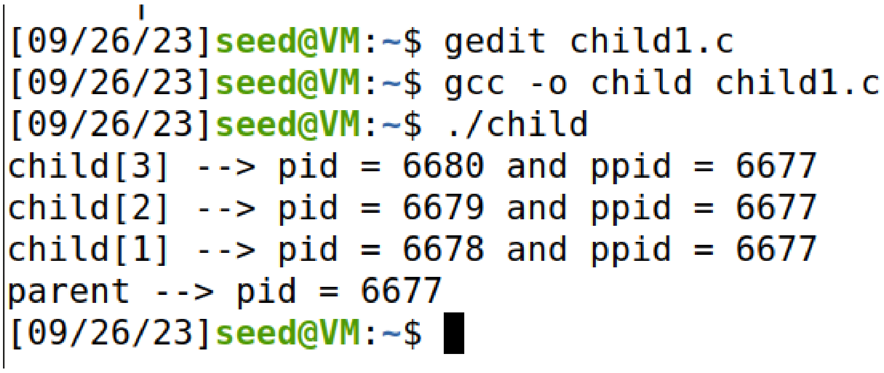
CB.SCP2CYS23017 SECURE CODING LAB

1. Use the appropriate system call(s) which creates 3 child process.

Source Code:

```
#include <stdio.h>
#include <stdlib.h>
#include <unistd.h>
int main()
{
  int pid, pid1, pid2;
  pid = fork();
  if (pid == 0)
  {
  sleep(3);
  printf("child[1] --> pid = %d and ppid = %d\n",
          getpid(), getppid());
  }
  else {
      pid1 = fork();
      if (pid1 == 0) {
         sleep(2);
         printf("child[2] --> pid = %d and ppid = %d\n",
              getpid(), getppid());
      }
      else {
         pid2 = fork();
         if (pid2 == 0) {
         printf("child[3] --> pid = %d and ppid = %d\n",
                 getpid(), getppid());
         }
      else {
      sleep(3);
           printf("parent --> pid = %d\n", getpid());
         }
      }
   }
```

OUTPUT:



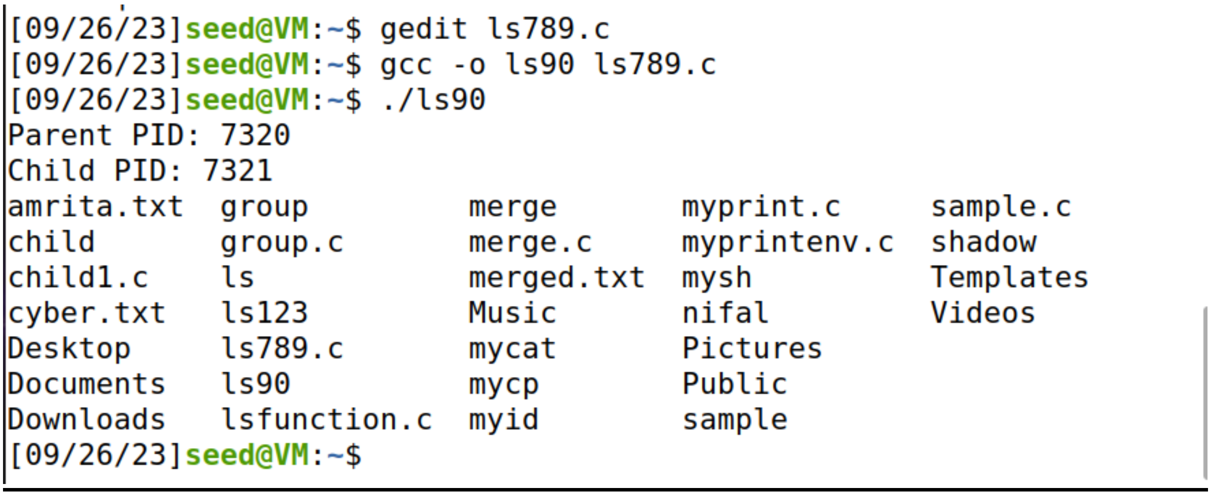
```
[09/26/23]seed@VM:~$ gedit child1.c
[09/26/23]seed@VM:~$ gcc -o child child1.c
[09/26/23]seed@VM:~$ ./child
child[3] --> pid = 6680 and ppid = 6677
child[2] --> pid = 6679 and ppid = 6677
child[1] --> pid = 6678 and ppid = 6677
parent --> pid = 6677
[09/26/23]seed@VM:~$ 
```

