VALYTICS

Answering Your Questions about Fuzz Testing

5 Bad Things That Can Happen if You Do Not Fuzz Test

What is Fuzz Testing?

Fuzz Testing is the deliberate injection of malformed (bad) data into an application by manual or automated tools in order to detect security vulnerabilities.

What can happen without Fuzz Testing?

- *SQL Injection Vulnerabilities* – Taking control of SQL queries with user controlled data in an unsafe manner, resulting in unauthorized reading or modifying critical or protected data (Data Breaches).
- *JavaScript Injection Vulnerabilities* - Hijacking of an application's URL that causes JavaScript code from an attacker to execute within a user's browser, resulting in running a potentially destructive application.
- *Clickjacking Vulnerabilities* - Overlay of an application's interface with an interface from an attacker, resulting in unauthorized actions.
- *Integer Arithmetic Vulnerabilities* - Unexpected results from calculations, due to the handling of integer data types, leading to unexpected downtime from system crashes and possible corruption of critical/protected data.
- *Buffer Overflows* - Data written beyond the end of an application's memory block, resulting in the ability to crash an application or damage the system by executing destructive code.

How can you learn more?

Contact us at info@valytics.com to learn more about Fuzz Testing or how Valytics' full service independent test capabilities can help your organization.