



РУКОВОДСТВО ПОЛЬЗОВАТЕЛЯ

Интеллектуальный сканер защищенности веб-приложений и API
SolidPoint



АННОТАЦИЯ

Настоящий документ является руководством пользователя и описывает принципы безопасной работы интеллектуального сканера защищенности веб-приложений и API SolidPoint (далее по тексту — SolidPoint DAST).

ОГЛАВЛЕНИЕ

1. ТЕРМИНЫ, ОПРЕДЕЛЕНИЯ И СОКРАЩЕНИЯ	6
2. ВВЕДЕНИЕ	8
2.1. Область применения	8
2.2. Описание возможностей	8
2.2.1. Назначение	8
2.2.2. Сценарии использования	8
2.2.3. Функциональные характеристики	8
2.3. Условия применения	9
2.4. Роли пользователей	10
2.5. Права доступа	10
2.5.1. Доступ к настройкам	11
2.5.2. Доступ к действиям с целями	11
2.5.3. Доступ к действиям со сканированием	12
2.5.4. Доступ к действиям с уязвимостями	14
2.5.5. Доступ к действиям с отчетами	14
2.5.6. Доступ к действиям с пользователями	16
2.5.7. Доступ к действиям с токенами	17
2.5.8. Доступ к ссылкам в меню	18
2.5.9. Доступ к действиям с организациями	18
2.5.10. Доступ к действиям со сканерами	18
2.5.11. Доступ к просмотру конечных точек	19
3. АУТЕНТИФИКАЦИЯ	20
4. НАСТРОЙКИ	25
4.1. Пользовательские настройки	25
4.1.1. Изменение пароля	25
4.1.2. Данные пользователя	26
4.1.3. Настройки сайта	27
4.2. Токен доступа	28
4.2.1. Создание токена доступа	29
4.2.2. Отзыв токена	31
5. ОПИСАНИЕ ИНТЕРФЕЙСА	33
5.1. Окно «Главная»	33
5.2. Окно «Сканирования»	35
5.2.1. Подробная информация о сканировании	41
5.2.2. Отчеты	52
5.3. Окно «Цели»	57

6.	ЦЕЛЬ.....	61
6.1.	Создание цели.....	61
6.2.	Подробная информация о цели	76
6.2.1.	Вкладка «Обзор».....	77
6.2.2.	Вкладка «Сканирования»	80
6.2.3.	Вкладка «Уязвимости»	83
6.2.4.	Вкладка «Стек технологий».....	83
6.3.	Редактирование цели	84
6.4.	Удаление цели.....	86
7.	СКАНИРОВАНИЕ	88
7.1.	Создание сканирования	88
7.2.	Запуск сканирования	96
7.3.	Управление сканированием	99
7.4.	Процесс сканирования	101
8.	ВЗАИМОДЕЙСТВИЕ С API	104
8.1.	Аутентификация по токену	104
8.2.	Примеры обращений к API.....	104
8.2.1.	Запросы к серверной части	104
8.2.2.	Запросы к сканеру.....	106
8.2.3.	Работа со сканированиями.....	108
8.3.	Работа с аутентификационными данными цели	113
8.3.1.	Типы аутентификационных данных.....	113
8.3.2.	Взаимодействие.....	113
8.3.3.	Проверка валидности аутентификационных данных.....	114
8.3.4.	Обновление аутентификационных данных	114
8.3.5.	Примеры.....	114
8.4.	Ограничение URL-адресов цели	116
8.4.1.	Конфигурация	116
8.4.2.	Пример	116
9.	ВСТРАИВАНИЕ В CI/CD. НАСТРОЙКА СКАНИРОВАНИЯ ВЕБ-ПРИЛОЖЕНИЙ С ПОМОЩЬЮ GITLAB	117
9.1.	Добавление переменных окружения	117
9.2.	Настройка конфигурации CI/CD	121
9.2.1.	Создание задачи для сканирования.....	122
9.3.	Просмотр запущенной задачи	124

ПРИЛОЖЕНИЕ А. АУТЕНТИФИКАЦИЯ В СКАНИРУЕМЫХ ПРИЛОЖЕНИЯХ	127
A.1. Механизм проверки аутентификации.....	127
A.2. Обновление аутентификационных данных с помощью HTTP-запроса.....	130
A.3. Обновление аутентификационных данных с помощью браузерного сценария	135
ПРИЛОЖЕНИЕ Б. МОДУЛИ СКАНИРОВАНИЯ СКАНЕРА SOLIDPOINT DAST	145
Б.1. Анализ веб-приложений или API	145
Б.2. Анализ сетей	149
ПРИЛОЖЕНИЕ В. ЖУРНАЛИРОВАНИЕ	150

1. ТЕРМИНЫ, ОПРЕДЕЛЕНИЯ И СОКРАЩЕНИЯ

В настоящем документе применены термины, приведенные в таблице 1.

Таблица 1. Термины и определения

Термины	Определение
Аутентификация	Процесс проверки подлинности
Веб-краулинг	Процесс автоматического сбора данных о веб-приложении
Конечная точка	Адрес для взаимодействия приложения с сервером или другим приложением. Конечные точки обычно представлены URL-адресами, которые могут принимать HTTP-запросы, отправлять данные, а также фиксировать формат принимаемых данных
Уязвимость	Потенциальная угроза, которая может привести к несанкционированному доступу к конфиденциальным данным или выполнению нелегитимных действий
Цель	Сканируемое приложение с известным URL-адресом и набором заданных настроек
DirBuster	Механизм анализа поверхности атаки приложения с помощью перебора URL-адресов по определенному словарю
IP-адрес	Уникальный номер устройства, подключенного к Интернету или локальной сети
SolidWall WAF	Интеллектуальный сетевой экран для защиты веб-приложений
TLS-сертификат	Цифровой сертификат, который подтверждает подлинность веб-сайта и шифрует информацию, передаваемую между сервером и клиентом

В настоящем документе приняты сокращения, приведенные в таблице 2.

Таблица 2. Сокращения и определения

Сокращения	Определение
ИТ	Информационные технологии
ОС	Операционная система
ПО	Программное обеспечение
СМС	Служба мобильных сообщений
API	Application programming interface — программный интерфейс приложения
DAST	Dynamic Application Security Testing — динамический анализатор веб-приложений на наличие уязвимостей
HTTP	Протокол прикладного уровня, который используется для обмена данными между клиентом и сервером в сети Интернет
ID	Identifier — уникальный идентификатор объекта

Сокращения	Определение
IP	Internet Protocol – основной протокол Интернета, по которому передают информацию разные устройства в сети Интернет
JSON	JavaScript Object Notation — текстовый формат для хранения и обмена структурированными данными
RFC	Request for Comments – документ, описывающий стандарты, протоколы и технологии, используемые в Интернете и сетях
RPS	Requests Per Second — настраиваемый параметр, указывающий количество запросов в секунду к целевому серверу
SDLC	Software Development Life Cycle — методология, используемая для организации процесса разработки ПО
SPA	Single Page Application – веб-приложение, которое загружает одну страницу и обновляет контент в ответ на действия пользователя
TLS	Transport Layer Security — криптографический протокол, который обеспечивает защищённый обмен данными между сервером и клиентом
URL	Uniform Resource Locator — унифицированный указатель ресурса, адрес веб-ресурса
WAF	Web application firewall — средство защиты веб-приложений, которое анализирует HTTP/HTTPS-трафик и блокирует вредоносные запросы

2. ВВЕДЕНИЕ

2.1. Область применения

Область применения интеллектуального сканера защищенности SolidPoint — поиск уязвимостей в ИТ-инфраструктуре, а также в веб-приложениях и API как на этапе их разработки, так и на этапе эксплуатации.

2.2. Описание возможностей

2.2.1. Назначение

SolidPoint DAST предназначен для:

- сканирования подсетей сети Интернет с обнаружением функционирующих машин и установленных на них веб-приложений;
- анализа веб-приложений с целью обнаружения их ресурсов, точек ввода данных, а также поиска и верификации в анализируемых веб-приложениях уязвимостей различных классов;
- долговременного хранения полученной информации о найденных веб-приложениях, их ресурсах, точках ввода данных и уязвимостях;
- представления информации оператору в графическом виде посредством веб-браузера, функционирующего на машине оператора.

2.2.2. Сценарии использования

Сценарии использования SolidPoint DAST следующие:

- анализ защищенности браузерных веб-приложений, в том числе путем статико-динамического анализа JavaScript кода;
- анализ защищенности мобильных приложений и веб-сервисов;
- тестирование на уязвимости инфраструктуры доставки приложений;
- проверка наличия уязвимостей, связанных с аутентификацией и авторизацией;
- инвентаризация компонентного состава веб-приложений, управление изменениями API;
- проверка безопасности приложений, находящихся в продуктивной эксплуатации;
- динамический анализ приложений в рамках процессов защищенной разработки SDLC;
- обнаружение уязвимостей ИТ-инфраструктуры в рамках процессов управления уязвимостями и патч-менеджмента;
- интеграция с SolidWall WAF и другими инструментами для повышения эффективности защиты;
- использование в формате облачного сервиса или в виде решения, размещаемого на площадке заказчика.

2.2.3. Функциональные характеристики

SolidPoint DAST обладает следующими основными возможностями:

- активное сканирование веб-приложений на наличие уязвимостей;
- поддержка SPA приложений;
- поддержка аутентификации с помощью HTTP Basic Authentication, файлов cookie, заголовка и X.509 сертификата;
- инвентаризация программных компонентов приложения с использованием активного сканирования;

- обнаружение потенциальных точек ввода данных (Data Entry Points) и блокировка их использования:
 - crawling (переход по ссылкам);
 - dirbusting (перебор URL по словарю);
 - JavaScript Static/Dynamic Testing (статико-динамический анализ JS);
 - FAST (функциональное тестирование безопасности приложений, получение данных DEP путем анализа трафика веб-приложения с использованием модуля proxy);
 - поддержка формата Open API (загрузка описаний API);
- информирование о наличии следующих видов уязвимостей веб-приложений:
 - уязвимости стандартных компонент приложений и инфраструктуры их доставки;
 - SQL Injection (внедрение команд языка SQL-запросов);
 - NoSQL Injection (внедрение команд языка нереляционных БД);
 - XSS (межсайтовая подделка запросов);
 - XXE (включение внешних сущностей XML);
 - Insecure Serialization (небезопасная десериализация);
 - JS Prototype Pollution (изменение прототипа базовых объектов);
 - JS DOM Based XSS (XSS с использованием DOM браузера);
 - использование небезопасных паролей;
- управление с использованием веб-интерфейса, интерфейса командной строки или REST API;
- встраивание в конвейер CI/CD;
- интеграция с внешними системами управления найденными недостатками приложения.

2.3. Условия применения

SolidPoint DAST может быть использован в двух форматах:

- дистрибутив (On-Premise);
- облачный сервис.

Дистрибутив вместе с Docker-образами предоставляется на носителе (USB-флеш-накопитель). Облачный сервис расположен по адресу <https://ru.cloud.solidpoint.net>.

Для сканирования ресурсов следует выполнить следующие предварительные шаги:

1. Необходимо добавить IP-адрес сканера в белый список на WAF и других средствах защиты, которые могут заблокировать трафик.
2. Рекомендуется получить разрешение владельца ресурса на сканирование в выбранном промежутке времени, так как:
 - При сканировании создается дополнительная нагрузка на приложение, которая может превысить расчетную. Ее можно регулировать параметром RPS.
 - Сканирование способно привести к возникновению множества ошибок в системе мониторинга приложения, что может повлечь нарушение внутренних соглашений об уровне услуг службы эксплуатации.
 - Возможно появление запросов к элементам API сканируемого приложения, вызывающим нежелательную внешнюю реакцию: отправку писем, СМС-сообщений, отправку запросов в связанные

системы. Такие запросы к API можно выявить заранее с владельцем ресурса и занести в список исключений.

2.4. Роли пользователей

Под пользователем SolidPoint DAST понимается сотрудник, в обязанности которого входит управление сканером.

Каждый пользователь имеет роль, которая предоставляет разный уровень доступа к функционалу SolidPoint DAST и определяет внешний вид интерфейса – видимость и доступность тех или иных функций (см. таблицу 3).

Таблица 3. Роли пользователей

Роль	Идентификатор	Описание
Неизвестный	unknown	Пользователь не активирован
Только для чтения	readOnly	Ограниченная функциональность. Доступны чтение, скачивание и переход по ссылкам в пределах своей организации
Аналитик	analyst	Ограниченная функциональность. Доступна генерация PDF-отчётов о сканировании в пределах своей организации, а также все возможности роли «Только для чтения»
Пользователь	user	Базовая функциональность. Пользователь может создавать сканирования и цели
Администратор	admin	Расширенная функциональность. Администратор имеет доступ ко всей доступной функциональности в пределах своей организации
Суперадминистратор	superAdmin	Максимально доступная функциональность. Может принадлежать только пользователям из тенанта по умолчанию (например, пользователь по умолчанию)

Роль пользователю назначает администратор организации, использующей сканер.

2.5. Права доступа

В следующих таблицах обозначены роли и имеющиеся у них права доступа.

2.5.1. Доступ к настройкам

В зависимости от роли пользователя (см. подраздел 2.4 «Роли пользователей») доступ к настройкам может быть полным или ограниченным (см. таблицу 4).

Таблица 4. Доступ к настройкам в зависимости от роли пользователя

Действие	Роль				
	Суперадминистратор	Администратор	Пользователь	Аналитик	Только на чтение
Просмотр настроек	✓	✓	✓	✓	✓
Редактирование данных пользователя	✓	✓	✓	✓	✓
Изменение адреса электронной почты	✓	✓	–	–	–
Изменение имени пользователя	✓	✓	✓	✓	✓
Изменение названия организации	–	–	–	–	–
Изменение должности	✓	✓	✓	✓	✓
Изменение пароля	✓	✓	✓	✓	✓

Действия с токенами (создание, отзыв, просмотр списка) доступны пользователям со всеми ролями, кроме роли «Неизвестный» (см. подраздел 2.4 «Роли пользователя»).

2.5.2. Доступ к действиям с целями

В зависимости от роли пользователя (см. подраздел 2.4 «Роли пользователей») доступ к действиям с целями может быть полным или ограниченным (см. таблицу 5).

Таблица 5. Доступ к действиям с целями в зависимости от роли пользователя

Действие	Организация	Роль				
		Суперадминистратор	Администратор	Пользователь	Аналитик	Только на чтение
Просмотр списка целей	Собственная	√	√	√	√	√
	Чужая	√	–	–	–	–
Просмотр детализации	Собственная	√	√	√	√	√
	Чужая	√	–	–	–	–
Создание новой цели	Собственная	√	√	√	–	–
	Чужая	–	–	–	–	–
Редактирование цели	Собственная	√	√	√	–	–
	Чужая	√	–	–	–	–
Удаление цели	Собственная	√	√	√	–	–
	Чужая	√	–	–	–	–

2.5.3. Доступ к действиям со сканированием

В зависимости от роли пользователя (см. подраздел 2.4 «Роли пользователей») доступ к действиям с целями может быть полным или ограниченным (см. таблицу 6).