2. LS command

SOURCE CODE

```
#include <stdio.h>
#include <unistd.h>
#include <sys/types.h>
#include <sys/wait.h>
#include <stdlib.h>
int main()
{
    pid_t parent_pid = getpid();
    printf("Parent PID: %d\n", parent_pid);

    pid_t child_pid = fork();

    if (child_pid == -1)
    {
        perror("fork");
        exit(1);
    } else if (child_pid == 0)
    {
        printf("Child PID: %d\n", getpid());
         if (system("ls") == -1)
        {
            perror("system");
            exit(1);
        }

        exit(0);
    } else
    {
        wait(NULL);
    }

    return 0;
}
```

OUTPUT



```
[09/26/23]seed@VM:~$ gedit ls789.c
[09/26/23]seed@VM:~$ gcc -o ls90 ls789.c
[09/26/23]seed@VM:~$ ./ls90
Parent PID: 7320
Child PID: 7321
amrita.txt  group          merge       myprint.c     sample.c
child       group.c        merge.c     myprintenv.c  shadow
child1.c    ls             merged.txt  mysh          Templates
cyber.txt   ls123          Music       nifal         Videos
Desktop     ls789.c        mycat       Pictures
Documents   ls90           mycp        Public
Downloads   lsfunction.c   myid        sample
[09/26/23]seed@VM:~$
```

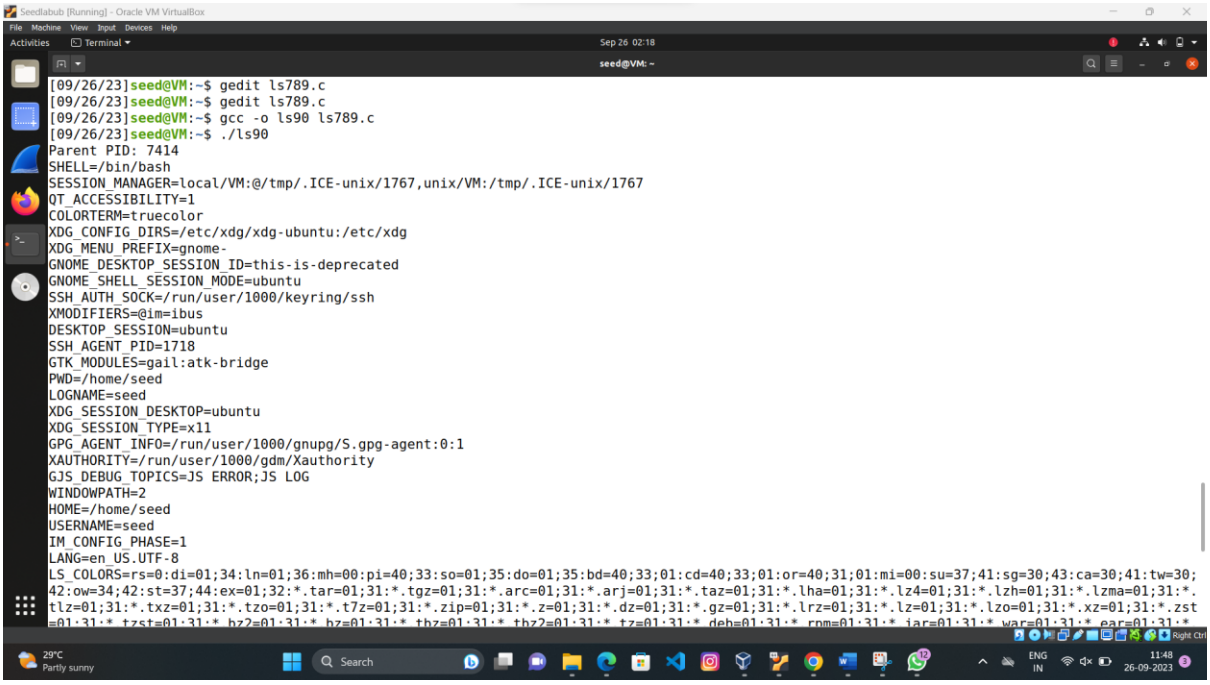
3.

