/\*

buffer overflow using a custom version of the strcpy() function.

\*/

char \*stringcopy(char \*str1, char \*str2)

{

while (\*str2)

\*str1++ = \*str2++;

return str2;

}

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

{

char \*buffer = (char \*)malloc(16 \* sizeof(char));

stringcopy(buffer, argv[1]);

printf("%s

", buffer);

}