

Fuzzwizard

Marion Lafon [Ponpon] | PTS 2026

[LEDGER]



DONJON



Pass
the SALT

FUZZWIZARD PLAYBOOK

 THE COACH
FuzzWizard

 TACTICAL SETUP
Env & Options : tactical setup before kick-off

 MATCH SHEET
State File who is playing, since when, with which setup

 THE VAR REPLAY
Reproducers act as unyielding play-by-play video footage proving how the security line fell.





The Wish List

Availability

Run fuzzers 24/7.

Deployment

Locally deployable tool.

Multi-project

Interact with multiple projects at the same time.

Independence

Update fuzzers independently from one another.

Configurability

Highly configurable for each fuzzer.

Centralization

Centralize reported information.

Observability

Feedback on fuzzer coverage.

Alerting

Be alerted in case of a crash.

Prioritization

Fuzzer prioritization system.



The Wish List

Availability

Run fuzzers 24/7.

Deployment

Locally deployable tool.

Multi-project

Interact with multiple projects at the same time.

Independence

Update fuzzers independently from one another.

Configurability

Highly configurable for each fuzzer.

Centralization

Centralize reported information.

Observability

Feedback on fuzzer coverage.

Alerting

Be alerted in case of a crash.

Prioritization

Fuzzer prioritization system.



Existing tools

Available tools did not meet all our needs:

Confidentiality

Hosted platforms do not allow testing of confidential code.

Integration speed

Tools limited to CI; impossible to quickly add a fuzzer outside of it.

Lack of Flexibility

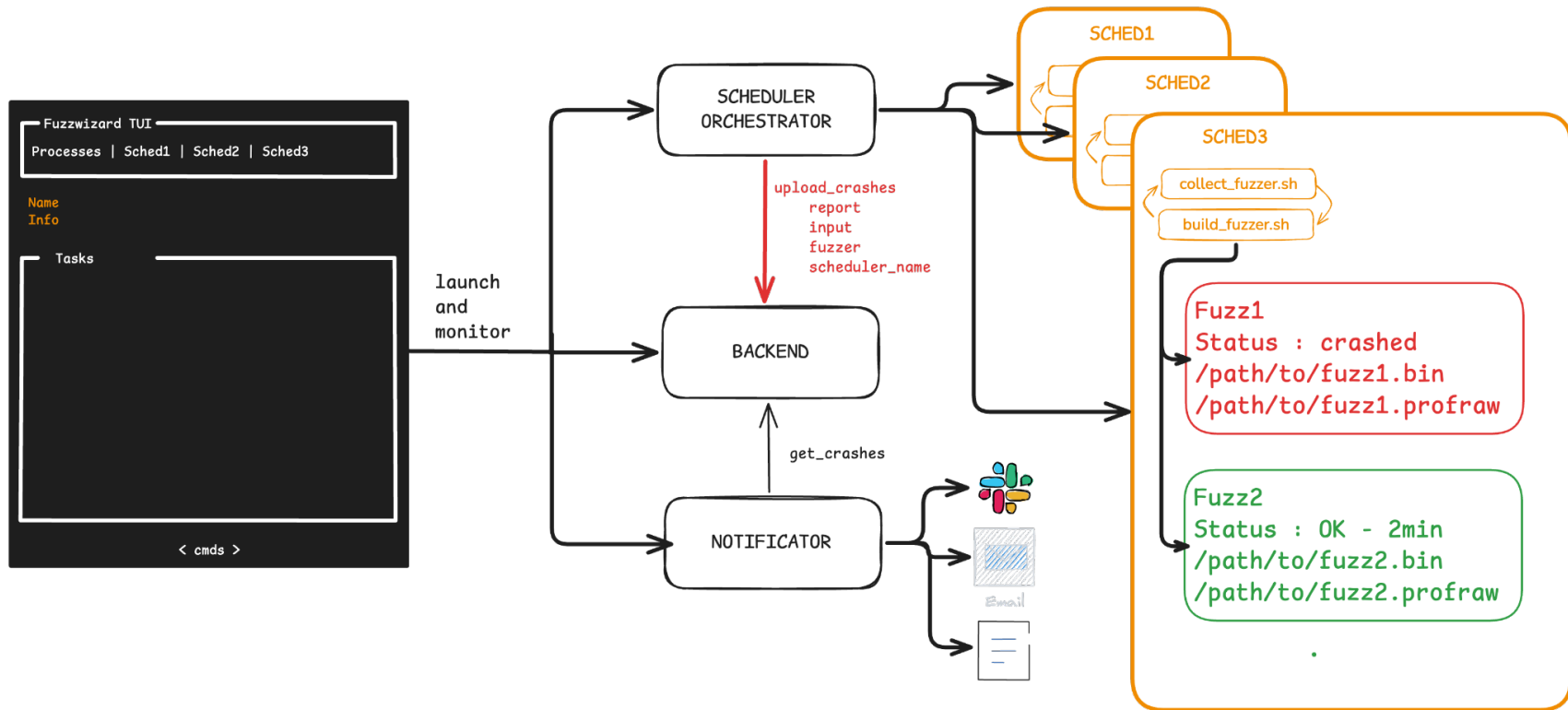
All fuzzers run with the same default options.

