We have made much effort to test almost all of the benchmark programs from FuzzBench [1], Magma [2], Binutils [3], Unibench [4] and AFLGO [5]. In the source code project, we would provide the scripts for adapting 5 representative fuzzers and about 40 programs in an unified way However, it is still an open issue to make effective and fair benchmark datasets for diverse fuzzing scenarios.

References

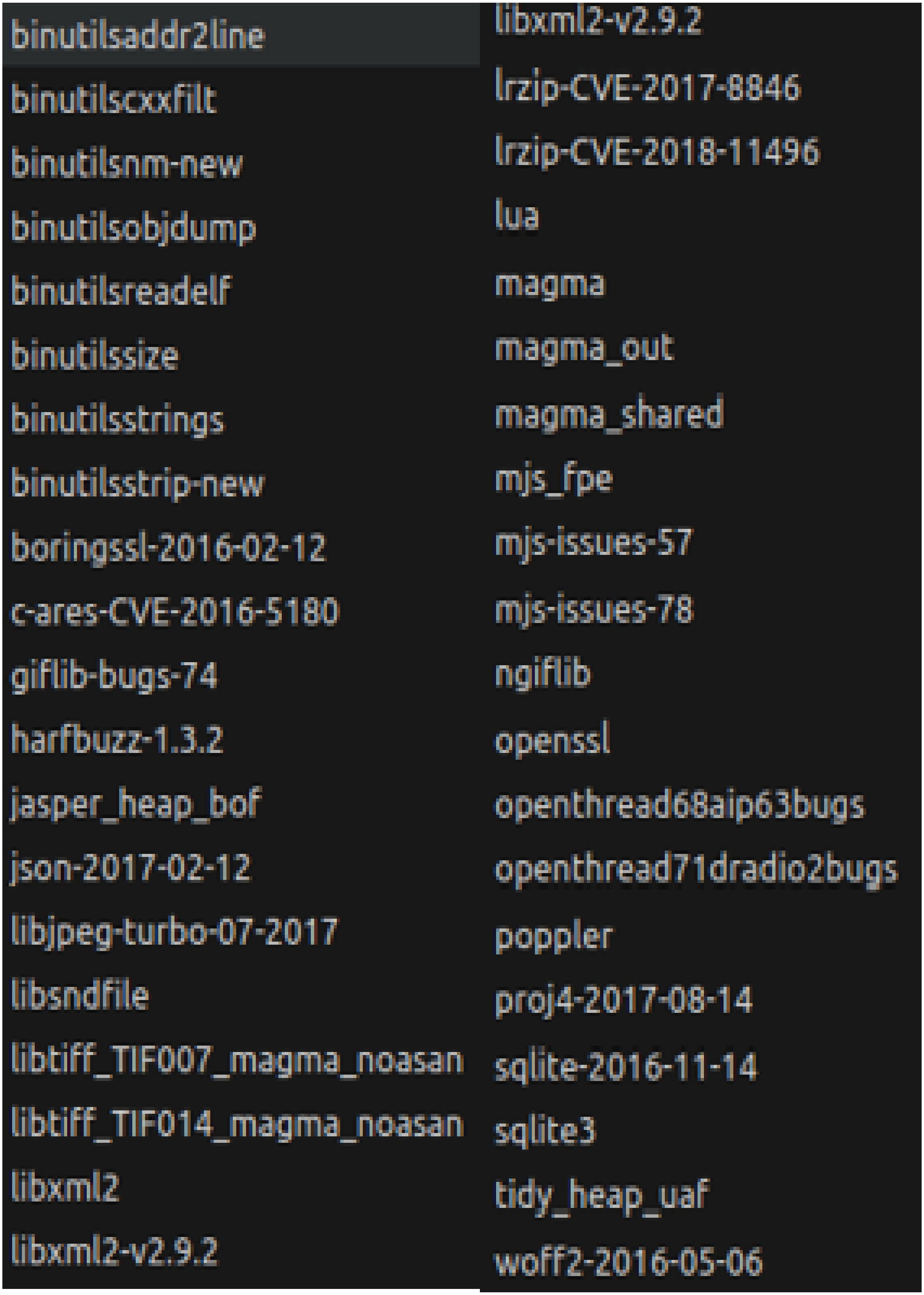
[1] J. Metzman, L. Szekeres, L. Simon, R. Sprabery, and A. Arya, "Fuzzbench: an open fuzzer benchmarking platform and service," in *Proceedings of the 29th ACM Joint Meeting on European Software Engineering Conference and Symposium on the Foundations of Software Engineering*, 2021, pp. 1393–1403.

