Ishita Hardasmalani

C14-2103058

EXPERIMENT NO. 10

Aim: Simulation of Buffer Overflow Attack

Theory:

Buffer overflow is a mistake that exist in some C implementations. These classes of bugs are dangerous as they write past the end of a buffer or array and hence corrupt the process stack They often change the return address of a process after a function call to a secret memory location where a malicious code is planted.

There are main two types

- Stack based attacks
- Heap based attacks

Heap-based attacks flood the memory space reserved for a program, but the difficulty involved with performing such an attack makes them rare. Stack-based buffer overflows are by far the most common.

Splint is a tool for statically checking C programs for security vulnerabilities and programming mistakes. Splint does many of the traditional lint checks including unused declarations, type inconsistencies, use before definition, unreachable code, ignored return values, execution paths with no return, likely infinite loops, and fall through cases. More powerful checks are made possible by additional information given in source code annotations. Annotations are stylized comments that document assumptions about functions, variables, parameters and types. In addition to the checks specifically enabled by annotations, many of the traditional lint checks are improved by exploiting this additional information. Splint is designed to be flexible and allow programmers to select appropriate points on the effort benefit curve for particular projects. As different checks are turned on and more information is given in code annotations the number of bugs that can be detected increases dramatically.

Problems detected by Splint include:

- Dereferencing a possibly null pointer
- Using possibly undefined storage or returning storage that is not properly defined
- Type mismatches, with greater precision and flexibility than provided by C compilers
- Violations of information hiding
- Memory management errors including uses of dangling references and memory leaks
- Dangerous aliasing
- Modifications and global variable uses that are inconsistent with specified interfaces

• Problematic control flow such as likely infinite loops, fall through cases or incomplete switches and suspicious statements

• Buffer overflow vulnerabilities

• Dangerous macro implementations or invocations

• Violations of customized naming conventions

Steps :

1. Installation

$ sudo apt-get install splint

2. Checking Vulnerability

$ splint program1.c

Program1.c is the program whose vulnerability is to be checked.

```
#include <stdio.h>
#include <string.h>
int main(void)
{
 char buff[15];
 int pass = 0;
 printf("\n Enter the password : \n");
 gets(buff);
 if(strcmp(buff, "thegeekstuff"))
 {
 printf ("\n Wrong Password \n");
 }
 else
 {
 printf ("\n Correct Password \n");
 pass = 1;
```