Non-Free Model

Existing solutions are proprietary and not auditable.



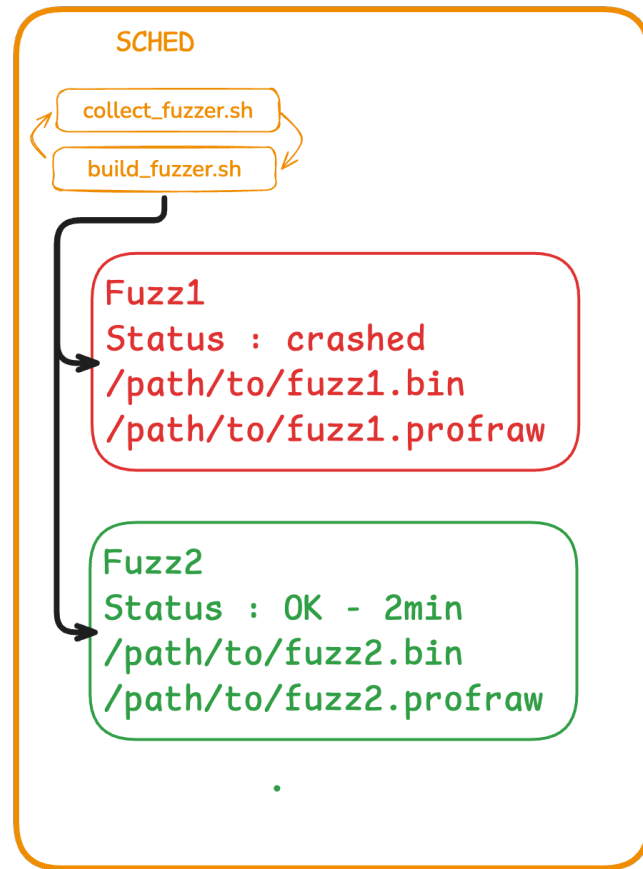
Fuzzwizard





Fuzzwizard

Each components can run independently





Fuzzwizzard - How to extend it

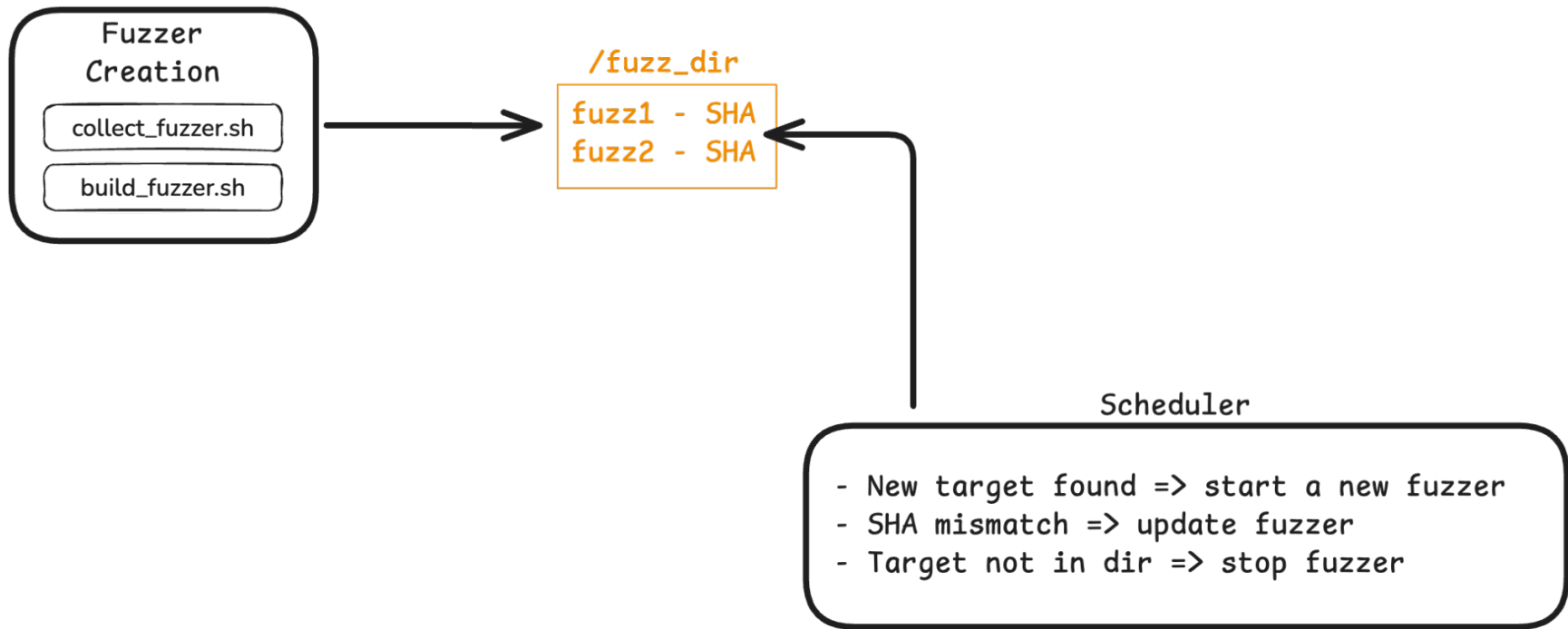
**Notification
Providers**

**Target
Collectors**

Containers



Fuzzwizzard - How fuzzers are collected





Fuzzwizard - General Config

```
{
  "schedulers": [
    {
      "name": "test_scheduler_build1",
      "config": ".../test_scheduler_build1_scheduler_config.json"
    },
    { /* ... scheduler2 config ... */ }
  ],

  "database_url": "postgres://127.0.0.1:5432/fuzzwizard",
  "backend_binary": ".../target/release/backend",
  "notificator_binary": ".../target/release/notificator",
  "logdir": ".../data/logs",
  "container_binary": null,

  "notifications": {
    "providers": {
      "slack": { "enabled": false },
      "file": { "enabled": true }
    }
  }
}
```



Fuzzwizard - Scheduler Config

```
{
  "scheduler_name": "test_scheduler_build1",

  "targets_directory": ["../src/build_dir1"],
  "build_script": "../scripts/build.sh",

  "backend_url": "http://127.0.0.1:3000",

  "corpus_directory": "../data/corpus",
  "crashes_directory": "../data/crashes",
  "coverage_directory": "../data/coverage",

  "has_coverage": true,
  "state_file": "../state/test_scheduler_build1_state.json",

  "container_image": null,
  "container_options": null
}
```



