SATE VI

Preliminary Results

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Alex-Kevin LOEMBE
SAMATE team, NIST

SATE VI

- Bugs injected in real software
- Traces representing each injected bug
- Comparison of tool warnings to our traces

Ratings

Match	Source and sink found
Alternate	Sink found, different source found
Partial	Source, sink or intermediate weakness location found
Hint	Source and sink not found, but warning could lead a developer to find the bug
Miss	Not found

Metrics

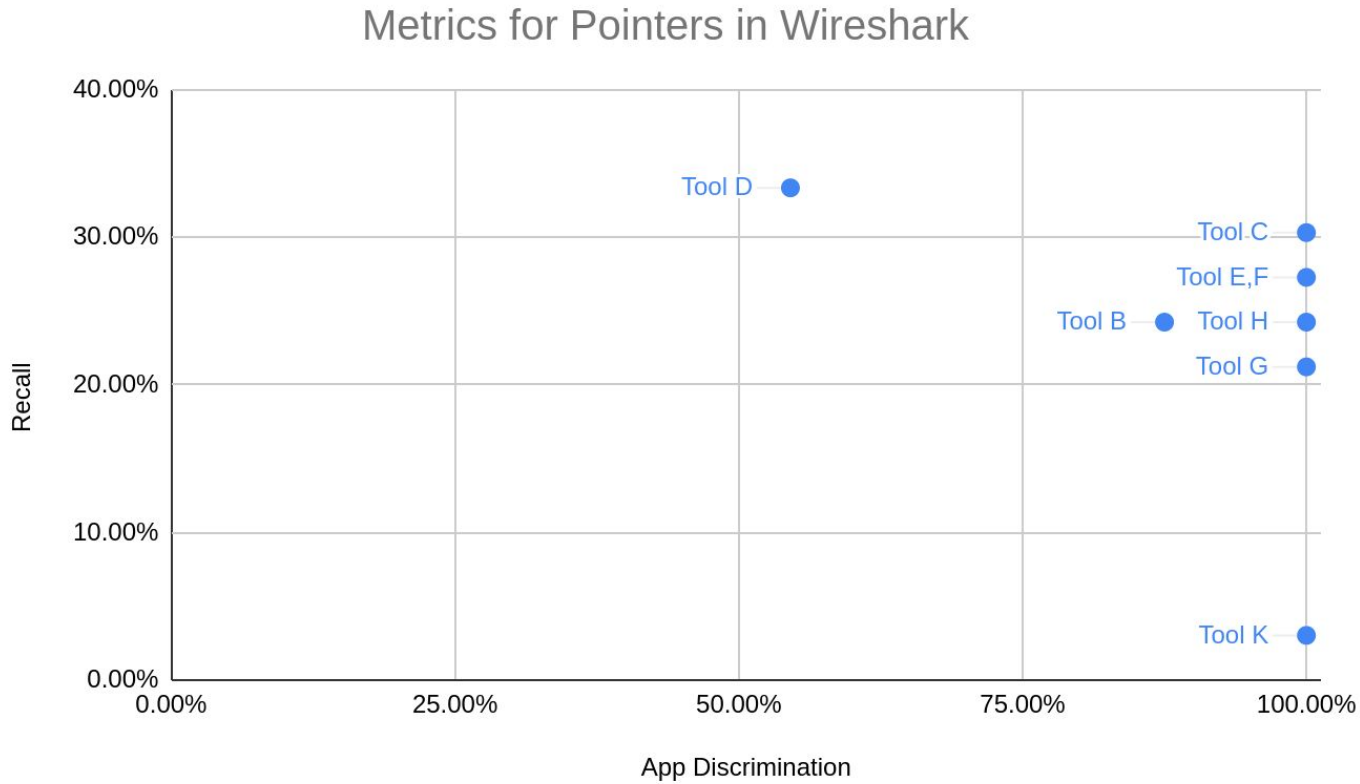
- Recall - What proportion of bugs can a tool find?
- Applicable Discrimination - Among found bugs, how many are not reported in the fixed version?
- Overlap - How many tools found the same bug?

