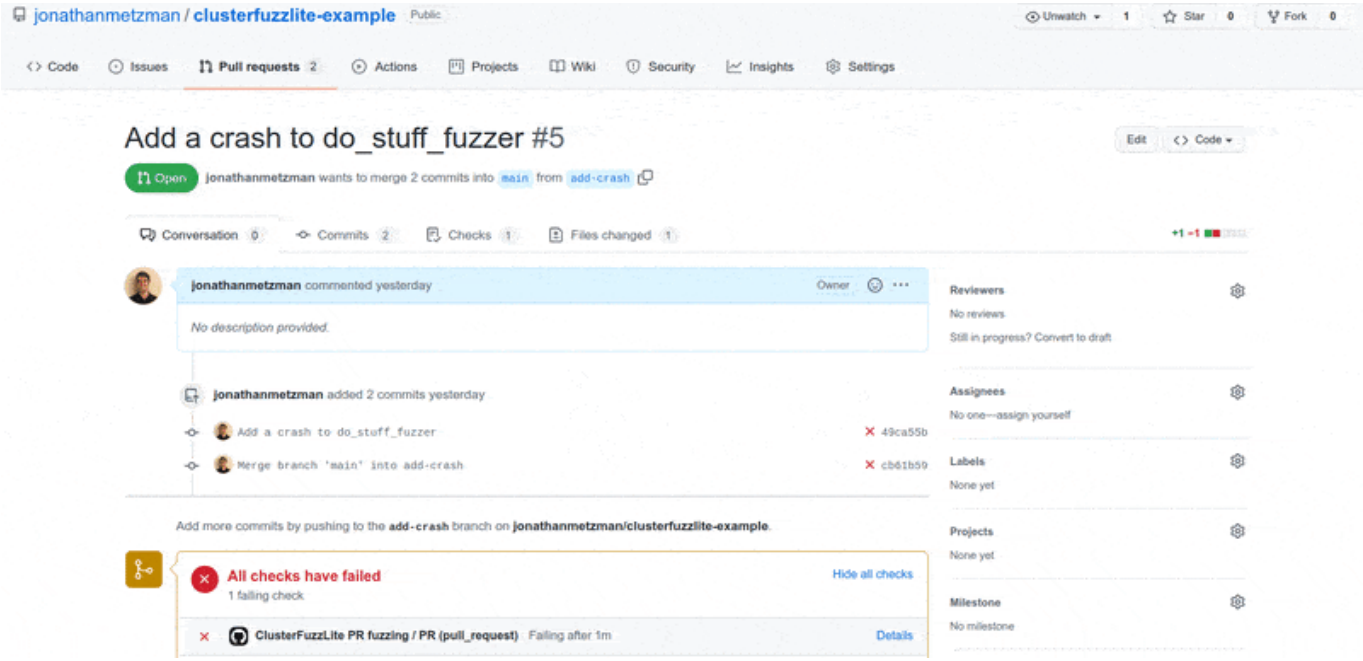
# Open source : Google complète sa boîte à outils de fuzzing

S'il devait n'en rester qu'un, serait-ce libFuzzer ? Google a en tout cas choisi ce moteur pour propulser ClusterFuzzLite. Pas d'AFL++ ni de Honggfuzz, donc, pour cette implémentation « allégée » de ClusterFuzz*. Mais le même principe : proposer une infrastructure distribuée de *fuzzing* (recherche de bugs par injection de code).

ClusterFuzzLite s'embarque dans les processus d'intégration continue. Pour le moment, il prend en charge GitHub Actions, Google Cloud Build et Prow (en bêta pour ce dernier). Côté langages, il supporte C, C++, Java (et dérivés JVM), Go, Python, Rust et Swift.




ClusterFuzzLite permet de réaliser deux types de tests. D'une part, « à la volée » sur chaque modification de code, avec une durée par défaut de 10 minutes. De l'autre, en lot et sur plus long terme, afin de constituer des corpus – qu'on pourra assainir par la suite, tout en produisant des rapports de couverture.

** Google héberge, sur son cloud, sa propre implémentation de ClusterFuzz : OSS-Fuzz. Il propose, par ce biais, de « fuzzer » des projets* open source*, sélectionnés au cas par cas. cURL et systemd en font partie.*

*Illustration principale © Scanrail – Adobe Stock*