SOURCE CODE:

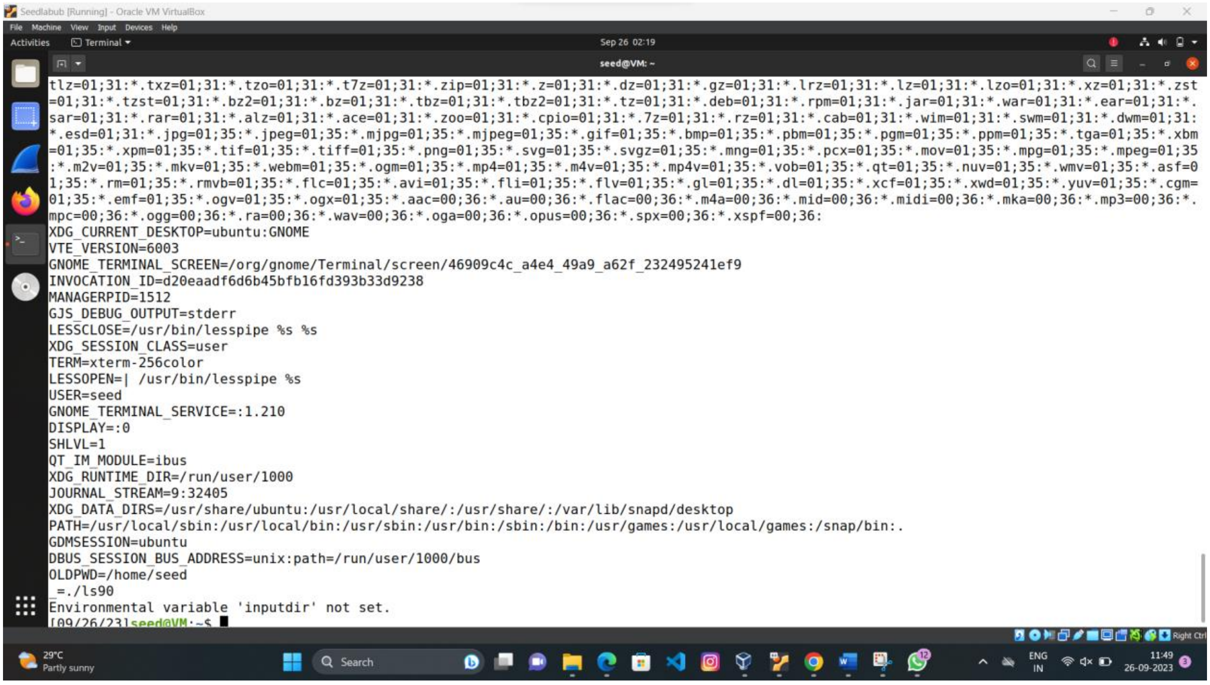
```
#include <stdio.h>
#include <unistd.h>
#include <sys/types.h>
#include <sys/wait.h>
#include <stdlib.h>
int main() {
   pid_t parent_pid = getpid();
   printf("Parent PID: %d\n", parent_pid);
 extern char** environ;
   char** env = environ;
   while (*env) {
      printf("%s\n", *env);
      env++;
   }
char* input_directory = getenv("inputdir");
   if (input_directory == NULL) {
      fprintf(stderr, "Environmental variable 'inputdir' not set.\n");
      exit(1);
   }
printf("Input Directory: %s\n", input_directory);

   pid_t child_pid = fork();

   if (child_pid == -1) {
      perror("fork");
      exit(1);
   } else if (child_pid == 0) {
      printf("Child PID: %d\n", getpid());
```

```
    char cmd[100];
    snprintf(cmd, sizeof(cmd), "ls %s", input_directory);
    if (system(cmd) == -1) {
      perror("system");
      exit(1);
    }

    exit(0);
    } else {
    wait(NULL);
  }
```