C Test Cases

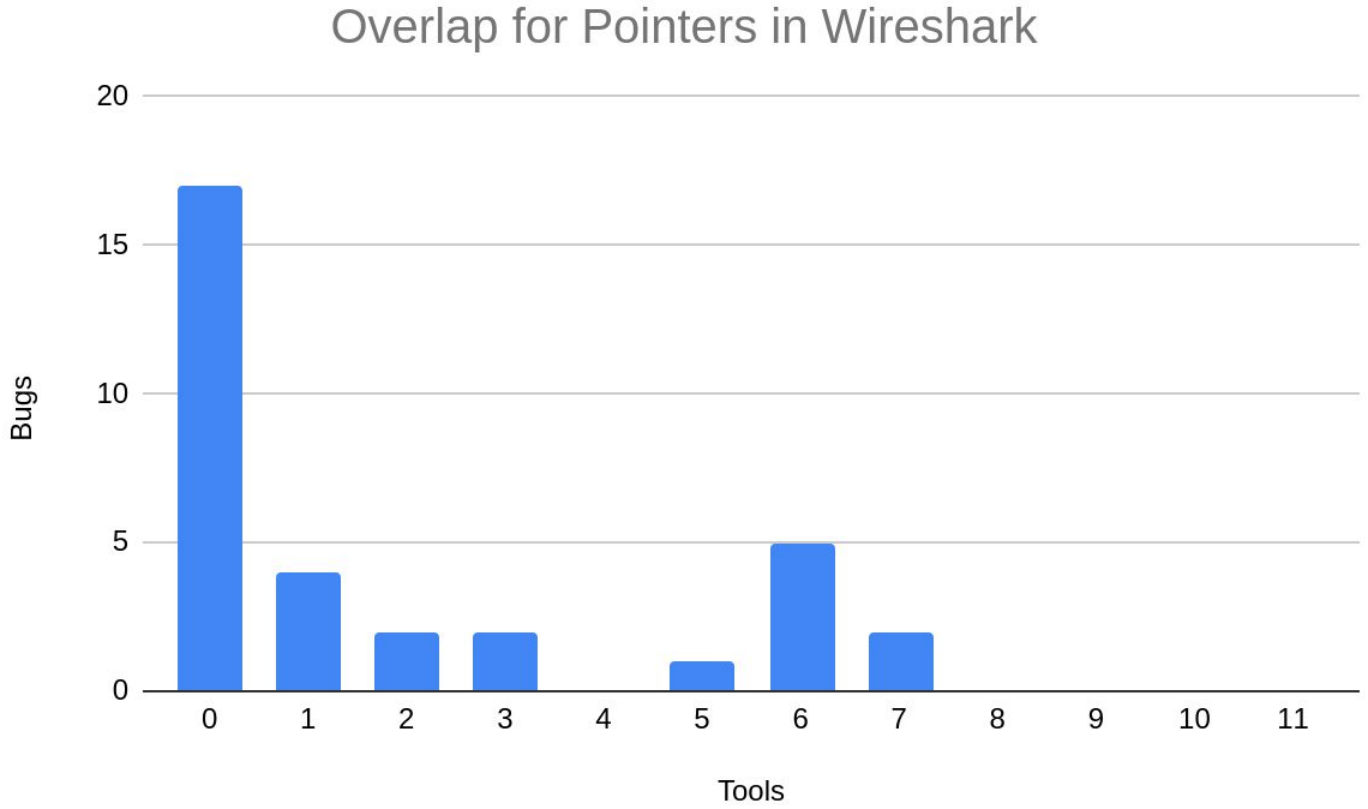

NIST
National Institute of
Standards and Technology
U.S. Department of Commerce
SAMATE

Wireshark-1.2

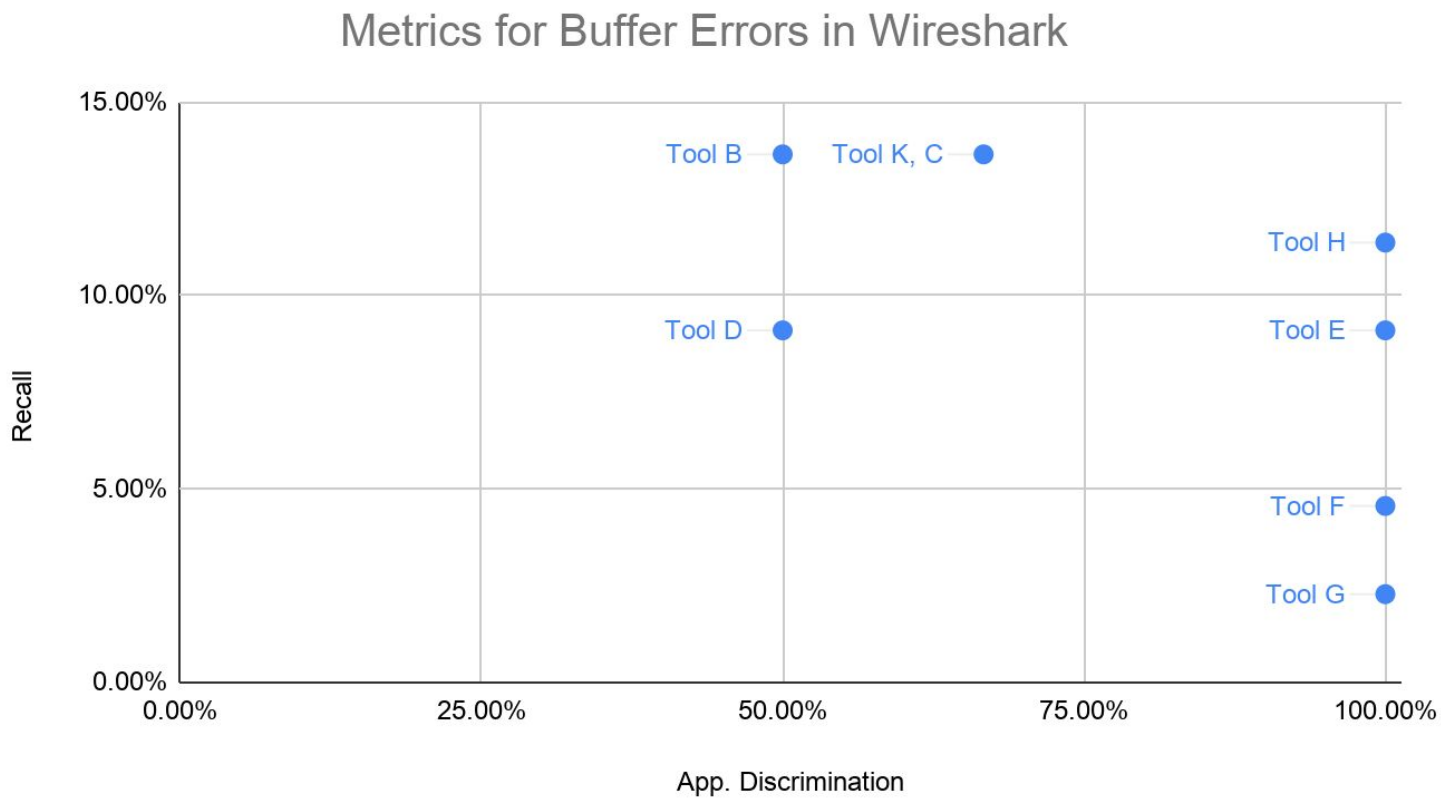
- Date of release: 2009
- Lines of code: 2 M
- Manually injected bugs
- Bugs: 75, including:
  - 44 Buffer Errors
  - 33 Pointer Errors
  - 12 Calculation and Numeric Errors
  - 11 Initialization Errors