Таблица 6. Доступ к действиям со сканированием в зависимости от роли пользователя

Действие	Организация	Роль				
		Суперадминистратор	Администратор	Пользователь	Аналитик	Только на чтение
	Собственная	√	√	√	√	√

Действие	Организация	Роль				
		Суперадминистратор	Администратор	Пользователь	Аналитик	Только на чтение
Просмотр списка сканирований	Чужая	√	–	–	–	–
Просмотр детализации сканирования	Собственная	√	√	√	√	√
	Чужая	√	–	–	–	–
Создание нового сканирования	Собственная	√	√	√	–	–
	Чужая	√	–	–	–	–
Создание прямого сканирования (запускается запросом API POST /api/scans с указанным параметром raw, при этом цель создавать не нужно, ее параметры задаются в запросе)	Собственная	√	–	–	–	–
	Чужая	√	–	–	–	–
Повтор сканирования	Собственная	√	√	√	–	–
	Чужая	√	–	–	–	–
Приостановка сканирования	Собственная	√	√	√	–	–
	Чужая	√	–	–	–	–
Возобновление сканирования	Собственная	√	√	√	–	–
	Чужая	√	–	–	–	–
Прерывание сканирования	Собственная	√	√	√	–	–
	Чужая	√	–	–	–	–
Удаление сканирования	Собственная	√	√	√	–	–
	Чужая	√	–	–	–	–

Действие	Организация	Роль				
		Суперадминистратор	Администратор	Пользователь	Аналитик	Только на чтение
Перемещение сканирований между организациями	–	√	–	–	–	–

2.5.4. Доступ к действиям с уязвимостями

В зависимости от роли пользователя (см. подраздел 2.4 «Роли пользователей») доступ к действиям с уязвимостями может быть полным или ограниченным (см. таблицу 7).

Таблица 7. Доступ к действиям с уязвимостями в зависимости от роли пользователя

Действие	Организация	Роль				
		Суперадминистратор	Администратор	Пользователь	Аналитик	Только на чтение
Отметка	Собственная	√	√	√	√	–
	Чужая	√	–	–	–	–

2.5.5. Доступ к действиям с отчетами

В зависимости от роли пользователя (см. подраздел 2.4 «Роли пользователя») просмотр отчета о конечных точках может быть полным или ограниченным (см. таблицу 8).

Таблица 8. Доступ к действиям с отчетом о конечных точках

Действие	Организация	Роль				
		Суперадминистратор	Администратор	Пользователь	Аналитик	Только на чтение
Просмотр	Собственная	√	√	√	√	√
	Чужая	√	–	–	–	–

В зависимости от роли пользователя (см. подраздел 2.4 «Роли пользователя») доступ к действиям с техническим отчетом может быть полным или ограниченным (см. таблицу 9).

Таблица 9. Доступ к действиям с техническим отчетом в зависимости от роли пользователя

Действие	Организация	Роль				
		Суперадминистратор	Администратор	Пользователь	Аналитик	Только на чтение
Просмотр	Собственная	√	√	√	√	√
	Чужая	√	–	–	–	–
Скачивание файла отчета в формате JSON	Собственная	√	√	√	√	√
	Чужая	√	–	–	–	–

В зависимости от роли пользователя (см. подраздел 2.4 «Роли пользователей») доступ к действиям с отчетом в формате PDF может быть полным или ограниченным (см. таблицу 10).

Таблица 10. Доступ к действиям с отчетом в формате PDF в зависимости от роли пользователя

Действие	Организация	Роль				
		Суперадминистратор	Администратор	Пользователь	Аналитик	Только на чтение
Просмотр списка отчётов	–	√	√	√	√	√
Генерация отчёта	Собственная	√	√	√	√	
	Чужая	√	–	–	–	–
Удаление отчёта	Собственная	√	√	√	–	–
	Чужая	√	–	–	–	–
Скачивание отчёта	Собственная	√	√	√	√	√
	Чужая	√	–	–	–	–

2.5.6. Доступ к действиям с пользователями

В зависимости от роли пользователя (см. подраздел 2.4 «Роли пользователей») доступ к действиям с пользователями может быть полным или ограниченным (см. таблицу 11).

Таблица 11. Доступ к действиям с пользователями в зависимости от роли пользователя

Действие	Организация	Роль целевого пользователя	Суперадминистратор	Администратор
Создание нового пользователя	Собственная	Неизвестный	√	√
	Чужая	–	√	–
Активация пользователя и назначение роли	Собственная	Суперадминистратор	√	–
	Чужая	–	–	–
	Собственная	Администратор	√	√
	Чужая	–	√	–
	Собственная	Иная	√	√

Действие	Организация	Роль целевого пользователя	Суперадминистратор	Администратор
	Чужая	–	√	–
Определение пользователя в организацию	Собственная	Неизвестный	√	√
	Чужая		√	–
Изменение адреса электронной почты себе	Собственная	–	√	√
Изменение адреса электронной почты другим пользователям	Собственная	Суперадминистратор	–	–
	Чужая		–	–
	Собственная	Администратор	√	–
	Чужая	–	√	–
	Собственная	Иная	√	√
	Чужая		√	
Изменение пароля себе	Собственная	–	√	√
Изменение пароля другим пользователям	Собственная	Суперадминистратор	–	–
	Чужая		–	–
	Собственная	Администратор	√	–
	Чужая		√	–
	Собственная	Иная	√	√
	Чужая		√	–
Изменение иных данных себе	Собственная	–	√	√
Изменение иных данных другим пользователям	Собственная	Суперадминистратор	–	–
	Чужая	–	–	–
	Собственная	Администратор	√	–
	Чужая	–	√	–
	Собственная	Иная	√	√
	Чужая	–	√	–

2.5.7. Доступ к действиям с токенами

Доступ к действиям с токенами доступа (просмотр списка, создание нового токена, отзыв токена) имеют пользователи со всеми ролями, кроме пользователей с ролью «Неизвестный» (см. подраздел 2.4 «Роли пользователей»).

2.5.8. Доступ к ссылкам в меню

Доступ к ссылкам в меню («Документация», «Спецификация API», «Связаться с нами») имеют пользователи со всеми ролями, кроме пользователей с ролью «Неизвестный» (см. подраздел 2.4 «Роли пользователей»).

2.5.9. Доступ к действиям с организациями

В зависимости от роли пользователя (см. подраздел 2.4 «Роли пользователей») доступ к действиям с организациями может быть полным или ограниченным (см. таблицу 12).

Таблица 12. Доступ к действиям с организациями в зависимости от роли пользователя

Действие	Организация	Роль				
		Суперадминистратор	Администратор	Пользователь	Аналитик	Только на чтение
Создание новой организации	–	√	–	–	–	–
Изменение организации	Собственная	√	√	–	–	
	Чужая	√	–	–	–	–
Добавление ограничений на домены	Собственная	√	–	–	–	–
	Чужая	√	–	–	–	–
Удаление ограничений на домены	Собственная	√	–	–	–	–
	Чужая	√	–	–	–	–

2.5.10. Доступ к действиям со сканерами

Важно! Все команды запускаются пользователем с ролью «Администратор».

Управление сканерами (сканирующими узлами) доступно только для пользователей с ролью «Суперадминистратор» (см. таблицу 13).

Таблица 13. Доступ к действиям со сканерами

Действие	Организация	Суперадминистратор
Просмотр списка сканеров	–	√

Действие	Организация	Суперадминистратор
Просмотр детализации сканера	–	√
Добавление нового сканера	–	√
Обновление настроек сканера	–	√
Отключение сканера	–	√
Назначение сканера организации	Собственная	√
	Чужая	√
Удаление сканера из организации	Собственная	√
	Чужая	√

2.5.11. Доступ к просмотру конечных точек

Доступ к просмотру конечных точек имеют пользователи собственной организации со всеми ролями. Доступ к просмотру конечных точек чужой организации имеет только «Суперадминистратор» (см. подраздел 2.4 «Роли пользователей»).

3. АУТЕНТИФИКАЦИЯ

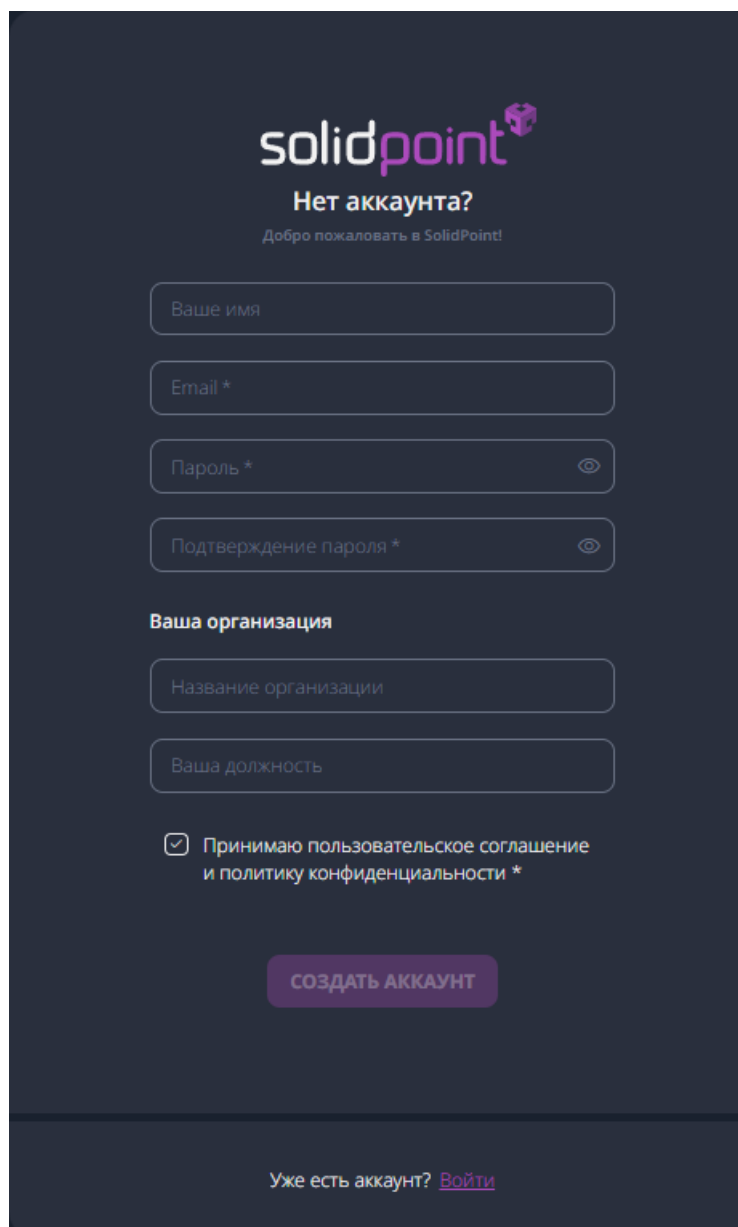
Для доступа к SolidPoint DAST необходимо открыть любой браузер и в адресной строке ввести адрес <https://ru.cloud.solidpoint.net>.

При первой аутентификации необходимо зарегистрироваться в системе. Для создания аккаунта нужно в открывшейся по ссылке выше форме доступа нажать надпись «Зарегистрироваться» (см. снимок экрана 1).

Снимок экрана 1. Форма доступа, кнопка «Зарегистрироваться»

Откроется форма создания аккаунта, в которой требуется заполнить следующие поля (см. снимок экрана 2):

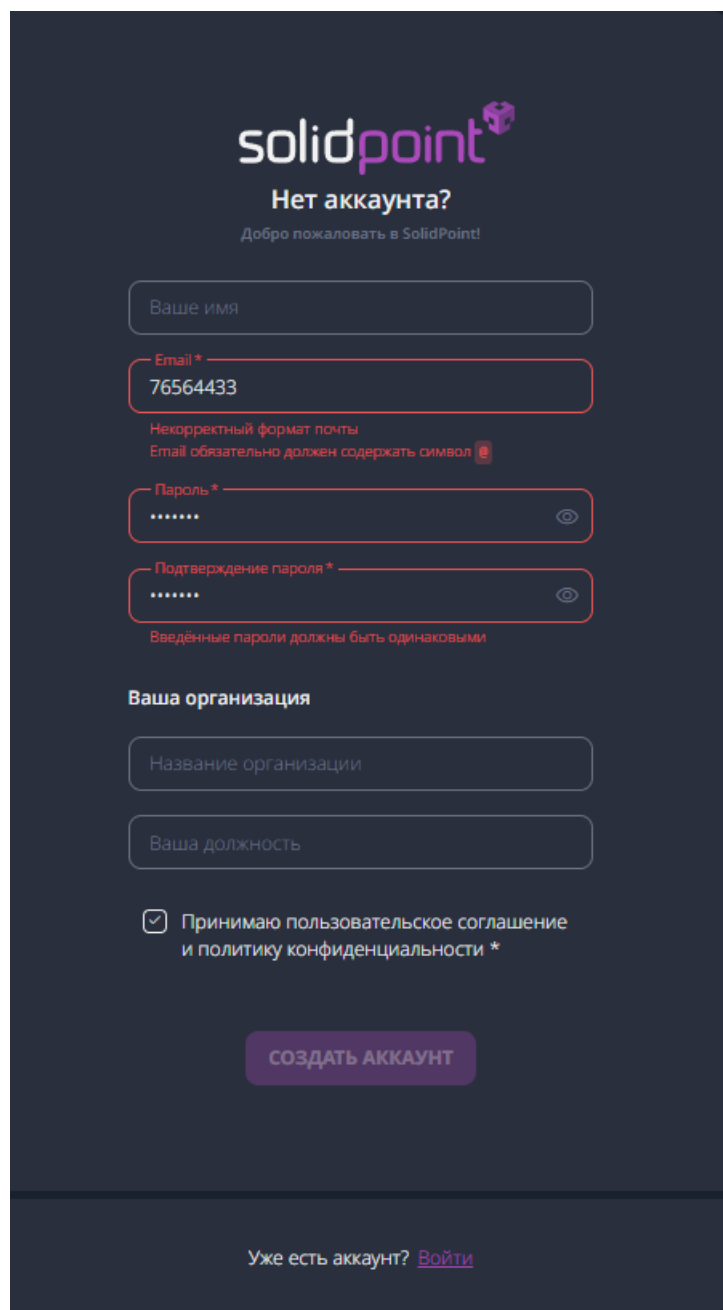
- Имя;
- E-mail — поле обязательно для заполнения;
- Пароль — поле обязательно для заполнения;
- Подтверждение пароля — поле обязательно для заполнения;
- Название организации;
- Должность.



