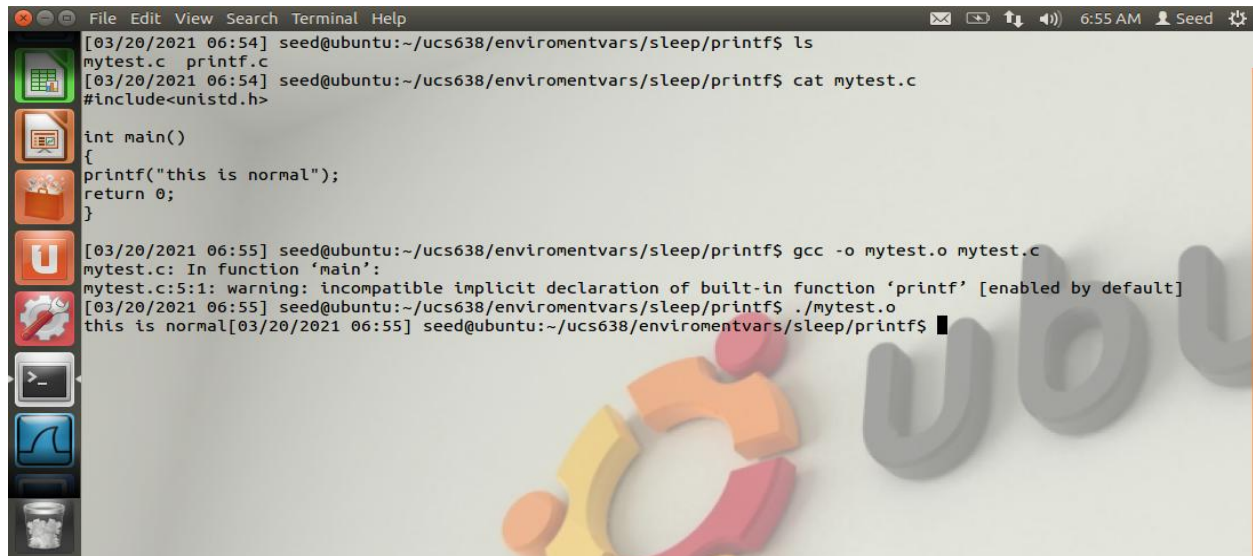


**Q:** Try to change the functionality of printf. Give success and failure scenarios (if any)

**Sol:**

### Successful Attempt

The following program (mytest.c) simply calls the printf function, which is present in libc.so, the standard libc shared library.

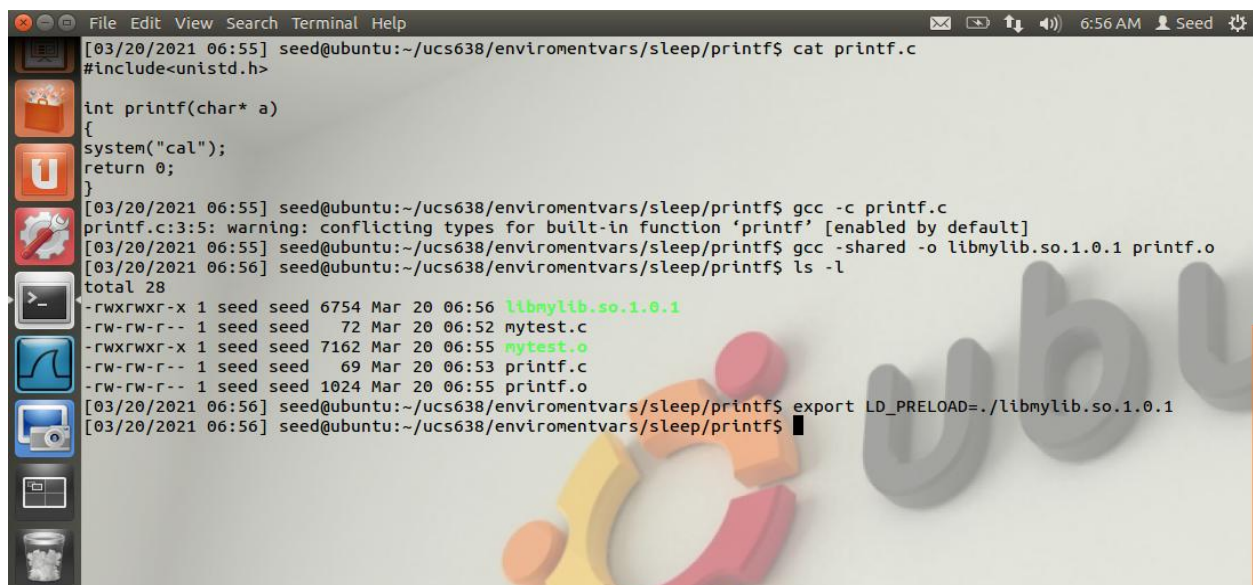


```
[03/20/2021 06:54] seed@ubuntu:~/ucs638/enviromentvars/sleep/printf$ ls
mytest.c  printf.c
[03/20/2021 06:54] seed@ubuntu:~/ucs638/enviromentvars/sleep/printf$ cat mytest.c
#include<unistd.h>

int main()
{
    printf("this is normal");
    return 0;
}
[03/20/2021 06:55] seed@ubuntu:~/ucs638/enviromentvars/sleep/printf$ gcc -o mytest.o mytest.c
mytest.c: In function 'main':
mytest.c:5:1: warning: incompatible implicit declaration of built-in function 'printf' [enabled by default]
[03/20/2021 06:55] seed@ubuntu:~/ucs638/enviromentvars/sleep/printf$ ./mytest.o
this is normal[03/20/2021 06:55] seed@ubuntu:~/ucs638/enviromentvars/sleep/printf$
```