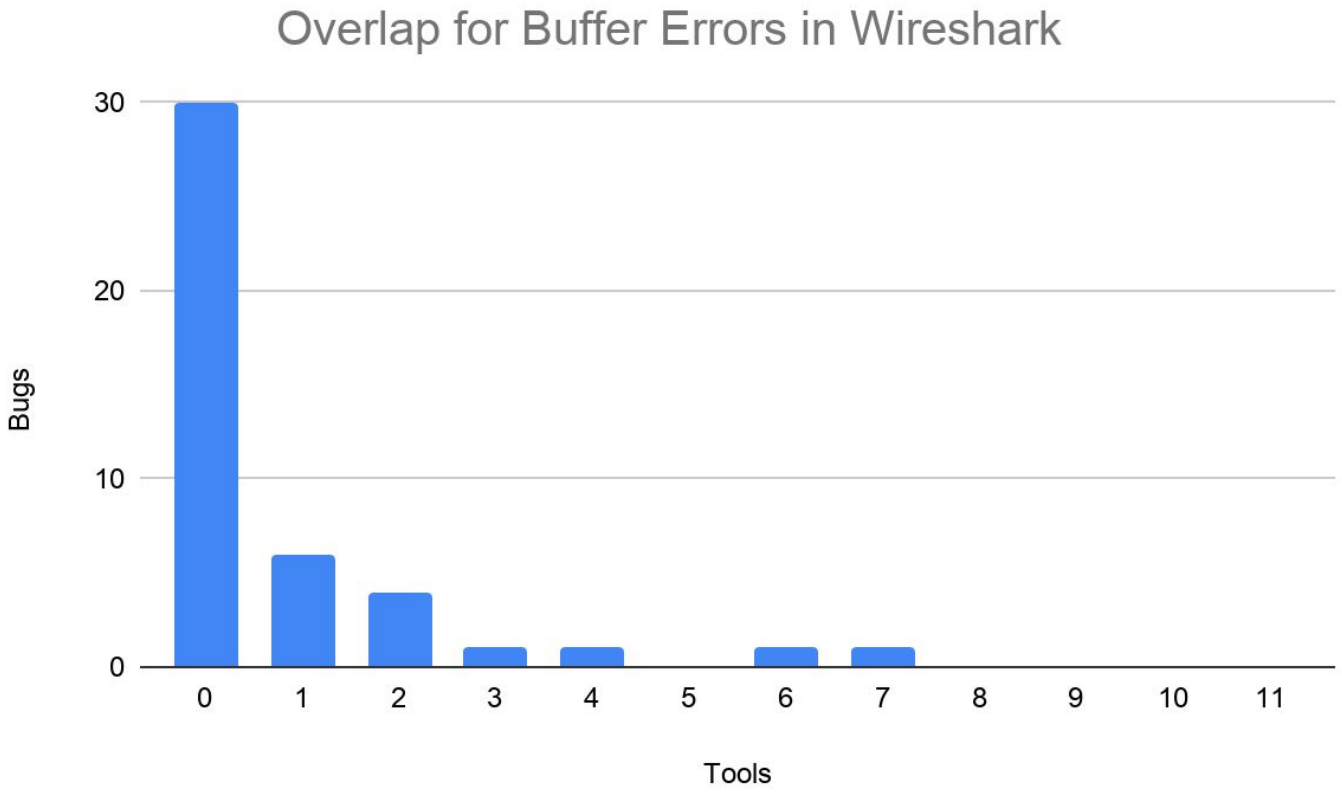
National Institute of Standards and Technology
U.S. Department of Commerce