The screenshot shows a registration form for SolidPoint. At the top is the SolidPoint logo and the heading "Нет аккаунта?" (No account?). Below this is a welcome message: "Добро пожаловать в SolidPoint!". The form contains several input fields: "Ваше имя" (Your name), "Email *" (Email), "Пароль *" (Password), and "Подтверждение пароля *" (Confirm password). Each password field has an eye icon for toggling visibility. Below these is a section titled "Ваша организация" (Your organization) with fields for "Название организации" (Organization name) and "Ваша должность" (Your position). A checkbox is present with the text "Принимаю пользовательское соглашение и политику конфиденциальности *" (I agree to the terms of use and privacy policy). At the bottom of the form is a purple button labeled "СОЗДАТЬ АККАУНТ" (Create account). At the very bottom of the page, there is a link: "Уже есть аккаунт? [Войти](#)" (Already have an account? [Login](#)).

Снимок экрана 2. Форма создания аккаунта

В случае неверно указанных данных в обязательных полях формы (некорректный формат почты, неодинаковые пароли) высветится сообщение об ошибке (см. снимок экрана 3).



The screenshot shows the SolidPoint registration interface. At the top is the logo and the heading "Нет аккаунта?" (No account?). Below it is a welcome message. The form contains several input fields: "Ваше имя" (Your name), "Email *" (Email), "Пароль *" (Password), and "Подтверждение пароля *" (Confirm password). The "Email" field contains "76564433" and has a red border with an error message: "Некорректный формат почты. Email обязательно должен содержать символ @". The "Пароль" and "Подтверждение пароля" fields contain masked text and have red borders with an error message: "Введённые пароли должны быть одинаковыми" (Entered passwords must be the same). Below these is a section "Ваша организация" (Your organization) with fields for "Название организации" (Organization name) and "Ваша должность" (Your position). At the bottom of this section is a checkbox labeled "Принимаю пользовательское соглашение и политику конфиденциальности *" (I agree with the terms of use and privacy policy *), which is checked. A large purple button labeled "СОЗДАТЬ АККАУНТ" (CREATE ACCOUNT) is centered below the form. At the very bottom, there is a link: "Уже есть аккаунт? Войти" (Already have an account? Log in).

Снимок экрана 3. Форма создания аккаунта, неверно указанные данные

После безошибочного заполнения обязательных полей необходимо в нижней части формы подтвердить согласие с политикой конфиденциальности (убедиться, что чекбокс включен) и нажать кнопку «СОЗДАТЬ АККАУНТ». Откроется форма входа, в которой нужно заполнить поля с электронной почтой и паролем, указанными при создании аккаунта, и нажать кнопку «ВОЙТИ» (см. снимок экрана 4).

Зарегистрироваться'." data-bbox="234 80 800 479"/>

solidpoint³

Dynamic Application
Security Testing

Email *

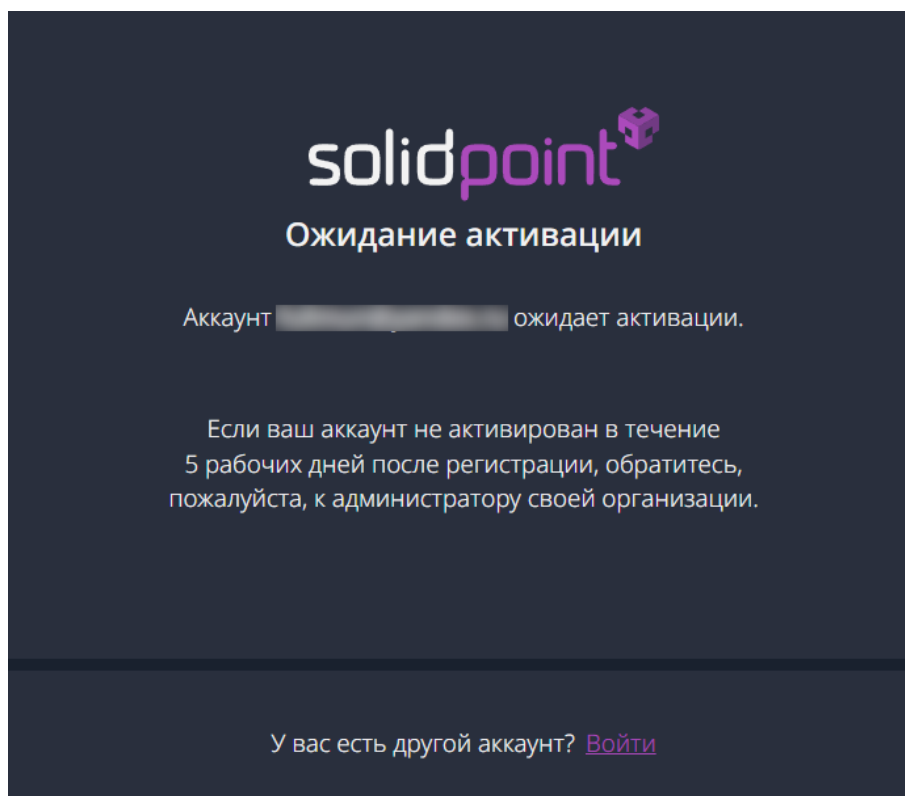
Пароль *

ВОЙТИ

Нет аккаунта? [Зарегистрироваться](#)

Снимок экрана 4. Форма входа

Далее откроется окно с сообщением об ожидании активации аккаунта (см. снимок экрана 5).



Снимок экрана 5. Ожидание активации

Необходимо дождаться активации: администратор организации, указанной при создании аккаунта, одобрит заявку, а также назначит пользователю роль. После одобрения заявки сканер будет доступен по форме входа, показанной на снимке экрана 4.

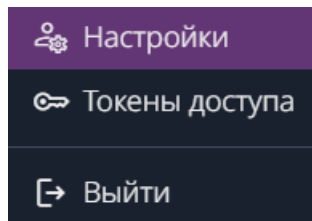
В случае если аккаунт не будет активирован в течение 5 рабочих дней после регистрации, следует обратиться к администратору организации.

4. НАСТРОЙКИ

Контекстное меню настроек расположено в правом верхнем углу во всех представлениях интерфейса.

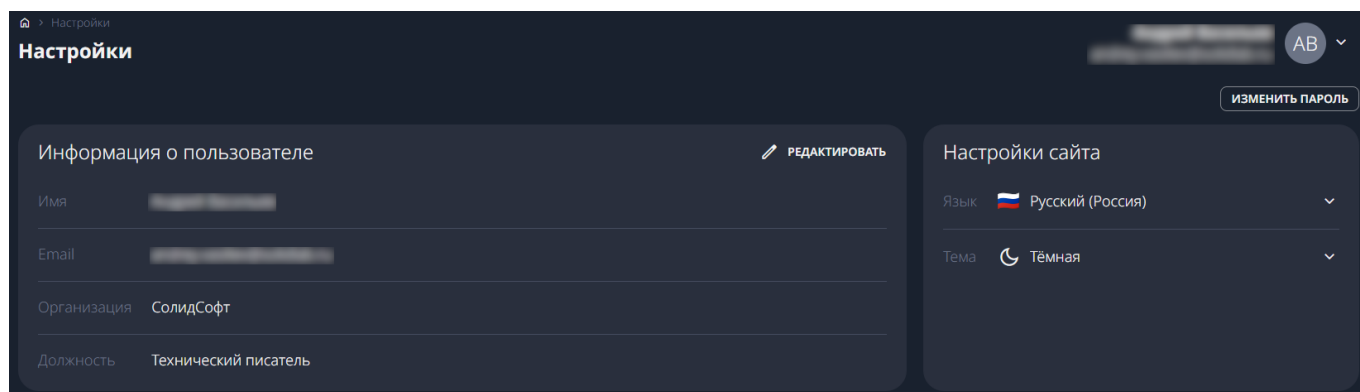
4.1. Пользовательские настройки

Для изменения пароля, данных пользователя и настроек сайта необходимо справа от имени пользователя нажать пиктограмму «▼» и в раскрывшемся контекстном меню выбрать пункт «Настройки» (см. снимок экрана 6).



Снимок экрана 6. Пункт меню «Настройки»

Откроется окно «Настройки», состоящее из двух функциональных секторов «Информация о пользователе» и «Настройки сайта» и кнопки «ИЗМЕНИТЬ ПАРОЛЬ» (см. снимок экрана 7).



Снимок экрана 7. Окно «настройки»

4.1.1. Изменение пароля

Для того чтобы изменить пароль, необходимо в правом верхнем углу окна «Настройки» нажать кнопку «ИЗМЕНИТЬ ПАРОЛЬ». Откроется форма изменения пароля, в которой требуется заполнить поля «Текущий пароль», «Новый пароль», «Подтвердите новый пароль» и нажать кнопку «ИЗМЕНИТЬ» (см. снимок экрана 8). Текущий пароль будет изменен на новый.

Снимок экрана 8. Форма «Изменение пароля»

Примечание. При неверном заполнении полей они подсвечиваются красным цветом с соответствующими подписями:

- текущий пароль введен неверно: «Пароль введен неверно»;
- поля текущего и нового пароля заполнены одинаково: «Старый и новый пароли не могут совпадать»;
- неверно подтвержден новый пароль: «Введенные пароли должны быть одинаковыми».

В случае вышеописанных ошибок необходимо заново ввести пароли и нажать кнопку «ИЗМЕНИТЬ». Чтобы пароли сделать видимыми, можно воспользоваться пиктограммой «», расположенной в конце каждого поля.

4.1.2. Данные пользователя

Для изменения данных пользователя необходимо в правом верхнем углу сектора «Информация о пользователе» нажать кнопку «Редактировать». Откроется форма редактирования данных пользователя (см. снимок экрана 9).

Снимок экрана 9. Форма «Редактирование пользователя»

Поля в форме для редактирования следующие:

- «Email». Поле обязательно для заполнения.
- «Ваше имя». Максимальное количество символов — 255. Поле необязательно для заполнения.
- «Должность». Максимальное количество символов — 255. Поле необязательно для заполнения.

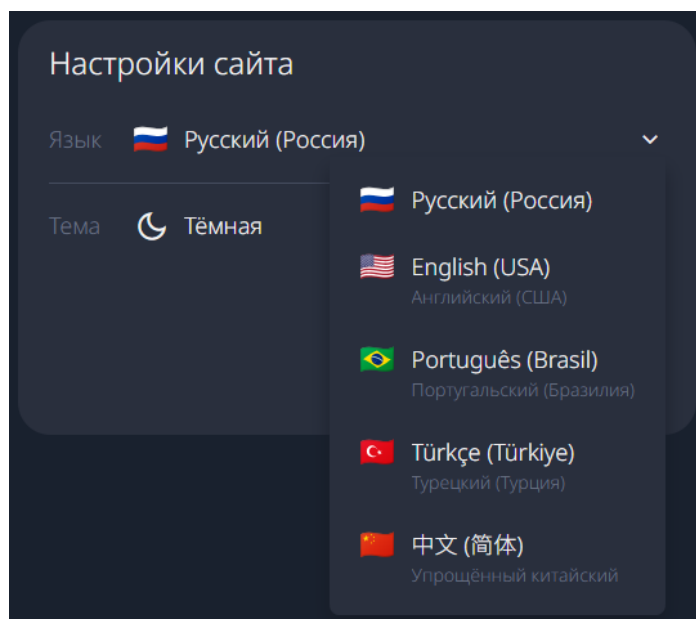
После заполнения полей необходимо нажать кнопку «СОХРАНИТЬ», чтобы применить измененные данные.

4.1.3. Настройки сайта

В секторе настройки сайта можно изменить язык отображения текстовой информации и цвет фона интерфейса (тему).

Для изменения языка следует раскрыть соответствующее меню и выбрать язык (см. снимок экрана 10):

- Русский;
- Английский;
- Португальский;
- Турецкий;
- Упрощенный китайский.

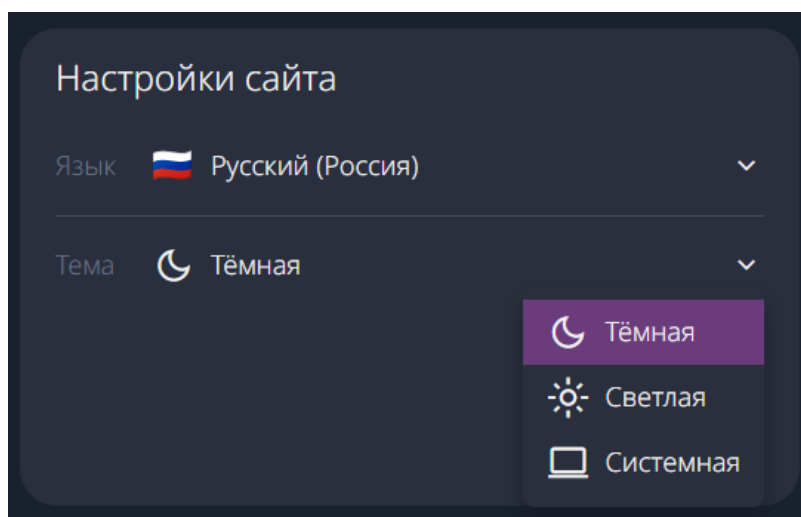


Снимок экрана 10. Выбор языка

После выбора языка на сайте изменится автоматически.

Для изменения темы интерфейса необходимо раскрыть соответствующее меню и выбрать тему (см. снимок экрана 11):

- Тёмная;
- Светлая;
- Системная (для версии On-Premise) — цвет фона интерфейса, установленного в ОС.



Снимок экрана 11. Выбор темы

После выбора темы цвет фона интерфейса изменится автоматически.

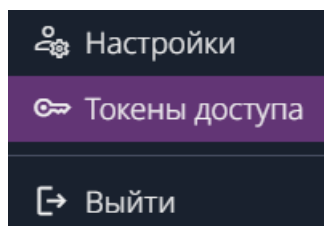
4.2. Токен доступа

Токен доступа необходим для решения задач интеграционного характера. Среди них можно выделить следующие основные задачи:

1. Взаимодействие с API сканера (данный процесс подробно описан в разделе 8 «Взаимодействие с API», а также в онлайн документации, расположенной по ссылке <https://docs.solidpoint.net/ru/userguide/further-work/API-management/>).
2. Автоматизация процесса сканирования какой-либо цели (данный процесс подробно описан в разделе 9 «Встраивание в CI/CD. Настройка сканирования веб-приложений с помощью GitLab», а также в онлайн документации, расположенной по ссылке <https://docs.solidpoint.net/ru/userguide/further-work/CI-setup/#cicd>).