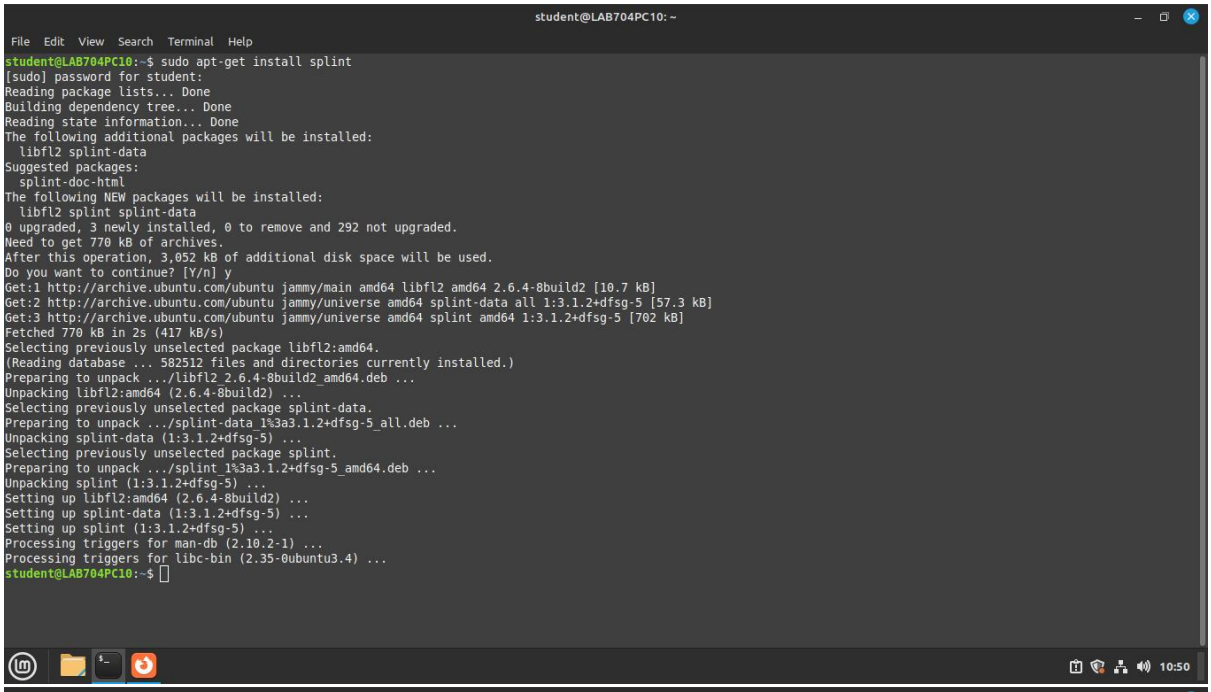
Program-2

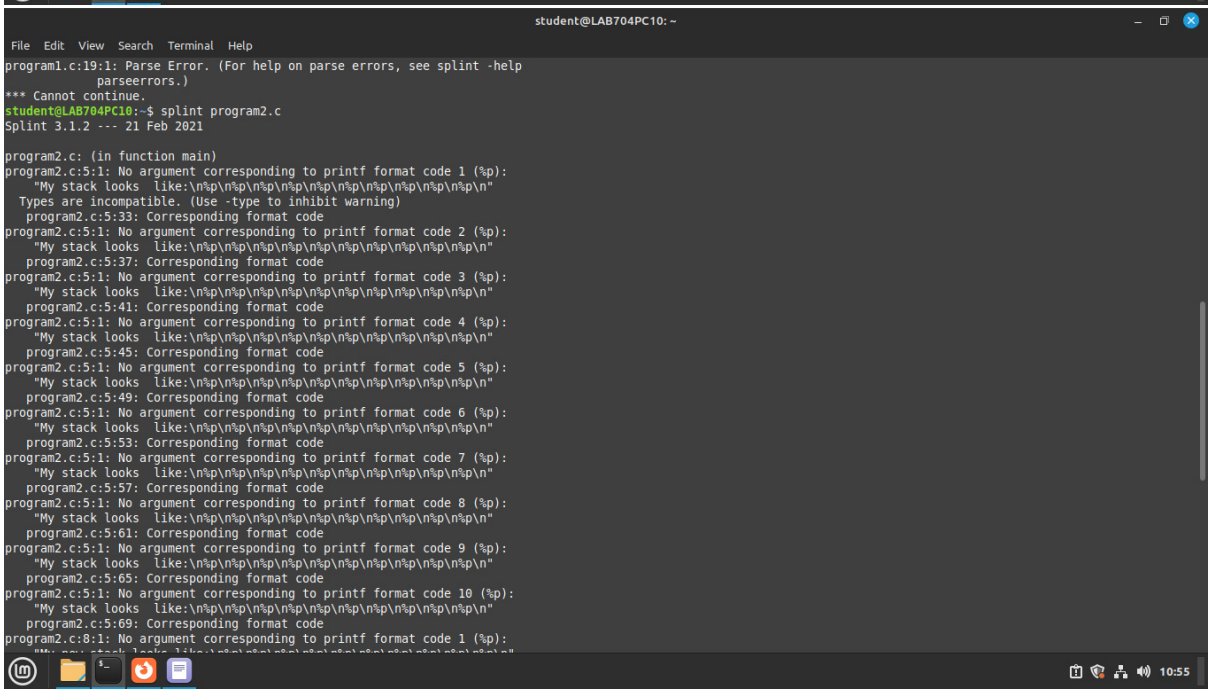
```
#include<stdio.h>
main()
{
char buff[5];
printf("My stack looks
like:\n%p\n%p\n%p\n%p\n%p\n%p\n%p\n%p\n%p\n%p\n%p\n");
buff[5]='abcdefghijklmnophsgkgfks';
printf("%c\n",buff[5]);
printf("My new stack looks
like:\n%p\n%p\n%p\n%p\n%p\n%p\n%p\n%p\n%p\n%p\n%p\n");
}
```

