

**УТВЕРЖДЕН**

643.СПЕН.24011-01 96 01-ЛУ

## **ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ**

**«Спин-Фаззер»**

Руководство пользователя

643.СПЕН.24011-01 96 01

Листов 13

Инв. № подл.	Подп. и дата	Взам. инв. №	Инв. № дубл.	Подп. и дата

2023

## **АННОТАЦИЯ**

Настоящий документ является руководством пользователя (далее – Руководство) для программного обеспечения «Спин-Фаззер».

Руководство содержит общие сведения о программном обеспечении, его характеристиках, а также порядке выполнения различных операций при эксплуатации программного обеспечения.

Руководство разработано с учетом положений ГОСТ 19.505–79 «Единая система программной документации. Руководство оператора. Требования к содержанию и оформлению».

## СОДЕРЖАНИЕ

1. Общие сведения .....	4
1.1. Наименование .....	4
1.2. Назначение .....	4
1.2.1. Функциональное назначение .....	4
1.2.2. Эксплуатационное назначение .....	4
1.3. Функции ПО .....	4
2. Описание характеристик ПО .....	5
2.1. Общее программное обеспечение, необходимое для работы ПО .....	5
2.2. Состав ПО .....	5
2.3. Технические средства, необходимые для работы ПО .....	5
2.4. Уровень квалификации пользователя .....	5
3. Подготовка к работе .....	6
4. Работа со «Спин-Фаззер» .....	7
4.1. Типовые операции.....	7
4.1.1. Назначение целевого веб-сервера для фаззинг-тестирования .....	7
4.1.2. Запуск и остановка .....	7
4.1.3. Запуск и остановка тестирования.....	7
4.1.4. Анализ ответов целевого веб-сервера.....	8
4.2. Решение проблем .....	10
4.2.1. Техническая поддержка .....	10
4.2.2. Типовые проблемы .....	10
Перечень сокращений.....	12

## **1. ОБЩИЕ СВЕДЕНИЯ**

### **1.1. Наименование**

Полное наименование программного обеспечения: «Спин-Фаззер».

В рамках настоящего документа употребляется также обозначение ПО.

Обозначение: 643.СПЕН.24011-01.

«Спин-Фаззер» – это российское программное обеспечение. Организация-разработчик: Акционерное общество «СПИН» (АО «СПИН»).

Сайт организации-разработчика: <https://spean.ru/>.

Организация-правообладатель: Акционерное общество «СПИН» (АО «СПИН»).

### **1.2. Назначение**

#### **1.2.1. Функциональное назначение**

ПО предназначено для проведения генерационного фаззинг-тестирования веб-приложений, API которых описано в спецификации Swagger или OpenAPI.

#### **1.2.2. Эксплуатационное назначение**

«Спин-Фаззер» представляет собой приложение для тестирования. Пользователи получают доступ к программному обеспечению путем установки дистрибутива приложения на ПЭВМ.

### **1.3. Функции ПО**

Основными функциями ПО являются:

- получение описаний параметров для отправки HTTP-запросов на целевой web-сервер на основе JSON-файла с описанием API по спецификации Swagger/OpenAPI;
- автоматическая авторизация на целевом веб-сервере;
- автоматическое генерирование параметров, формирование и отправка HTTP-запросов к целевому веб-серверу;
- анализ и классификация ответов целевого веб-сервера.

## **2. ОПИСАНИЕ ХАРАКТЕРИСТИК ПО**

### **2.1. Общее программное обеспечение, необходимое для работы ПО**

Общее программное обеспечение (ОПО), которое должно быть установлено для функционирования ПО на пользовательской ПЭВМ – ОС Linux.

### **2.2. Состав ПО**

«Спин-Фаззер» представляет собой консольное приложение и состоит из совокупности связанных файлов.

### **2.3. Технические средства, необходимые для работы ПО**

Для выполнения ПО ПЭВМ должна иметь характеристики не хуже:

- процессор с архитектурой x86-64 (AMD, Intel);
- оперативная память – не менее 2 ГБ;
- объем свободного дискового пространства – не менее 2 ГБ;
- сетевая плата: Ethernet 100 Мбит/с (или адаптер Wi-Fi).

Приведенные выше требования к техническим средствам являются минимально допустимыми. Применение более производительных технических средств улучшает эксплуатационные свойства ПО.

### **2.4. Уровень квалификации пользователя**

Установка ПО в процессе основного жизненного цикла выполняется силами организации-заказчика. Для установки ПО сотрудник организации-заказчика должен обладать основными навыками работы с ПЭВМ под управлением ОС Linux. Установка производится согласно «Инструкции по установке», поставляемой в комплекте с дистрибутивом ПО.

Эксплуатация выполняется конечными пользователями, которые должны обладать следующими знаниями и навыками:

- навыки работы на персональном компьютере;
- навыки работы с командной оболочкой ОС Linux;
- навыки работы с консольными приложениями.

### **3. ПОДГОТОВКА К РАБОТЕ**

Пользователи получают доступ к «Спин-Фаззер» путем установки дистрибутива ПО на ПЭВМ. Сведения об установке ПО содержатся в документе «Инструкция по установке», поставляемом в комплекте с дистрибутивом ПО.

