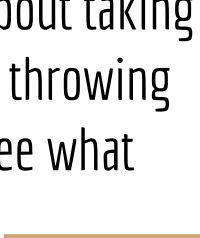





Intro to Fuzzing

“Sometimes hacking isn’t about taking a program apart: It’s about throwing random objects at it to see what breaks.” 




“The story of Fuzz testing began on a dark and stormy night in 1988.”






“With a group of students, Miller created the first purpose-built fuzzing tool to try to exploit that method of haphazardly stumbling into security flaws, and they submitted a paper on it to conferences.”





“Fuzz Testing was open source before open source
was a phrase.”

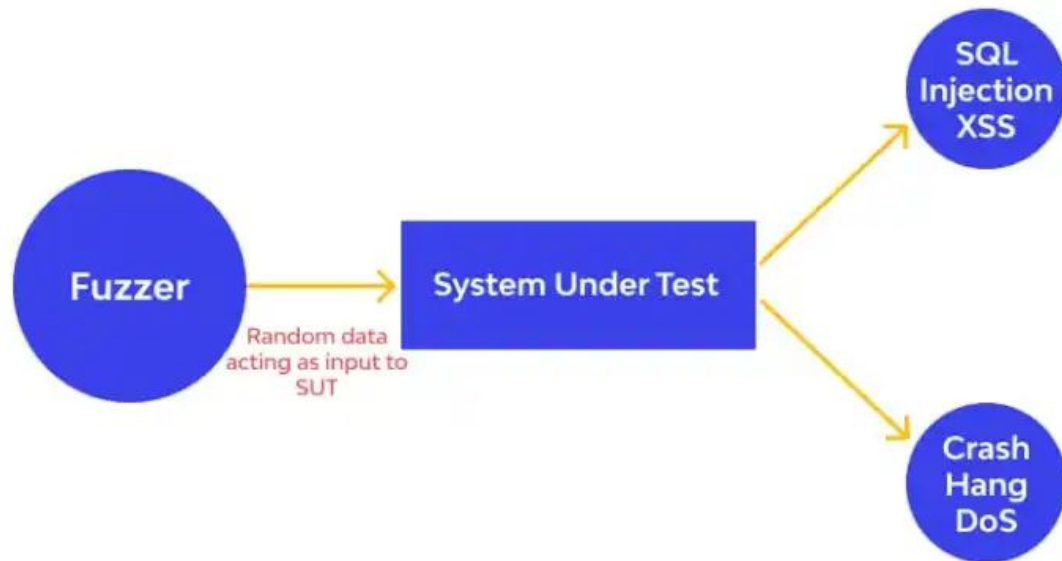




"You're throwing a whole lot of data at a program, mutating it quickly and relying on your monitoring of the software to find when something bad has happened instead of meticulously mapping out the data flow to find a bug...It's a way of killing off a lot of bugs very quickly."



- Pedram Amini, CTO of the cybersecurity firm InQuest



Big List of Naughty Strings

minimaxir/**big-list-of-naughty-strings**

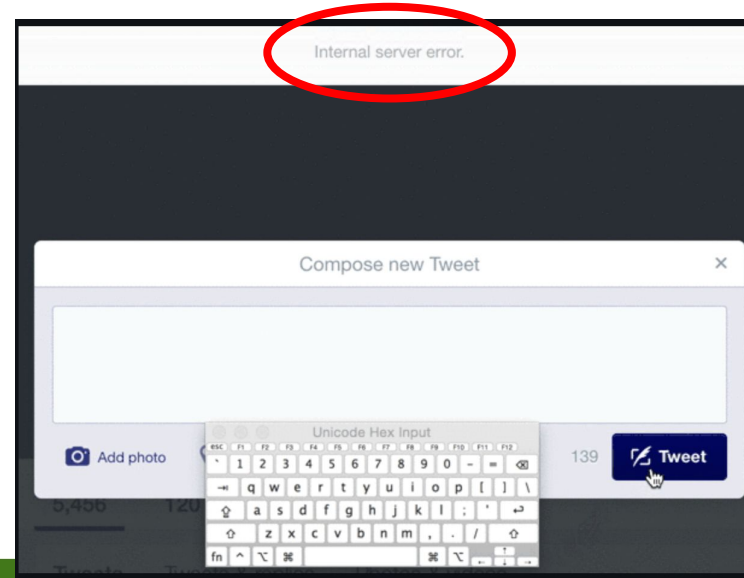
The Big List of Naughty Strings is a list of strings which have a high probability of causing issues when...

72
Contributors

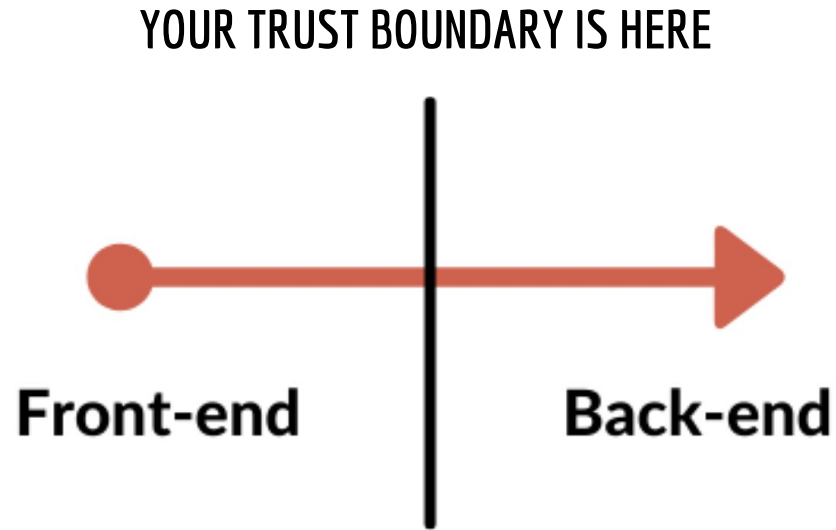
30
Used by

45k
Stars

2k
Forks



Trust Boundary





Vulnerability
Introduced



Vulnerability
Discovered



You Find It



You Fix It

HIGHEST SECURITY RISK



Exploits
Published



Hackers
Attack

Types of Fuzzing

1. **Black Box Fuzzing:**

- a. The internal workings of the target program are unknown.
- b. The fuzzer generates input data without any knowledge of how the target program works or how it handles input.
- c. Effective for finding basic bugs such as crashes, hangs, and buffer overflows.