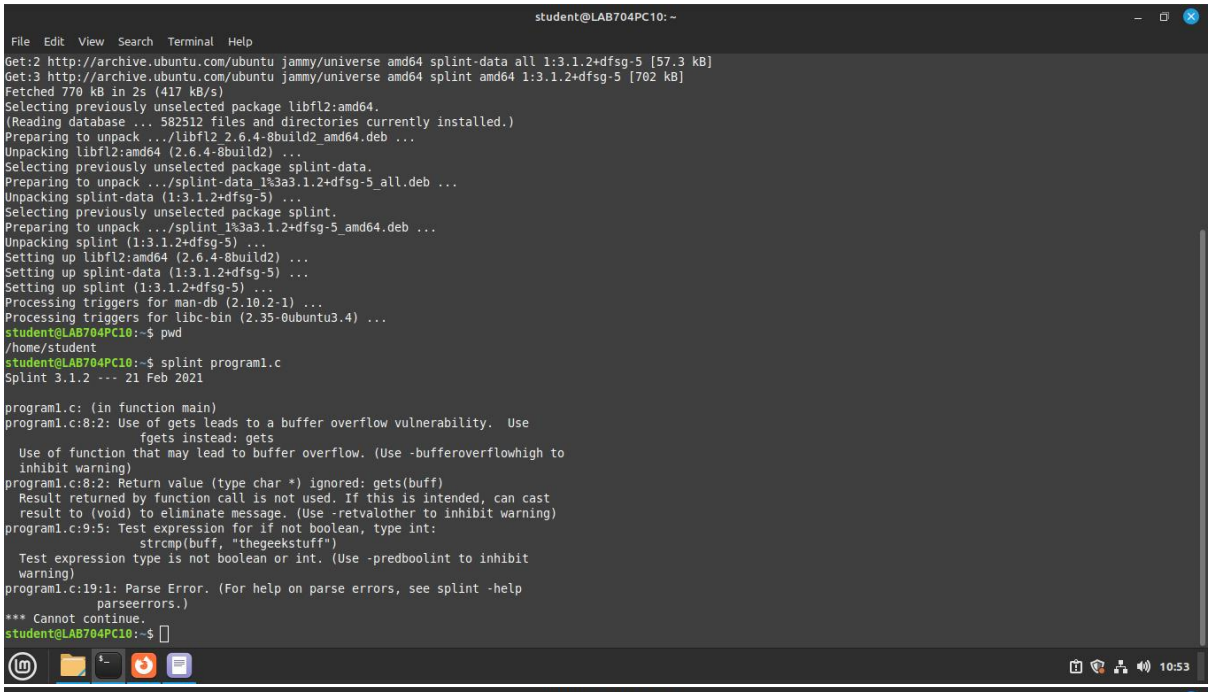
Program 3

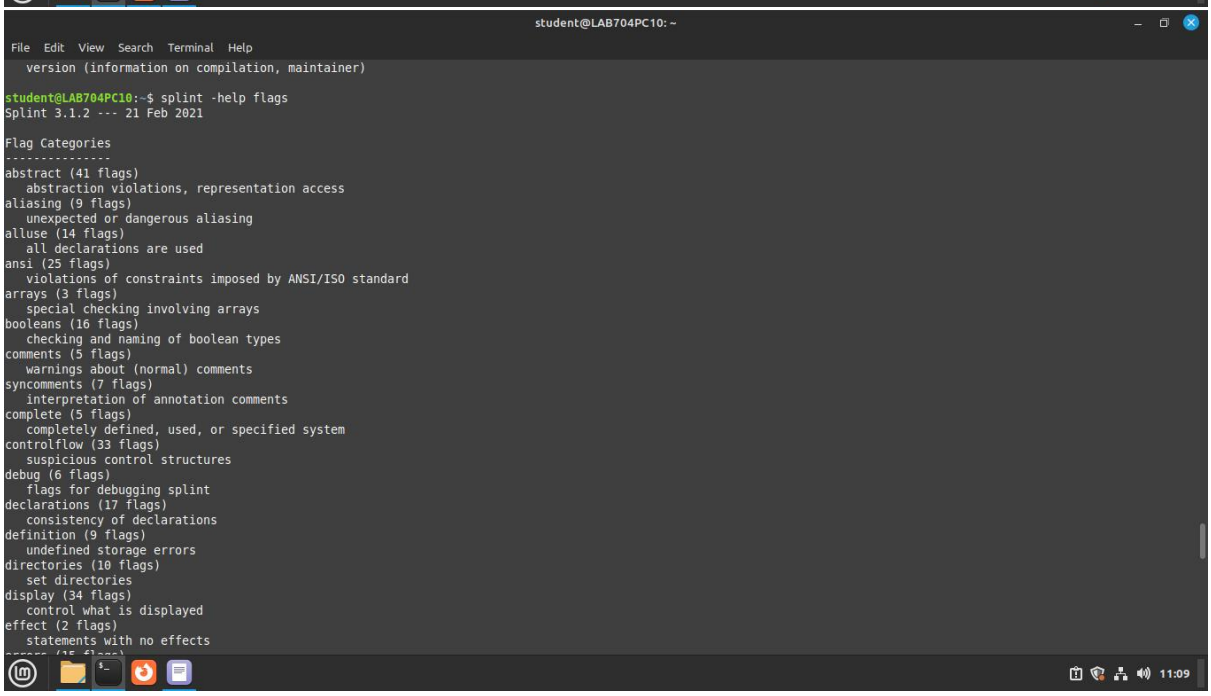
```
#include <stdio.h>
#include <string.h>
char password[] = "password";
int get_password() {
 int auth_ok = 0;
 char buff[16];
 printf("Enter password: ");
 scanf("%s", buff);
 if(strncmp(buff, password, sizeof(password)) == 0)
 auth_ok = 1;
 return auth_ok; }
void success() {
 printf("Success!
\n");
}
int main(int argc, char** argv) {
```

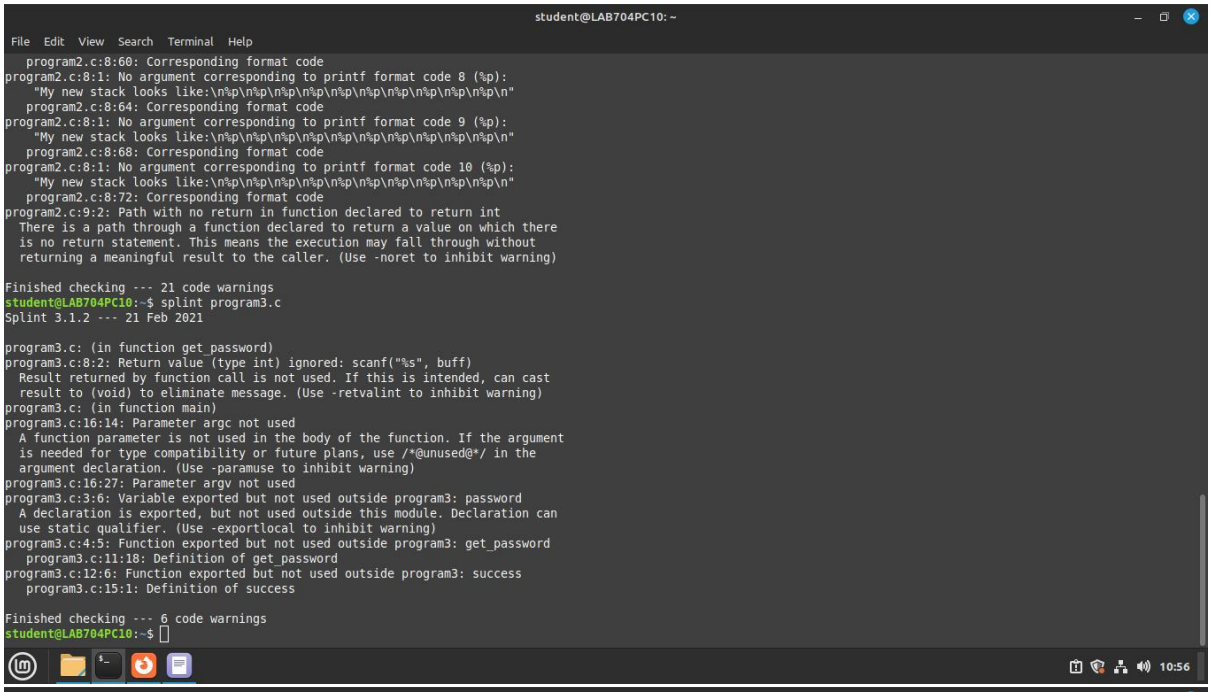
```
int res = get_password();
if (res == 0) {
printf("Failure \n");
return 0;
}
success();
return 0;
}
```