Fuzzwizard - State file

```
{
  "fuzzers": [
    {
      "path": "/path/to/
fuzzer_binary",
      "sha": abc.. ,
      "state": "RUNNING"
    }
  ]
}
```

```
{
  "path": "/path/to/fuzzer",
  "sha": "abc...",
  "state": "STOPPED",
  "var_env": {
    "ASAN_OPTIONS": "detect_leaks=1",
    "UBSAN_OPTIONS": "halt_on_error=1"
  },
  "cmd_options": [
    "-max_total_time=3600",
    "-jobs=1"
  ]
}
```



Code Coverage

How to obtain coverage on the fly with libfuzzer?

Method

SIGUSR1 triggers
`__llvm_profile_write_file`

```
// Signal handler implementation
static void on_sigusr1(int p) {
    int tmp = __llvm_profile_write_file();
    __llvm_profile_reset_counters();
}

void init(void) {
    struct sigaction sa = {0};
    sa.sa_handler = on_sigusr1;
    sigaction(SIGUSR1, &sa, NULL);
}
```

PROS

No fuzzer modifications

CONS

Handler needed at compilation time



```
erage_handler.o -o build_dir2/fuzz_5
Build completed successfully

Created data directory structure

Created /Users/ponpon/Project/fuzzwizard_scheduler_test-main/data/config/test_scheduler_build1_scheduler_config.json
Created /Users/ponpon/Project/fuzzwizard_scheduler_test-main/data/config/test_scheduler_build2_scheduler_config.json
Created /Users/ponpon/Project/fuzzwizard_scheduler_test-main/data/config/config.json

=== Installation completed successfully! ===
Configuration files are in: /Users/ponpon/Project/fuzzwizard_scheduler_test-main/data/config
Main config file: /Users/ponpon/Project/fuzzwizard_scheduler_test-main/data/config/config.json
~/Project/fuzzwizard_scheduler_test-main >

~/Project/fuzzwizard_scheduler_test-main >
```

```
~/Project/fuzzwizard/target/release > pwd
/Users/ponpon/Project/fuzzwizard/target/release
~/Project/fuzzwizard/target/release > ll ../../../../fuzzwizard_scheduler_test-main/data/config
total 24
drwxr-xr-x@ 5 ponpon  staff  160  2 juin  08:15  .
drwxr-xr-x@ 8 ponpon  staff  256  2 juin  08:15  ..
-rw-r--r--@ 1 ponpon  staff 1273  2 juin  08:15  config.json
-rw-r--r--@ 1 ponpon  staff  749  2 juin  08:15  test_scheduler_build1_scheduler_config.json
-rw-r--r--@ 1 ponpon  staff  749  2 juin  08:15  test_scheduler_build2_scheduler_config.json
~/Project/fuzzwizard/target/release > ll ../../../../fuzzwizard_scheduler_test-main/data/config/test_scheduler_build1_scheduler_config.json
-rw-r--r--@ 1 ponpon  staff  749  2 juin  08:15  ../../../../fuzzwizard_scheduler_test-main/data/config/test_scheduler_build1_scheduler_config.json
~/Project/fuzzwizard/target/release > less ../../../../fuzzwizard_scheduler_test-main/data/config/test_scheduler_build1_scheduler_config.json
~/Project/fuzzwizard/target/release > less ../../../../fuzzwizard_scheduler_test-main/data/config/config.json
~/Project/fuzzwizard/target/release > ./fuzztui /Users/ponpon/Project/fuzzwizard_scheduler_test-main/data/config/config.json
bck-i-search: fuzztui_
```



```
~/Project/fuzzwizard_scheduler_test-main > cd data
```

```
~/Project/fuzzwizard_scheduler_test-main >
```



```