## 4. РАБОТА СО «СПИН-ФАЗЗЕР»

### 4.1. Типовые операции

#### 4.1.1. Назначение целевого веб-сервера для фаззинг-тестирования

Чтобы назначить целевой веб-сервер для фаззинг-тестирования, необходимо выполнить шаги, описанные ниже.

**Шаг 1.** Находясь в каталоге с файлами ПО, открыть конфигурационный файл тестирования при помощи текстового редактора.

**Шаг 2.** В открывшемся при помощи текстового редактора конфигурационном файле (config.py) найти строку

**BASE =**

Ввести в нее URL целевого сервера для фаззинг-тестирования.

**Шаг 3.** Найти строку

**SWAGGER\_PATH =**

Ввести в нее имя файла с описанием API целевого сервера по спецификации Swagger/OpenAPI.

#### 4.1.2. Запуск и остановка

Вход в ПО осуществляется посредством POSIX-совместимой командной оболочки (консоли) путем ввода команды перехода к каталогу, содержащему взаимосвязанные файлы и каталоги ПО.

**cd <имя каталога с файлами ПО>**

#### 4.1.3. Запуск и остановка тестирования

Чтобы запустить тестирование целевого веб-сервера, необходимо, находясь в каталоге с файлами ПО, ввести команду

**python3 swagger.py**

Чтобы остановить тестирование целевого веб-сервера, необходимо нажать на клавиатуре клавиши Ctrl + C (Рис. 1).

```

tester@fuzzer-swagger:~/spin-fuzzer$ python3 swagger.py
/home/tester/.local/lib/python3.9/site-packages/swagger-spec-validator/validator20.py:49: SwaggerValidationWarning: Found "#ref: #/definitions/Tag" with siblings that will be overwritten. See https://stackoverflow.com/a/48114924 for more information. (path #/definitions/Pet/properties/tags/items)
  warnings.warn(
path is ['/v2/pet/{petId}/uploadImage', '/v2/pet', '/v2/pet/findByStatus', '/v2/pet/findByTags', '/v2/pet/{petId}', '/v2/store/order', '/v2/store/order/{orderId}', '/v2/store/inventory', '/v2/user/createWithBasic', '/v2/user/createWithList', '/v2/user/{username}', '/v2/user/login', '/v2/user/logout', '/v2/user']
FuzzRequest.base is https://petstore.swagger.io
auth header() start
auth_res is <Response [200]>
token is keep-alive
FuzzRequest.headers from swagger {'Connection': 'keep-alive'}
len(paths) is 14
get_definition_name_from_ref(ref) Pet
get_definition_name_from_ref(ref) Category
get_definition_name_from_ref(ref) Pet
get_definition_name_from_ref(ref) Category
get_definition_name_from_ref(ref) Order
get_definition_name_from_ref(ref) User
get_definition_name_from_ref(ref) User
get_definition_name_from_ref(ref) User
get_definition_name_from_ref(ref) User
obj.total_requests 1
obj.total_requests 1
obj.total_requests 1
obj.total_requests 1
obj.total_requests 1
obj.total_requests 1
obj.total_requests 1
obj.total_requests 1
obj.total_requests 1
obj.total_requests 1
obj.total_requests 1
obj.total_requests 1
obj.total_requests 1
obj.total_requests 17
obj.total_requests 17
obj.total_requests 17
obj.total_requests 17
obj.total_requests 16
obj.total_requests 1
obj.total_requests 17
^CCtrl-C detected. Collecting logs
tester@fuzzer-swagger:~/spin-fuzzer$

```

Рис. 1

#### 4.1.4. Анализ ответов целевого веб-сервера

Чтобы увидеть и проанализировать ответы целевого веб-сервера, по окончании фаззинг-тестирования необходимо, находясь в каталоге с файлами ПО, открыть лог-файл тестирования при помощи текстового редактора.

Лог-файл содержит как обобщенную статистику отправленных запросов и полученных от целевого веб-сервера ответов, так и наименования автоматически сформированных по итогам фаззинг-тестирования подкаталогов, по которым распределены файлы, содержащие описание зарегистрированных ошибок сервера. Для детального изучения подкаталогов с файлами, содержащими описание ошибок, а также самих файлов, следует выполнить следующие действия:

- перейти в каталог, содержащий подкаталоги, в которых сгруппированы файлы со сведениями о зарегистрированных ошибках по критерию возникновения ошибки при выполнении одного вида запроса с различными параметрами, введя команду **ls bugs** (Рис. 2);
- перейти в подкаталог с файлами зарегистрированных в ходе фаззинг-тестирования ошибок при помощи команды **ls -l bugs/<первые 8 символов наименования подкаталога>-\*** (Рис. 3)<sup>1</sup>;

<sup>1</sup> Символы наименования подкаталога, содержащего файлы со сведениями о зарегистрированных ошибках по критерию возникновения ошибки при выполнении одного вида запроса с различными параметрами, генерируются на основании идентификаторов отправленных запросов и могут отличаться от представленного на рисунке



