УТВЕРЖДЕН

643.СПЕН.24011-01 96 01-ЛУ

ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ

«Спин-Фаззер»

Руководство пользователя

643.СПЕН.24011-01 96 01

Листов 13

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

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

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).

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 описания 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)[1];

[1] 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)[2].

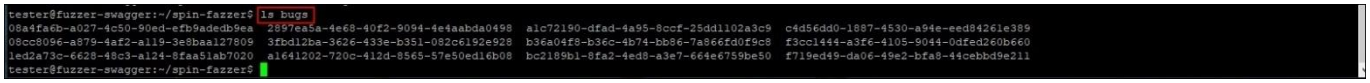

Рис. 2

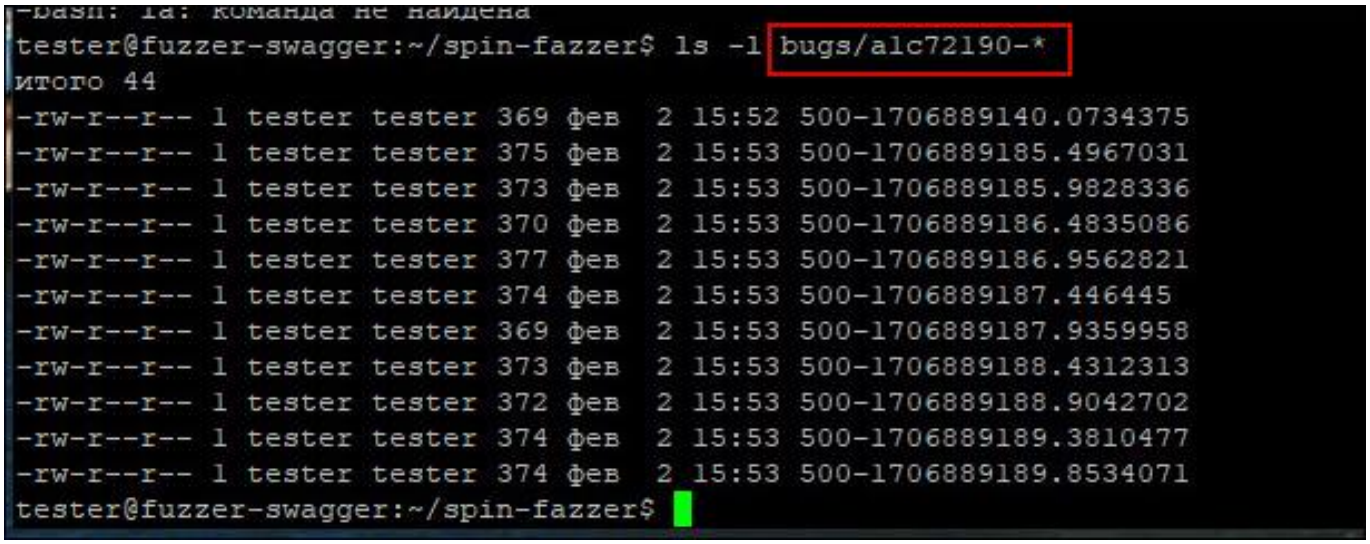

Рис. 3

[2] Содержание файла зависит от полученных данных об ошибке и может отличаться от рисунка

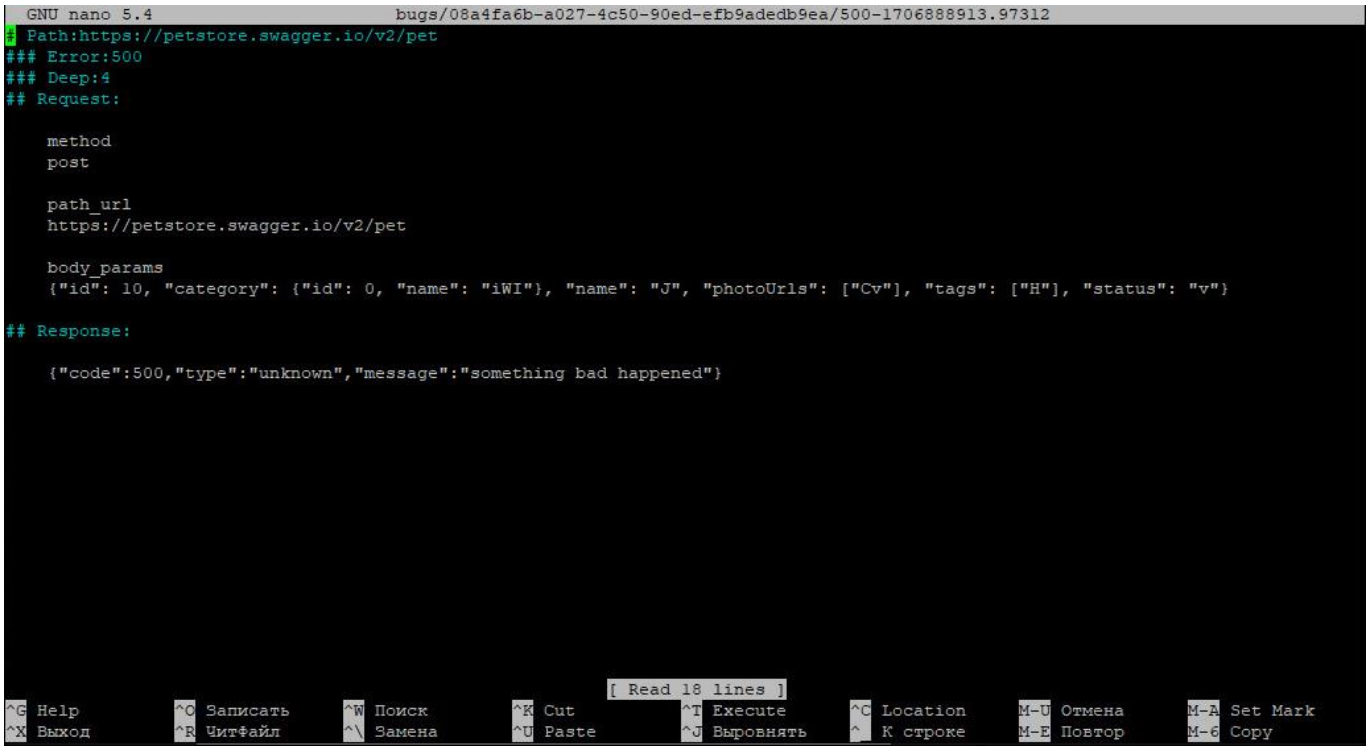

Рис. 4

Анализ тестовых файлов с результатами фаззинга также может производится 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)

Лист регистрации изменений

Изм.	Номера листов (страниц)				Всего листов (страниц) в докум.	№ документа	Входящий № сопроводи-тельного документа и дата	Подпись	Дата
	измененных	замененных	новых	аннулиро-ванных					