National Institute of Standards and Technology
U.S. Department of Commerce



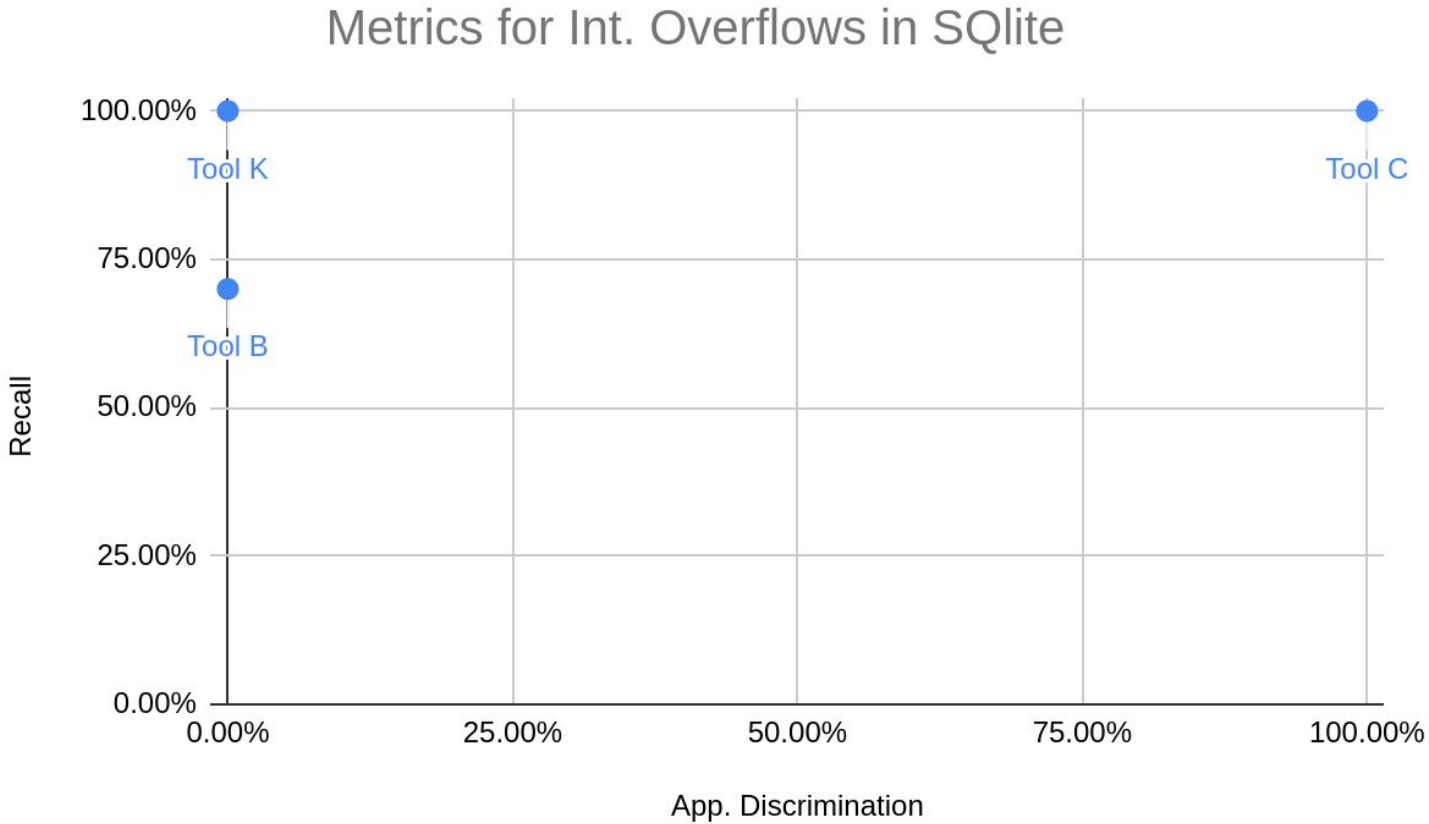
National Institute of Standards and Technology
U.S. Department of Commerce



National Institute of Standards and Technology
U.S. Department of Commerce

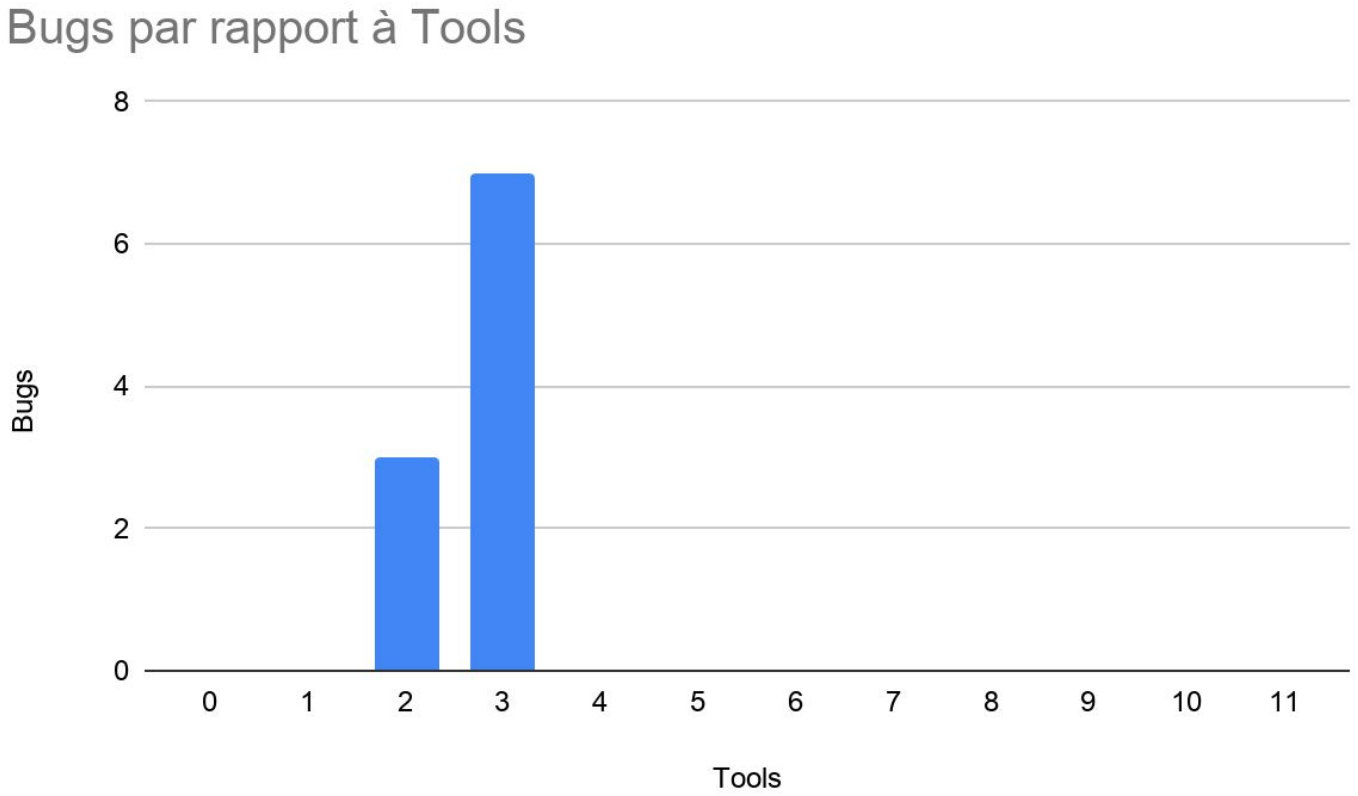
SQlite-3.21

- Date of release: 2017
- Lines of code: 350 k
- Automatically injected bugs
- Bugs :
  - 20 Buffer Errors
  - 10 Integer Overflows