When we compile the above program, by default, the printf function is dynamically linked. Thus, when this program is run, the dynamic linker will find the function in the libc.so library. The program will print for the specified text as expected.

### Molded printf function created by Attacker



```
[03/20/2021 06:55] seed@ubuntu:~/ucs638/enviromentvars/sleep/printf$ cat printf.c
#include<unistd.h>

int printf(char* a)
{
    system("cal");
    return 0;
}
[03/20/2021 06:55] seed@ubuntu:~/ucs638/enviromentvars/sleep/printf$ gcc -c printf.c
printf.c:3:5: warning: conflicting types for built-in function 'printf' [enabled by default]
[03/20/2021 06:55] seed@ubuntu:~/ucs638/enviromentvars/sleep/printf$ gcc -shared -o libmylib.so.1.0.1 printf.o
[03/20/2021 06:56] seed@ubuntu:~/ucs638/enviromentvars/sleep/printf$ ls -l
total 28
-rwxrwxr-x 1 seed seed 6754 Mar 20 06:56 libmylib.so.1.0.1
-rw-rw-r-- 1 seed seed 72 Mar 20 06:52 mytest.c
-rwxrwxr-x 1 seed seed 7162 Mar 20 06:55 mytest.o
-rw-rw-r-- 1 seed seed 69 Mar 20 06:53 printf.c
-rw-rw-r-- 1 seed seed 1024 Mar 20 06:55 printf.o
[03/20/2021 06:56] seed@ubuntu:~/ucs638/enviromentvars/sleep/printf$ export LD_PRELOAD=./libmylib.so.1.0.1
[03/20/2021 06:56] seed@ubuntu:~/ucs638/enviromentvars/sleep/printf$
```

Attacker needed to compile the above code, create a shared library, and add the shared library to the LD\_PRELOAD environment variable.

A terminal window on an Ubuntu system. The title bar shows 'File Edit View Search Terminal Help' and the system clock is 6:56 AM. The user 'seed' is logged in. The prompt is 'seed@ubuntu:~/ucs638/enviromentvars/sleep/printf\$'. The user enters './mytest.o'. The output shows a calendar for March 2021 with the 20th highlighted. The prompt changes to 'seed@ubuntu:~/ucs638/enviromentvars/sleep/printf\$'.

```
[03/20/2021 06:56] seed@ubuntu:~/ucs638/enviromentvars/sleep/printf$ ./mytest.o
March 2021
Su Mo Tu We Th Fr Sa
      1  2  3  4  5  6
 7  8  9 10 11 12 13
14 15 16 17 18 19 20
21 22 23 24 25 26 27
28 29 30 31

[03/20/2021 06:56] seed@ubuntu:~/ucs638/enviromentvars/sleep/printf$
```

After that, if we run our previous mytest program again, we can see from the above result that attacker's printf function is invoked instead of the one from libc.