erage_handler.o -o build_dir2/fuzz_5
```

```
Build completed successfully
```

```
Created data directory structure
```

```
Created /Users/ponpon/Project/fuzzwizard_scheduler_test-main/data/config/test_scheduler_build1_scheduler_config.json
```

```
Created /Users/ponpon/Project/fuzzwizard_scheduler_test-main/data/config/test_scheduler_build2_scheduler_config.json
```

```
Created /Users/ponpon/Project/fuzzwizard_scheduler_test-main/data/config/config.json
```

```
=== Installation completed successfully! ===
```

```
Configuration files are in: /Users/ponpon/Project/fuzzwizard_scheduler_test-main/data/config
```

```
Main config file: /Users/ponpon/Project/fuzzwizard_scheduler_test-main/data/config/config.json
```

```
~/Project/fuzzwizard_scheduler_test-main >
```

```
2026-06-02 08:19:44 INFO scheduler collecting coverage for: "/Users/ponpon/Project/fuzzwizard_scheduler_test-main/src/build_dir3/fuzz_4"
```

```
2026-06-02 08:19:44 INFO scheduler Coverage collection successful for fuzzer : fuzz_4
```

```
2026-06-02 08:19:44 INFO scheduler collecting coverage for: "/Users/ponpon/Project/fuzzwizard_scheduler_test-main/src/build_dir3/fuzz_5"
```

```
2026-06-02 08:19:44 INFO scheduler Coverage collection successful for fuzzer : fuzz_5
```

```
2026-06-02 08:19:44 INFO scheduler STOP (paths):
```

```
2026-06-02 08:19:44 INFO scheduler CHECK (paths):
```

```
2026-06-02 08:19:44 INFO scheduler - CHECK: b7bbd3b3e66213e19ac5410ea387f7767626a91de33255b2f5e65393bfe6cb81 : "/Users/ponpon/Project/fuzzwizard_scheduler_test-main/src/build_dir3/fuzz_4"
```

```
2026-06-02 08:19:44 INFO scheduler - CHECK: ffe40aaadf227d588b404fdc69a2895d0af2584184b299c6ed4c369971949ba8 : "/Users/ponpon/Project/fuzzwizard_scheduler_test-main/src/build_dir3/fuzz_5"
```

```
2026-06-02 08:19:44 INFO scheduler - CHECK: 77f74670df3862b33bf51ff8d593a7fa7da6cc1a62084a72ff1fa9caba6d0cfd : "/Users/ponpon/Project/fuzzwizard_scheduler_test-main/src/build_dir3/fuzz_2"
```

```
2026-06-02 08:19:44 INFO scheduler START (paths):
```

```
Fuzzwizard TUI
```

```
Processes | test_scheduler_build1 | test_scheduler_build2 | test_schedule
```

```
Name: test_scheduler_build3
```

```
Status: Running
```

```
Info: Scheduler test_scheduler_build3 started
```

```
State File: /Users/ponpon/Project/fuzzwizard_scheduler_test-main/data/state/
```

```
Tasks:
```

SHA	FileName	Status	StatusTime
0x77f74670df3862b33bf51	fuzz_2	Running	1m 5s ago
0xb7bbd3b3e66213e19ac54	fuzz_4	Running	1m 5s ago
0xffe40aaadf227d588b404	fuzz_5	Running	1m 5s ago

```
t/Right> | Navigate Tasks <Up/Down> | Reload Config <C> | Manage Task <
```




The Wish List

Independence

Update fuzzers
independently from one
another.

Configurability

Highly configurable for
each fuzzer.

Observability

Feedback on fuzzer
coverage.

Prioritization

Fuzzer prioritization
system.

Questions

Fuzzwizard :

<https://github.com/Ledger-Donjon/fuzzwizard>

Tests:

https://github.com/Ledger-Donjon/fuzzwizard_scheduler_test



DONJON



Pass
the SALT