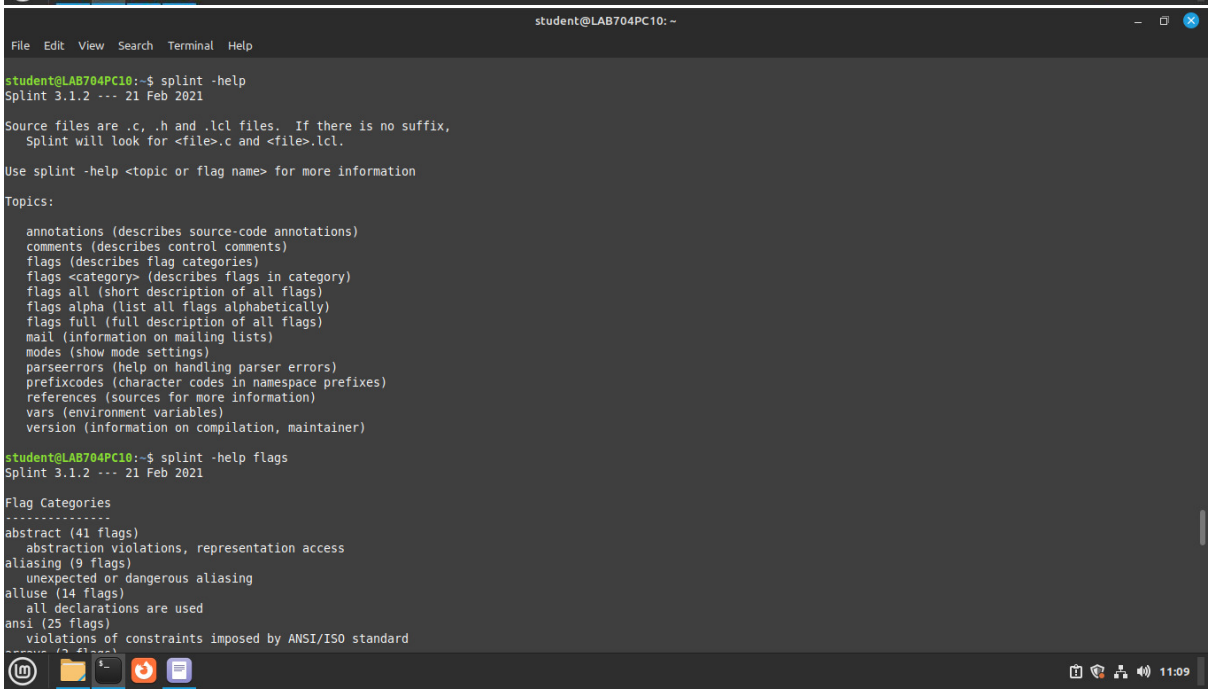

student@LAB704PC10: ~
File Edit View Search Terminal Help
student@LAB704PC10:~$ sudo apt-get install splint
[sudo] password for student:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
libfl2 splint-data
Suggested packages:
splint-doc-html
The following NEW packages will be installed:
libfl2 splint splint-data
0 upgraded, 3 newly installed, 0 to remove and 292 not upgraded.
Need to get 770 kB of archives.
After this operation, 3,052 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://archive.ubuntu.com/ubuntu jammy/main amd64 libfl2 amd64 2.6.4-8build2 [10.7 kB]
Get:2 http://archive.ubuntu.com/ubuntu jammy/universe amd64 splint-data all 1:3.1.2+dfsg-5 [57.3 kB]
Get:3 http://archive.ubuntu.com/ubuntu jammy/universe amd64 splint amd64 1:3.1.2+dfsg-5 [702 kB]
Fetched 770 kB in 2s (417 kB/s)
Selecting previously unselected package libfl2:amd64.
(Reading database ... 582512 files and directories currently installed.)
Preparing to unpack .../libfl2_2.6.4-8build2_amd64.deb ...
Unpacking libfl2:amd64 (2.6.4-8build2) ...
Selecting previously unselected package splint-data.
Preparing to unpack .../splint-data_1%3a3.1.2+dfsg-5_all.deb ...
Unpacking splint-data (1:3.1.2+dfsg-5) ...
Selecting previously unselected package splint.
Preparing to unpack .../splint_1%3a3.1.2+dfsg-5_amd64.deb ...
Unpacking splint (1:3.1.2+dfsg-5) ...
Setting up libfl2:amd64 (2.6.4-8build2) ...
Setting up splint-data (1:3.1.2+dfsg-5) ...
Setting up splint (1:3.1.2+dfsg-5) ...
Processing triggers for man-db (2.10.2-1) ...
Processing triggers for libc-bin (2.35-0ubuntu3.4) ...
student@LAB704PC10:~$
10:50