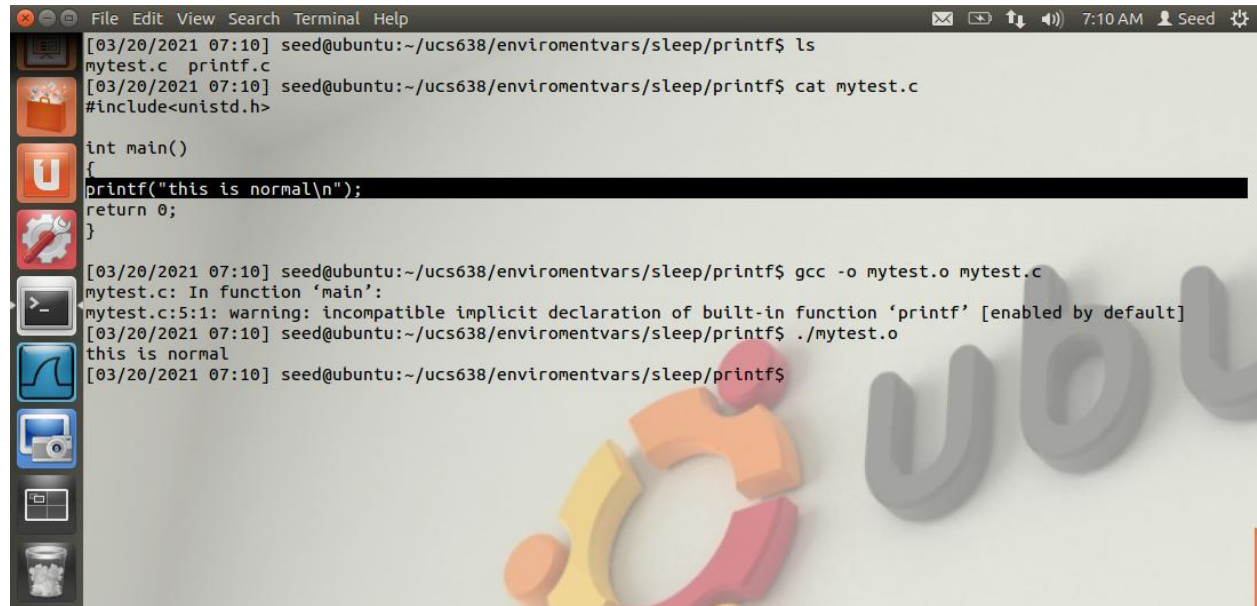
A terminal window on an Ubuntu system. The title bar shows 'File Edit View Search Terminal Help' and the system clock is 7:07 AM. The user 'seed' is logged in. The prompt is 'seed@ubuntu:~/ucs638/enviromentvars/sleep/printf\$'. The user enters 'unset LD\_PRELOAD'. The prompt changes to 'seed@ubuntu:~/ucs638/enviromentvars/sleep/printf\$'. The user enters './mytest.o'. The output is 'this is normal'. The prompt changes to 'seed@ubuntu:~/ucs638/enviromentvars/sleep/printf\$'.

```
[03/20/2021 07:06] seed@ubuntu:~/ucs638/enviromentvars/sleep/printf$ unset LD_PRELOAD
[03/20/2021 07:07] seed@ubuntu:~/ucs638/enviromentvars/sleep/printf$ ./mytest.o
this is normal[03/20/2021 07:07] seed@ubuntu:~/ucs638/enviromentvars/sleep/printf$
```

If we unset the environment variable, everything goes back to normal.

### Unsuccessful Attempt

The following program (mytest.c) simply calls the printf function, same as previous program. The only difference is of '\n' at the end of string argument in printf function.

