**Tutorial -3**

**Date of Posting:** 10th Aug, 2018 **Date of Submission: 17th**  Aug, 2018

Q1. #include <stdio.h>

#include <string.h>

#include <stdlib.h>

int main(int argc, char \*argv[])

{

char buffer[5];

if (argc < 2)

{

printf("strcpy() NOT executed....\n");

printf("Syntax: %s <characters>\n", argv[0]);

exit(0);

}

strcpy(buffer, argv[1]);

printf("buffer content= %s\n", buffer);

printf("strcpy() executed...\n");

return 0;

}

Write the output of above program for inputs: - 1234,12345,123456,12345678,123456789.

Which attack does it demonstrate?

Buffer[5]=”0123(null)”

1234

Buffer content 1234

For all others it will lead to Buffer Overflow Error

Q2. int main(int argc, char argv[]){

char buff[256];

strcpy(buff, argv[1], 200);

printf(buff); return 0; }

Write and explain the output, if buff=“%s%s”; OR buff=“%x%x” OR buff=“\x30\xa0\x04\x08%x%x%x%n”;

Q3. What will be the interpretation of the string char a[] = “\xe0\x85” , if a is used as argument in printf();

Q4. Explore objdump and Gdb- GNU Debugger tool for analysing stack/ memory contents during program execution.

Q5. A tool name flaw finder has been given in tools directory. Try this tool on the codes written in q1 and 2.

Q6. Find an example of a site where Input data to a web form is transferred to the server by embedding it in a URL and it can be exploited fro incomplete mediation. Write your answer with snapshots of request response.

Still Exploring

**Execution is included in other files**.