OUTPUT:



```
[09/26/23]seed@VM:~$ gedit ls789.c
[09/26/23]seed@VM:~$ gedit ls789.c
[09/26/23]seed@VM:~$ gcc -o ls90 ls789.c
[09/26/23]seed@VM:~$ ./ls90
Parent PID: 7414
SHELL=/bin/bash
SESSION_MANAGER=local/VM:@/tmp/.ICE-unix/1767,unix/VM:/tmp/.ICE-unix/1767
QT_ACCESSIBILITY=1
COLORTERM=truecolor
XDG_CONFIG_DIRS=/etc/xdg/xdg-ubuntu:/etc/xdg
XDG_MENU_PREFIX=gnome-
GNOME_DESKTOP_SESSION_ID=this-is-deprecated
GNOME_SHELL_SESSION_MODE=ubuntu
SSH_AUTH_SOCK=/run/user/1000/keyring/ssh
XMODIFIERS=@im=ibus
DESKTOP_SESSION=ubuntu
SSH_AGENT_PID=1718
GTK_MODULES=gail:atk-bridge
PWD=/home/seed
LOGNAME=seed
XDG_SESSION_DESKTOP=ubuntu
XDG_SESSION_TYPE=x11
GPG_AGENT_INFO=/run/user/1000/gnupg/S.gpg-agent:0:1
XAUTHORITY=/run/user/1000/gdm/Xauthority
GJS_DEBUG_TOPICS=JS ERROR;JS LOG
WINDOWPATH=2
HOME=/home/seed
USERNAME=seed
IM_CONFIG_PHASE=1
LANG=en_US.UTF-8
LS_COLORS=rs=0:di=01;34:ln=01;36:mh=00:pi=40;33:so=01;35:do=01;35:bd=40;33;01:cd=40;33;01:or=40;31;01:mi=00:su=37;41:sg=30;43:ca=30;41:tw=30;
42:ow=34;42:st=37;44:ex=01;32:*.tar=01;31:*.tgz=01;31:*.arc=01;31:*.arj=01;31:*.taz=01;31:*.lha=01;31:*.lz4=01;31:*.lzh=01;31:*.lzma=01;31:*.
tlz=01;31:*.txz=01;31:*.tzo=01;31:*.t7z=01;31:*.zip=01;31:*.z=01;31:*.dz=01;31:*.gz=01;31:*.lrz=01;31:*.lz=01;31:*.lzo=01;31:*.xz=01;31:*.zst
=01;31:*.tzst=01;31:*.bz2=01;31:*.bz=01;31:*.tbz=01;31:*.tbz2=01;31:*.tz=01;31:*.deb=01;31:*.rpm=01;31:*.jar=01;31:*.war=01;31:*.ear=01;31:*.
```