[2] A. Hazimeh, A. Herrera, and M. Payer, "Magma: A ground-truth fuzzing benchmark," *Proceedings of the ACM on Measurement and Analysis of Computing Systems*, vol. 4, no. 3, pp. 1–29, 2020.

[3] GNU, "Binutils- GNU Project - Free Software Foundation," https://www.gnu.org/software/binutils/, [Online; accessed 2024-09-06].

[4] Y. Li, S. Ji, Y. Chen, S. Liang, W.-H. Lee, Y. Chen, C. Lyu, C. Wu, R. Beyah, and P. Cheng, "Unifuzz: A holistic and pragmatic metrics-driven platform for evaluating fuzzers." in *USENIX Security Symposium*, 2021, pp. 2777–2794.

[5] M. Böhme, V.-T. Pham, M.-D. Nguyen, and A. Roychoudhury, "Directed greybox fuzzing," in *Proceedings of the 2017 ACM SIGSAC conference on computer and communications security*, 2017, pp. 2329–2344.



binutilsaddr2line

binutilscxxfilt

binutilsnm-new

binutilsobjdump

binutilsreadelf

binutilssize

binutilsstrings

binutilsstrip-new

boringssl-2016-02-12

c-ares-CVE-2016-5180

giflib-bugs-74

harfbuzz-1.3.2

jasper_heap_bof

json-2017-02-12

libjpeg-turbo-07-2017

libsndfile

libtiff_TIF007_magma_noasan

libtiff_TIF014_magma_noasan

libxml2

libxml2-v2.9.2

libxml2-v2.9.2

lrzip-CVE-2017-8846

lrzip-CVE-2018-11496

lua

magma

magma_out

magma_shared

mjs_fpe

mjs-issues-57

mjs-issues-78

ngiflib

openssl

openthread68aip63bugs

openthread71dradio2bugs

poppler

proj4-2017-08-14

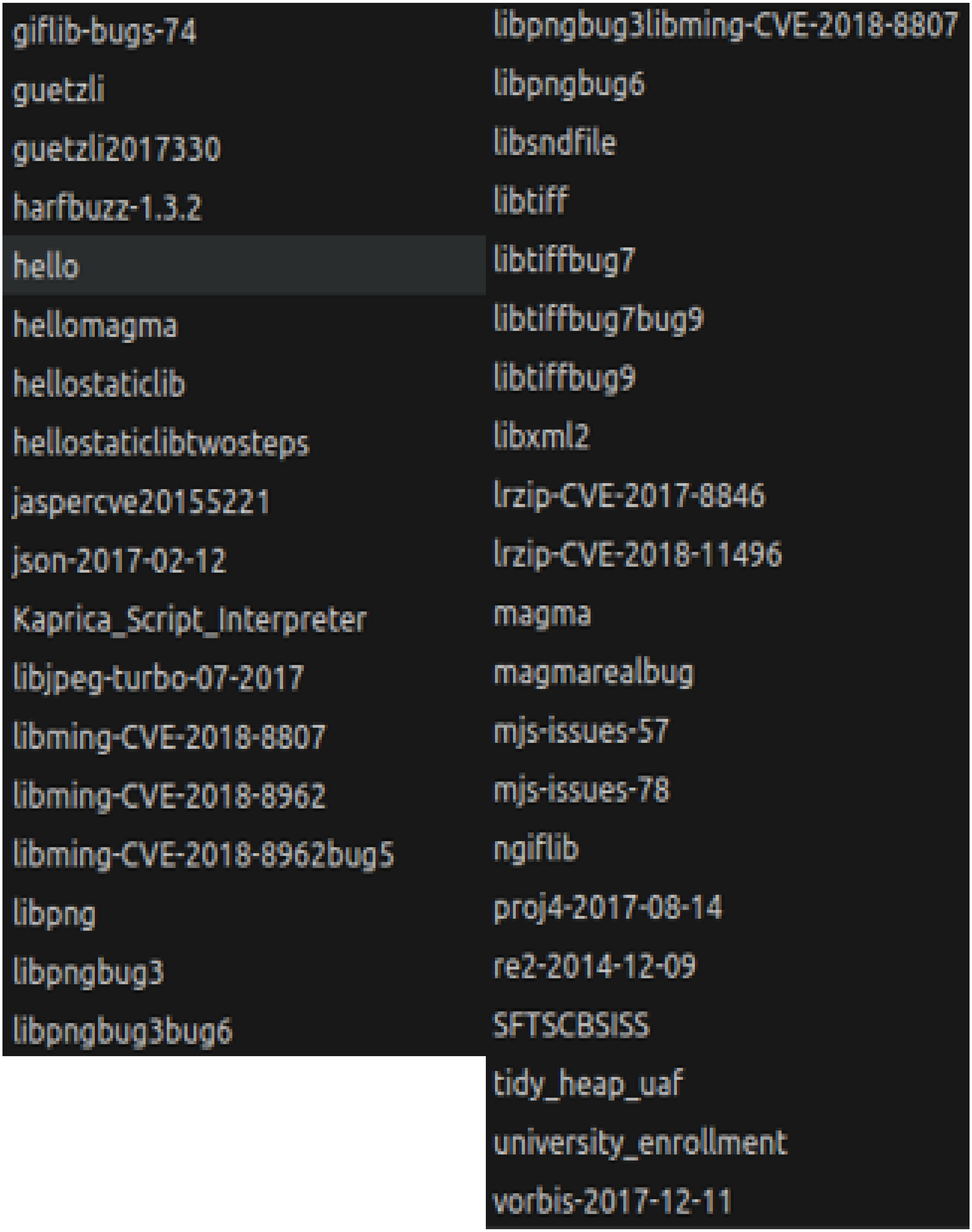
sqlite-2016-11-14

sqlite3

tidy_heap_uaf

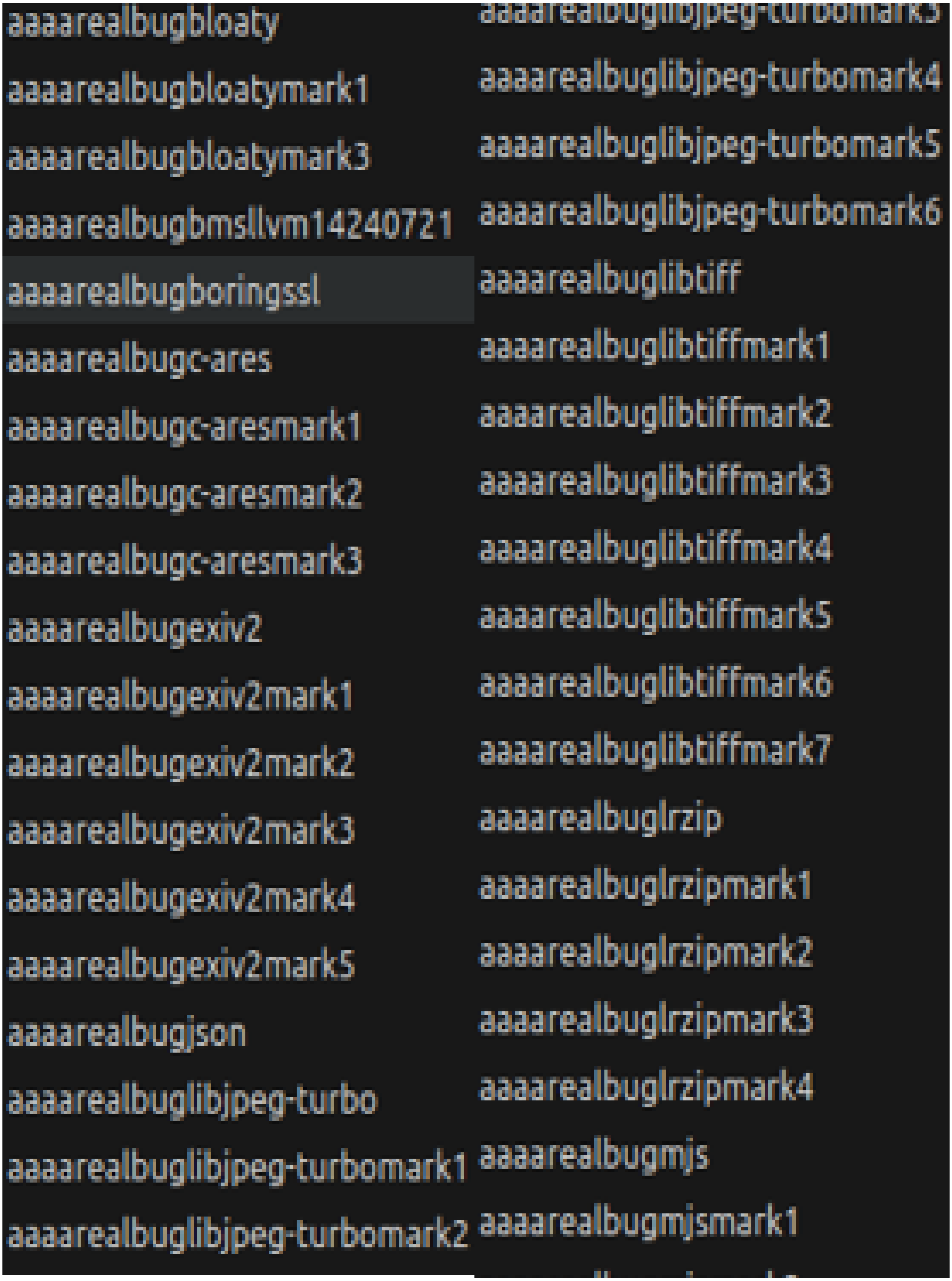