A terminal window on an Ubuntu system. The user is in the directory ~/ucs638/enviromentvars/sleep/printf. They list files, showing mytest.c and printf.c. They then view mytest.c, which contains a main function that calls printf("this is normal\n");. The user compiles mytest.c with gcc -o mytest.o mytest.c. A warning is shown about an incompatible implicit declaration of printf. Finally, they run ./mytest.o, which outputs "this is normal".

```
[03/20/2021 07:10] seed@ubuntu:~/ucs638/enviromentvars/sleep/printf$ ls
mytest.c  printf.c
[03/20/2021 07:10] seed@ubuntu:~/ucs638/enviromentvars/sleep/printf$ cat mytest.c
#include<unistd.h>

int main()
{
    printf("this is normal\n");
    return 0;
}
[03/20/2021 07:10] seed@ubuntu:~/ucs638/enviromentvars/sleep/printf$ gcc -o mytest.o mytest.c
mytest.c: In function 'main':
mytest.c:5:1: warning: incompatible implicit declaration of built-in function 'printf' [enabled by default]
[03/20/2021 07:10] seed@ubuntu:~/ucs638/enviromentvars/sleep/printf$ ./mytest.o
this is normal
[03/20/2021 07:10] seed@ubuntu:~/ucs638/enviromentvars/sleep/printf$
```

Following same procedure as previous program, this one is also compiled and run, as displayed above.

### Molded printf function created by Attacker

A terminal window on an Ubuntu system. The user is in the directory ~/ucs638/enviromentvars/sleep/printf. They view printf.c, which contains a printf function that calls system("cal");. They then compile printf.c with gcc -c printf.c. A warning is shown about conflicting types for printf. Next, they create a shared library libmylib.so.1.0.1 with gcc -shared -o libmylib.so.1.0.1 printf.o. Finally, they set the LD\_PRELOAD environment variable to ./libmylib.so.1.0.1 and run the program.

```
[03/20/2021 07:14] seed@ubuntu:~/ucs638/enviromentvars/sleep/printf$ cat printf.c
#include<unistd.h>

int printf(char* a)
{
    system("cal");
    return 0;
}
[03/20/2021 07:14] seed@ubuntu:~/ucs638/enviromentvars/sleep/printf$ gcc -c printf.c
printf.c:3:5: warning: conflicting types for built-in function 'printf' [enabled by default]
[03/20/2021 07:14] seed@ubuntu:~/ucs638/enviromentvars/sleep/printf$ gcc -shared -o libmylib.so.1.0.1 printf.o
[03/20/2021 07:14] seed@ubuntu:~/ucs638/enviromentvars/sleep/printf$ export LD_PRELOAD=./libmylib.so.1.0.1
[03/20/2021 07:15] seed@ubuntu:~/ucs638/enviromentvars/sleep/printf$
```

Above procedure is same as previous one. Attacker needed to compile the above code, create a shared library, and add the shared library to the LD\_PRELOAD environment variable.

A terminal window on an Ubuntu system. The window title is "Terminal". The menu bar includes "File", "Edit", "View", "Search", "Terminal", and "Help". The status bar at the bottom shows the date and time as "03/20/2021 07:16", the user as "seed", and the host as "ubuntu". The terminal content shows a prompt "seed@ubuntu:~/ucs638/enviromentvars/sleep/printf\$ ./mytest.o" followed by the output "this is normal". The next prompt is "seed@ubuntu:~/ucs638/enviromentvars/sleep/printf\$". The background of the terminal window features a large, stylized "ubuntu" logo in the bottom right corner.

```
[03/20/2021 07:16] seed@ubuntu:~/ucs638/enviromentvars/sleep/printf$ ./mytest.o
this is normal
[03/20/2021 07:16] seed@ubuntu:~/ucs638/enviromentvars/sleep/printf$
```

After that, if we run our mytest program again, we can see from the above result that attacker's printf function is not invoked at all, but the one from libc is (as it should have in normal).

A terminal window on an Ubuntu system, similar to the one above. The status bar shows the time as "03/20/2021 07:18". The terminal content shows a prompt "seed@ubuntu:~/ucs638/enviromentvars/sleep/printf\$ env | grep "LD"" followed by the output "LD\_PRELOAD=./libmylib.so.1.0.1". The next prompt is "seed@ubuntu:~/ucs638/enviromentvars/sleep/printf\$". The background of the terminal window features a large, stylized "ubuntu" logo in the bottom right corner.

```
[03/20/2021 07:18] seed@ubuntu:~/ucs638/enviromentvars/sleep/printf$ env | grep "LD"
LD_PRELOAD=./libmylib.so.1.0.1
OLDPWD=/home/seed
[03/20/2021 07:18] seed@ubuntu:~/ucs638/enviromentvars/sleep/printf$
```

Although, the shared library has been added to the LD\_PRELOAD environment variable successfully, the attack is not successful.

The only difference made is '\n' delimiter at the end of string argument, passed in printf function.