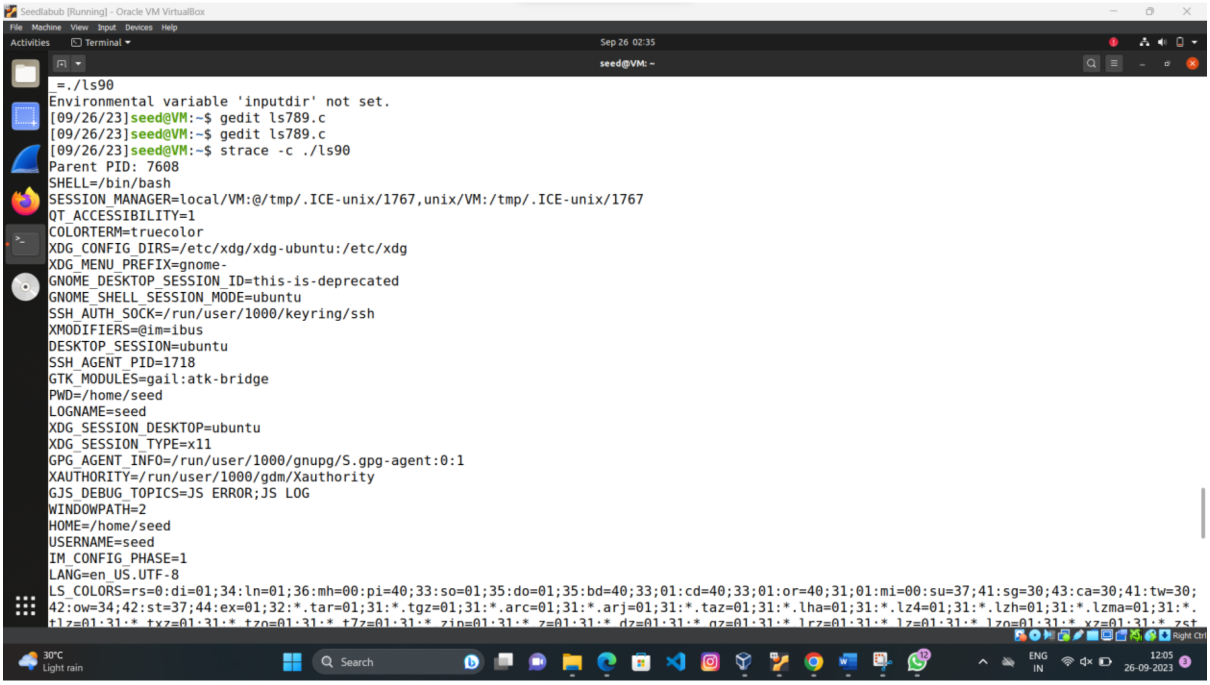
```
tlz=01;31:*.txz=01;31:*.tzo=01;31:*.t7z=01;31:*.zip=01;31:*.z=01;31:*.dz=01;31:*.gz=01;31:*.lrz=01;31:*.lz=01;31:*.lzo=01;31:*.xz=01;31:*.zst
=01;31:*.tzst=01;31:*.bz2=01;31:*.bz=01;31:*.tbz=01;31:*.tbz2=01;31:*.tz=01;31:*.deb=01;31:*.rpm=01;31:*.jar=01;31:*.war=01;31:*.ear=01;31:*.
sar=01;31:*.rar=01;31:*.alz=01;31:*.ace=01;31:*.zoo=01;31:*.cpio=01;31:*.7z=01;31:*.rz=01;31:*.cab=01;31:*.wim=01;31:*.swm=01;31:*.dwm=01;31:
*.esd=01;31:*.jpg=01;35:*.jpeg=01;35:*.mjpg=01;35:*.mjpeg=01;35:*.gif=01;35:*.bmp=01;35:*.pbm=01;35:*.pgm=01;35:*.ppm=01;35:*.tga=01;35:*.xbm
=01;35:*.xpm=01;35:*.tif=01;35:*.tiff=01;35:*.png=01;35:*.svg=01;35:*.svgz=01;35:*.mng=01;35:*.pcx=01;35:*.mov=01;35:*.mpg=01;35:*.mpeg=01;35
:*.m2v=01;35:*.mkv=01;35:*.webm=01;35:*.ogm=01;35:*.mp4=01;35:*.m4v=01;35:*.mp4v=01;35:*.vob=01;35:*.qt=01;35:*.nuv=01;35:*.wmv=01;35:*.asf=0
1;35:*.rm=01;35:*.rmvb=01;35:*.flc=01;35:*.avi=01;35:*.fli=01;35:*.flv=01;35:*.gl=01;35:*.dl=01;35:*.xcf=01;35:*.xwd=01;35:*.yuv=01;35:*.cgm=
01;35:*.emf=01;35:*.ogv=01;35:*.ogx=01;35:*.aac=00;36:*.au=00;36:*.flac=00;36:*.m4a=00;36:*.mid=00;36:*.midi=00;36:*.mka=00;36:*.mp3=00;36:*.
mpc=00;36:*.ogg=00;36:*.ra=00;36:*.wav=00;36:*.oga=00;36:*.opus=00;36:*.spx=00;36:*.xspf=00;36:
XDG_CURRENT_DESKTOP=ubuntu:GNOME
VTE_VERSION=6003
GNOME_TERMINAL_SCREEN=/org/gnome/Terminal/screen/46909c4c_a4e4_49a9_a62f_232495241ef9
INVOCATION_ID=d20eaadf6d6b45bfb16fd393b33d9238
MANAGERPID=1512
GJS_DEBUG_OUTPUT=stderr
LESSCLOSE=/usr/bin/lesspipe %s %s
XDG_SESSION_CLASS=user
TERM=xterm-256color
LESSOPEN=| /usr/bin/lesspipe %s
USER=seed
GNOME_TERMINAL_SERVICE=:1.210
DISPLAY=:0
SHLVL=1
QT_IM_MODULE=ibus
XDG_RUNTIME_DIR=/run/user/1000
JOURNAL_STREAM=9:32405
XDG_DATA_DIRS=/usr/share/ubuntu:/usr/local/share/:/usr/share/:/var/lib/snapd/desktop
PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games:/snap/bin:.
GDMSESSION=ubuntu
DBUS_SESSION_BUS_ADDRESS=unix:path=/run/user/1000/bus
OLDPWD=/home/seed
_=./ls90
Environmental variable 'inputdir' not set.
[09/26/23]seed@VM:~$
```