woff2-2016-05-06

Fig. 1. The first part of the benchmark programs tested.



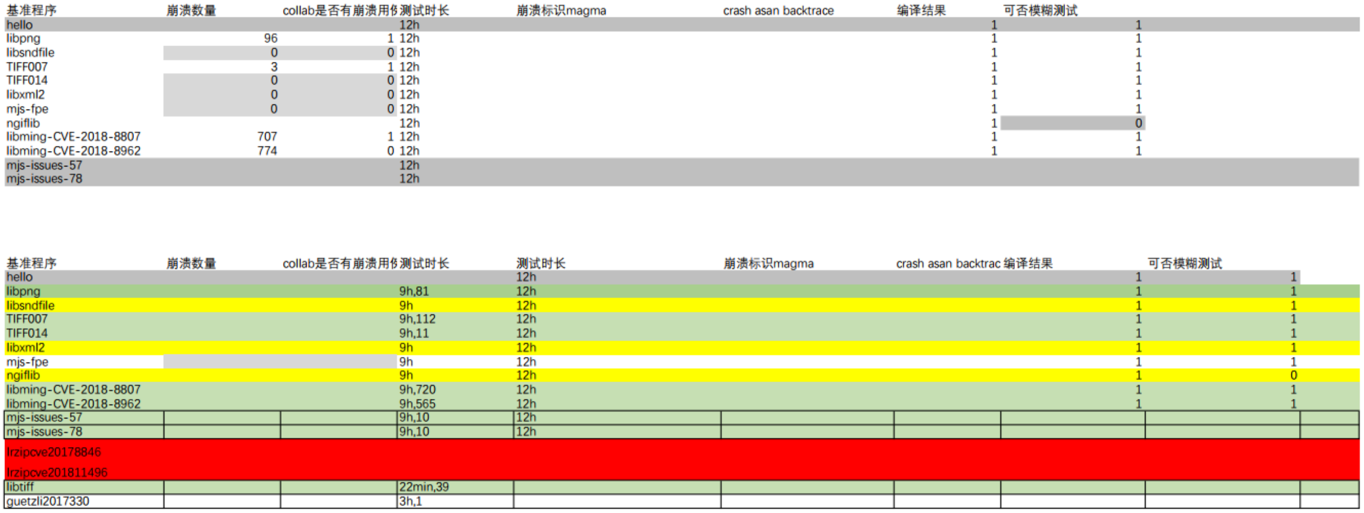
```
giflib-bugs-74
guetzli
guetzli2017330
harfbuzz-1.3.2
hello
hellomagma
hellostaticlib
hellostaticlibtwosteps
jaspercve20155221
json-2017-02-12
Kaprica_Script_Interpreter
libjpeg-turbo-07-2017
libming-CVE-2018-8807
libming-CVE-2018-8962
libming-CVE-2018-8962bug5
libpng
libpngbug3
libpngbug3bug6
libpngbug3libming-CVE-2018-8807
libpngbug6
libsndfile
libtiff
libtiffbug7
libtiffbug7bug9
libtiffbug9
libxml2
lrzip-CVE-2017-8846
lrzip-CVE-2018-11496
magma
magmarealbug
mjs-issues-57
mjs-issues-78
ngiflib
proj4-2017-08-14
re2-2014-12-09
SFTSCBSISS
tidy_heap_uaf
university_enrollment
vorbis-2017-12-11
```

