Domato

List

- Domato
  - Additional details of the fuzzing setup
    - Google Chrome
    - Mozilla Firefox
    - Apple Safari
  - Usage
  - Example
    - Create fuzz file
    - Test fuzz file
- Related site

Domato

- **Domato는 DOM fuzzer입니다.**
- **Domato는 2개의 Python 스크립트 파일에 의해 동작합니다.**
  - generator.py 파일은 main 스크립트 입니다.
  - grammar.py 파일은 라이브러리 및 DOM 퍼징을 위한 추가 help 코드가 포함되어 있습니다.
  - *.txt 파일에는 HTML, CSS 및 JavaScript 문법이 저장되어 있습니다.
    - html.txt, css.txt, js.txt
- **Domato를 이용해 시장 점유율이 가장 높은 5개의 브라우저에서 취약성을 찾았습니다.**
  - **대략 100,000,000번의 반복적인 반복을 주고 충돌을 기록**

Additional details of the fuzzing setup

Google Chrome

- ClusterFuzz 라는 크롬 내부의 보안 퍼징 클러스터를 이용합니다.
- ClusterFuzz 에 fuzzer를 업로드하면 다양한 Chrome 빌드에 대해 자동으로 실행됩니다.

Mozilla Firefox

- Mozilla 에서는 이미 Firefox ASAN builds를 제공하고 있으며, Firefox ASAN builds를 대상으로 퍼징을 진행합니다.
- 각 릴리즈 버전에 대해서는 추가로 확인이 필요합니다.

Apple Safari

- Linux기반의 인프라에서 실행되는 WebKitGTK+를 이용합니다.
- WebKitGTK+ 릴리스 버전을 이용해 ASAN 빌드를 제작이 필요합니다.
- 확인된 각각의 crash는 Mac에서 동작하는 ASAN WebKit build 에서 다시 확인합니다.

> Experimenting with coverage-guided DOM fuzzing
>
> - https://googleprojectzero.blogspot.jp/2017/09/the-great-dom-fuzz-off-of-2017.html

Usage

- **다음과 같이 Domato를 설치 할 수 있습니다.**

Install

```
$ git clone https://github.com/google/domato.git ~/domato
$ cd domato
```

- 다음과 같이 한개의 샘플 파일을 생성 할 수 있습니다.

$ python generator.py <output file>

```
$ python generator.py sample.html
```

- 다음과 같은 방법으로 여러개의 샘플 파일을 생성 할 수 있습니다.

$ python generator.py --output_dir <output directory> --no_of_files <number of output files>

```
$ mkdir sample
$ python generator.py --output_dir sample --no_of_files 100
```

Example

Create fuzz file

Create one fuzz file

```
lazenca0x0@ubuntu:~/domato$ python generator.py sample.html
Writing a sample to sample.html
lazenca0x0@ubuntu:~/domato$
```

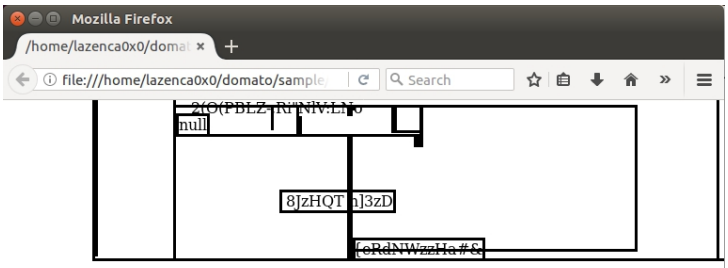
Create multiple fuzz files

```
lazenca0x0@ubuntu:~/domato$ python generator.py --output_dir sample --no_of_files 10
Running on ClusterFuzz
Output directory: sample
Number of samples: 10
Writing a sample to sample/fuzz-0.html
Writing a sample to sample/fuzz-1.html
Writing a sample to sample/fuzz-2.html
Writing a sample to sample/fuzz-3.html
Writing a sample to sample/fuzz-4.html
Writing a sample to sample/fuzz-5.html
Writing a sample to sample/fuzz-6.html
Writing a sample to sample/fuzz-7.html
Writing a sample to sample/fuzz-8.html
Writing a sample to sample/fuzz-9.html
lazenca0x0@ubuntu:~/domato$
```

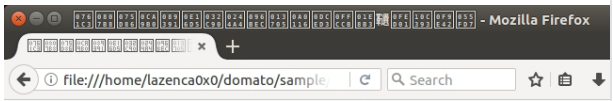
Test fuzz file

Read fuzz file

fuzz-0.html



fuzz-1.html



Related site

- https://github.com/google/domato
- https://googleprojectzero.blogspot.jp/2017/09/the-great-dom-fuzz-off-of-2017.html
- https://chromium.googlesource.com/chromium/src/+/master/testing/libfuzzer/README.md