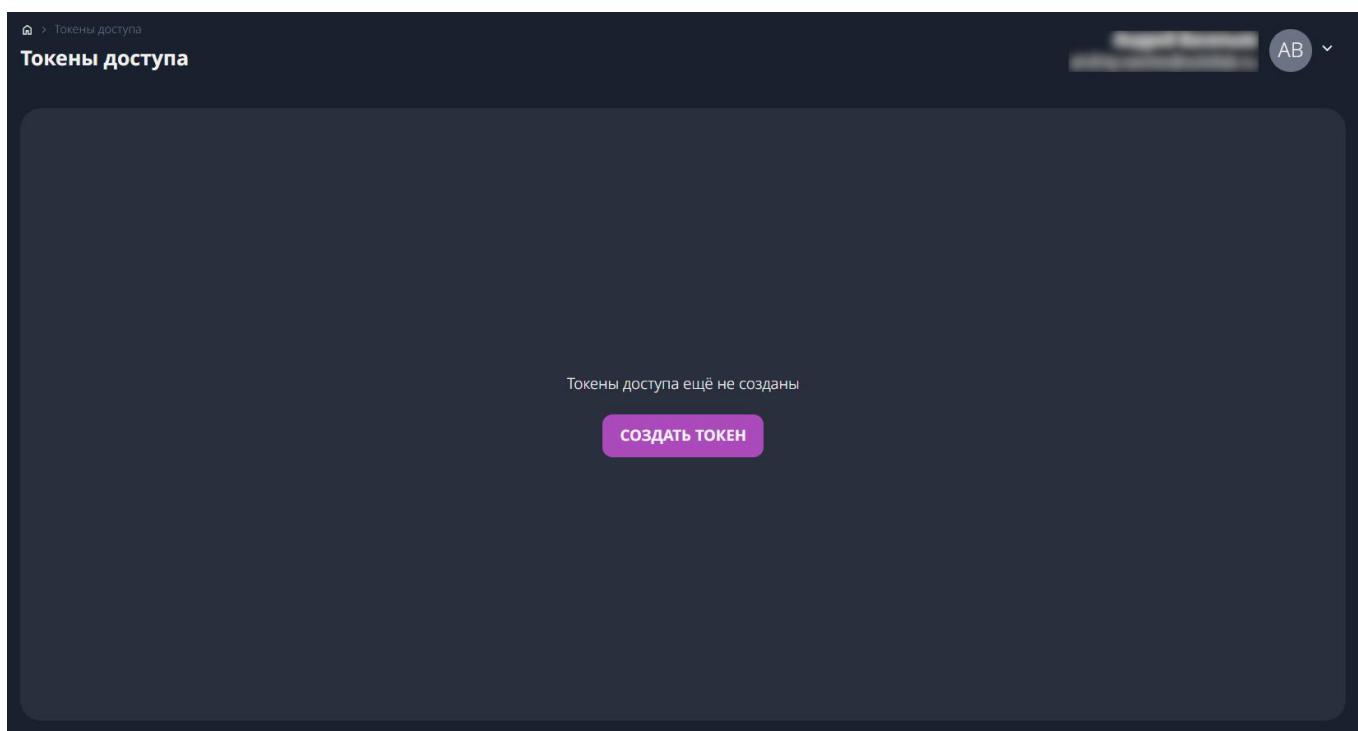
4.2.1. Создание токена доступа

Для создания токена доступа необходимо справа от имени пользователя нажать пиктограмму «» и в раскрывшемся контекстном меню выбрать пункт «Токены доступа» (см. снимок экрана 12).



Снимок экрана 12. Пункт меню «Токены доступа»

Откроется окно «Токены доступа», в котором следует нажать кнопку «СОЗДАТЬ ТОКЕН» (см. снимок экрана 13).



Снимок экрана 13. Окно «Токены доступа»

Далее в открывшейся форме «Новый токен доступа» нужно заполнить следующие поля (см. снимок экрана 14):

- «Название». Максимальное количество символов – 255. Поле обязательно для заполнения.
- «Срок действия». Дата истечения токена в формате ДД.ММ.ГГГГ. Если не указать дату истечения токена, то срок его действия будет неограничен.

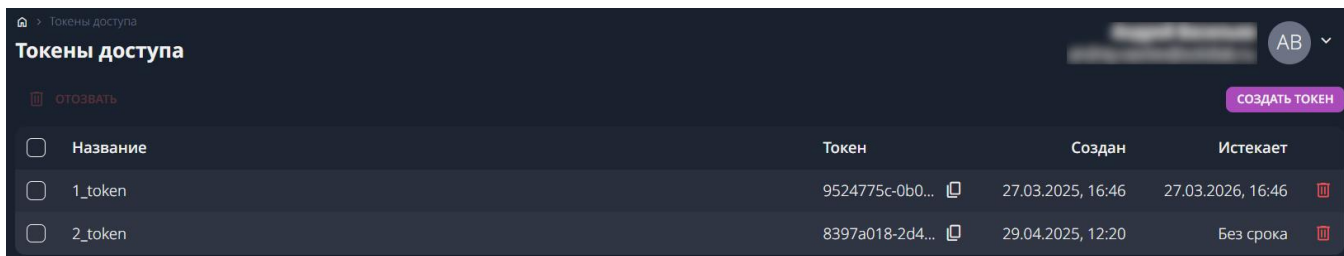
Снимок экрана 14. Форма «Новый токен доступа»

В случае неверно заполненных полей формы или пропуска заполнения поля «Название» высветятся соответствующие сообщения об ошибках (см. снимок экрана 15).

Снимок экрана 15. Форма «Новый токен доступа» с ошибками

После безошибочного заполнения полей необходимо нажать кнопку «СОЗДАТЬ». Созданный токен отобразится в списке окна «Токены доступа» в табличном виде с указанием (см. снимок экрана 16):

- названия токена;
- токена (доступно копирование в буфер обмена по нажатию);
- даты создания токена;
- даты истечения токена (в случае пропуска заполнения поля «Срок действия» при создании токена, срок истечения будет «Без срока»).



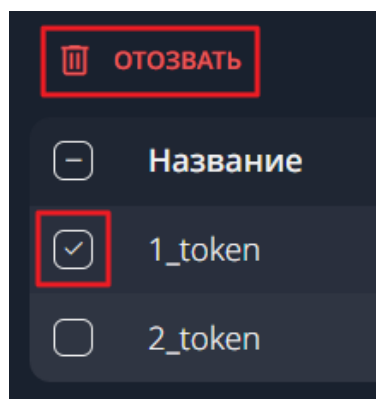
Название	Токен	Создан	Истекает
1_token	9524775c-0b0...	27.03.2025, 16:46	27.03.2026, 16:46
2_token	8397a018-2d4...	29.04.2025, 12:20	Без срока

Снимок экрана 16. Список токенов

4.2.2. Отзыв токена

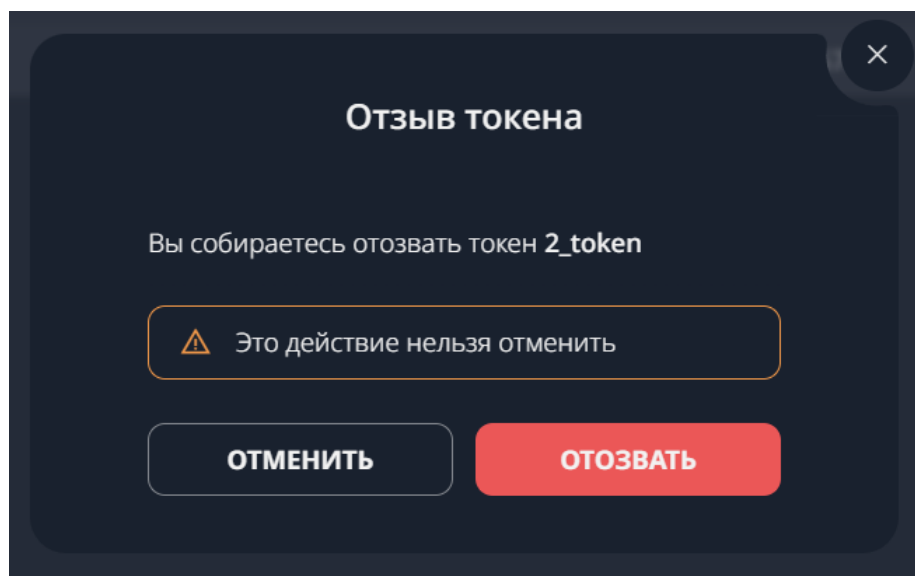
Отозвать токен можно 2-мя способами:

1. В конце строки нажать пиктограмму «».
2. Включить чекбокс токена, который требуется отозвать, и в левом верхнем углу нажать кнопку «ОТОЗВАТЬ» (см. снимок экрана 17).



Снимок экрана 17. Отзыв (удаление) токена

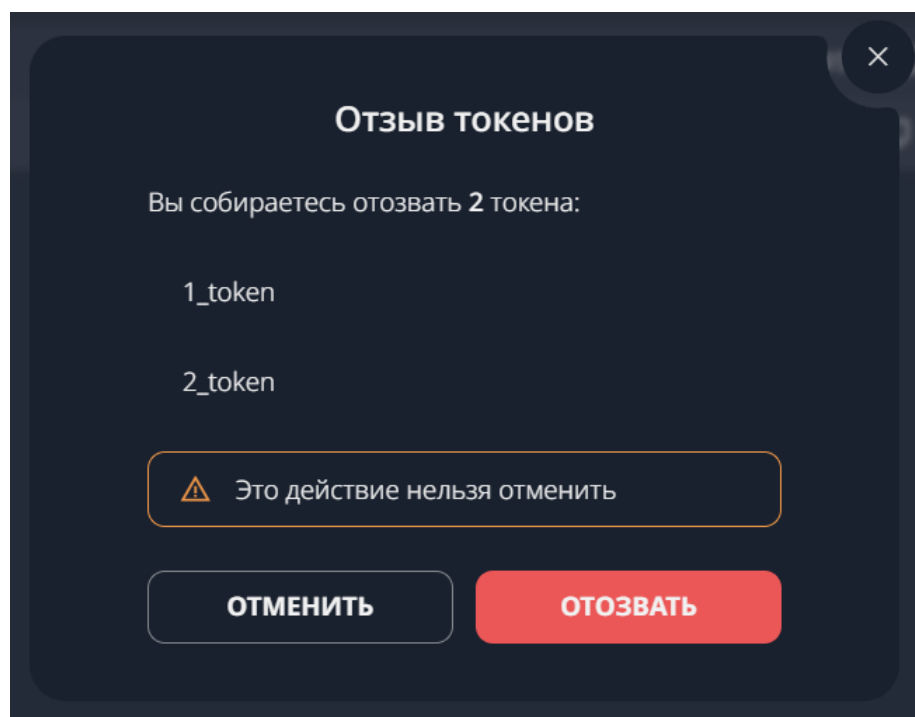
После нажатие на пиктограмму или кнопку «ОТОЗВАТЬ» необходимо в открывшемся окне «Отзыв токена» нажать кнопку «ОТОЗВАТЬ» (см. снимок экрана 18).



Снимок экрана 18. Окно «Отзыв токена»

Токен будет отозван и удален из списка.

Можно отозвать несколько токенов сразу. Для этого следует выполнить действия, описанные в п. 2, включив несколько чекбоксов, и в открывшемся окне «Отзыв токенов» нажать кнопку «Отозвать» (см. снимок экрана 19).



Снимок экрана 19. Окно «Отзыв токенов»

Токены будут отозваны и удалены из списка.

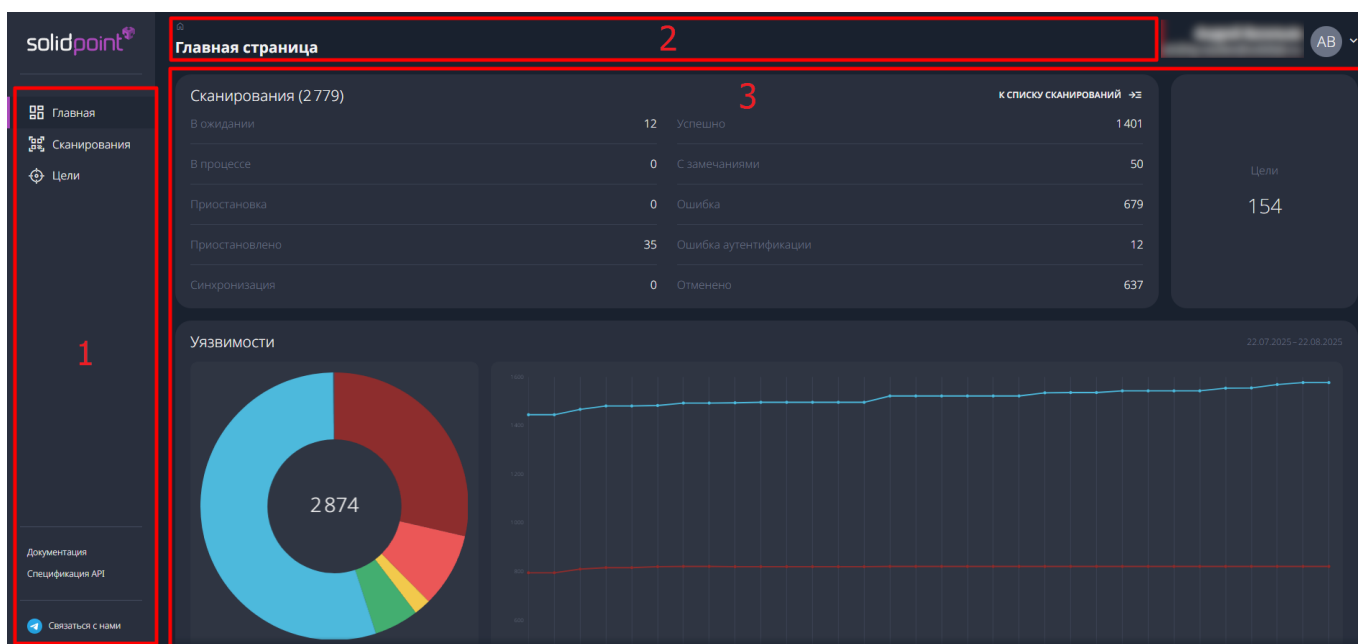
Меню, логотип в левом верхнем углу, иконка для перехода на главную страницу, имя пользователя с выпадающим списком настроек в правом верхнем углу отображаются во всех представлениях.

5.1. Окно «Главная»

Окно «Главная» является домашней страницей, т.е. страницей, которая открывается по умолчанию после аутентификации. В данном окне отображается статистическая информация о проведенных сканированиях.

