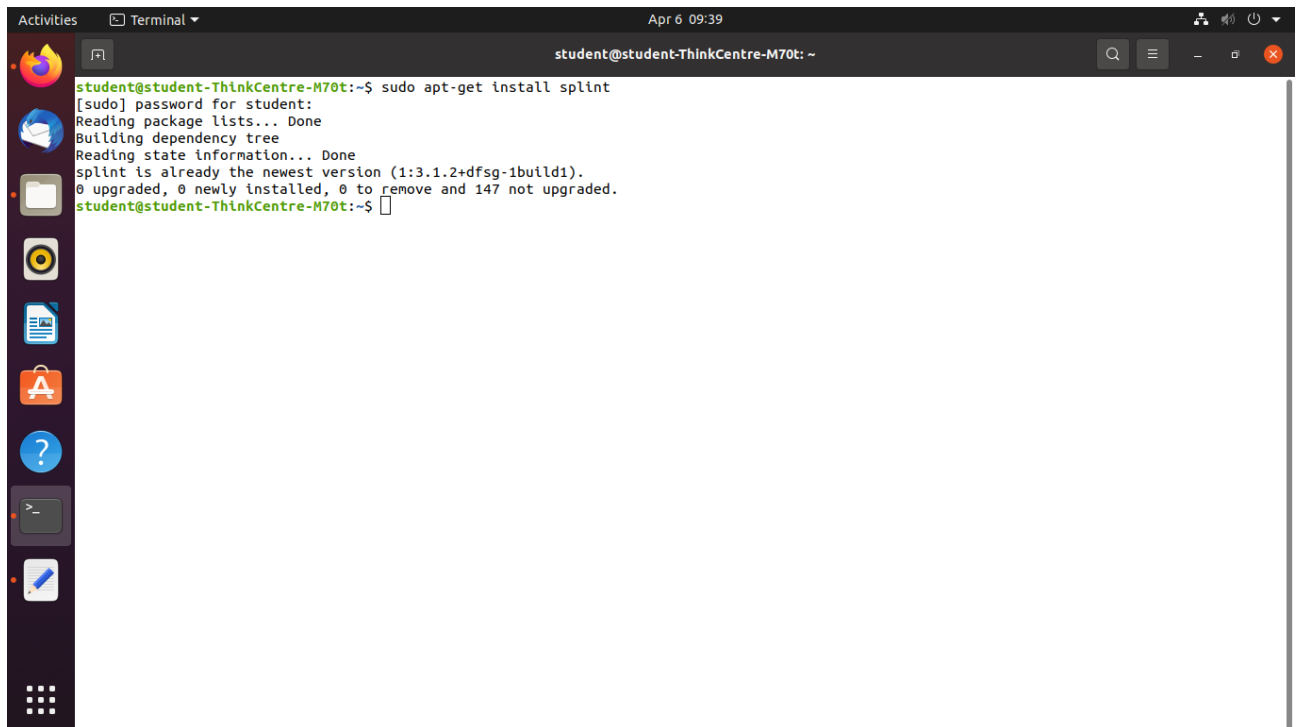


## CSS Splint tool

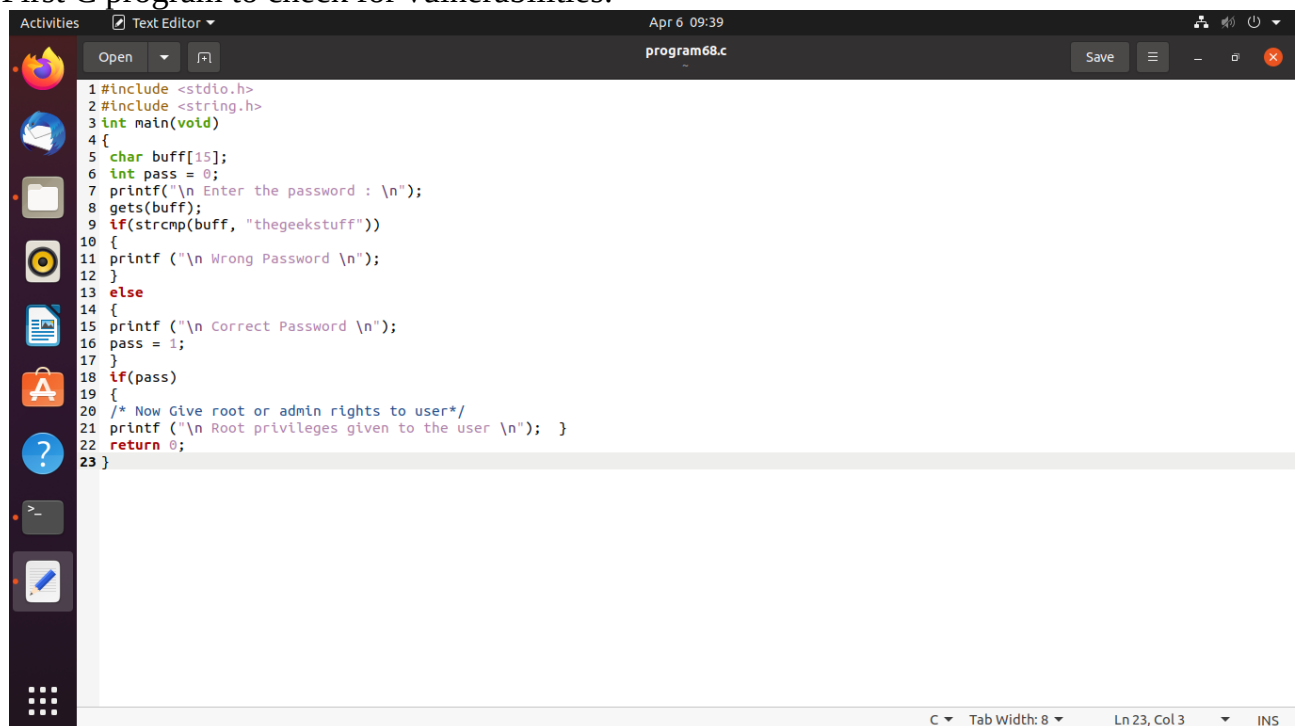
### Install splint tool:



A terminal window titled 'student@student-ThinkCentre-M70t: ~' showing the command to install the splint tool. The output indicates that splint is already installed at the latest version.

```
student@student-ThinkCentre-M70t:~$ sudo apt-get install splint
[sudo] password for student:
Reading package lists... Done
Building dependency tree
Reading state information... Done
splint is already the newest version (1:3.1.2+dfsg-1build1).
0 upgraded, 0 newly installed, 0 to remove and 147 not upgraded.
student@student-ThinkCentre-M70t:~$
```

### First C program to check for vulnerabilities:



A text editor window titled 'program68.c' showing a C program that checks for a password. The program includes headers for stdio.h and string.h, defines a main function, and uses printf, gets, and strcmp to validate the password 'thegeekstuff'. If the password is correct, it prints a message about root privileges.

```
1 #include <stdio.h>
2 #include <string.h>
3 int main(void)
4 {
5     char buff[15];
6     int pass = 0;
7     printf("\n Enter the password : \n");
8     gets(buff);
9     if(strcmp(buff, "thegeekstuff"))
10    {
11        printf ("\n Wrong Password \n");
12    }
13    else
14    {
15        printf ("\n Correct Password \n");
16        pass = 1;
17    }
18    if(pass)
19    {
20        /* Now Give root or admin rights to user*/
21        printf ("\n Root privileges given to the user \n"); }
22    return 0;
23 }
```

Output:

The screenshot shows a terminal window with the following content:

```

student@student-ThinkCentre-M70t: ~
student@student-ThinkCentre-M70t:~$ sudo apt-get install splint
[sudo] password for student:
Reading package lists... Done
Building dependency tree
Reading state information... Done
splint is already the newest version (1:3.1.2+dfsg-1build1).
0 upgraded, 0 newly installed, 0 to remove and 147 not upgraded.
student@student-ThinkCentre-M70t:~$ splint program68.c
Splint 3.1.2 --- 20 Feb 2018

program68.c: (in function main)
program68.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)
program68.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)
program68.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)
program68.c:18:5: Test expression for if not boolean, type int: pass

Finished checking --- 4 code warnings
student@student-ThinkCentre-M70t:~$
  
```

## Bufferoverflow c code:

Activities

The image shows a terminal window on a Linux desktop. The desktop background is dark, and the terminal window has a dark theme. The terminal output shows the following:

```
Finished checking --- 4 code warnings
student@student-ThinkCentre-M70t:~$ splint bufferoverflow.c
Splint 3.1.2 --- 20 Feb 2018

bufferoverflow.c: (in function main)
bufferoverflow.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)
bufferoverflow.c:5:34: Corresponding format code
bufferoverflow.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"
    bufferoverflow.c:5:38: Corresponding format code
bufferoverflow.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"
    bufferoverflow.c:5:42: Corresponding format code
bufferoverflow.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"
    bufferoverflow.c:5:46: Corresponding format code
bufferoverflow.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"
    bufferoverflow.c:5:50: Corresponding format code
bufferoverflow.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"
    bufferoverflow.c:5:54: Corresponding format code
bufferoverflow.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"
    bufferoverflow.c:5:58: Corresponding format code
bufferoverflow.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"
```

Activities Terminal

student@student-ThinkCentre-M70t: ~

```
"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"
bufferoverflow.c:9:46: Corresponding format code
bufferoverflow.c:9:1: No argument corresponding to printf format code 4 (%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"
bufferoverflow.c:9:50: Corresponding format code
bufferoverflow.c:9:1: No argument corresponding to printf format code 5 (%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"
bufferoverflow.c:9:54: Corresponding format code
bufferoverflow.c:9:1: No argument corresponding to printf format code 6 (%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"
bufferoverflow.c:9:58: Corresponding format code
bufferoverflow.c:9:1: No argument corresponding to printf format code 7 (%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"
bufferoverflow.c:9:62: Corresponding format code
bufferoverflow.c:9:1: 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%p\n"
bufferoverflow.c:9:66: Corresponding format code
bufferoverflow.c:9:1: 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"
bufferoverflow.c:9:70: Corresponding format code
bufferoverflow.c:9:1: 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"
bufferoverflow.c:9:74: Corresponding format code
bufferoverflow.c:11:2: 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 -Wno-return to inhibit warning)

Finished checking --- 21 code warnings
student@student-ThinkCentre-M70t:~$
```