4.Yes it is possible to inject additional commands to invoke a shell in a program but it is risky.

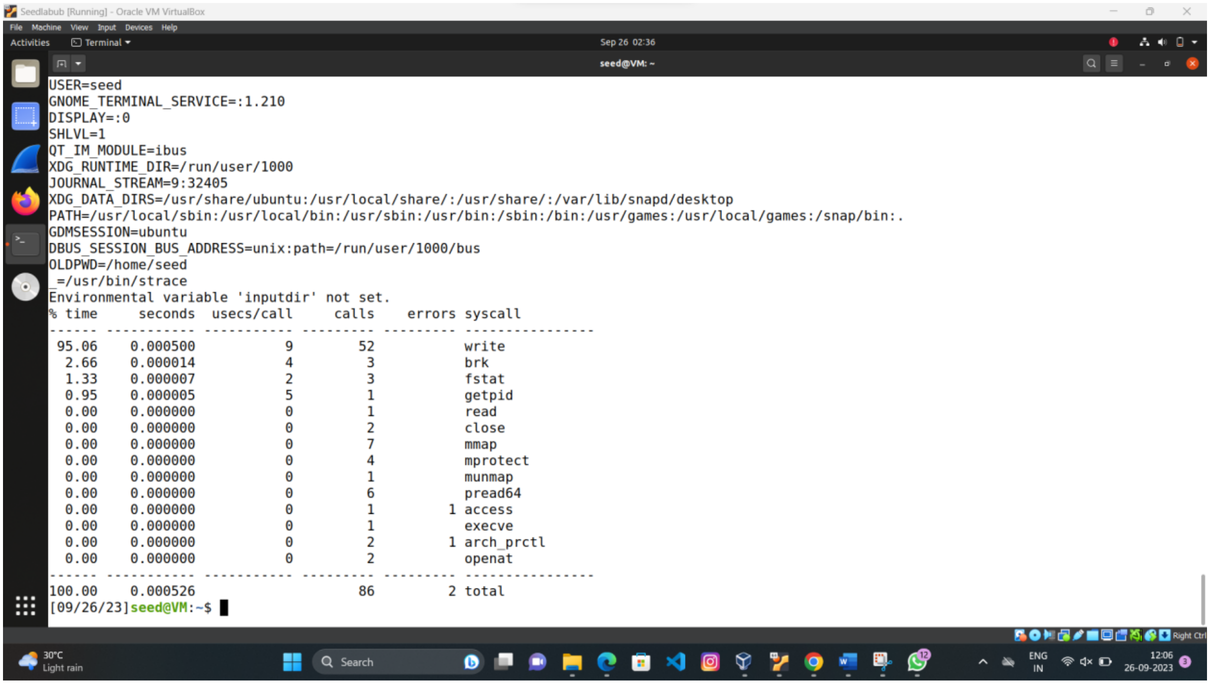
6. Count of the system calls can be found by using

