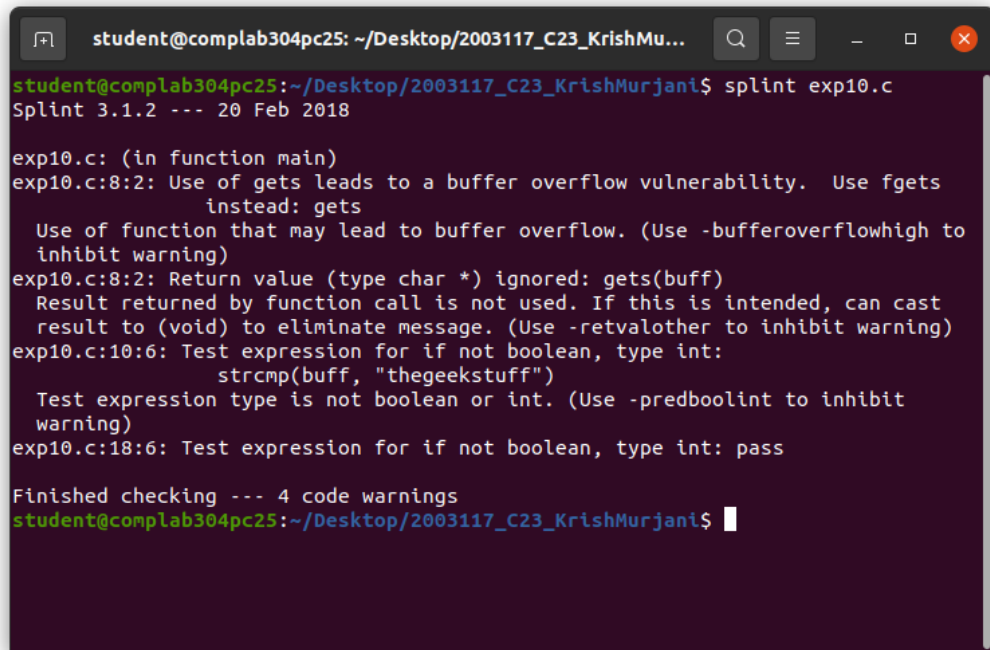


Program :

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

Output



```
student@complab304pc25: ~/Desktop/2003117_C23_KrishMu...
student@complab304pc25:~/Desktop/2003117_C23_KrishMurjani$ splint exp10.c
Splint 3.1.2 --- 20 Feb 2018

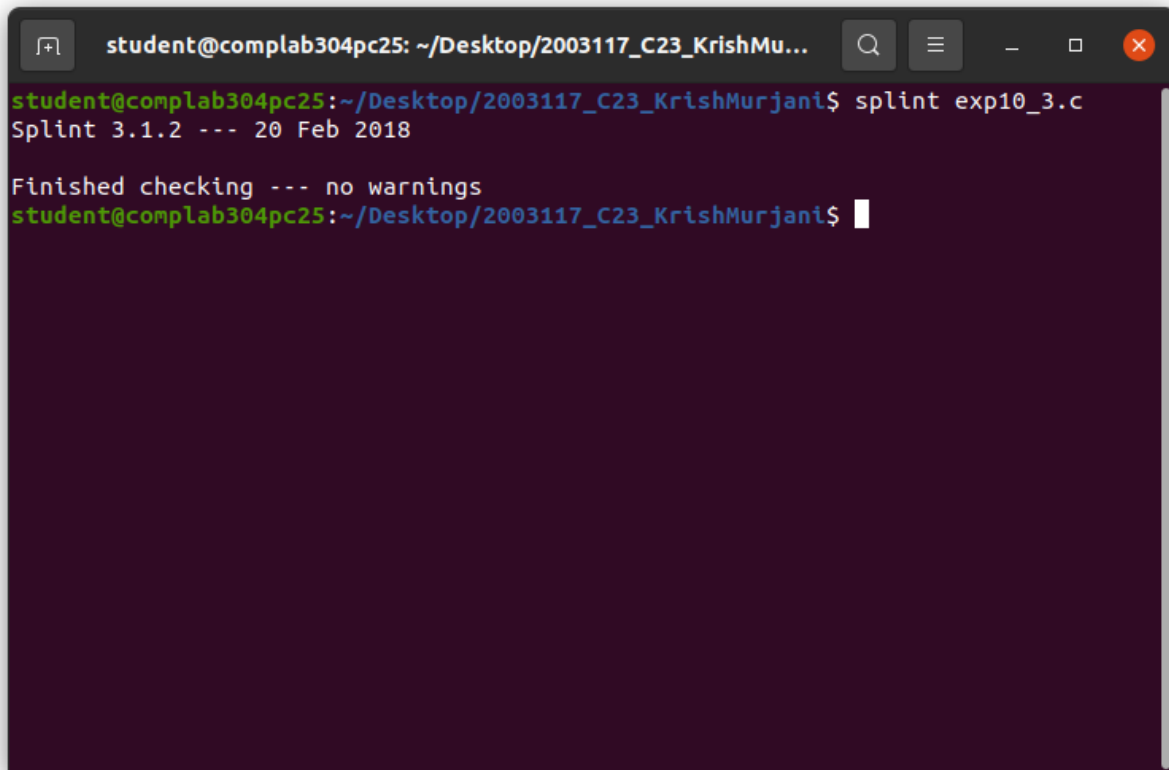
exp10.c: (in function main)
exp10.c:8:2: Use of gets leads to a buffer overflow vulnerability.  Use fgets
           instead: gets
    Use of function that may lead to buffer overflow. (Use -bufferoverflowhigh to
    inhibit warning)
exp10.c:8:2: Return value (type char *) ignored: gets(buff)
    Result returned by function call is not used. If this is intended, can cast
    result to (void) to eliminate message. (Use -retvalother to inhibit warning)
exp10.c:10:6: Test expression for if not boolean, type int:
           strcmp(buff, "thegeekstuff")
    Test expression type is not boolean or int. (Use -predboolint to inhibit
    warning)
exp10.c:18:6: Test expression for if not boolean, type int: pass

Finished checking --- 4 code warnings
student@complab304pc25:~/Desktop/2003117_C23_KrishMurjani$
```

Program

```
#include<stdio.h>
int main()
{
printf("Hello,world!");
return 0;
}
```

Output



```
student@complab304pc25: ~/Desktop/2003117_C23_KrishMu...
student@complab304pc25:~/Desktop/2003117_C23_KrishMurjani$ splint exp10_3.c
Splint 3.1.2 --- 20 Feb 2018

Finished checking --- no warnings
student@complab304pc25:~/Desktop/2003117_C23_KrishMurjani$
```