Fig. 2. The second part of the benchmark programs tested.



```
aaaarealbugbloaty
aaaarealbugbloatymark1
aaaarealbugbloatymark3
aaaarealbugbmsllvm14240721
aaaarealbugboringssl
aaaarealbugc-ares
aaaarealbugc-aresmark1
aaaarealbugc-aresmark2
aaaarealbugc-aresmark3
aaaarealbugexiv2
aaaarealbugexiv2mark1
aaaarealbugexiv2mark2
aaaarealbugexiv2mark3
aaaarealbugexiv2mark4
aaaarealbugexiv2mark5
aaaarealbugjson
aaaarealbuglibjpeg-turbo
aaaarealbuglibjpeg-turbomark1
aaaarealbuglibjpeg-turbomark2
aaaarealbuglibjpeg-turbomark3
aaaarealbuglibjpeg-turbomark4
aaaarealbuglibjpeg-turbomark5
aaaarealbuglibjpeg-turbomark6
aaaarealbuglibtiff
aaaarealbuglibtiffmark1
aaaarealbuglibtiffmark2
aaaarealbuglibtiffmark3
aaaarealbuglibtiffmark4
aaaarealbuglibtiffmark5
aaaarealbuglibtiffmark6
aaaarealbuglibtiffmark7
aaaarealbuglrzip
aaaarealbuglrzipmark1
aaaarealbuglrzipmark2
aaaarealbuglrzipmark3
aaaarealbuglrzipmark4
aaaarealbugmjs
aaaarealbugmjsmark1
```

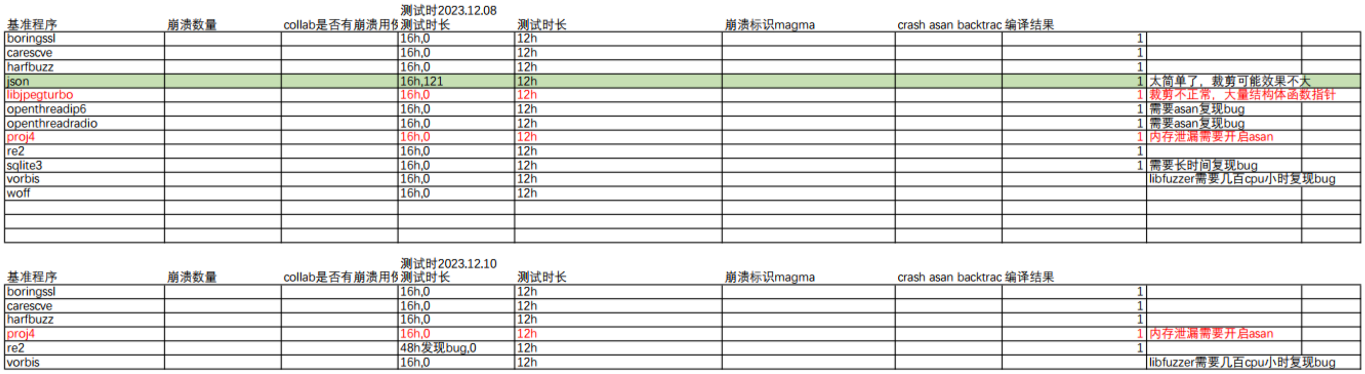
Fig. 3. The third part of the benchmark programs tested.



基准程序	崩溃数量	collab是否有崩溃用例	测试时长	崩溃标识magma	crash asan backtrace	编译结果	可否模糊测试
hello			12h			1	1
libpng	96	1	12h			1	1
libsndfile	0	0	12h			1	1
TIFF007	3	1	12h			1	1
TIFF014	0	0	12h			1	1
libxml2	0	0	12h			1	1
mjs-fpe	0	0	12h			1	1
ngiflib			12h			1	0
libming-CVE-2018-8807	707	1	12h			1	1
libming-CVE-2018-8962	774	0	12h			1	1
mjs-issues-57			12h				
mjs-issues-78			12h				