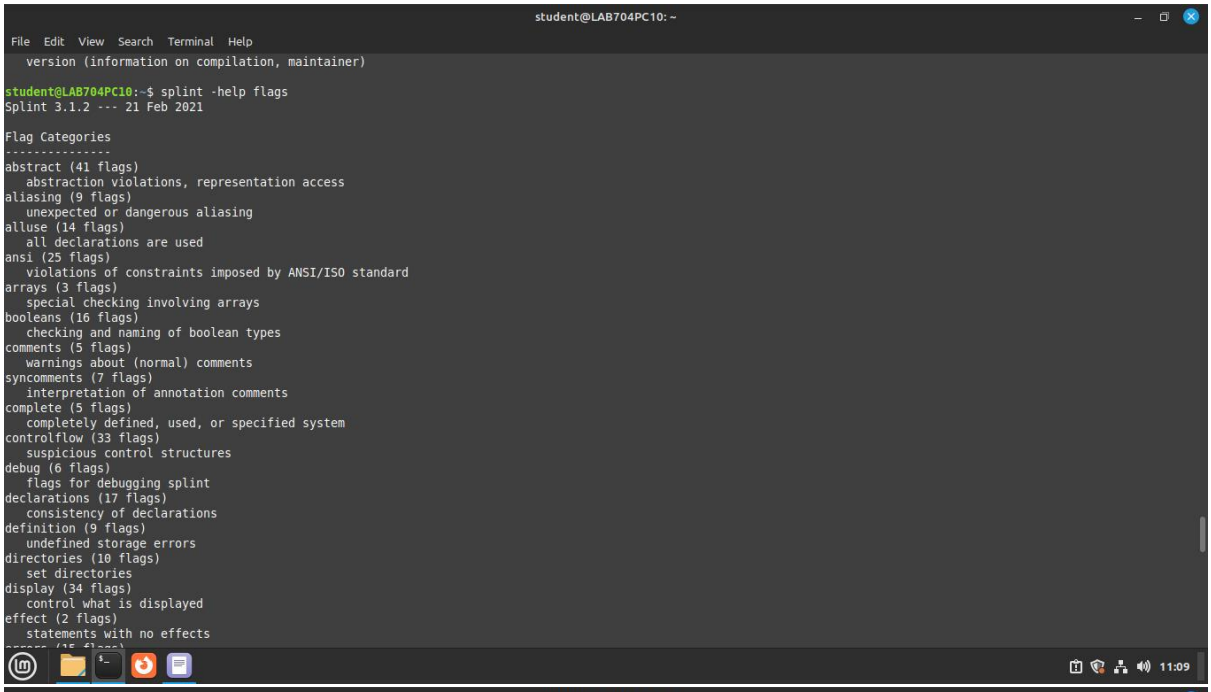

student@LAB704PC10: ~
File Edit View Search Terminal Help
program1.c:19:1: Parse Error. (For help on parse errors, see splint -help
parseerrors.)
*** Cannot continue.
student@LAB704PC10:~$ splint program2.c
Splint 3.1.2 --- 21 Feb 2021
program2.c: (in function main)
program2.c:5:1: No argument corresponding to printf format code 1 (%p):
"My stack looks like:\n%p\n%p\n%p\n%p\n%p\n%p\n%p\n%p\n%p\n%p\n"
Types are incompatible. (Use -type to inhibit warning)
program2.c:5:33: Corresponding format code
program2.c:5:1: No argument corresponding to printf format code 2 (%p):
"My stack looks like:\n%p\n%p\n%p\n%p\n%p\n%p\n%p\n%p\n%p\n%p\n"
program2.c:5:37: Corresponding format code
program2.c:5:1: No argument corresponding to printf format code 3 (%p):
"My stack looks like:\n%p\n%p\n%p\n%p\n%p\n%p\n%p\n%p\n%p\n%p\n"
program2.c:5:41: Corresponding format code
program2.c:5:1: No argument corresponding to printf format code 4 (%p):
"My stack looks like:\n%p\n%p\n%p\n%p\n%p\n%p\n%p\n%p\n%p\n%p\n"
program2.c:5:45: Corresponding format code
program2.c:5:1: No argument corresponding to printf format code 5 (%p):
"My stack looks like:\n%p\n%p\n%p\n%p\n%p\n%p\n%p\n%p\n%p\n%p\n"
program2.c:5:49: Corresponding format code
program2.c:5:1: No argument corresponding to printf format code 6 (%p):
"My stack looks like:\n%p\n%p\n%p\n%p\n%p\n%p\n%p\n%p\n%p\n%p\n"
program2.c:5:53: Corresponding format code
program2.c:5:1: No argument corresponding to printf format code 7 (%p):
"My stack looks like:\n%p\n%p\n%p\n%p\n%p\n%p\n%p\n%p\n%p\n%p\n"
program2.c:5:57: Corresponding format code
program2.c:5:1: No argument corresponding to printf format code 8 (%p):
"My stack looks like:\n%p\n%p\n%p\n%p\n%p\n%p\n%p\n%p\n%p\n%p\n"
program2.c:5:61: Corresponding format code
program2.c:5:1: No argument corresponding to printf format code 9 (%p):
"My stack looks like:\n%p\n%p\n%p\n%p\n%p\n%p\n%p\n%p\n%p\n%p\n"
program2.c:5:65: Corresponding format code
program2.c:5:1: No argument corresponding to printf format code 10 (%p):
"My stack looks like:\n%p\n%p\n%p\n%p\n%p\n%p\n%p\n%p\n%p\n%p\n"
program2.c:5:69: Corresponding format code
program2.c:8:1: No argument corresponding to printf format code 1 (%p):
10:55

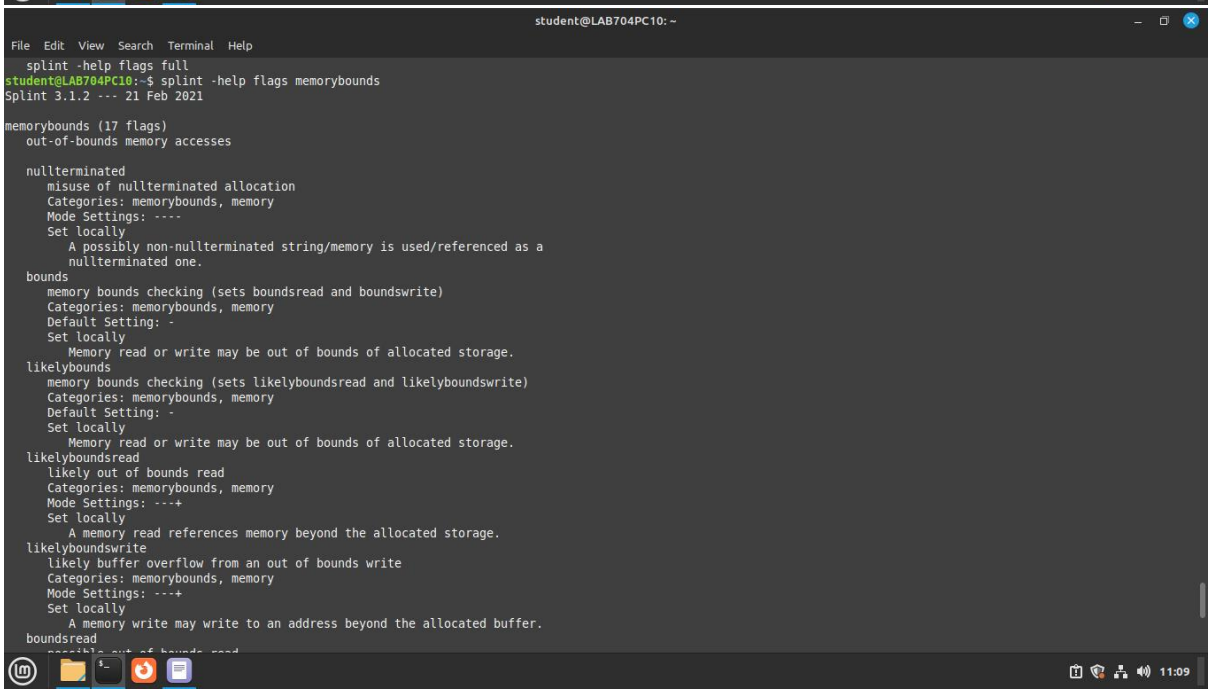

student@LAB704PC10: ~
File Edit View Search Terminal Help
Get:2 http://archive.ubuntu.com/ubuntu jammy/universe amd64 splint-data all 1:3.1.2+dfsg-5 [57.3 kB]
Get:3 http://archive.ubuntu.com/ubuntu jammy/universe amd64 splint amd64 1:3.1.2+dfsg-5 [702 kB]
Fetched 770 kB in 2s (417 kB/s)
Selecting previously unselected package libfl2:amd64.
(Reading database ... 582512 files and directories currently installed.)
Preparing to unpack .../libfl2_2.6.4-8build2_amd64.deb ...
Unpacking libfl2:amd64 (2.6.4-8build2) ...
Selecting previously unselected package splint-data.
Preparing to unpack .../splint-data_1%3a3.1.2+dfsg-5_all.deb ...
Unpacking splint-data (1:3.1.2+dfsg-5) ...
Selecting previously unselected package splint.
Preparing to unpack .../splint_1%3a3.1.2+dfsg-5_amd64.deb ...
Unpacking splint (1:3.1.2+dfsg-5) ...
Setting up libfl2:amd64 (2.6.4-8build2) ...
Setting up splint-data (1:3.1.2+dfsg-5) ...
Setting up splint (1:3.1.2+dfsg-5) ...
Processing triggers for man-db (2.10.2-1) ...
Processing triggers for libc-bin (2.35-0ubuntu3.4) ...
student@LAB704PC10:~$ pwd
/home/student
student@LAB704PC10:~$ splint program1.c
Splint 3.1.2 --- 21 Feb 2021
program1.c: (in function main)
program1.c:8:2: Use of gets leads to a buffer overflow vulnerability. Use
fgets instead: gets
Use of function that may lead to buffer overflow. (Use -bufferoverflowhigh to
inhibit warning)
program1.c:8:2: Return value (type char *) ignored: gets(buff)
Result returned by function call is not used. If this is intended, can cast
result to (void) to eliminate message. (Use -retvalother to inhibit warning)
program1.c:9:5: Test expression for if not boolean, type int:
strcmp(buff, "thegeekstuff")
Test expression type is not boolean or int. (Use -predboolint to inhibit
warning)
program1.c:19:1: Parse Error. (For help on parse errors, see splint -help
parseerrors.)
*** Cannot continue.
student@LAB704PC10:~$
10:53