Окно «Главная» содержит три функциональных блока (см. снимок экрана 20):

1. Меню – позволяет выбрать необходимое представление и содержит пункты:
 - Главная;
 - Сканирования;
 - Цели;
 - Документация (при нажатии открывается веб-ресурс с документацией SolidPoint DAST);
 - Спецификация API (при нажатии открывается веб-ресурс со спецификацией API по управлению SolidPoint DAST);
 - Связаться с нами (при нажатии открывается телеграм-канал для связи с технической поддержкой SolidPoint DAST в мессенджере «Telegram»).
2. Заголовок окна с неактивной иконкой «🏠» в левом верхнем углу для перехода на главную страницу.
3. Информация о проведенных сканированиях.



Снимок экрана 20. Раздел «Главная»

Блок 3 информации о проведенных сканированиях вертикально прокручивается, он разделен на следующие секторы:

- Сканирования — статистика по сканированиям. В данном секторе содержится следующая информация:

- В ожидании — количество сканирований в ожидании сканирования;
- В процессе — количество сканирований, осуществляющихся в текущий момент;
- Приостановка — количество сканирований, переходящих в статус «Приостановлено»;
- Приостановлено — количество приостановленных сканирований;
- Синхронизация — количество сканирований, переходящих в статус «В процессе» или «Отменено»;
- Успешно — количество успешно завершённых сканирований;
- С замечаниями — количество сканирований, завершённых с замечаниями (сканирование в целом завершено успешно, но в нем отработали не все модули);
- Ошибка — количество аварийно завершившихся сканирований;
- Ошибка аутентификации — количество сканирований, в которых возникли ошибки при аутентификации;
- Отменено — количество сканирований, отменённых пользователем;

Кнопка «К СПИСКУ СКАНИРОВАНИЙ» предназначена для перехода в окно «Сканирования».

- «Цели» — в данном секторе отображается общее количество созданных целей. При нажатии на данный сектор осуществляется переход в окно «Цели».
- Круговая диаграмма «Уязвимости» и линейный график — секторы для отображения в графическом виде найденных разного уровня критичности уязвимостей за последний месяц. Линейный график интерактивный, на нем можно отображать нужные уровни критичности найденных уязвимостей, нажимая соответствующие названия с цветным индикатором (см. снимок экрана 21).



Снимок экрана 21. Сектор «Уязвимости»

Отображается пять уровней критичности:

- ■ Крайне высокая;
- ■ Высокая;
- ■ Средняя;
- ■ Низкая;
- ■ Информационная;
- ■ Не определена.

- «Последние сканирования» — список последних десяти сканирований в табличном виде с указанием (см. снимок экрана 22):
 - цели;
 - даты начала сканирования;
 - профиля сканирования;
 - статуса сканирования;
 - продолжительности сканирования;
 - количества найденных уязвимостей;
 - локации;
 - ID организации.

Последние сканирования 3

Цель	Начало	Профиль	Статус	Длительность	Уязвимости	Локации	ID организации
http://juice-shop.stands.fuchsia/profile	15.09.2025, 13:55	Полное	Успешно	9 м		10	1
http://combined-1s.stands.fuchsia	15.09.2025, 13:55	Полное	Успешно	6 м		3	1
http://xxe-shop.stands.appsecuritytesting.fun	15.09.2025, 13:55	Полное	Успешно	32 м		35	1
http://target-tenant2.solidpoint	15.09.2025, 13:45	Выборочное	Отменено	<1 м		0	1
http://test-sync-v2s.solidpoint	15.09.2025, 13:41	Полное	Ошибка	<1 м		0	1
http://test-sync-local-v02.solidpoint	15.09.2025, 13:40	Выборочное	Успешно	3 м		1	1
http://test-sync-local-v02.solidpoint	15.09.2025, 13:32	Выборочное	Успешно	3 м		1	1
http://test-sync-v2s.solidpoint	15.09.2025, 13:23	Полное	Ошибка	<1 м		0	1
http://test-sync-v2s.solidpoint	15.09.2025, 13:23	Полное	Ошибка	<1 м		0	1
http://test-sync-v2s.solidpoint	15.09.2025, 13:21	Полное	Ошибка	<1 м		0	1

Снимок экрана 22. Сектор «Последние сканирования»

5.2. Окно «Сканирования»

Окно «Сканирования» предназначено для создания нового сканирования (более подробно см. подраздел 7.1 «Создание сканирования»), а также управления уже созданными сканированиями.

Данное окно содержит три функциональных блока (см. снимок экрана 23):

1. Меню.
2. Заголовок окна с активной иконкой «» в левом верхнем углу для перехода на домашнюю страницу.
3. Список ранее созданных сканирований в табличном виде со следующими колонками:
 - Цель — ссылка на страницу детализации сканирования, представленная URL-адресом цели.
 - Начало — дата и время запуска сканирования.
 - Профиль — тип сканирования, установленный при создании сканирования.
 - Статус — состояние сканирования.
 - Длительность — время, прошедшее с момента запуска сканирования.
 - Уязвимости — количество найденных уязвимостей с маркерами для визуализации уровня угрозы. Маркеры выводятся при нахождении уязвимостей в процессе сканирования, поэтому оценка возможна даже для незавершённых сканирований. Цвета маркеров показывают уровень критичности обнаруженных уязвимостей, а число внутри — их количество. При наведении курсора на маркер с подписью «9+» будет показано точное количество уязвимостей.
 - Локации — число, отражающее количество локаций, найденных во время сканирования.

- ID организации — эта колонка доступна для просмотра только пользователям с правами уровня «Суперадминистратор». Значение в поле показывает идентификационный номер организации, для которой проводится сканирование.
- Кнопка «⋮» при нажатии раскрывает контекстное меню дополнительных действий со сканированием. Например, «Просмотр», «Повторить», «Удалить» или «Просмотр», «Приостановить», «Прервать». Набор доступных действий зависит от статуса выбранного сканирования и прав пользователя.

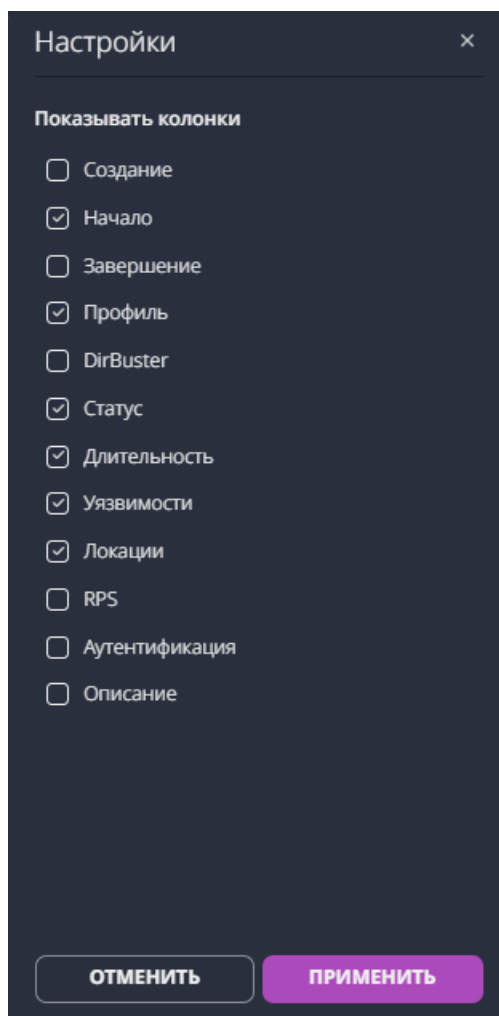
Цель	Начало	Профиль	Статус	Длительность	Уязвимости	Локации	ID организации
☐ http://95.217.83.73:3012/	04.09.2025, 14:39	Выборочное	Ошибка	1 м		0	1
☐ http://vampi-secure.stands.fuchsia	04.09.2025, 14:15	Выборочное	Успешно	2 м	0 0 0 0 0 0 0 0	1	1
☐ http://vampi.stands.fuchsia	04.09.2025, 13:42	Выборочное	Успешно	<1 м		1	1
☐ http://auth-combined.stands.fuchsia	03.09.2025, 21:20	Выборочное	Отменено	1 м		1	1
☐ http://auth-combined.stands.fuchsia	03.09.2025, 16:29	Выборочное	Успешно	11 м	9+ 1 0 0 0 0 0 0	64	1
☐ http://juiceshop.stands.appsecuritytesting.fun	03.09.2025, 16:14	Выборочное	Успешно	22 м		270	1
☐ http://juiceshop.stands.appsecuritytesting.fun/profile	03.09.2025, 15:57	Выборочное	Успешно	20 м	1 0 0 0 0 0 0 0	221	1
☐ http://vampi.stands.fuchsia	03.09.2025, 14:12	Выборочное	Успешно	43 м	0 0 0 0 0 0 0 0	1	1
☐ http://vampi.stands.fuchsia	03.09.2025, 11:33	Выборочное	С замечаниями	1 м		1	1
☐ http://vampi.stands.fuchsia	03.09.2025, 11:18	Выборочное	С замечаниями	21 м	0 0 0 0 0 0 0 0	1	1
☐ http://95.217.83.73:3012/#/	02.09.2025, 17:43	Выборочное	Ошибка	1 м		0	1
☐ http://95.217.83.73:3012/#/	02.09.2025, 17:31	Выборочное	Ошибка	1 м		0	1
☐ http://95.217.83.73:3012/	02.09.2025, 17:17	Выборочное	С замечаниями	2 ч 2 м		216	1
☐ http://95.217.83.73:3012/	02.09.2025, 16:51	Выборочное	Успешно	6 м		134	1
☐ http://vampi.stands.fuchsia	02.09.2025, 14:39	Выборочное	Успешно	2 м	0 0 0 0 0 0 0 0	1	1
☐ http://example.com:6000	02.09.2025, 13:49	Полное	Отменено	<1 м		0	1

Снимок экрана 23. Окно «Сканирования»

Примечание 1. Если сканирование завершено и в графе «Уязвимости» нет записей, значит, для этой цели не было обнаружено уязвимостей.

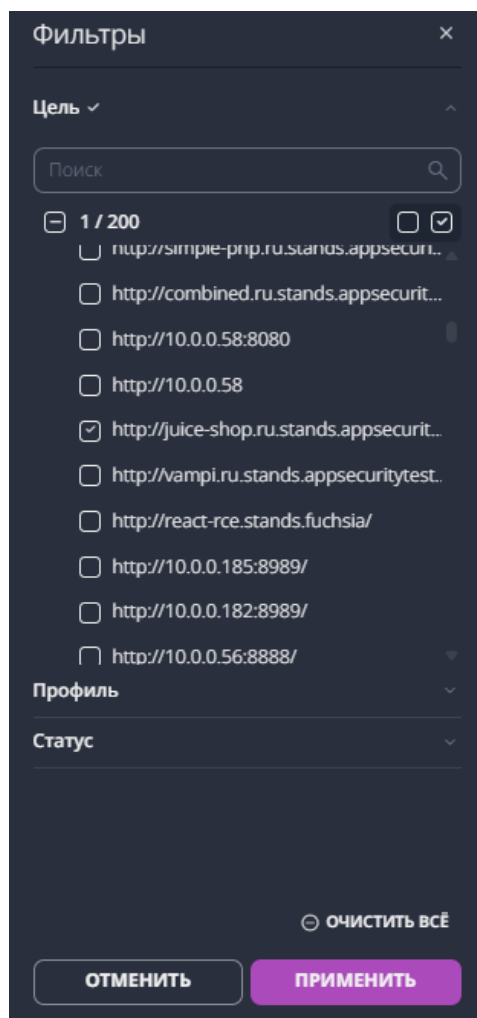
Примечание 2. Если сканирований пока не было создано, на странице будет отображаться кнопка «Новое сканирование».

Для отображения или скрытия колонок можно воспользоваться фильтром, нажав кнопку «Настройки» в правом верхнем углу. В открывшемся окне «Настройки» следует включить/отключить чекбоксы соответствующих колонок и нажать кнопку «ПРИМЕНИТЬ» (см. снимок экрана 24).

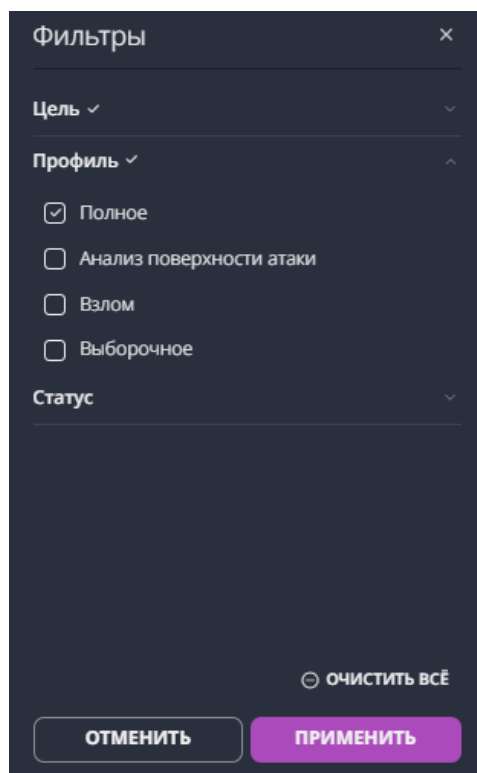


Снимок экрана 24. Окно «Настройки» (фильтр колонок)

Для быстрого поиска нужной цели сканирования можно воспользоваться фильтром, нажав в правом верхнем углу кнопку «ФИЛЬТРЫ». Фильтрация доступна по адресу цели: в поле «Поиск», поиск по списку с включением чекбокса (см. снимок экрана 25), типу сканирования (см. снимок экрана 26) и/или по статусу сканирования (см. снимок экрана 27). Далее следует нажать кнопку «ПРИМЕНИТЬ».



Снимок экрана 25. Окно «Фильтры», поиск по адресу цели



Фильтры

Цель ✓

Профиль ✓

☒ Полное

☐ Анализ поверхности атаки

☐ Взлом

☐ Выборочное

Статус

ОЧИСТИТЬ ВСЁ

ОТМЕНИТЬ ПРИМЕНИТЬ

Снимок экрана 26. Окно «Фильтры», поиск по типу сканирования

Фильтры

Цель

Профиль

Статус ✓

1 / 10

☒ Успешно

☐ С замечаниями

☐ Ошибка

☐ Ошибка аутентификации

☐ Отменено

☐ В ожидании

☐ В процессе

☐ Приостановка

☐ Приостановлено

☐ Синхронизация

ОЧИСТИТЬ ВСЁ

ОТМЕНИТЬ ПРИМЕНИТЬ

Снимок экрана 27. Окно «Фильтры», поиск по статусу сканирования

Уже созданные сканирования можно повторить, возобновить, приостановить, прервать или удалить в зависимости от статуса сканирования (см. таблицу 14).