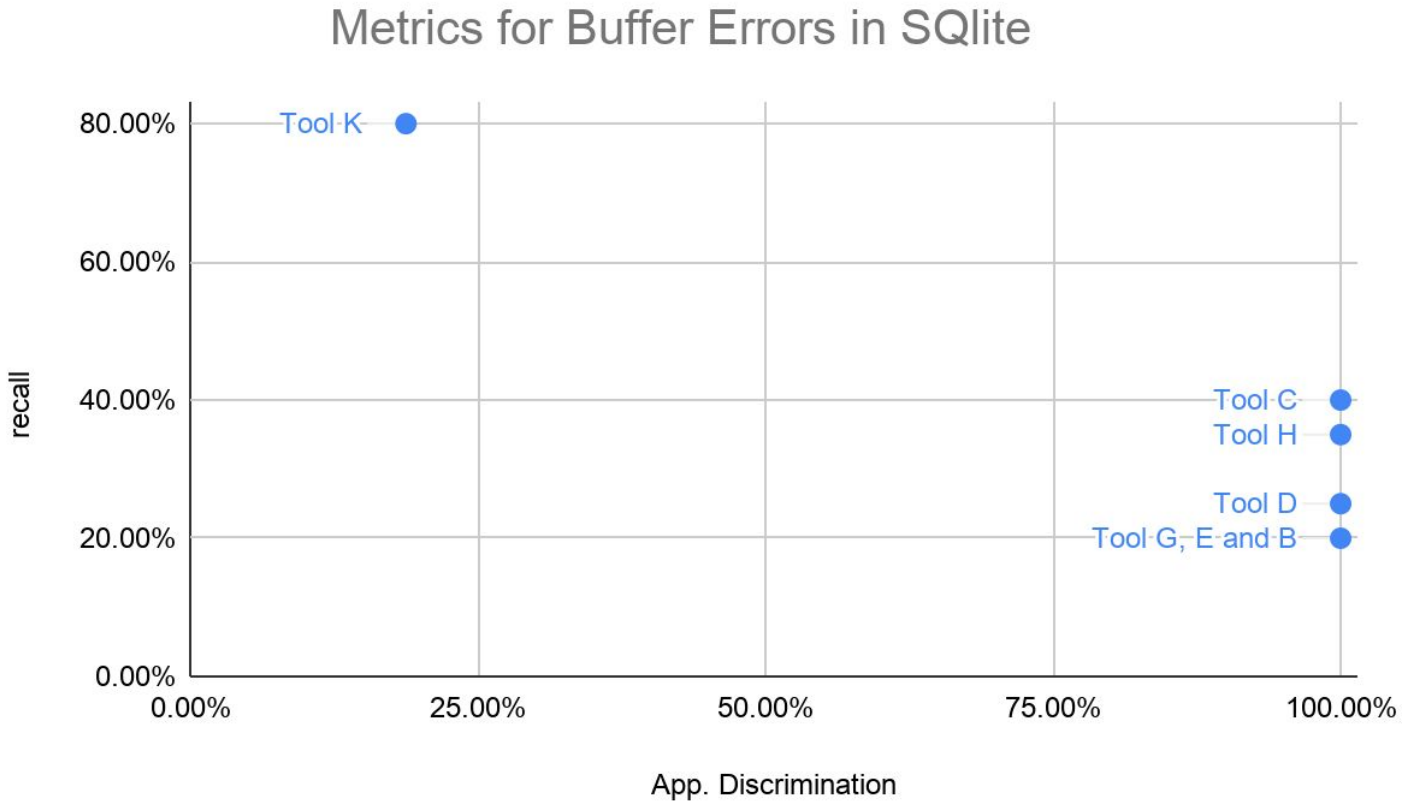


NIST National Institute of Standards and Technology U.S. Department of Commerce

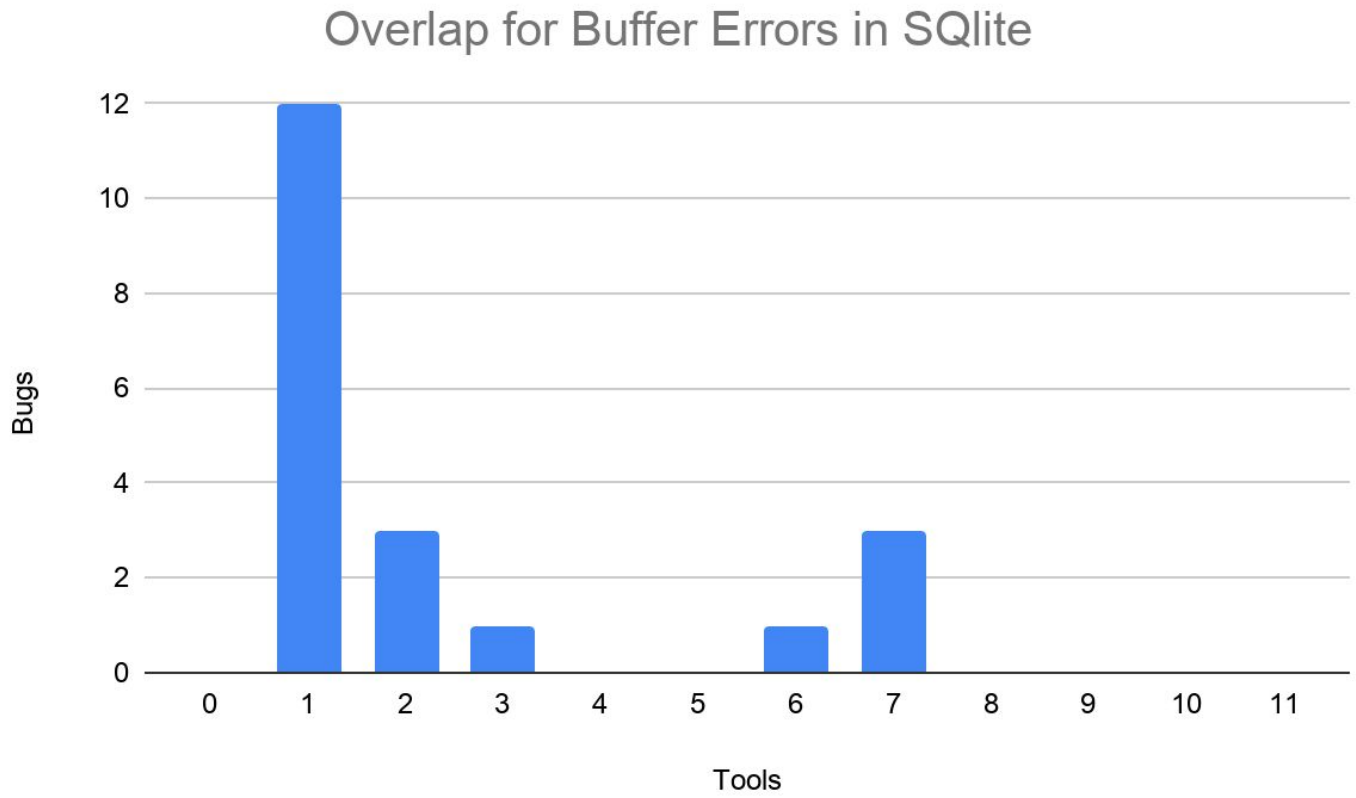
SAMATE



National Institute of Standards and Technology