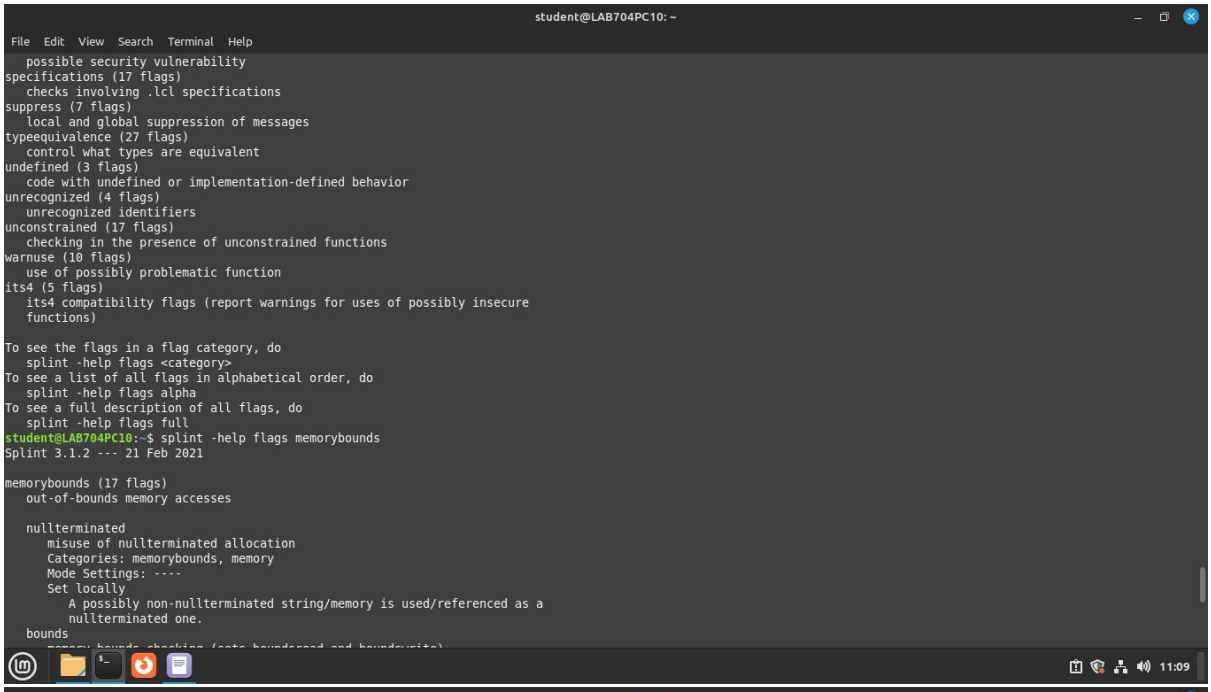

student@LAB704PC10: ~
File Edit View Search Terminal Help
version (information on compilation, maintainer)
student@LAB704PC10:~$ splint -help flags
Splint 3.1.2 --- 21 Feb 2021
Flag Categories
abstract (41 flags)
abstraction violations, representation access
aliasing (9 flags)
unexpected or dangerous aliasing
alluse (14 flags)
all declarations are used
ansi (25 flags)
violations of constraints imposed by ANSI/ISO standard
arrays (3 flags)
special checking involving arrays
booleans (16 flags)
checking and naming of boolean types
comments (5 flags)
warnings about (normal) comments
syncomments (7 flags)
interpretation of annotation comments
complete (5 flags)
completely defined, used, or specified system
controlflow (33 flags)
suspicious control structures
debug (6 flags)
flags for debugging splint
declarations (17 flags)
consistency of declarations
definition (9 flags)
undefined storage errors
directories (10 flags)
set directories
display (34 flags)
control what is displayed
effect (2 flags)
statements with no effects
11:09