Таблица 14. Статусы сканирования и возможные действия

Статус	Возможные действия
В ожидании	– Приостановить; – Прервать
В процессе	– Приостановить; – Прервать
Отменено	– Повторить; – Удалить
Ошибка (см. примечание ниже)	– Повторить, – Удалить
Приостановлено	– Возобновить; – Прервать
С замечаниями	– Повторить; – Удалить

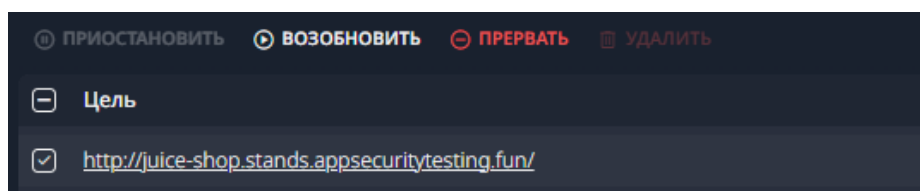
Статус	Возможные действия
Успешно	– Повторить; – Удалить

Примечание. Ошибка сканирования может возникать при некорректных данных аутентификации или в связи с нештатной работой какого-либо модуля сканирования. Рекомендуется проверить данные аутентификации и перезапустить сканирование, а в случае повторной ошибки – обратиться в техническую поддержку для диагностики.

Статусы «Синхронизация» и «Приостановка» являются переходными между основными состояниями сканирования, в связи с чем действия при данных статусах не предусмотрены.

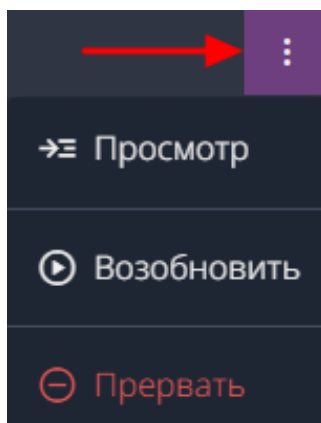
Выбрать необходимое действие можно двумя способами:

1. Над списком сканирований, если при включении чекбокса выбранной цели становятся активными кнопки действий (см. снимок экрана 28). Можно выбрать сразу несколько сканирований.



Снимок экрана 28. Активные кнопки действий при включенном чекбоксе выбранной цели

2. В конце строки цели в контекстном меню, раскрывающемся при нажатии на кнопку «⋮». Пункт меню «Просмотр» отображается при любом статусе и открывает страницу подробной информации о сканировании (см. снимок экрана 29).

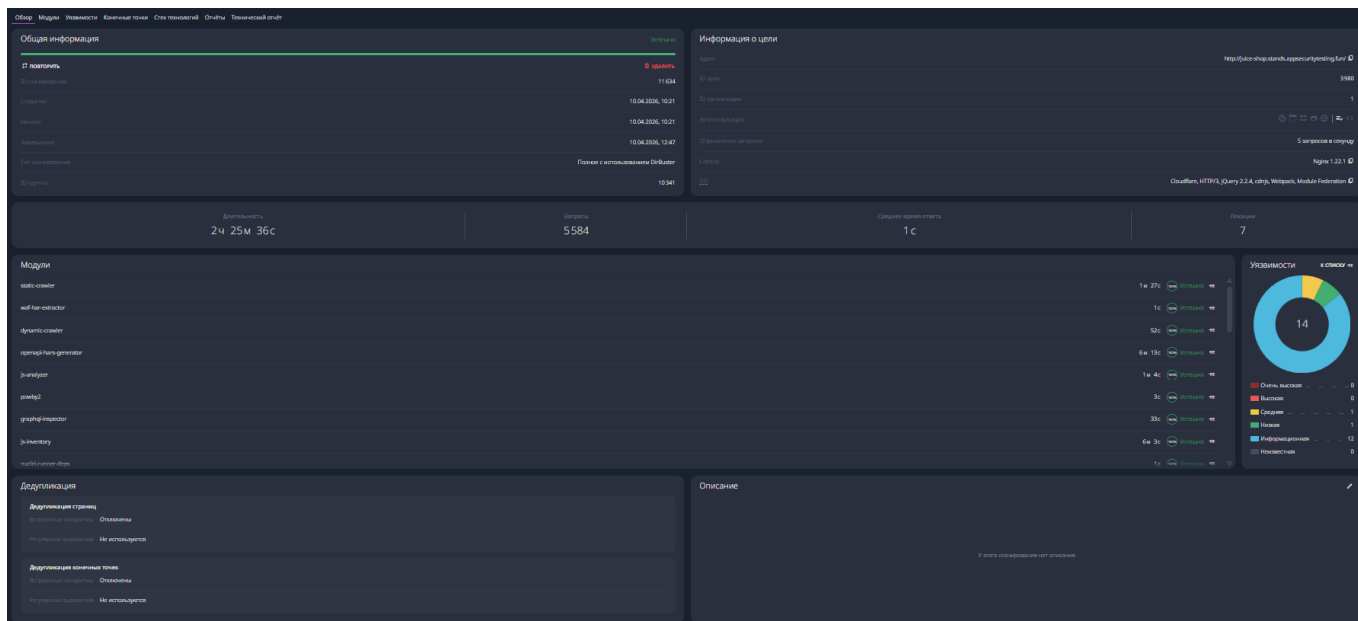


Снимок экрана 29. Контекстное меню выбранной цели

5.2.1. Подробная информация о сканировании

О любом сканировании из списка можно просмотреть подробную информацию. Для этого следует нажать на адрес выбранной цели или пункт «Просмотр» контекстного меню (см. снимок экрана 29).

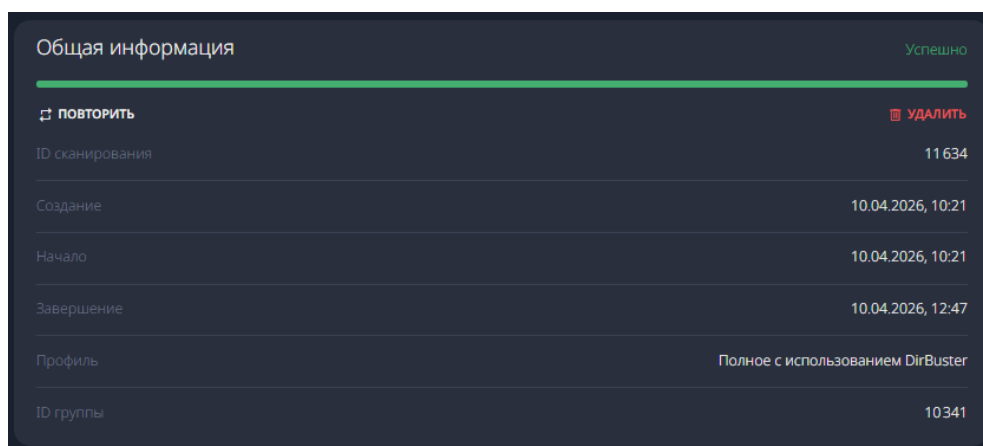
В открывшемся окне детализация сканирования представлена в семи информационных секторах: «Общая информация», «Информация о цели», сектор со статистикой о сканировании, «Модули», «Уязвимости», «Дедупликация» и «Описание» (см. снимок экрана 30).



Снимок экрана 30. Окно подробной информации о сканировании выбранной цели

В секторе «Общая информация» содержатся следующие данные (см. снимок экрана 31):

- ID сканирования;
- дата создания сканирования;
- дата и время начала сканирования;
- дата и время завершения сканирования;
- Профиль;
- ID группы.

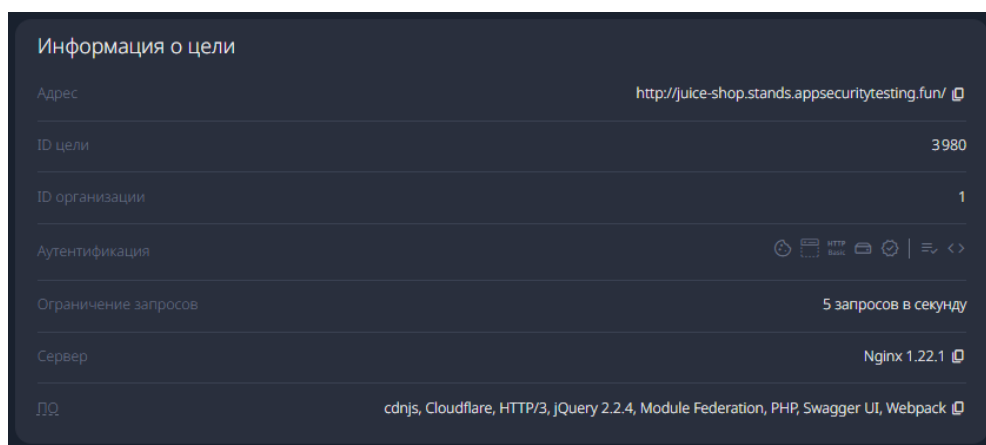


Снимок экрана 31. Сектор «Общая информация» заверщенного сканирования

В данном секторе при статусах «Успешно», «Отменено», и «Ошибка» сканирование можно удалить, нажав соответствующую кнопку в правом верхнем углу. При статусе «Приостановлено» сканирование можно возобновить или прервать. Более подробную информацию о возобновлении и прерывании сканирования см. в подразделе 7.3 «Управление сканированием».

В секторе «Информация о цели» содержатся следующие данные (см. снимок экрана 32):

- адрес цели (доступно копирование по нажатию на иконку );
- ID цели;
- ID организации;
- Аутентификация;
- Ограничение запросов;
- Сервер (доступно копирование по нажатию на иконку );
- ОС (доступно копирование по нажатию на иконку );
- ПО (доступно копирование по нажатию на иконку ).



Снимок экрана 32. Сектор «Информация о цели»

Сектор со статистикой о сканировании содержит данные о (см. снимок экрана 33):

- общей продолжительности сканирования;
- общем количестве запросов;
- среднем времени ответа;
- общем количестве локаций.

Продолжительность	Запросы	Среднее время ответа	Локации
19м 53с	239213	71 мс	64

Снимок экрана 33. Сектор «Статистика»

В секторе «Модули» представлен список задействованных при сканировании цели модулей с информацией об их названии, длительности работы и статусе сканирования (см. снимок экрана 34).

Модули		
static-crawler	1 м 27 с	100% Успешно ➔
waf-har-extractor	1 с	100% Успешно ➔
dynamic-crawler	54 с	100% Успешно ➔
openapi-hars-generator	6 м 17 с	100% Успешно ➔
js-analyzer	1 м 5 с	100% Успешно ➔

Снимок экрана 34. Сектор «Модули»

В данном секторе можно просмотреть записи журналов модулей сканирования, завершивших работу. Для этого следует нажать кнопку просмотра «➔», расположенную в конце строки информации о модуле. Откроется окно просмотра записей журнала выбранного модуля, по умолчанию на вкладке «Стандартный».

Журнал модуля **static-crawler**
Стандартный | Лог HTTP | Проверка аутентификации

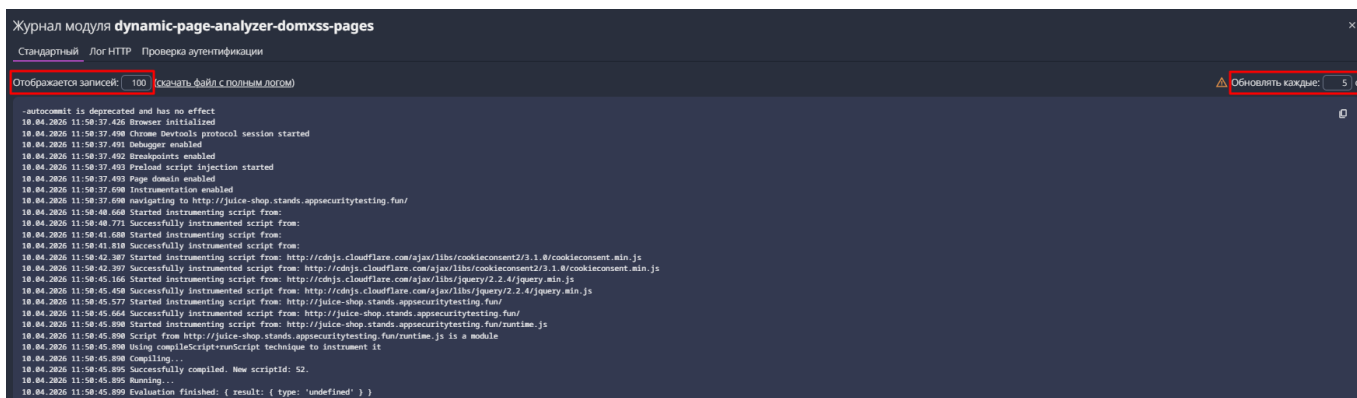
Отображается записей: 1 024 (скачать файл с полным логом)

