

TABLE I
THE DETAIL OF BENCHMARK PROGRAMS FOR EVALUATION.

Benchmark	Source	Usage	Bug details (label, type, function, file:line)
addr2line	Binutils [1]	GNU binutils tool for converting addresses in binaries to source code line numbers	BUG001, SEGV, <i>slurp_symtab</i> , addr2line.c:147 BUG002, SEGV, <i>slurp_symtab</i> , addr2line.c:177
guetzli 2017330	Fuzzbench [2]	JPEG encoder for high compression density at high visual quality	BUG001, ABRT, <i>SaveToJpegData</i> , output_image.cc:403
libming cve2018807	AFLGO [3]	Flash (SWF) output library	BUG001, heap-buffer-overflow, <i>OpCode</i> , decompile.c:927 BUG002, SEGV, <i>getString</i> , decompile.c:373
libming cve20188962	AFLGO	Flash (SWF) output library	BUG001, SEGV, <i>getString</i> , decompile.c:366 BUG002, heap-buffer-overflow, <i>OpCode</i> , decompile.c:950 BUG003, SEGV, <i>getName</i> , decompile.c:449 BUG004, heap-use-after-free, <i>decompileIF</i> decompile.c:2471 BUG005, SEGV, <i>outputSWF_TEXT_RECORD</i> , outputscript.c:1470
libpng	Magma [4]	support library for PNG image files	BUG003, semantic error, <i>png_handle_PLTE</i> , pngutil.c:992
mjs issues78	AFLGO	restricted JavaScript engine	BUG003, ABRT, <i>get_cb_impl_by_signature</i> , mjs.c:10446

REFERENCES

- [1] GNU, “Binutils- GNU Project - Free Software Foundation,” <https://www.gnu.org/software/binutils/>, [Online; accessed 2024-06-14].
- [2] 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.
- [3] 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.
- [4] 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.