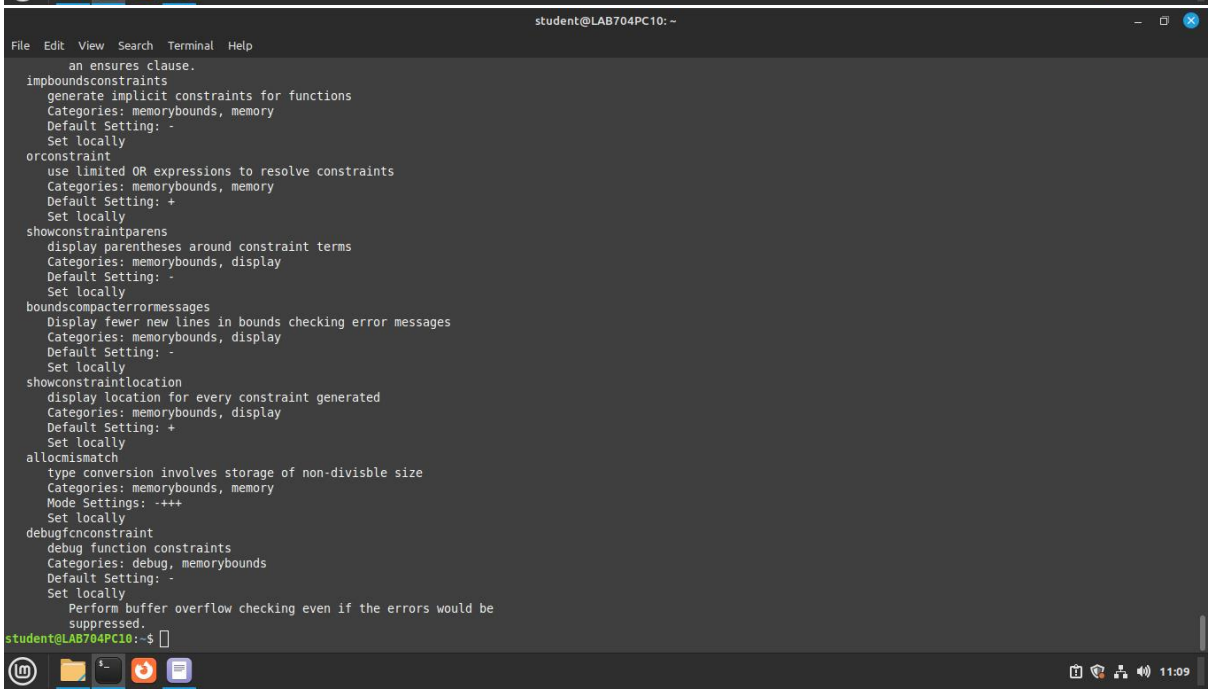

student@LAB704PC10: ~
File Edit View Search Terminal Help
program2.c:8:60: Corresponding format code
program2.c:8:1: No argument corresponding to printf format code 8 (%p):
"My new stack looks like:\n%p\n%p\n%p\n%p\n%p\n%p\n%p\n%p\n%p\n"
program2.c:8:64: Corresponding format code
program2.c:8:1: No argument corresponding to printf format code 9 (%p):
"My new stack looks like:\n%p\n%p\n%p\n%p\n%p\n%p\n%p\n%p\n%p\n%p\n"
program2.c:8:68: Corresponding format code
program2.c:8:1: No argument corresponding to printf format code 10 (%p):
"My new stack looks like:\n%p\n%p\n%p\n%p\n%p\n%p\n%p\n%p\n%p\n%p\n%p\n"
program2.c:8:72: Corresponding format code
program2.c:9:2: Path with no return in function declared to return int
There is a path through a function declared to return a value on which there
is no return statement. This means the execution may fall through without
returning a meaningful result to the caller. (Use -noret to inhibit warning)
Finished checking --- 21 code warnings
student@LAB704PC10:~$ splint program3.c
Splint 3.1.2 --- 21 Feb 2021
program3.c: (in function get_password)
program3.c:8:2: Return value (type int) ignored: scanf("%s", buff)
Result returned by function call is not used. If this is intended, can cast
result to (void) to eliminate message. (Use -retvalint to inhibit warning)
program3.c: (in function main)
program3.c:16:14: Parameter argc not used
A function parameter is not used in the body of the function. If the argument
is needed for type compatibility or future plans, use /*@unused@*/ in the
argument declaration. (Use -paramuse to inhibit warning)
program3.c:16:27: Parameter argv not used
program3.c:3:6: Variable exported but not used outside program3: password
A declaration is exported, but not used outside this module. Declaration can
use static qualifier. (Use -exportlocal to inhibit warning)
program3.c:4:5: Function exported but not used outside program3: get_password
program3.c:11:18: Definition of get_password
program3.c:12:6: Function exported but not used outside program3: success
program3.c:15:1: Definition of success
Finished checking --- 6 code warnings
student@LAB704PC10:~$
10:56

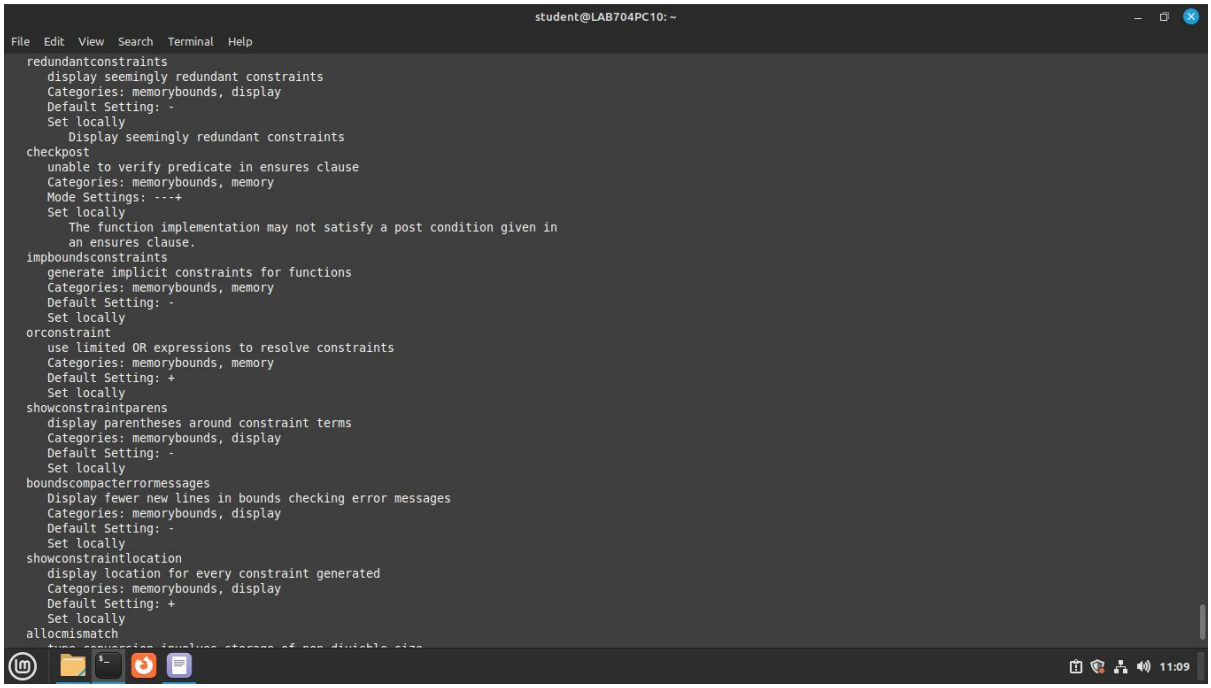

student@LAB704PC10: ~
File Edit View Search Terminal Help
student@LAB704PC10:~$ splint -help
Splint 3.1.2 --- 21 Feb 2021
Source files are .c, .h and .lcl files. If there is no suffix,
Splint will look for <file>.c and <file>.lcl.
Use splint -help <topic or flag name> for more information
Topics:
annotations (describes source-code annotations)
comments (describes control comments)
flags (describes flag categories)
flags <category> (describes flags in category)
flags all (short description of all flags)
flags alpha (list all flags alphabetically)
flags full (full description of all flags)
mail (information on mailing lists)
modes (show mode settings)
parseerrors (help on handling parser errors)
prefixcodes (character codes in namespace prefixes)
references (sources for more information)
vars (environment variables)
version (information on compilation, maintainer)
student@LAB704PC10:~$ splint -help flags
Splint 3.1.2 --- 21 Feb 2021
Flag Categories
abstract (41 flags)
abstraction violations, representation access
aliasing (9 flags)
unexpected or dangerous aliasing
alluse (14 flags)
all declarations are used
ansi (25 flags)
violations of constraints imposed by ANSI/ISO standard
11:09