2026-03-17T12:05:45:440+0300	[364MINFO] [m	Using proxy server	("url": "http://127.0.0.1:59001")	
2026-03-17T12:05:45:440+0300	[364MINFO] [m	Starting crawling	("base_url": "http://juice-shop-stands.appsecuritestesting.fun/", "scan_id": 11278)	
2026-03-17T12:05:46:053+0300	[364MINFO] [m	crawler fetched URL	("base_url": "http://juice-shop-stands.appsecuritestesting.fun/", "scan_id": 11278, "url": "http://juice-shop-stands.appsecuritestesting.fun/", "original_url": "http://juice-shop-stands.appsecuritestesting.fun/", "parent": {"name": "http://juice-shop-stands.appsecuritestesting.fun/", "type": "css", "content_type": "text/css; charset=utf-8", "size": 4065}, "status_code": 0, "retries_attempted": 0})	
2026-03-17T12:05:46:212+0300	[364MINFO] [m	crawler fetched URL	("base_url": "http://juice-shop-stands.appsecuritestesting.fun/", "scan_id": 11278, "url": "http://cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.css", "original_url": "http://cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.css", "parent": {"name": "http://juice-shop-stands.appsecuritestesting.fun/", "type": "css", "content_type": "text/css; charset=utf-8", "size": 28868}, "status_code": 0, "retries_attempted": 0})	
2026-03-17T12:05:47:303+0300	[364MINFO] [m	crawler fetched URL	("base_url": "http://juice-shop-stands.appsecuritestesting.fun/", "scan_id": 11278, "url": "http://cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js", "original_url": "http://cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js", "parent": {"name": "http://juice-shop-stands.appsecuritestesting.fun/", "type": "javascript", "content_type": "application/javascript; charset=utf-8", "size": 85578}, "status_code": 0, "retries_attempted": 0})	
2026-03-17T12:05:47:775+0300	[364MINFO] [m	crawler fetched URL	("base_url": "http://juice-shop-stands.appsecuritestesting.fun/", "scan_id": 11278, "url": "http://juice-shop-stands.appsecuritestesting.fun/runtime.js", "original_url": "http://juice-shop-stands.appsecuritestesting.fun/runtime.js", "parent": {"name": "http://juice-shop-stands.appsecuritestesting.fun/", "type": "javascript", "content_type": "application/javascript; charset=utf-8", "size": 2358}, "status_code": 0, "retries_attempted": 0})	
2026-03-17T12:05:56:171+0300	[336MWARN] [m	crawler onError called	("base_url": "http://juice-shop-stands.appsecuritestesting.fun/", "scan_id": 11278, "error": "context deadline exceeded (Client.Timeout or context cancellation while reading body)", "url": "http://juice-shop-stands.appsecuritestesting.fun/styles.css", "status_code": 0, "retries_attempted": 0})	
2026-03-17T12:05:56:171+0300	[364MINFO] [m	crawler will retry after delay	("base_url": "http://juice-shop-stands.appsecuritestesting.fun/", "scan_id": 11278, "delay": "5s", "url": "http://juice-shop-stands.appsecuritestesting.fun/styles.css")	
2026-03-17T12:05:56:171+0300	[336MWARN] [m	crawler onError called	("base_url": "http://juice-shop-stands.appsecuritestesting.fun/", "scan_id": 11278, "error": "context deadline exceeded (Client.Timeout or context cancellation while reading body)", "url": "http://juice-shop-stands.appsecuritestesting.fun/vendor.js", "status_code": 0, "retries_attempted": 0})	
2026-03-17T12:05:56:171+0300	[364MINFO] [m	crawler will retry after delay	("base_url": "http://juice-shop-stands.appsecuritestesting.fun/", "scan_id": 11278, "delay": "5s", "url": "http://juice-shop-stands.appsecuritestesting.fun/vendor.js")	
2026-03-17T12:05:56:171+0300	[336MWARN] [m	crawler onError called	("base_url": "http://juice-shop-stands.appsecuritestesting.fun/", "scan_id": 11278, "error": "context deadline exceeded (Client.Timeout or context cancellation while reading body)", "url": "http://juice-shop-stands.appsecuritestesting.fun/main.js", "status_code": 0, "retries_attempted": 1})	
2026-03-17T12:05:56:171+0300	[364MINFO] [m	crawler will retry after delay	("base_url": "http://juice-shop-stands.appsecuritestesting.fun/", "scan_id": 11278, "delay": "5s", "url": "http://juice-shop-stands.appsecuritestesting.fun/main.js")	
2026-03-17T12:05:56:171+0300	[336MWARN] [m	crawler onError called	("base_url": "http://juice-shop-stands.appsecuritestesting.fun/", "scan_id": 11278, "error": "context deadline exceeded (Client.Timeout or context cancellation while reading body)", "url": "http://juice-shop-stands.appsecuritestesting.fun/vendor.js", "status_code": 0, "retries_attempted": 1})	
2026-03-17T12:05:56:171+0300	[364MINFO] [m	crawler will retry after delay	("base_url": "http://juice-shop-stands.appsecuritestesting.fun/", "scan_id": 11278, "delay": "5s", "url": "http://juice-shop-stands.appsecuritestesting.fun/vendor.js")	
2026-03-17T12:05:56:171+0300	[336MWARN] [m	crawler onError called	("base_url": "http://juice-shop-stands.appsecuritestesting.fun/", "scan_id": 11278, "error": "context deadline exceeded (Client.Timeout or context cancellation while reading body)", "url": "http://juice-shop-stands.appsecuritestesting.fun/main.js", "status_code": 0, "retries_attempted": 1})	
2026-03-17T12:05:56:171+0300	[364MINFO] [m	crawler will retry after delay	("base_url": "http://juice-shop-stands.appsecuritestesting.fun/", "scan_id": 11278, "delay": "5s", "url": "http://juice-shop-stands.appsecuritestesting.fun/main.js")	
2026-03-17T12:05:56:171+0300	[336MWARN] [m	crawler onError called	("base_url": "http://juice-shop-stands.appsecuritestesting.fun/", "scan_id": 11278, "error": "context deadline exceeded (Client.Timeout or context cancellation while reading body)", "url": "http://juice-shop-stands.appsecuritestesting.fun/main.js", "status_code": 0, "retries_attempted": 2})	
2026-03-17T12:05:56:171+0300	[364MINFO] [m	crawler will retry after delay	("base_url": "http://juice-shop-stands.appsecuritestesting.fun/", "scan_id": 11278, "delay": "5s", "url": "http://juice-shop-stands.appsecuritestesting.fun/main.js")	
2026-03-17T12:05:56:171+0300	[336MWARN] [m	crawler onError called	("base_url": "http://juice-shop-stands.appsecuritestesting.fun/", "scan_id": 11278, "error": "context deadline exceeded (Client.Timeout or context cancellation while reading body)", "url": "http://juice-shop-stands.appsecuritestesting.fun/main.js", "status_code": 0, "retries_attempted": 2})	
2026-03-17T12:05:56:171+0300	[364MINFO] [m	crawler will retry after delay	("base_url": "http://juice-shop-stands.appsecuritestesting.fun/", "scan_id": 11278, "delay": "5s", "url": "http://juice-shop-stands.appsecuritestesting.fun/main.js")	
2026-03-17T12:05:56:171+0300	[336MWARN] [m	crawler onError called	("base_url": "http://juice-shop-stands.appsecuritestesting.fun/", "scan_id": 11278, "error": "context deadline exceeded (Client.Timeout or context cancellation while reading body)", "url": "http://juice-shop-stands.appsecuritestesting.fun/main.js", "status_code": 0, "retries_attempted": 2})	

Снимок экрана 35. Журнал модуля

Помимо стандартного типа записи журнала, данное окно содержит вкладки «Лог HTTP» и «Проверка аутентификации» с соответствующей информацией. Доступно скачивание записей журнала по ссылке, расположенной строкой ниже меню выбора вкладок — файл с данными в формате «.ndjson» будет загружен в локальное хранилище. Также есть возможность скопировать записи в буфер обмена, нажав кнопку копирования «□», расположенную в правой верхней части окна.

Для модулей, не завершивших работу (статус «В процессе»), на вкладке «Стандартный» можно изменять параметры запроса: максимальное число одновременно отображаемых записей журнала и частоту запросов. По умолчанию установлено отображение 100 записей с обновлением раз в 5 секунд — уменьшение частоты запросов может снизить производительность (см. снимок экрана 36).



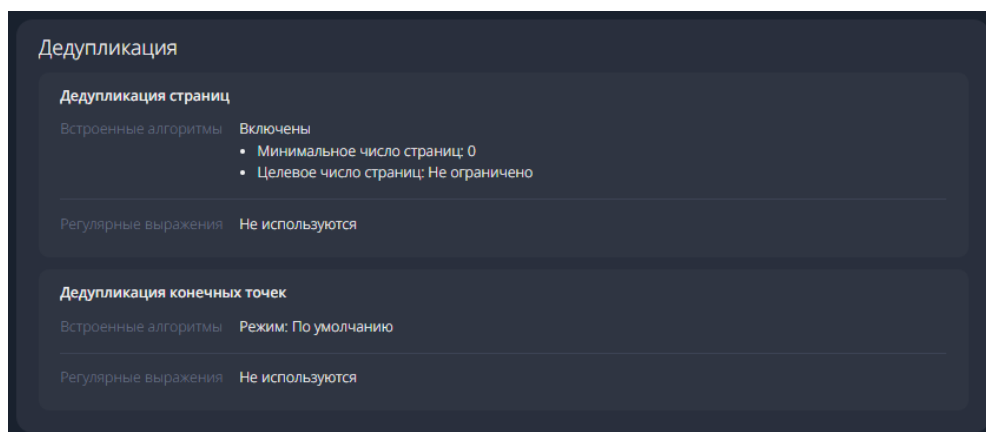
Снимок экрана 36. Параметры запроса модуля, не завершившего работу

В секторе «Уязвимости» содержатся данные о количестве выявленных уязвимостей, отображённые по уровню критичности списком и круговой диаграммой (см. снимок экрана 37).



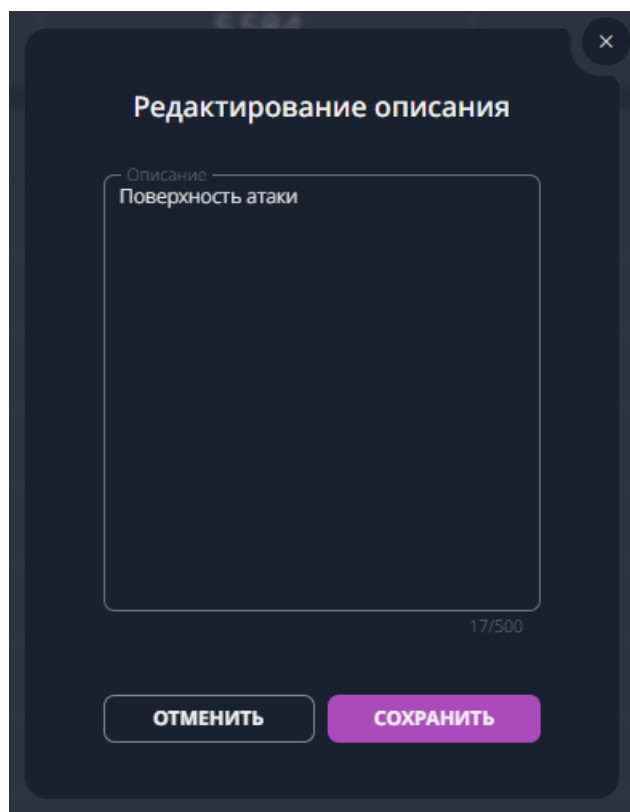
Снимок экрана 37. Сектор «Уязвимости»

В секторе «Дедупликация» отображается сводная информация о параметрах дедупликации (см. снимок экрана 38).



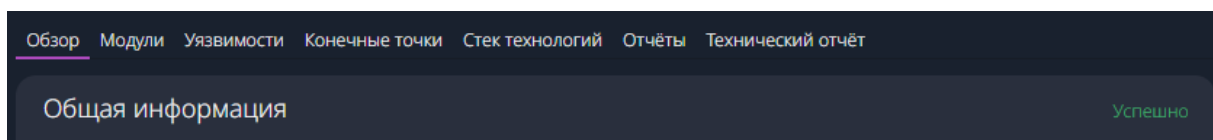
Снимок экрана 38. Сектор «Дедупликация»

Сектор «Описание» содержит описание данного сканирования, добавленное при создании сканирования на вкладке «Дополнительная информация» в мастере создания нового сканирования (см. подраздел 7.1 «Создание сканирования», п. 3). Кнопка редактирования, расположенная в правом верхнем углу сектора, позволяет добавить или изменить описание в окне «Редактирование описания», после чего следует нажать кнопку «ПРИМЕНИТЬ» (см. снимок экрана 39).



Снимок экрана 39. Окно «Редактирование описания»

Окно подробной информации о сканировании цели содержит вкладки «Обзор» (открывается по умолчанию), «Модули», «Уязвимости» (активна после завершения сканирования), «Конечные точки» (активна после завершения сканирования), «Стек технологий», «Экспериментальные данные», «Дедупликация», «Технический отчет» и «Отчёты», расположенные над сектором «Общая информация» (см. снимок экрана 40).



Снимок экрана 40. Вкладки «Обзор», «Модули», «Уязвимости», «Конечные точки», «Стек технологий», «Отчёты» и «Технический отчет» над сектором «Общая информация»

Отображение вкладок регулируется определенными условиями и может отличаться для разных сканирований: чтобы страница детализации была максимально информативной, пустые вкладки для завершённых сканирований скрываются, а для незавершённых остаются неактивными до момента появления в них данных. В таблице 15 представлены условия доступности и отображения вкладок.

Таблица 15. Условия доступности и отображения вкладок

Вкладка	Условие	Для незавершенных сканирований	Для завершённых сканирований	Комментарий
Обзор	Не задано	Доступна	Доступна	Вкладка по умолчанию
Модули	Не задано	Доступна	Доступна	–
Уязвимости	Уязвимости не найдены	Недоступна	Скрыта	–
	Уязвимости найдены	Доступна	Доступна	–
Конечные точки	Конечные точки не найдены	Недоступна	Скрыта	–
	Конечные точки найдены	Доступна	Доступна	–
Стек технологий	Не участвует модуль пассивного сигнатурного анализа Rowby2	Скрыта	Скрыта	Без данного модуля технологии цели не могут быть обнаружены
	Участвует пассивного сигнатурного анализа модуль Rowby2 и технологии не обнаружены	Недоступна	Скрыта	
	Участвует пассивного сигнатурного анализа модуль Rowby2 и технологии обнаружены	Доступна	Доступна	

Вкладка	Условие	Для незавершенных сканирований	Для завершенных сканирований	Комментарий
Экспериментальные параметры	Экспериментальные параметры не заданы	Скрыта	Скрыта	–
	Экспериментальные параметры заданы	Доступна	Доступна	–
Дедупликация	Параметры дедупликации не заданы	Скрыта	Скрыта	–
	Параметры дедупликации заданы	Доступна	Доступна	–
Отчёты	Уязвимости не найдены	Недоступна	Скрыта	PDF-отчеты можно генерировать только для сканирований, в которых найдены уязвимости
	Уязвимости найдены	Доступна	Доступна	
Технический отчет	Локаци не найдены	Недоступна	Скрыта	–
	Локации найдены	Доступна	Доступна	

Подробную информацию о конечных точках и техническом отчете см. в подразделе 5.2.2 «Отчеты».

На вкладке «Стек технологий» в табличном виде отображается информация о технологическом стеке, выявленном при сканировании цели, с указанием технологии, ее типа и категории, достоверности распознавания, URL и расположенной вне сканируемой цели внешней технологии, если она была обнаружена (см. снимок экрана 41).

Обзор	Уязвимости	HTTP endpoints	Стек технологий	Отчёты	Технический отчёт
Технология	Тип	Категории	Достоверность	URL	Внешняя ⓘ
Ubuntu	Операционная система	os	Высокая	http://juice-shop.stands.fuchsia/profile	
Nginx 1.18.0	Сервер	web-servers, reverse-proxies	Высокая	http://juice-shop.stands.fuchsia/profile	

Снимок экрана 41. Вкладка «Стек технологий»

Детальную информацию о выявленных уязвимостях можно просмотреть, перейдя на вкладку «Уязвимости» или нажав в секторе «Уязвимости» кнопку «К СПИСКУ». Откроется окно «Уязвимости», в котором представлен список уязвимостей в табличном виде с указанием (см. снимок экрана 42):

- типа уязвимости;
- URL;
- модуля обнаружения;
- селектора;
- уровнем достоверности;

- отметки (см. описание ниже).

