PEACH FUZZER™ FUZZQUAL TESTING FRAMEWORK

Version 1.1

For effective fuzz testing assurance efforts, mapping the rigor of testing to the objectives is key. In particular, testing teams are keen to determine how often and how much to fuzz a solution.

Peach Tech, in consultation with key partners and customers, undertook a rigorous analysis of fuzz testing efforts. This analysis determined four key factors that inform effective fuzz testing and assurance efforts. These factors are:

1. Complexity of the solution being tested
2. Frequency of testing
3. Maturity of the software development process
4. Desired quality assurance goal

These factors were leveraged to define the **FuzzQual™** testing framework.

The FuzzQual testing framework consists of recommended testing levels that enable users to achieve their desired objectives. It consists of two guidance benchmarks to determine how often and how much to fuzz a solution:

1. FuzzQual Testing: best suited for one-time testing of solutions by QA or internal testing team
2. FuzzQual Verification: best suited for repeatable compliance that can be assessed and verified by a third party

FuzzQual is ideally suited for organizations seeking a consistent, measurable, and expert recommended standard for conducting automated security testing.

FUZZQUAL Testing Benchmark

FuzzQual Testing benchmark is designed for a one-time test pass during solution development or testing. Its primary goal is to provide testing guidance for QA teams, testers, and penetration testers. The purpose of this is to provide guidance on software quality evaluation across different releases of the same solution.

It consists of 4 levels (TL1-TL4), with higher levels denoting greater testing rigor. TL1 and TL2 are best suited for quick checks during daily builds, TL2 is specifically suitable for red teams and penetration testing efforts. TL3-TL4 are intended for major releases. Organizations adopting these benchmarks will benefit from standardized testing across releases, consistency of testing, and robust regression testing.

Table 1. FUZZQUAL Testing Benchmarks

Testing Level	Minimum Test Cases	Recommended For
FuzzQual TL1	100,000	Daily or weekly builds
FuzzQual TL2	250,000	Penetration testing & for low risk protocols and file formats
FuzzQual TL3	500,000	Protocols & file formats with mature security profiles
FuzzQual TL4	1,000,000	Critical components with mature security profiles

FUZZQUAL VERIFICATION BENCHMARK

The FuzzQual Verification benchmark is designed for third party compliance and verification testing. The purpose of this is to provide guidance to evaluate software quality with respect to other solutions within the same class. In contrast to FuzzQual Testing benchmarks, the FuzzQual Verification benchmarks allow for the comparison of security quality between competing solutions.

It consists of 3 levels (VL2-VL4), with higher levels denoting greater testing rigor. FuzzQual Verification Levels VL2-VL4 add an additional constraint, Test Cases Between Failure, to corresponding FuzzQual Testing Levels TL2-TL4. This makes Verification benchmarks more rigorous than their corresponding FuzzQual Testing benchmarks.

TABLE 2. FUZZQUAL Verification Benchmarks

Verification Level	Min Test Cases	Test Cases Between Failure	Recommended For
FuzzQual VL2	250,000	150,000	New protocols & file formats with minimal ship criteria
FuzzQual VL3	500,000	250,000	Protocols & file formats with mature security profile
FuzzQual VL4	1,000,000	500,000	Critical components with mature security profile

Vendors can leverage these benchmarks as a competitive advantage to demonstrate the quality of their solutions. Purchasing organizations can bolster the integrity of their software supply chain by evaluating competing solutions against these benchmarks.

About The Authors

Akshay Aggarwal – Peach Tech CEO
Akshay has over ten years of leadership experience at Microsoft and other technology companies. He holds an MS in Computer Science from UC Davis, where he researched Internet worms and intrusion detection systems.

Michael Eddington – Peach Tech CTO
Michael is the principal architect of the Peach Fuzzer Platform. An authority on embedded system security, cloud security, and application security, he has worked for leading technology companies including Hewlett-Packard.

About Peach Tech

Peach Tech was founded by a group of information security veterans with leadership experience at Microsoft, Amazon, and HP. They draw on over thirty years of experience as “ethical hackers” to turn attacker methodology into powerful and accessible tools to secure products. Peach Fuzzer is now the industry leading fuzz testing platform, used to secure hardware and software solutions across a range of industries.