Adam Bradford
CS5959
Fuzzer Analysis.
My fuzzer accomplished 83.3%

Line 161 – This was not covered because I only input types that are supported by printf.

224,226,228 – I'm not sure what this is accomplishing, but it looks to be dealing with sign bits and formatting the number of leading and trailing digits. My fuzzer was very precise about which types of strings it tried to print, and I feel perhaps could have been more random.

257-261 – This is accomplishing a round with a negative number, Perhaps my fuzzer wasn't properly creating the required range of negative floats.

307-317 This looks like the kind of code that would run to handle exponential numbers, which were not fuzzed.

384-386 – I'm not quite sure what these lines do…

470-471 – It looks the fizzer did not get into a large enough string to make this code execute, the sizes were limited to 500 or 1000.

599-502, 513-514 – This code looks like it deals with the '$' char which was not explicitly included in the random set of inputs. It might have been executed, but not enough time had passed.

560-565 – I'm not sure what these are doing. Some comments would be extremely helpful here.

651 – 655 – This code looks like it deals with exceeding the max number of arguments, the fuzzer only put in at most 2.

675 – 687 – I think these are used with normal printf, and not sprint, which is why they were not executed.