- открыть интересующий файл зарегистрированной в ходе фаззинг-тестирования ошибки при помощи команды `nano bugs/<первые 8 символов наименования подкаталога>-*/<наименование файла>` (Рис. 4)<sup>2</sup>.

```
tester@fuzzer-swagger:~/spin-fuzzer$ ls bugs
084fa6b-a027-4c50-90ed-efb9adedb9ea 2897ea5a-4e68-40f2-9094-4e4aabda0498 alc72190-dfad-4a95-8ccf-25dd1102a3c9 c4d56dd0-1887-4530-a94e-eed84261e389
08cc8096-a879-4af2-a119-3e8baa127809 3fbd12ba-3626-433e-b351-092c6192e928 b36a04f8-b36c-4b74-bb86-7a866fd0f9c8 f3cc1444-a3f6-4105-9044-0dfed260b660
1ed2a73c-c628-48c3-a124-8faa51ab7020 al641202-720c-412d-8565-57e50ed16b08 bc2189d1-8fa2-4ed8-a3e7-664e6759be50 f719ed49-da06-49e2-bfa8-44cebbd9e211
tester@fuzzer-swagger:~/spin-fuzzer$
```

Рис. 2

```
-bash: ls: команда не найдена
tester@fuzzer-swagger:~/spin-fuzzer$ ls -l bugs/alc72190-*
итого 44
-rw-r--r-- 1 tester tester 369 фев  2 15:52 500-1706889140.0734375
-rw-r--r-- 1 tester tester 375 фев  2 15:53 500-1706889185.4967031
-rw-r--r-- 1 tester tester 373 фев  2 15:53 500-1706889185.9828336
-rw-r--r-- 1 tester tester 370 фев  2 15:53 500-1706889186.4835086
-rw-r--r-- 1 tester tester 377 фев  2 15:53 500-1706889186.9562821
-rw-r--r-- 1 tester tester 374 фев  2 15:53 500-1706889187.446445
-rw-r--r-- 1 tester tester 369 фев  2 15:53 500-1706889187.9359958
-rw-r--r-- 1 tester tester 373 фев  2 15:53 500-1706889188.4312313
-rw-r--r-- 1 tester tester 372 фев  2 15:53 500-1706889188.9042702
-rw-r--r-- 1 tester tester 374 фев  2 15:53 500-1706889189.3810477
-rw-r--r-- 1 tester tester 374 фев  2 15:53 500-1706889189.8534071
tester@fuzzer-swagger:~/spin-fuzzer$
```

Рис. 3

<sup>2</sup> Содержание файла зависит от полученных данных об ошибке и может отличаться от рисунка

```
GNU nano 5.4          bugs/08a4fa6b-a027-4c50-90ed-efb9adedb9ea/500-1706888913.97312
## Path:https://petstore.swagger.io/v2/pet
## Error:500
## Deep:4
## Request:

method
post

path_url
https://petstore.swagger.io/v2/pet

body_params
{"id": 10, "category": {"id": 0, "name": "iWI"}, "name": "J", "photoUrls": ["Cv"], "tags": ["H"], "status": "v"}

## Response:

{"code":500,"type":"unknown","message":"something bad happened"}
```

[ Read 18 lines ]

^G Help	^O Записать	^W Поиск	^K Cut	^T Execute	^C Location	M-U Отмена	M-A Set Mark
^X Выход	^R Чит.файл	^_ Замена	^U Paste	^J Выровнять	^_ К строке	M-E Повтор	M-6 Copy

Рис. 4

Анализ тестовых файлов с результатами фаззинга также может производиться автоматически, например с использованием, таких средств обработки текстов как `grep`, `sed`, `awk`.

## 4.2. Решение проблем

### 4.2.1. Техническая поддержка

В случае возникновения проблем пользователь может обратиться в службу технической поддержки по электронной почте: <https://spean.ru/>.

Время работы технической поддержки: по будням с 09:00 до 18:00 (по московскому времени).

### 4.2.2. Типовые проблемы

#### 4.2.2.1. Не происходит фаззинг-тестирование указанного целевого веб-сервера

В случае, если при запуске ПО фаззинг-тестирование указанного целевого веб-сервера не происходит, следует убедиться, что:

- адрес целевого веб-сервера в конфигурационном файле тестирования указан без ошибок;
- файл с описанием API целевого сервера содержит корректные данные;
- не нарушено сетевое соединение.

**4.2.2.2. Не открываются файлы зарегистрированных в ходе фаззинг-тестирования ошибок**

В случае, если файлы зарегистрированных в ходе фаззинг-тестирования ошибок не найдены в файловой системе, следует убедиться, что наименование файла введено корректно. Повторить попытку с корректно введенным наименованием файла.

## **ПЕРЕЧЕНЬ СОКРАЩЕНИЙ**

ОС	операционная система
ПО	программное обеспечение
ПЭВМ	персональная электронно-вычислительная машина
API	Application Programming Interface (программный интерфейс)