U.S. Department of Commerce



National Institute of Standards and Technology
U.S. Department of Commerce

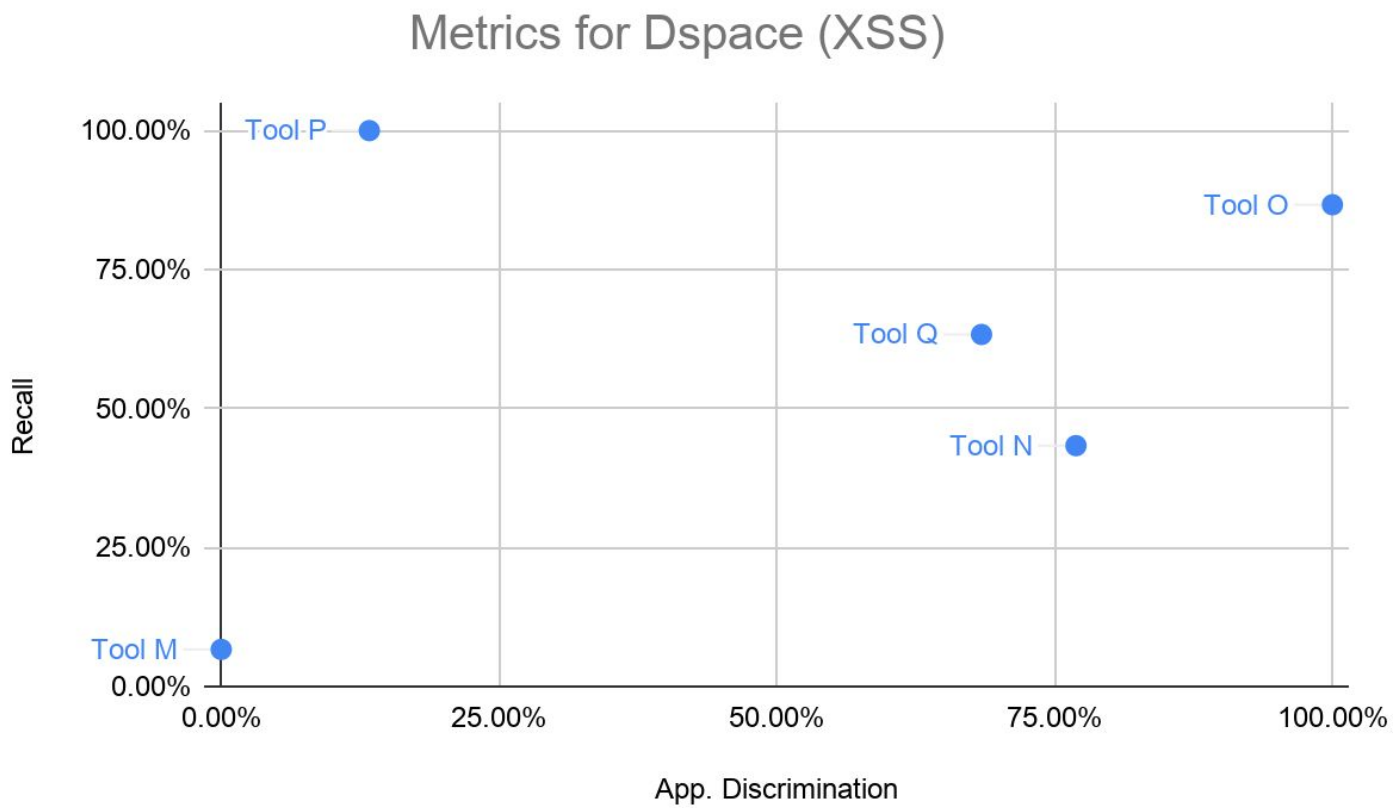


National Institute of Standards and Technology
