1 hashmap

1.1 项目介绍

https://github.com/goossaert/hashmap

Hashmap的具体实现

1.2 编译过程

1. 编译hashmap项目：`make clean && make`
2. 编写驱动target.cc并编译：`clang++ -g -fsanitize=address -fsanitize-coverage=trace-pc-guard target.cc -c`
3. 串联所有，编译生成fuzzer可执行文件：`clang++ -g -fsanitize=fuzzer,address -fsanitize-coverage=trace-pc-guard hamming.o murmurhash3.o monitoring.o bitmap_hashmap.o probing_hashmap.o tombstone_hashmap.o backshift_hashmap.o shadow_hashmap.o target.o ../libfuzzer-workshop/libFuzzer/libFuzzer.a -o app`
4. 执行：`mkdir corpus`和`./app corpus`

```
CC=clang++
CFLAGS=-O3 -c -Wall -g
LDFLAGS=-g
SOURCES=bitmap_hashmap.cc shadow_hashmap.cc probing_hashmap.cc
tombstone_hashmap.cc backshift_hashmap.cc testcase.cc monitoring.cc
murmurhash3.cc hamming.cc
SOURCES_MAIN=main.cc
OBJECTS=$(SOURCES:.cc=.o)
OBJECTS_MAIN=$(SOURCES_MAIN:.cc=.o)
EXECUTABLE=hashmap

all: $(SOURCES) $(EXECUTABLE)

$(EXECUTABLE): $(OBJECTS) $(OBJECTS_MAIN)
    $(CC) $(LDFLAGS) $(OBJECTS) $(OBJECTS_MAIN) -o $@

.cc.o:
    $(CC) $(CFLAGS) $< -o $@

clean:
    rm -f *~ *.o $(EXECUTABLE)
```

2 动态字符串sds

2.1 项目介绍

https://github.com/antirez/sds.git

```
sds sdsnewlen(const void *init, size_t initlen);
sds sdsnew(const char *init);
sds sdsempty(void);
sds sdsdup(const sds s);
```

2.2 编译过程

1. `clang -g -fsanitize=address -fsanitize-coverage=trace-pc-guard -Wall -std=c99 -pedantic -O2 target.c -c`
2. `clang++ -g -fsanitize=fuzzer,address -fsanitize-coverage=trace-pc-guard target.o ../libfuzzer-workshop/libFuzzer/libFuzzer.a -o app`
3. `mkdir corpus`
4. `./app corpus`

3 XML解析器libexpat

3.1 项目介绍

https://github.com/libexpat/libexpat

xml解析器

3.2 编译过程

1. `cd expat`
2. `./buildconfig`
3. 新建目录路径为`/new/`，`./configure --prefix=/new/`
4. `make`和`make install`
5. 将驱动`xml_parse_fuzzer.c`置于`./expat/lib`下，并`clang -g -fsanitize=address -fsanitize-coverage=trace-pc-guard -Wall -std=c99 -pedantic -O2 xml_parse_fuzzer.c -c`
6. 将生成的`xml_parse_fuzzer.o`移至`/new/lib`下
7. `clang++ -g -fsanitize=fuzzer,address -fsanitize-coverage=trace-pc-guard xml_parse_fuzzer.o libexpat.a libFuzzer.a -o app`
8. `mkdir corpus`和`./app corpus/`