student@LAB704PC10: ~
File Edit View Search Terminal Help
version (information on compilation, maintainer)
student@LAB704PC10:~$ splint -help flags
Splint 3.1.2 --- 21 Feb 2021
Flag Categories
abstract (41 flags)
abstraction violations, representation access
aliasing (9 flags)
unexpected or dangerous aliasing
alluse (14 flags)
all declarations are used
ansi (25 flags)
violations of constraints imposed by ANSI/ISO standard
arrays (3 flags)
special checking involving arrays
booleans (16 flags)
checking and naming of boolean types
comments (5 flags)
warnings about (normal) comments
syncomments (7 flags)
interpretation of annotation comments
complete (5 flags)
completely defined, used, or specified system
controlflow (33 flags)
suspicious control structures
debug (6 flags)
flags for debugging splint
declarations (17 flags)
consistency of declarations
definition (9 flags)
undefined storage errors
directories (10 flags)
set directories
display (34 flags)
control what is displayed
effect (2 flags)
statements with no effects
11:09


student@LAB704PC10: ~
File Edit View Search Terminal Help
splint -help flags full
student@LAB704PC10:~$ splint -help flags memorybounds
Splint 3.1.2 --- 21 Feb 2021
memorybounds (17 flags)
out-of-bounds memory accesses
nullterminated
misuse of nullterminated allocation
Categories: memorybounds, memory
Mode Settings: ----
Set locally
A possibly non-nullterminated string/memory is used/referenced as a
nullterminated one.
bounds
memory bounds checking (sets boundsread and boundswrite)
Categories: memorybounds, memory
Default Setting: -
Set locally
Memory read or write may be out of bounds of allocated storage.
likelybounds
memory bounds checking (sets likelyboundsread and likelyboundswrite)
Categories: memorybounds, memory
Default Setting: -
Set locally
Memory read or write may be out of bounds of allocated storage.
likelyboundsread
likely out of bounds read
Categories: memorybounds, memory
Mode Settings: ---+
Set locally
A memory read references memory beyond the allocated storage.
likelyboundswrite
likely buffer overflow from an out of bounds write
Categories: memorybounds, memory
Mode Settings: ---+
Set locally
A memory write may write to an address beyond the allocated buffer.
boundsread
11:09


student@LAB704PC10: ~
File Edit View Search Terminal Help
possible security vulnerability
specifications (17 flags)
checks involving .lcl specifications
suppress (7 flags)
local and global suppression of messages
typeequivalence (27 flags)
control what types are equivalent
undefined (3 flags)
code with undefined or implementation-defined behavior
unrecognized (4 flags)
unrecognized identifiers
unconstrained (17 flags)
checking in the presence of unconstrained functions
warnuse (10 flags)
use of possibly problematic function
its4 (5 flags)
its4 compatibility flags (report warnings for uses of possibly insecure
functions)
To see the flags in a flag category, do
splint -help flags <category>
To see a list of all flags in alphabetical order, do
splint -help flags alpha
To see a full description of all flags, do
splint -help flags full
student@LAB704PC10:~$ splint -help flags memorybounds
Splint 3.1.2 --- 21 Feb 2021
memorybounds (17 flags)
out-of-bounds memory accesses
nullterminated
misuse of nullterminated allocation
Categories: memorybounds, memory
Mode Settings: ----
Set locally
A possibly non-nullterminated string/memory is used/referenced as a
nullterminated one.
bounds
11:09


student@LAB704PC10: ~
File Edit View Search Terminal Help
an ensures clause.
impboundsconstraints
generate implicit constraints for functions
Categories: memorybounds, memory
Default Setting: -
Set locally
orconstraint
use limited OR expressions to resolve constraints
Categories: memorybounds, memory
Default Setting: +
Set locally
showconstraintparens
display parentheses around constraint terms
Categories: memorybounds, display
Default Setting: -
Set locally
boundscompacterrormessages
Display fewer new lines in bounds checking error messages
Categories: memorybounds, display
Default Setting: -
Set locally
showconstraintlocation
display location for every constraint generated
Categories: memorybounds, display
Default Setting: +
Set locally
allocmismatch
type conversion involves storage of non-divisble size
Categories: memorybounds, memory
Mode Settings: -+++
Set locally
debugfcnconstraint
debug function constraints
Categories: debug, memorybounds
Default Setting: -
Set locally
Perform buffer overflow checking even if the errors would be
suppressed.
student@LAB704PC10:~$
11:09


student@LAB704PC10: ~
File Edit View Search Terminal Help
redundantconstraints
display seemingly redundant constraints
Categories: memorybounds, display
Default Setting: -
Set locally
Display seemingly redundant constraints
checkpost
unable to verify predicate in ensures clause
Categories: memorybounds, memory
Mode Settings: ---+
Set locally
The function implementation may not satisfy a post condition given in
an ensures clause.
impboundsconstraints
generate implicit constraints for functions
Categories: memorybounds, memory
Default Setting: -
Set locally
orconstraint
use limited OR expressions to resolve constraints
Categories: memorybounds, memory
Default Setting: +
Set locally
showconstraintparens
display parentheses around constraint terms
Categories: memorybounds, display
Default Setting: -
Set locally
boundscompacterrormessages
Display fewer new lines in bounds checking error messages
Categories: memorybounds, display
Default Setting: -
Set locally
showconstraintlocation
display location for every constraint generated
Categories: memorybounds, display
Default Setting: +
Set locally
allocmismatch
11:09