GHARDA FOUNDATION

GHARDA FOUNDATION'S
GHARDA INSTITUTE OF TECHNOLOGY

Department of Computer Engineering

GIT GHARDA INSTITUTE OF TECHNOLOGY

Evaluation Sheet

Class: T.E Computer Engineering **Sem:** VI

Subject: Cryptography and System Security

Experiment No: 13

Date:

Title of Experiment: Simulate buffer overflow attack using Cppcheck, Splint etc.

Sr. No.	Evaluation Criteria	Max Marks	Marks Obtained
1	Practical Performance	12	
2	Oral	2	
3	Timely Submission	1	
	Total	15	

Signature of Subject Teacher
[Vijesh M.Nair]

Output –

```
student@student-HP-Desktop-Pro-G1-MT:~$ sudo apt-get install cppcheck
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following package was automatically installed and is no longer required:
  gir1.2-goa-1.0
Use 'sudo apt autoremove' to remove it.
The following additional packages will be installed:
  libtinyxml2-6a python3-pygments
Suggested packages:
  cppcheck-gui python-pygments-doc ttf-bitstream-vera
The following NEW packages will be installed:
  cppcheck libtinyxml2-6a python3-pygments
0 upgraded, 3 newly installed, 0 to remove and 124 not upgraded.
Need to get 2,253 kB of archives.
After this operation, 10.4 MB of additional disk space will be used.
Do you want to continue? [Y/n] y
Err:1 http://in.archive.ubuntu.com/ubuntu focal/universe amd64 libtinyxml2-6a amd64
 7.0.0+dfsg-1build1
  Temporary failure resolving 'in.archive.ubuntu.com'
Ign:2 http://in.archive.ubuntu.com/ubuntu focal-updates/main amd64 python3-pygments
 all 2.3.1+dfsg-1ubuntu2.2
Err:3 http://in.archive.ubuntu.com/ubuntu focal/universe amd64 cppcheck amd64 1.90-
4build1
  Temporary failure resolving 'in.archive.ubuntu.com'
```

```
student@student-HP-Desktop-Pro-G1-MT:~/Documents/68_TE$ sudo apt install splint
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following package was automatically installed and is no longer required:
  gir1.2-goa-1.0
Use 'sudo apt autoremove' to remove it.
The following additional packages will be installed:
  splint-data
Suggested packages:
  splint-doc-html
The following NEW packages will be installed:
  splint splint-data
0 upgraded, 2 newly installed, 0 to remove and 124 not upgraded.
Need to get 740 kB of archives.
After this operation, 2,883 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://in.archive.ubuntu.com/ubuntu focal/universe amd64 splint-data all 1:3.
1.2+dfsg-1build1 [57.5 kB]
Get:2 http://in.archive.ubuntu.com/ubuntu focal/universe amd64 splint amd64 1:3.1.2
+dfsg-1build1 [683 kB]
Fetched 740 kB in 20s (36.6 kB/s)
Selecting previously unselected package splint-data.
(Reading database ... 186803 files and directories currently installed.)
```

```
student@student-HP-Desktop-Pro-G1-MT:~/Documents/68_TE$ splint sample2.c
Splint 3.1.2 --- 20 Feb 2018

sample2.c: (in function firstChar1)
sample2.c:3:10: Dereference of possibly null pointer s: *s
  A possibly null pointer is dereferenced.  Value is either the result of a
  function which may return null (in which case, code should check it is not
  null), or a global, parameter or structure field declared with the null
  qualifier. (Use -nullderef to inhibit warning)
   sample2.c:1:35: Storage s may become null
sample2.c: (in function firstChar2)
sample2.c:7:25: Invalid character (ascii: 96), skipping character
  Code cannot be parsed.  For help on parse errors, see splint -help
  parseerrors. (Use -syntax to inhibit warning)
sample2.c:7:28: Invalid character (ascii: 96), skipping character
sample2.c:7:26: Return value type int does not match declared type char: 0
  Types are incompatible. (Use -type to inhibit warning)

Finished checking --- 4 code warnings
```

```
student@student-HP-Desktop-Pro-G1-MT:~/Documents/68_TE$ splint sample3.c
Splint 3.1.2 --- 20 Feb 2018

sample3.c: (in function main)
sample3.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)
sample3.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)
sample3.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)
sample3.c:18:5: Test expression for if not boolean, type int: pass

Finished checking --- 4 code warnings
```

```
student@student-HP-Desktop-Pro-G1-MT:~/Documents/68_TE$ splint sample4.c
Splint 3.1.2 --- 20 Feb 2018

sample4.c: (in function get_password)
sample4.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)
sample4.c: (in function main)
sample4.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)
sample4.c:16:27: Parameter argv not used
sample4.c:3:6: Variable exported but not used outside sample4: password
  A declaration is exported, but not used outside this module. Declaration can
  use static qualifier. (Use -exportlocal to inhibit warning)
sample4.c:4:5: Function exported but not used outside sample4: get_password
   sample4.c:12:1: Definition of get_password
sample4.c:13:6: Function exported but not used outside sample4: success
   sample4.c:15:1: Definition of success

Finished checking --- 6 code warnings
```