



WHITEBOX FUZZING

An introduction to an advanced and automated testing method

slido

Are you aware of what fuzzing is?


 Start presenting to display the poll results on this slide.

TABLE OF CONTENTS

01

What is
fuzzing

02

What is
whitebox
fuzzing

03

Example from
the industry

04

Future
potential



01

What is (blackbox) fuzzing



“Fuzz testing is the process of repeatedly feeding modified inputs to a program in order to uncover security bugs, such as buffer overflows.”

A TRIVIAL EXAMPLE

```
function foo(int input) {  
  case (input)  
    case 0:  
      dog()  
    case 1:  
      cat()  
    case 2:  
      return true  
  return false  
}
```

LIMITATIONS OF BLACKBOX FUZZING

```
function foo(int input) {  
  case (input)  
    case 0:  
      dog()  
    case 1:  
      cat()  
    case 2:  
      return true  
    case 12:  
      return true  
  return false  
}
```



02

What is whitebox fuzzing

WHITEBOX FUZZING



Whitebox

Software testing of internal structures of programs.



Fuzzing

Finding software bugs by creating random malformed or semi-malformed input.
data

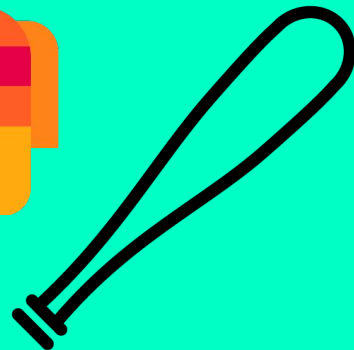
WHITEBOX FUZZING

```
function foo(int input) {  
  case (input)  
    case 0:  
      dog()  
    case 1:  
      cat()  
    case 2:  
      return true  
    case 12:  
      return true  
  return false  
}
```

Blackbox fuzzing

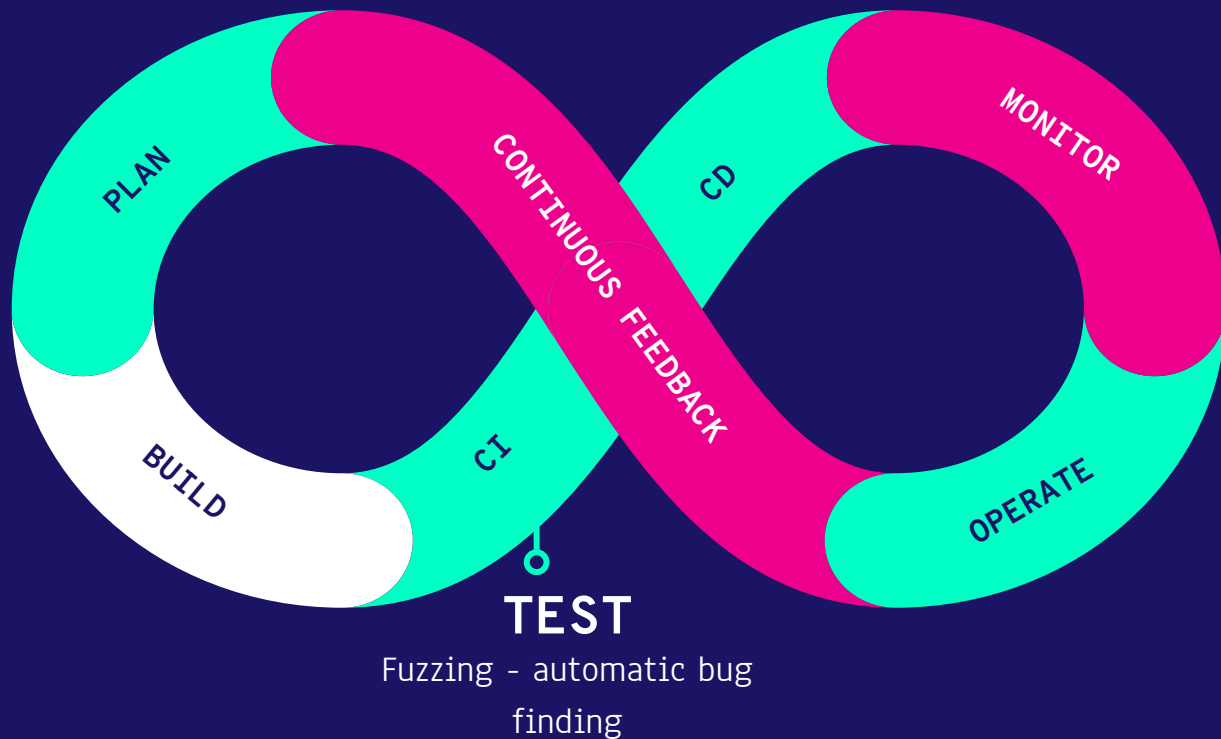


VS



Whitebox fuzzing

HOW IS IT RELATED TO DEVOPS





03

An practical example from the
industry

SAGE

Scalable Automated Guided Execution

200

average number of machines
SAGE running on each day

~ 33 %

percentage of all bugs found
by SAGE during development
of Windows 7

**“[...] saving millions of dollars
in potential security
vulnerabilities”**



04

Future potential in the
industry

LESSONS OF THE DAY

Whitebox fuzzing can be a good addition to other forms of testing. Especially in situations where bugs cause very expensive consequences.

Fuzzing

Simple yet efficient

Whitebox fuzzing

Leverages program analysis

SAGE

Microsoft's whitebox fuzzer



THANKS!

Do you have any questions?

kittyt@kth.se

sebene@kth.se

CREDITS: This presentation template was created by
Slidesgo, including icons by Flaticon, and
infographics & images by Freepik.

REFERENCES

- P. Ammann and J. Offutt, Introduction to Software Testing, Cambridge University Press, 2nd Edition, 2017, ISBN 978-1-107-17201-2.
- OWASP. Fuzzing. Retrieved from <https://owasp.org/www-community/Fuzzing>.
- GitLab. What is fuzz testing? Retrieved from <https://about.gitlab.com/topics/application-security/what-is-fuzz-testing/>.
- Ella Bounimova, Patrice Godefroid, and David Molnar. 2013. Billions and billions of constraints: whitebox fuzz testing in production. In Proceedings of the 2013 International Conference on Software Engineering (ICSE '13). IEEE Press, 122-131.
- Patrice Godefroid, Michael Y. Levin, and David Molnar. 2012. SAGE: whitebox fuzzing for security testing. Commun. ACM 55, 3 (March 2012), 40-44.
DOI:<https://doi-org.focus.lib.kth.se/10.1145/2093548.2093564>
- M. Boehme, C. Cadar and A. ROYCHOUDHURY, "Fuzzing: Challenges and Reflections," in IEEE Software, vol. 38, no. 3, pp. 79-86, May-June 2021, doi: 10.1109/MS.2020.3016773.