U.S. Department of Commerce

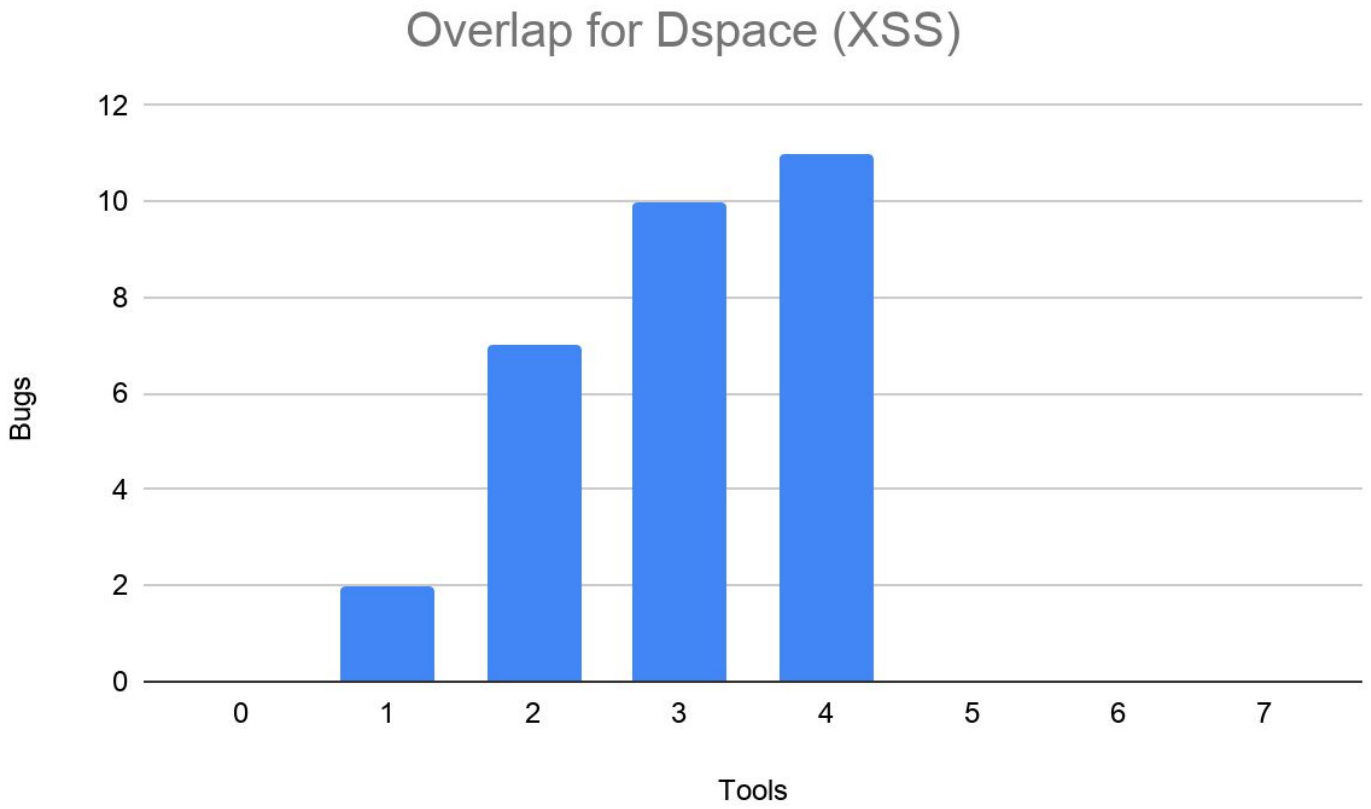
Java Test Cases

Dspace-6.2

- Date of release: 2017
- Lines of code: 234 k
- Manually injected weaknesses
- Bugs: 30 Cross Site Scripting



