Generating test cases to abuse a BNF grammar automagically

Asked 14 years, 8 months ago Modified 9 years, 2 months ago

Viewed 837 times

▲

4

▼

I am wondering if there is a tool or technique which, given a BNF grammar, *adjusts* it randomly(but intelligently) and generates a stream of output for use in detecting cases that slip past the BNF (but shouldn't).

edit: Fuzz testing a parser, in other words.

Thanks

testing bnf fuzzing

Share

Improve this question

Follow

edited Dec 11, 2013 at 23:31

LJNielsenDk

1,460 ● 1 ● 16 ● 32

asked Apr 23, 2010 at 23:00

Paul Nathan

40.2k ● 30 ● 120 ● 215

2 Answers

Sorted by: Highest score (default)

3

Spending some tender time with Google, I found that automated grammar-based fuzz testing is *hard*, and a subject of current research. In particular, P. Godefroid at Microsoft Research is working on a piece of software called SAGE.

I dug up a research paper by him.

Automated Whitebox Fuzz Testing (joint work with Michael Y. Levin and David Molnar) Proceedings of NDSS'2008 (Network and Distributed Systems Security), pages 151-166, San Diego, February 2008.

I also found the XML-based Peach software, but it is unclear to me on a casual reading how I might leverage it in an afternoon of work for a non-security application.

So my conclusion is: **"It's a subject of current (Apr '10) research and there's no quick-use tool out there".**

Share Improve this answer

Follow

answered Apr 24, 2010 at 15:41

Paul Nathan

40.2k ● 30 ● 120 ● 215

0

Not strictly a BNF fuzzing tool, but american fuzzy lop employs artificial intelligence methods and can walk around the lack of BNF knowledge quite well. It already found bugs in many open source parsers, so it might be the right tool for yours as well.

Share Improve this answer

Follow

answered Oct 13, 2015 at 22:00

d33tah

11.5k ● 15 ● 74 ● 171