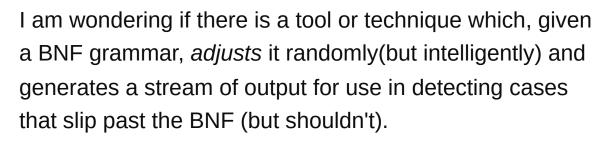
Generating test cases to abuse a BNF grammar automagically

Asked 14 years, 8 months ago Modified 9 years, 2 months ago Viewed 837 times



4





edit: Fuzz testing a parser, in other words.



Thanks



testing bnf fuzzing

Share

Improve this question

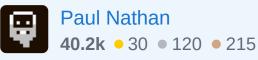
Follow

edited Dec 11, 2013 at 23:31

LJNielsenDk

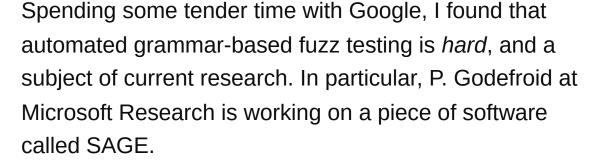
1,460 • 1 • 16 • 32

asked Apr 23, 2010 at 23:00





3

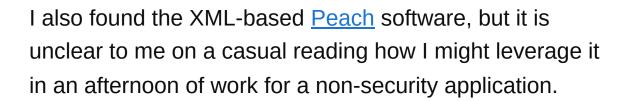




I dug up a research paper by him.



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.



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





0



Not strictly a BNF fuzzing tool, but <u>american fuzzy lop</u> 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