2. **White Box Fuzzing:**

- a. Internal workings are known.
- b. Generates intelligent data based on the feedback from the system and uses code coverage information.
- c. Useful for finding logical errors or security vulnerabilities

3. **Grey Box Fuzzing:**

- a. Somewhere in between white box and black box - uses partial knowledge
- b. Test program behavior in a more general sense & less computationally expensive than white box.

Types of Fuzzers

1. **Generation Fuzzers:**

- a. They can be anything from random data to slightly designed data.
- b. They usually take a valid input based on the specification, break it into pieces, and then fuzz each of the selected pieces randomly.
- c. Advantages: Better coverage, reduced noise, increased automation & early detection of bugs.

2. **Mutation Fuzzers:**

- a. Take a set of valid inputs and perform mutations on them.
- b. Techniques such as least significant bit flipping fall into mutation fuzzing.
- c. For example, when fuzzing an mp3 processing library, the user would provide a selection of valid mp3 files, and then the fuzzer would modify these files to produce semi-valid variants of each file.

3. **Evolution Fuzzers:**

- a. Evolutionary fuzzing is based on the use of genetic programming, which aims to converge toward the discovery of vulnerabilities.

Evolution Fuzzers

Genetic algorithms are used to create continuous sets of test cases. The first set of test cases will be generated in a similar way to a generational fuzzer (described previously), and all further test cases will be generated through the steps described below:

1. **Score:** Each member of the current set of test cases is given a score, which is a combination of multiple metrics defined by the user and monitored through the fuzzing test
2. **Removal of weak cases:** Lowest scoring test cases are discarded
3. **Mutation:** Minor changes are applied to each remaining test case, similar to those described in the mutation fuzzing section
4. **Combination:** Involves combining test cases with high scores to generate test cases that find other optimums. This process is also used to replenish the test cases that were discarded in step 2

Limitations

- Often takes an extremely long time to run.
- Crashes can often be difficult to analyze, especially when using black box fuzzing.
- Mutation templates for applications with complex inputs can often be time consuming to produce.
- Fuzzers are less effective at identifying vulnerabilities that are unrelated to system crashes, such as spyware or Trojans.

HOW THE HEARTBLEED BUG WORKS:

SERVER, ARE YOU STILL THERE?
IF SO, REPLY "POTATO" (6 LETTERS).



secure connection using key "4538538374224"
User Meg wants these 6 letters: POTATO. User
da wants pages about "irl games". Unlocking
secure records with master key 513098573343
Isabel wants pages about "snakes but not too long". User Karen wants to change account password to "C0rRUpt10n"



POTATO

is pages about "locks". User Meg wants these 6 letters: POTATO. User
da wants pages about "irl games". Unlocking
secure records with master key 513098573343
Isabel wants pages about "snakes but not too long". User Karen wants to change account password to "C0rRUpt10n"



SERVER, ARE YOU STILL THERE?
IF SO, REPLY "BIRD" (4 LETTERS).



see Olivia from 2004 want pages about "snakes in car why". Note: Files for IP 375.381.
83.17 are in /tmp/files-3843. User Meg wants
these 4 letters: BIRD. There are currently 34
connections open. User Brendan uploaded the file
14835038534. User Karen wants to change account password to "C0rRUpt10n"



HMM...



BIRD



see Olivia from 2004 want pages about "snakes in car why". Note: Files for IP 375.381.
83.17 are in /tmp/files-3843. User Meg wants
these 4 letters: BIRD. There are currently 34
connections open. User Brendan uploaded the file
14835038534. User Karen wants to change account password to "C0rRUpt10n"

SERVER, ARE YOU STILL THERE?
IF SO, REPLY "HAT" (500 LETTERS).



a connection. User requested pictures of dead
User Meg wants these 500 letters: HAT. Lucas
requests the "missed connections" page. Eve
(administrator) wants to set server's master
key to "14835038534". Isabel wants pages about
snakes but not too long". User Karen wants to
change account password to "C0rRUpt10n"



HAT. Lucas requests the "missed connections" page. Eve (administrator) wants to set server's master key to "14835038534". Isabel wants pages about "snakes but not too long". User Karen wants to change account password to "C0rRUpt10n"



a connection. User requested pictures of dead
User Meg wants these 500 letters: HAT. Lucas
requests the "missed connections" page. Eve
(administrator) wants to set server's master
key to "14835038534". Isabel wants pages about
snakes but not too long". User Karen wants to
change account password to "C0rRUpt10n"

Fuzzing Tools

Commercial

- Codenomicon's product suite
- Peach Fuzzing Platform
- Beyond Security's beSTORM product
- ForAllSecure Mayhem for Code
- CI Fuzz
- Fuzzbuzz

Open Source

- American fuzzy lop
- Radamsa - a flock of fuzzers
- APIFuzzer - fuzz test without coding
- Jazzer - fuzzing for the JVM
- ForAllSecure Mayhem for API