COLLECTION OF DIRECTED GREYBOX FUZZERS

Category	Tools	Publication	Fitness goal	Fitness metric	Target identify	Base tool	Binary support	Kernel support	Open sourced	Multi-targets	Multi-objective
Directed for target location	AFLGo [17]	CCS'17	target sites	distance	manual label	AFL	×	×	✓	✓	×
	SemFuzz [18]	CCS'17	target function/site	distance	automatic by NLP	Syzkaller	×	✓	×	✓	×
	Hawkeye [38]	CCS'18	target site	distance	manual label	AFL	×	×	×	✓	×
	LOLLY [53]	ICPC'19	target sequence	sequence coverage	manual label	AFL	×	×	×	✓	×
	TAFL [46]	ICSE'19	vulnerable region	customized path weights	static semantic analysis	AFL	×	×	✓	✓	×
	DrillerGo [23]	CCS'19	vulnerable function	coverage	manually based on CVE info	AFL	Angr	×	×	×	×
	1DVUL [19]	DSN'19	binary patches	distance	binary diffing	Driller	QEMU	×	×	✓	×
	Wüstholz [39]	Arxiv'19	target sites	path reachability	static analysis	HARVEY	BRAN	×	×	✓	×
	SUZZER [27]	ICISC'19	vulnerable function	vulnerable probability	predict by deep learning	VUzzer	IDA	×	×	✓	×
	V-Fuzz [26]	TCM'20	vulnerable function	vulnerable probability	predict by deep learning	VUzzer	IDA	×	×	✓	×
	DeFuzz [28]	Arxiv'20	vulnerable location	vulnerable probability	predict by deep learning	AFLGo	×	×	×	✓	×
	AFLPro [56]	JISA'20	sanity checks	multi-dimensional fitness	automatic	AFL	QEMU	×	×	✓	✓
	TortoiseFuzz [22]	NDSS'20	vulnerable function	sensitive edge hit rate	manually based on CVE info	AFL	×	×	×	✓	×
	Berry [47]	SANER'20	target sequence	execution trace similarity	static analysis	AFL	×	×	×	✓	×
	RDFuzz [40]	MPE'20	target sites	distance, frequency	manual label	AFL	×	×	×	✓	×
	TOFU [41]	Arxiv'20	target sites	distance	manual label	-	×	×	×	✓	×
	GTFuzz [43]	PRDC'20	guard tokens	distance	static analysis	AFLGo	×	×	×	✓	×
	ParmeSan [29]	Sec'20	sanitizer checks	distance	static analysis	Angora	×	×	✓	✓	×
	UAFuzz [24]	RAID'20	use-after-free	sequence coverage;	automatic	AFL	QEMU	×	×	✓	×
	UAFL [31]	ICSE'20	use-after-free	operation sequence coverage	automatic	AFL	×	×	×	✓	×
	FuzzGuard [59]	Sec'20	target sites	distance	manual label	AFLGo	×	×	×	✓	×
	BEACON [60]	S&P'21	target sites	distance	manual label	AFLGo	×	×	✓	✓	×
	CAFL [54]	Sec '21	target sites	conditions to the target	manual label	AFL	×	×	✓	✓	×
	AFLChurn [21]	CCS '21	target sites	distance	all commits	AFL	×	×	✓	✓	×
	DeltaFuzz [20]	JCST '21	target sites	distance	change point	AFL	×	×	×	✓	×
	DirectFuzz [74]	DAC'21	target sites	distance	manual label	AFL	×	×	✓	✓	×
	DGF-CFG Constructor [73]	MDPI'21	target sites	distance	indirect jump	AFLGo	×	×	×	✓	×
	KCFuzz [42]	ICAIS'21	target sites	keypoint coverage	static analysis	AFLGo	×	×	×	×	×
	WindRanger [52]	ICSE'22	target sites	distance	static analysis	AFL	×	×	×	✓	×
	SlowFuzz [34]	CCS'17	algorithmic complexity vulnerability	resource usage	automatic	LibFuzzer	×	×	×	×	×

continued on next page

continued from previous page

Category	Tools	Publication	Fitness goal	Fitness metric	Target identify	Base tool	Binary support	Kernel support	Open sourced	Multi-targets	Multi-objective
Directed for target behavior	PERFFUZZ [33]	ISSTA'18	algorithmic complexity vulnerability	coverage and edge hit count	automatic	AFL	×	×	✓	✓	✓
	TIFF [58]	ACSAC'18	buffer overflow, integer overflow	new coverage	manual label	VUzzer	×	×	×	×	×
	Joffe [5]	ICST'19	crash	crash likelihood	identified by machine learning	AFL	×	×	×	✓	×
	FuzzFactory [72]	OOPSLA'19	domain-specific goal	domain-specific multi-dimensional objectives	automatic	AFL	×	×	✓	×	✓
	RVFUZZER [32]	Sec'19	input validation bug	control instability	automatic	-	✓	×	×	×	×
	SAVIOR [44]	S&P'20	out-of-boundary, integer overflow, oversized shift	bug potential coverage	Annotate by UBSan	AFL	×	×	×	✓	×
	AFL-HR [51]	ICSEW'20	buffer overflow, integer overflow	coverage and headroom	automatic	AFL	×	×	×	✓	✓
	GREYHOUND [11]	TDSC'20	vulnerable behavior	multi-dimensional cost functions	manually by CVE report	AFL	×	×	×	✓	✓
	Memlock [30]	ICSE'20	memory consumption bug	memory usage and path coverage	automatic	AFL	×	×	×	✓	✓
	IJON [25]	S&P'20	deep stateful bug	path coverage	human annotation	AFL	×	×	✓	✓	×
	HDR-Fuzz [55]	Arxiv '21	buffer overrun	coverage and headroom	ASAN	AFL	×	×	×	✓	✓
	MDPERFFUZZ [68]	ASE'21	algorithmic complexity vulnerability	coverage and edge hit count	automatic	PERFFUZZ	×	×	×	✓	✓

TABLE III. Collection of directed greybox fuzzers