基准程序	崩溃数量	collab是否有崩溃用例	测试时长	测试时长	崩溃标识magma	crash asan backtrac	编译结果	可否模糊测试	
hello				12h			1	1	
libpng			9h,81	12h			1	1	
libsndfile			9h	12h			1	1	
TIFF007			9h,112	12h			1	1	
TIFF014			9h,11	12h			1	1	
libxml2			9h	12h			1	1	
mjs-fpe			9h	12h			1	1	
ngiflib			9h	12h			1	0	
libming-CVE-2018-8807			9h,720	12h			1	1	
libming-CVE-2018-8962			9h,565	12h			1	1	
mjs-issues-57			9h,10	12h					
mjs-issues-78			9h,10	12h					
lrzipcve20178846									
lrzipcve201811496									
libtiff			22min,39						
guetzli2017330			3h,1						

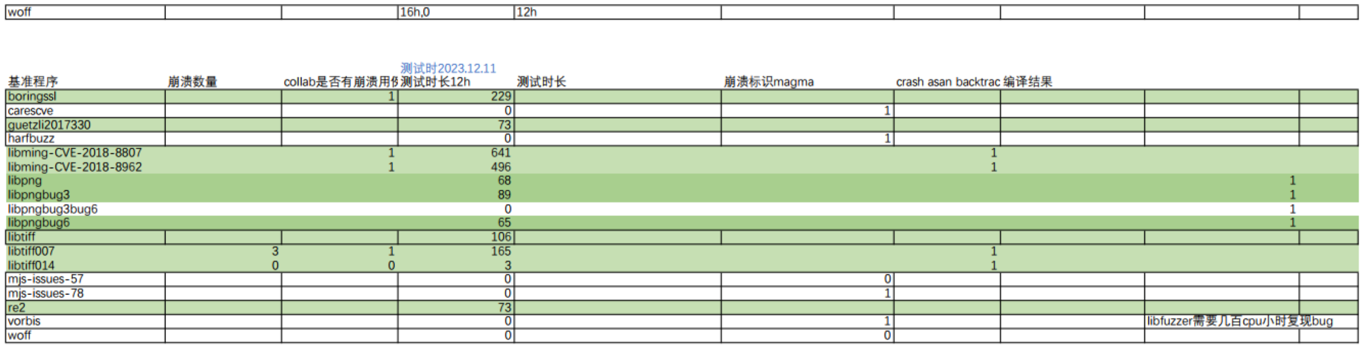
Fig. 4. Much effort for testing benchmarks.



基准程序	崩溃数量	collab是否有崩溃用例	测试时2023.12.08 测试时长	测试时长	崩溃标识magma	crash asan backtrac	编译结果		
boringssl			16h,0	12h			1		
carescve			16h,0	12h			1		
harfbuzz			16h,0	12h			1		
json			16h,121	12h			1	太简单了，裁剪可能效果不大	
libjpegturbo			16h,0	12h			1	裁剪不正常，大量结构体函数指针	
openthreadip6			16h,0	12h			1	需要asan复现bug	
openthreadradio			16h,0	12h			1	需要asan复现bug	
proj4			16h,0	12h			1	内存泄漏需要开启asan	
re2			16h,0	12h			1		
sqlite3			16h,0	12h			1	需要长时间复现bug	
vorbis			16h,0	12h				libfuzzer需要几百cpu小时复现bug	
woff			16h,0	12h					

基准程序	崩溃数量	collab是否有崩溃用例	测试时2023.12.10 测试时长	测试时长	崩溃标识magma	crash asan backtrac	编译结果		
boringssl			16h,0	12h			1		
carescve			16h,0	12h			1		
harfbuzz			16h,0	12h			1		
proj4			16h,0	12h			1	内存泄漏需要开启asan	
re2			48h发现bug,0	12h			1		
vorbis			16h,0	12h				libfuzzer需要几百cpu小时复现bug	

