Fuzz Testing

Fuzzing or fuzz testing is an automated software testing technique that involves providing invalid, unexpected, or random data as inputs to a computer program to discover coding errors and security loopholes.

The purpose of fuzz testing is inserting data using automated or semi-automated techniques and testing the system for various exceptions like system crashing or failure of built-in code, etc.

Fuzz testing or fuzzing is a Software testing technique, and it is a type of **Security Testing**.

Why to do Fuzz Testing?

* Usually, Fuzzy testing finds the most serious security fault or defect.
* Fuzz testing gives more effective result when used with [**Black Box Testing**](https://www.guru99.com/black-box-testing.html), Beta Testing, and other debugging methods.
* Fuzz testing is used to check the Vulnerability of software. It is very cost effective testing techniques.
* Fuzz testing is one of the black box testing technique. Fuzzing is one of the most common method hackers used to find vulnerability of the system.

## 

## Types of bugs detected by Fuzz Testing

* **Assertion failures and memory leaks** this methodology is widely used for large applications where bugs are affecting the safety of memory, which is a severe vulnerability.
* **Invalid input** in fuzz testing, fuzzers are used to generate an invalid input which is used for testing error-handling routines, and this is important for the software which does not control its input. Simple fuzzing can be known as a way to automate negative testing.
* **Correctness bugs** fuzzing can also be used to detect some types of “correctness” bugs. Such as a corrupted database, poor search results, etc.

Fuzz Testing Phases

