**解决了个安全领域的小问题**

* 您的fuzz测试需要执行多长时间？或者要执行多少次？
* Fuzz测试跑了n长时间，或n次，但有效吗？值得吗？
* 做了Fuzz测试就可以放心了吗？靠谱吗？

估计很多人都不知道fuzz测试需要执行多长时间，或执行多少次。以笔者了解，在大厂这些指标都是靠测试人员拍脑袋定的，毫无依据和标准。至于fuzz测试是否靠谱，可能有人说找出的问题肯定靠谱。但是是否还有没找出的问题就不敢说了。更多的时候，fuzz测试没有发现任何问题，那测试究竟做了什么？大厂fuzz测试都是花费大量的服务器，投入大量的时间和人力做，这个值得吗？估计很少有人能回答。

专业人员都知道GCC、java、python等都有关于fuzz测试的覆盖率评估工具，可以用于评估fuzz测试的效果。但是，在实际应用中，fuzz测试的工程师很少根据这个覆盖率指标来制定测试计划，为什么呢？具体原因是GCC等的覆盖率只是所谓的行覆盖或分支覆盖，从技术原理上可以分析论证这个指标基本没有实际的参考价值。

为解决fuzz测试的执行效率问题，我们对fuzz测试做了一系列的优化措施。本文推出的是其中之一：fuzz测试的执行效率评估优化方案。

针对fuzz测试的执行效率评估问题，我们提出了优于GCC相关指标的fuzz覆盖率评估解决方案。与GCC等的行覆盖或分支覆盖不同，我们的工具采用路径覆盖率分析，从原理上就有本质区别。就我们所知，国内外好像还没有相关的，或更优的评估工具出现。

除给出解决方案外，我们还研发相关工具，该工具完成了多次技术验证；完成了初步功能设计和实现开发；当前这个工具正处于测试阶段。具体的工具介绍参考公众号文档《Fuzz覆盖率评估工具FP-cov》。

下一步，我们将开发显示fuzz究竟在做什么，哪些计算是有效的；哪些计算是无效的；fuzz测试的目标对象的风险点在哪；如何指导fuzz定位到风险点等等。相关工具将会陆续推出。

这只是小意思，希望上半年还能推出个大的，敬请关注。