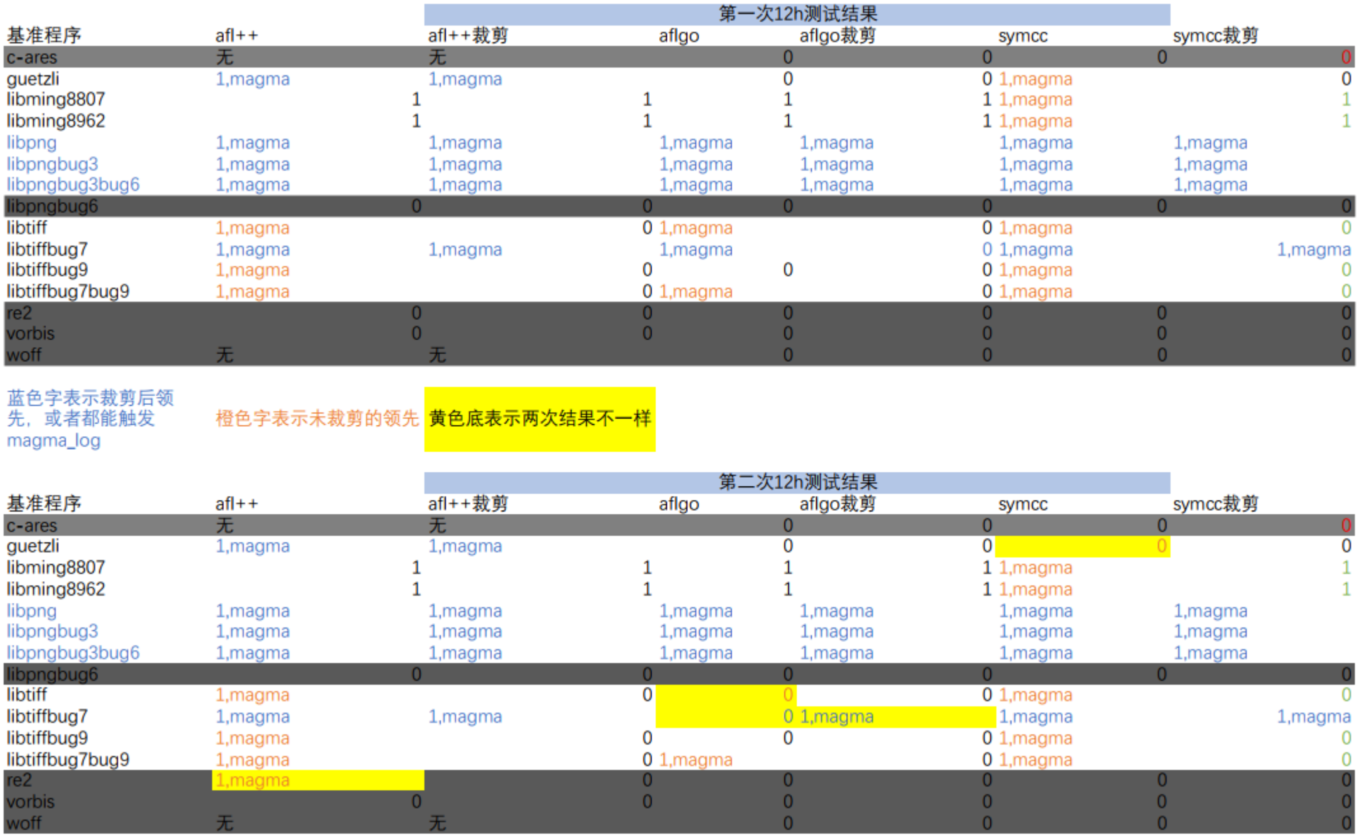
Fig. 5. Much effort for testing benchmarks.



woff			16h,0	12h					

基准程序	崩溃数量	collab是否有崩溃用例	测试时2023.12.11 测试时长12h	测试时长	崩溃标识magma	crash asan backtrac	编译结果		
boringssl		1	229						
carescve			0		1				
guetzli2017330			73						
harfbuzz			0		1				
libming-CVE-2018-8807		1	641			1			
libming-CVE-2018-8962		1	496			1			
libpng			68					1	
libpngbug3			89					1	
libpngbug3bug6			0					1	
libpngbug6			65					1	
libtiff			106						
libtiff007	3	1	165			1			
libtiff014	0	0	3			1			
mjs-issues-57			0		0				
mjs-issues-78			0		1				
re2			73						
vorbis			0		1			libfuzzer需要几百cpu小时复现bug	
woff			0		0				

Fig. 6. Much effort for testing benchmarks.