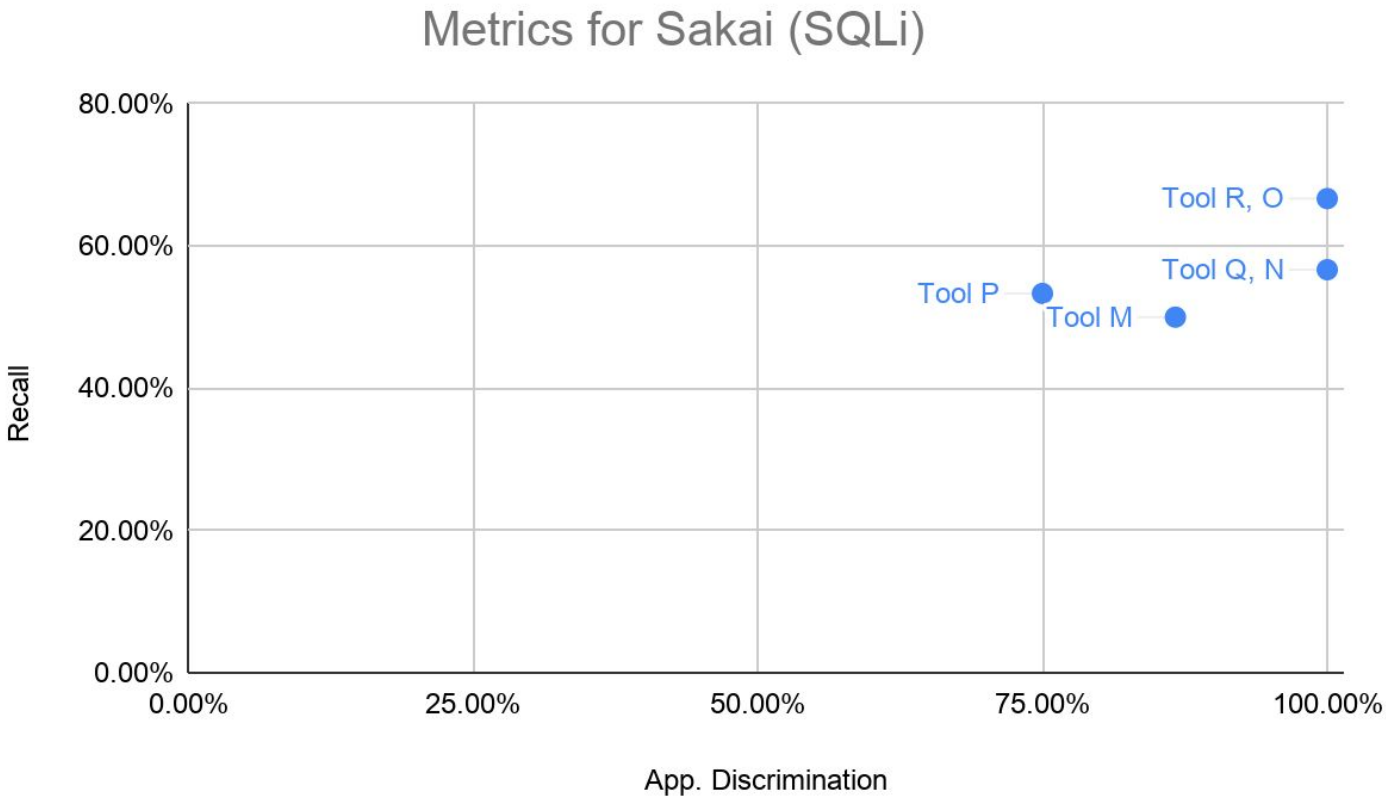
National Institute of Standards and Technology
U.S. Department of Commerce



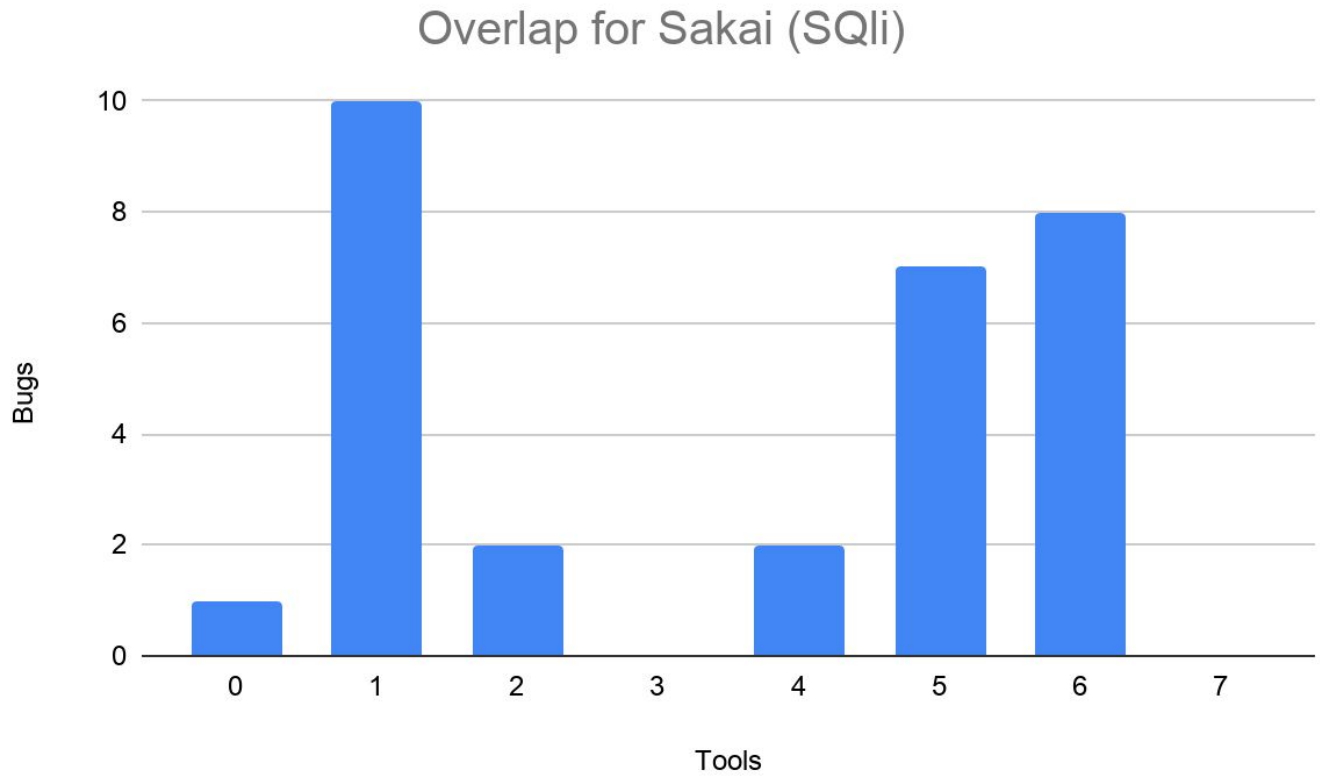
National Institute of Standards and Technology
U.S. Department of Commerce

Sakai-11.2

- Date of release: 2016
- Lines of code: 810 k
- Manually injected weaknesses
- Bugs: 30 SQL Injections



National Institute of Standards and Technology
U.S. Department of Commerce



National Institute of Standards and Technology
U.S. Department of Commerce

Any Questions?