Command – starce -c

OUTPUT:



```
_=./ls90
Environmental variable 'inputdir' not set.
[09/26/23]seed@VM:~$ gedit ls789.c
[09/26/23]seed@VM:~$ gedit ls789.c
[09/26/23]seed@VM:~$ strace -c ./ls90
Parent PID: 7608
SHELL=/bin/bash
SESSION_MANAGER=local/VM:@/tmp/.ICE-unix/1767,unix/VM:/tmp/.ICE-unix/1767
QT_ACCESSIBILITY=1
COLORTERM=truecolor
XDG_CONFIG_DIRS=/etc/xdg/xdg-ubuntu:/etc/xdg
XDG_MENU_PREFIX=gnome-
GNOME_DESKTOP_SESSION_ID=this-is-deprecated
GNOME_SHELL_SESSION_MODE=ubuntu
SSH_AUTH_SOCK=/run/user/1000/keyring/ssh
XMODIFIERS=@im=ibus
DESKTOP_SESSION=ubuntu
SSH_AGENT_PID=1718
GTK_MODULES=gail:atk-bridge
PWD=/home/seed
LOGNAME=seed
XDG_SESSION_DESKTOP=ubuntu
XDG_SESSION_TYPE=x11
GPG_AGENT_INFO=/run/user/1000/gnupg/S.gpg-agent:0:1
XAUTHORITY=/run/user/1000/gdm/Xauthority
GJS_DEBUG_TOPICS=JS ERROR;JS LOG
WINDOWPATH=2
HOME=/home/seed
USERNAME=seed
IM_CONFIG_PHASE=1
LANG=en_US.UTF-8
LS_COLORS=rs=0:di=01;34:ln=01;36:mh=00:pi=40;33:so=01;35:do=01;35:bd=40;33;01:cd=40;33;01:or=40;31;01:mi=00:su=37;41:sg=30;43:ca=30;41:tw=30;
42:ow=34;42:st=37;44:ex=01;32:*.tar=01;31:*.tgz=01;31:*.arc=01;31:*.arj=01;31:*.taz=01;31:*.lha=01;31:*.lz4=01;31:*.lzh=01;31:*.lzma=01;31:*.
tlz=01;31:*.txz=01;31:*.tzo=01;31:*.t7z=01;31:*.zip=01;31:*.z=01;31:*.dz=01;31:*.gz=01;31:*.lrz=01;31:*.lz=01;31:*.lzo=01;31:*.xz=01;31:*.zst
```



```
USER=seed
GNOME_TERMINAL_SERVICE=:1.210
DISPLAY=:0
SHLVL=1
QT_IM_MODULE=ibus
XDG_RUNTIME_DIR=/run/user/1000
JOURNAL_STREAM=9:32405
XDG_DATA_DIRS=/usr/share/ubuntu:/usr/local/share/:/usr/share/:/var/lib/snapd/desktop
PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games:/snap/bin:.
GDMSESSION=ubuntu
DBUS_SESSION_BUS_ADDRESS=unix:path=/run/user/1000/bus
OLDPWD=/home/seed
_=/usr/bin/strace
Environmental variable 'inputdir' not set.
% time     seconds  usecs/call     calls    errors syscall
------ ----------- ----------- --------- --------- ----------------
 95.06    0.000500           9        52           write
  2.66    0.000014           4         3           brk
  1.33    0.000007           2         3           fstat
  0.95    0.000005           5         1           getpid
  0.00    0.000000           0         1           read
  0.00    0.000000           0         2           close
  0.00    0.000000           0         7           mmap
  0.00    0.000000           0         4           mprotect
  0.00    0.000000           0         1           munmap
  0.00    0.000000           0         6           pread64
  0.00    0.000000           0         1         1 access
  0.00    0.000000           0         1           execve
  0.00    0.000000           0         2         1 arch_prctl
  0.00    0.000000           0         2           openat
------ ----------- ----------- --------- --------- ----------------
100.00    0.000526                    86         2 total
[09/26/23]seed@VM:~$ 
```

7. A line of code injects a vulnerability:

```
snprintf (cmd, sizeof(cmd), “ls %s, input directory)
```