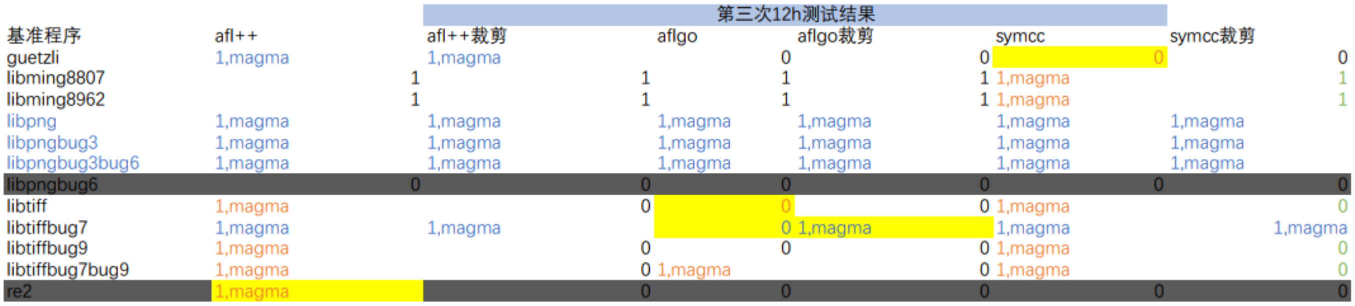


		第一次12h测试结果				
基准程序	afl++	afl++裁剪	aflgo	aflgo裁剪	symcc	symcc裁剪
c-ares	无	无	0	0	0	0
guetzli	1,magma	1,magma	0	0	1,magma	0
libming8807	1	1	1	1	1,magma	1
libming8962	1	1	1	1	1,magma	1
libpng	1,magma	1,magma	1,magma	1,magma	1,magma	1,magma
libpngbug3	1,magma	1,magma	1,magma	1,magma	1,magma	1,magma
libpngbug3bug6	1,magma	1,magma	1,magma	1,magma	1,magma	1,magma
libpngbug6	0	0	0	0	0	0
libtiff	1,magma	0	1,magma	0	1,magma	0
libtiffbug7	1,magma	1,magma	1,magma	0	1,magma	1,magma
libtiffbug9	1,magma	0	0	0	1,magma	0
libtiffbug7bug9	1,magma	0	1,magma	0	1,magma	0
re2	0	0	0	0	0	0
vorbis	0	0	0	0	0	0
woff	无	无	0	0	0	0

蓝色字表示裁剪后领先，或者都能触发magma_log	橙色字表示未裁剪的领先	黄色底表示两次结果不一样

		第二次12h测试结果				
基准程序	afl++	afl++裁剪	aflgo	aflgo裁剪	symcc	symcc裁剪
c-ares	无	无	0	0	0	0
guetzli	1,magma	1,magma	0	0	0	0
libming8807	1	1	1	1	1,magma	1
libming8962	1	1	1	1	1,magma	1
libpng	1,magma	1,magma	1,magma	1,magma	1,magma	1,magma
libpngbug3	1,magma	1,magma	1,magma	1,magma	1,magma	1,magma
libpngbug3bug6	1,magma	1,magma	1,magma	1,magma	1,magma	1,magma
libpngbug6	0	0	0	0	0	0
libtiff	1,magma	0	0	0	1,magma	0
libtiffbug7	1,magma	1,magma	0	1,magma	1,magma	1,magma
libtiffbug9	1,magma	0	0	0	1,magma	0
libtiffbug7bug9	1,magma	0	1,magma	0	1,magma	0
re2	1,magma	0	0	0	0	0
vorbis	0	0	0	0	0	0
woff	无	无	0	0	0	0

Fig. 7. Much effort for testing benchmarks.



		第三次12h测试结果				
基准程序	afl++	afl++裁剪	aflgo	aflgo裁剪	symcc	symcc裁剪
guetzli	1,magma	1,magma	0	0	0	0
libming8807	1	1	1	1	1,magma	1
libming8962	1	1	1	1	1,magma	1
libpng	1,magma	1,magma	1,magma	1,magma	1,magma	1,magma
libpngbug3	1,magma	1,magma	1,magma	1,magma	1,magma	1,magma
libpngbug3bug6	1,magma	1,magma	1,magma	1,magma	1,magma	1,magma
libpngbug6	0	0	0	0	0	0
libtiff	1,magma	0	0	0	1,magma	0
libtiffbug7	1,magma	1,magma	0	1,magma	1,magma	1,magma
libtiffbug9	1,magma	0	0	0	1,magma	0
libtiffbug7bug9	1,magma	0	1,magma	0	1,magma	0
re2	1,magma	0	0	0	0	0

Fig. 8. Much effort for testing benchmarks.