# ファジングツールの機能調査

## A Functional Investigation of Fuzzing Tools

福山潤・システム分科会・情報セキュリティ大学院大学

**Abstract:** Fuzzing is one method of inspecting the safety of information systems. Fuzzing is a vulnerability test that detects vulnerabilities by sending many illegal packets to an information system such as HTTP and monitoring the response and behaviors. But, there are many types of fuzzing tools, and the user is unclear which fuzzing tools are used effectively for inspection. Therefore, investigating in the difference of data generated by many robust fuzzing tools such as Peach and Sulley and the latest Boofuzz fuzzing tool.

### Peach※

Version: 3.1.124
License: MIT
First Release: 2004
OS: Windows/Linux
Pattern File: XML
※CommunityEdition

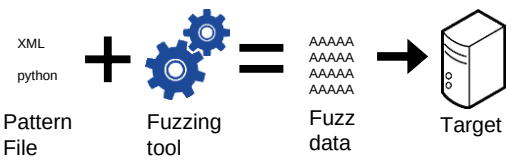
### Sulley

Version: 1.0
License: GNU GPL v2.0
First Release: 2007
OS: Windows/Linux
Pattern File: python

### Boofuzz

Version: 0.0.11
License: GNU GPL v2.0
First Release: 2016
OS: Windows/Linux
Pattern File: python

### ファジングの流れ




それぞれのファジングツールに対応するパターンファイルをファジングツールに読み込ませることでファズデータを作成、検査対象に送信する

### パターンファイル

| Peach | Sulley | Boofuzz |
|---|---|---|
| XMLヘッダ | Data Model<br>データ構造と値の定義 | Data Model<br>データ構造と値の定義 |
| Data Model<br>データ構造と値の定義 | State Model<br>ファズデータ入出力定義 | State Model<br>ファズデータ入出力定義 |
| State Model<br>ファズデータ入出力定義 | Target<br>Targetの定義 | Target<br>Targetの定義 |
| Test<br>Target・ログ出力先 | | Logging<br>ログ出力先・出力方法 |

### ファズデータ生成

**Peach** (Random + Heuristic)

26種類のMutatorから詳細なファズデータを生成

BlobBitFlipperMutator　：対象のビット値を反転させる
DataElementDuplicateMutator：対象を2～50倍に複製
FiniteRandomNumbersMutator：ランダムな値を生成

**Sulley / Boofuzz** (Random + Heuristic)

個別に定義

“¥xde¥xad¥xbe¥xef” * 10000　：バイナリデータ
“1;SELECT%20*”　：SQL文
256, 513, 1024,4097,20000　：ランダムな値の長さ指定

### ツール比較

| *tools* | *Install* | *Pattern File* | *Custom* | *Support* | *Last Update* | *Other* |
|---|---|---|---|---|---|---|
| ***Peach*** | ○<br>Zipファイル | ○<br>サンプル入手が容易 | △<br>再コンパイルが必要 | ◎<br>企業サポート | 2014 / 11 | seed値での同一データ生成<br>ファイルファジングツール同梱 |
| ***Sulley*** | △<br>多くの依存環境 | ○<br>サンプル入手が容易 | ○<br>Python | △<br>更新停止 | 2014 / 06 | 有志による解説が豊富 |
| ***Boofuzz*** | ◎<br>Pipコマンド | △<br>サンプルは少ない | ○<br>python | ○<br>頻繁に更新 | 2017 / 11 | CSVファイル出力<br>IPレイヤのファズデータ生成 |