CAP 6135 - Malware and Software Vulnerability Analysis

Spring 2018

Programming Project 2: Fuzz Testing

Submitted by: Rajib Dey

Design

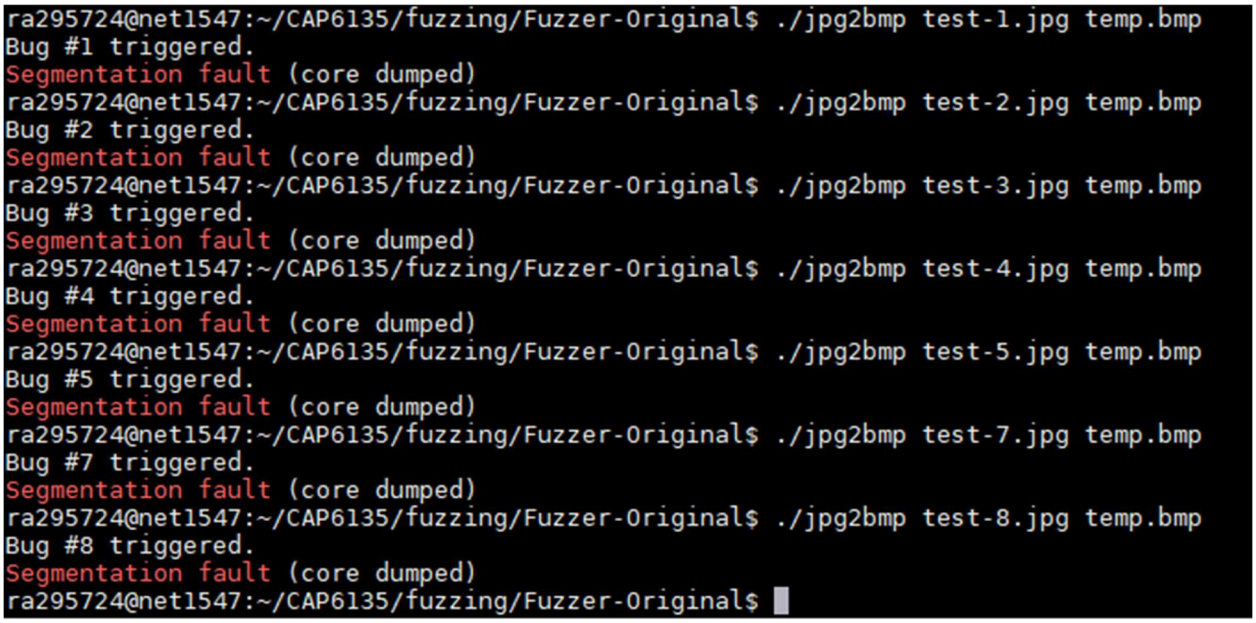
The fuzz testing is done by mutating the code of the given *cross.jpg*. The file is opened in binary using FILE pointers copied to a temporary variable *jpeg_data[]* , then modification operation are done in the char array.

Then this char array is written to a temporary file *cross-1.jpg* and fed to *jpgtobmp* executable file as input.

The return status is checked for faulty execution. If due to mutated input, faulty execution is found, then the input file is saved in root directory. The input file is renamed according to the bug # that it generates.

Screenshot

I was able to find 7 out of the 8 bugs mentioned in the assignment. The Screenshot is provided below



Empirical Results

Five programs were used to fuzz test the program. To get the desired result, each program was executed between 50,000 times to 1000 times.

The *rand()* in C Language, is sometimes unpredictable hence some programs were executed more than others.

# of times Generated	Test Program name				
	rajibfuzz.cpp	rajibfuzz2.cpp	rajibfuzz3.cpp	rajibfuzz4.cpp	rajibfuzz5.cpp
# of Iterations	50000	1000	1000	1000	5000
Bug #1	0	0	0	0	6
Bug #2	0	3	0	2	16
Bug #3	0	0	3	0	0
Bug #4	3799	70	7	5	25
Bug #5	0	6	1	1	30
Bug #6	0	0	0	0	0
Bug #7	251	7	8	9	35
Bug #8	253	48	20	28	112

File-List and Description

JPG Test files:

The Images are named test-x.jpg, where x is the number of bug, attached with the report. It can be found in code subfolder.

Source code:

Source code as well as executable is attached in the zip folder.

Test JPG file are present in the code folder.

Screenshot:

The screenshot image file is also available in the root folder.

Instruction on how to Run

To see the exact # of bug being generated, run the *jpg2bmp* executable file by inputting the corresponding test jpg file. Output file name can be anything, but the extension needs to be in bmp format, but as there will be bug this file will not be generated.

For example, to see bug #1 being generated, in the code folder run the following command:

./jpg2bmp test-1.jpg temp.bmp