

# BenchPress: Analyzing Android App Vulnerability Benchmark Suites

Submitted by grigby1 on Fri, 08/14/2020 - 11:43am

Title BenchPress: Analyzing Android App Vulnerability Benchmark Suites

Publication Type Conference Paper

Year of Publication 2019

Authors [Mitra, Joydeep](#), [Ranganath, Venkatesh-Prasad](#), [Narkar, Aditya](#)

Conference Name 2019 34th IEEE/ACM International Conference on Automated Software Engineering Workshop (ASEW)

Keywords [android](#), [Android \(operating system\)](#), [Android app development](#), [Android app vulnerability benchmark suite analysis](#), [Android security analysis tools](#), [Android-specific benchmark suites](#), [APIs](#), [application program interfaces](#), [application programming interface](#), [benchmark](#), [BenchPress](#), [compositionality](#), [DroidBench](#), [empirical software engineering](#), [evaluation](#), [Ghera](#), [ICCBench](#), [mobile computing](#), [pubcrawl](#), [Representativeness](#), [resilience](#), [Resiliency](#), [security](#), [security of data](#), [security-related APIs](#), [stack overflow](#), [temperature 227.0 K](#), [tool developers](#), [UBCBench](#)

Abstract In recent years, various benchmark suites have been developed to evaluate the efficacy of Android security analysis tools. Tool developers often choose such suites based on the availability and popularity of suites and not on their characteristics and relevance due to the lack of information about them. In this context, based on a recent effort, we empirically evaluated four Android-specific benchmark suites: DroidBench, Ghera, ICCBench, and UBCBench. For each benchmark suite, we identified the APIs used by the suite that were discussed on Stack Overflow in the context of Android app development and measured the usage of these APIs in a sample of 227K real-world apps (coverage). We also identified security-related APIs used in real-world apps but not in any of the above benchmark suites to assess the opportunities to extend benchmark suites (gaps).

DOI [10.1109/ASEW.2019.00020](https://doi.org/10.1109/ASEW.2019.00020)

Citation Key mitra\_benchpress\_2019



[security of data](#) [security pubcrawl](#) [resilience](#) [Resiliency](#) [mobile computing](#) [APIs](#) [application program interfaces](#) [Compositionality](#) [android](#) [evaluation](#) [Android \(operating system\)](#) [Android app development](#) [Android app vulnerability benchmark suite analysis](#) [Android security analysis tools](#) [Android-specific benchmark suites](#) [benchmark](#) [BenchPress](#) [DroidBench](#) [Empirical Software Engineering](#) [Ghera](#) [ICCBench](#) [Representativeness](#) [security-related APIs](#) [stack overflow](#) [temperature 227.0 K](#) [tool developers](#) [UBCBench](#) [application programming interface](#)

---