Уязвимость	URL	Модуль	Селекторы	Достоверность	Отметка
☐ SQL Injection	http://bricks.stands.appsecuritytesting.fun/content-2/ind...	sql-franziscanner	value-querySt...	Средняя	Открыта
☐ SQL Injection	http://bricks.stands.appsecuritytesting.fun/content-1/ind...	sql-franziscanner	value-query... (3)	Средняя	Открыта
☐ SQL Injection	http://bricks.stands.appsecuritytesting.fun/content-1/ind...	SQL injection scann...	value-query... (2)	Высокая	Открыта
☐ SQL Injection	http://bricks.stands.appsecuritytesting.fun/content-2/ind...	SQL injection scann...	value-querySt...	Высокая	Открыта
☐ Reflected Cross Site Scripting (XSS)	http://bricks.stands.appsecuritytesting.fun/content-2/ind...	Reflected XSS Scan...	value-query... (6)	Высокая	Открыта
☐ Reflected Cross Site Scripting (XSS)	http://bricks.stands.appsecuritytesting.fun/content-1/ind...	Reflected XSS Scan...	value-query... (6)	Высокая	Открыта
☐ Git Configuration - Detect	http://bricks.stands.appsecuritytesting.fun/	Active Signature Sc...	unknown	Высокая	Открыта
☐ OpenSSH.Terrapin Attack - Detection	bricks.stands.appsecuritytesting.fun:22	Active Signature Sc...	unknown	Высокая	Открыта
☐ CAA Record	http://bricks.stands.appsecuritytesting.fun/	Active Signature Sc...	unknown	Высокая	Открыта
☐ WAF Detection	http://bricks.stands.appsecuritytesting.fun/	Active Signature Sc...	unknown	Высокая	Открыта
☐ HTTP Missing Security Headers	http://bricks.stands.appsecuritytesting.fun/	Active Signature Sc...	unknown	Высокая	Открыта
☐ OpenSSH Service - Detect	bricks.stands.appsecuritytesting.fun:22	Active Signature Sc...	unknown	Высокая	Открыта
☐ SSH Server Software Enumeration	bricks.stands.appsecuritytesting.fun:22	Active Signature Sc...	unknown	Высокая	Открыта
☐ Wappalizer Technology Detection	http://bricks.stands.appsecuritytesting.fun/	Active Signature Sc...	unknown	Высокая	Открыта
☐ HTTP Missing Security Headers	http://bricks.stands.appsecuritytesting.fun/	Active Signature Sc...	unknown	Высокая	Открыта
☐ HTTP Missing Security Headers	http://bricks.stands.appsecuritytesting.fun/	Active Signature Sc...	unknown	Высокая	Открыта

Снимок экрана 42. Окно «Уязвимости»

Для отображения списка с уязвимостями нужной степени критичности следует воспользоваться кнопкой «ФИЛЬТРЫ», расположенной в верхнем правом углу. В открывшемся окне необходимо включить нужные чекбоксы и нажать внизу кнопку «ПРИМЕНИТЬ» (см. снимок экрана 43).

Фильтры

Критичность ✓

☒ Очень высокая

☒ Высокая

☒ Средняя

☐ Низкая

☐ Информационная

☐ Неизвестная

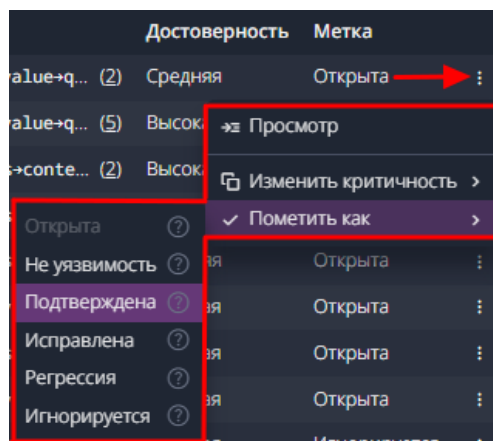
ОЧИСТИТЬ ВСЁ

ОТМЕНИТЬ ПРИМЕНИТЬ

Снимок экрана 43. Окно «Фильтры»

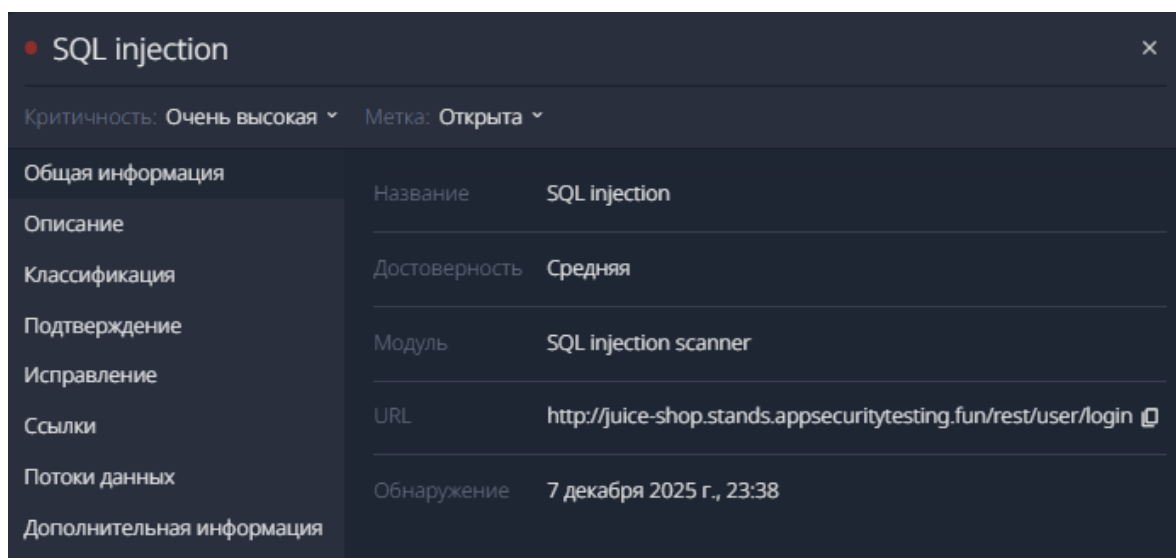
Обнаруженной уязвимости можно уточнить статус, установив ей соответствующую метку. Для этого следует в конце строки с записью об уязвимости нажать на кнопку «:» и в раскрывающемся списке выбрать соответствующую метку (см. снимок экрана 44):

- Не уязвимость — не является уязвимостью и будет игнорироваться при последующих сканированиях цели.
- Подтверждена — подтвержденная уязвимость, которая требует сканирований.
- Исправлена — уязвимость исправлена, и ее появление в новых сканированиях не ожидается.
- Регрессия — вновь найденная уязвимость, ранее помеченная исправленной.
- Игнорируется — подтвержденная уязвимость, не требующая исправления; уязвимости с такой меткой не учитываются при последующих сканированиях цели.



Снимок экрана 44. Выбор метки для найденной уязвимости

В окне «Уязвимости» можно просмотреть подробную информацию о каждой найденной уязвимости. Для этого следует нажать на интересующую уязвимость или выбрать пункт меню «Просмотр» (см. снимок экрана 44). В правой части экрана появится всплывающее окно с названием выбранной уязвимости (см. снимок экрана 45).



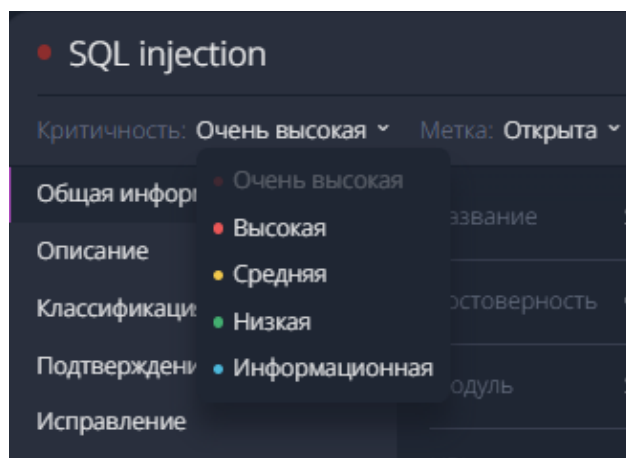
Снимок экрана 45. Окно подробной информации о выбранной уязвимости

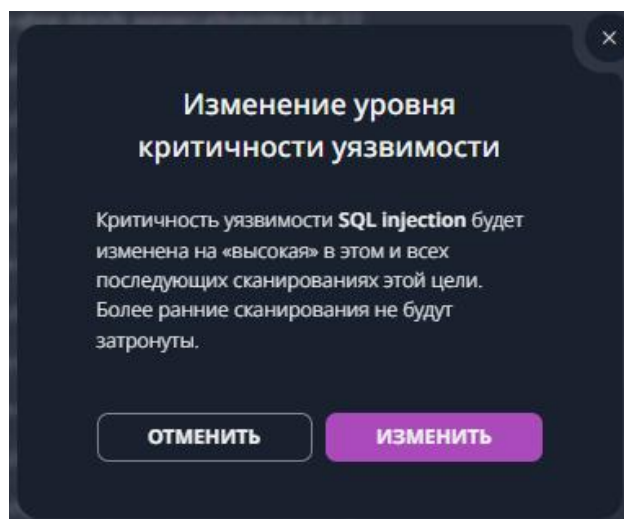
Окно подробной информации содержит семь вкладок, описание которых представлено в таблице 16.

Таблица 16. Вкладки окна подробной информации об уязвимости

Вкладка	Описание
Общая информация	Содержит сведения о: – названии уязвимости; – уровне достоверности; – модуле, обнаружившем уязвимость; – URL
Описание	Описание выявленной уязвимости, рекомендации по ее устранению, а также последствия, если данную уязвимость не устранить
Классификация	Классификация выявленной уязвимости по трем стандартам: – CVE — идентификационный номер уязвимости согласно базе данных уязвимостей CVE; – CWE — класс уязвимости; – CVSS — числовая оценка, показывающая потенциальную серьёзность уязвимости от 0 до 10, где 10 выражает максимальную опасность. Оценка определяется на основании ряда метрик: базовой, временной и метрики окружения
Подтверждение	Описание селектора, вектора атаки, отправленного запроса и полученного ответа
Исправление	Общие рекомендации по устранению уязвимости
Ссылки	Ссылки на описание выявленных уязвимостей
Потоки данных	Часть клиентского JS-кода с потенциальной уязвимостью
Дополнительная информация	Дополнительная информация о найденной уязвимости

Также в данном окне в соответствующих раскрывающихся списках можно поменять метку (см. пункты меню на снимке экрана 45) и уровень критичности (см. снимок экрана 46), подтвердив выбор в окне «Изменение уровня критичности уязвимости» (см. снимок экрана 47).

**Снимок экрана 46.** Меню выбора уровня критичности



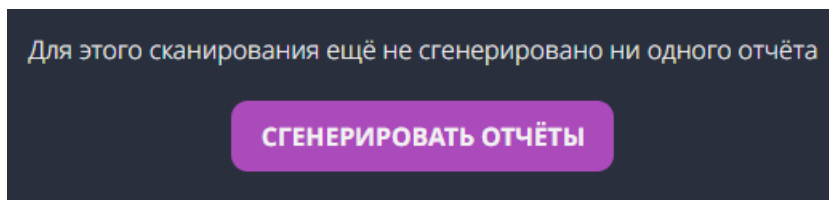
Снимок экрана 47. Окно «Изменение уровня критичности уязвимости»

5.2.2. Отчеты

Сканер SolidPoint DAST позволяет сгенерировать полный или краткий отчет о сканировании в формате PDF на русском, английском, португальском, турецком и упрощенном китайском языке.

Для генерации отчета необходимо:

1. Перейти на вкладку «Отчёты», расположенную над сектором «Общая информация» в окне подробной информации о сканировании (см. снимок экрана 40).
2. Нажать кнопку «СГЕНЕРИРОВАТЬ ОТЧЁТЫ» (кнопка становится активной после завершения сканирования, см. снимок экрана 48). При уже созданных отчетах кнопка «СГЕНЕРИРОВАТЬ ОТЧЁТЫ» расположена в правой части экрана (см. снимок экрана 51).

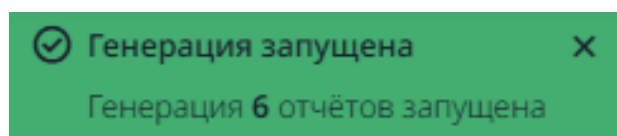


Снимок экрана 48. Кнопка «СГЕНЕРИРОВАТЬ ОТЧЁТЫ»

3. В открывшемся окне «Генерация отчётов» в выпадающих списках выбрать тип и язык отчета. При необходимости генерации нескольких отчетов следует нажать кнопку «Добавить». Если нужно удалить какой-либо отчет из списка на генерацию, следует нажать иконку  » (см. снимок экрана 49).

Снимок экрана 49. Окно «Генерация отчетов»

4. После установки параметров нажать кнопку «СГЕНЕРИРОВАТЬ». В правой нижней части экрана появится уведомление о ходе генерации отчетов (см. снимок экрана 50).



Снимок экрана 50. Уведомление о генерации отчетов

После генерации список отчетов отобразится в табличном виде (см. снимок экрана 51).

Тип отчёта	Статус сканирования	Создание	Язык	Размер	Статус отчёта	Скачать
Полный	Успешно	30.03.2026, 15:02	Упрощённый китайский	3.7 Мб	Успешно	📄
Краткий	Успешно	30.03.2026, 15:01	Турецкий (Турция)	669.4 Кб	Успешно	📄
Полный	Успешно	30.03.2026, 15:02	Португальский (Бразилия)	1.8 Мб	Успешно	📄
Полный	Успешно	30.03.2026, 15:02	Английский (США)	1.8 Мб	Успешно	📄
Краткий	Успешно	30.03.2026, 15:02	Русский (Россия)	719.5 Кб	Успешно	📄
Полный	Успешно	30.03.2026, 15:02	Русский (Россия)	1.8 Мб	Успешно	📄

Снимок экрана 51. Сгенерированные отчеты

При нажатии на иконку «📄» в локальное хранилище будет загружен файл в формате PDF. При нажатии на иконку «🗑️» строка записи отчета будет удалена.

Сканер SolidPoint DAST также имеет функциональность просмотра следующих отчетов:

- Конечные точки — отчет о конечных точках веб-приложения.
- Технический отчет — для экспертного анализа уязвимостей и ресурсов, обнаруженных в сканируемом веб-приложении.

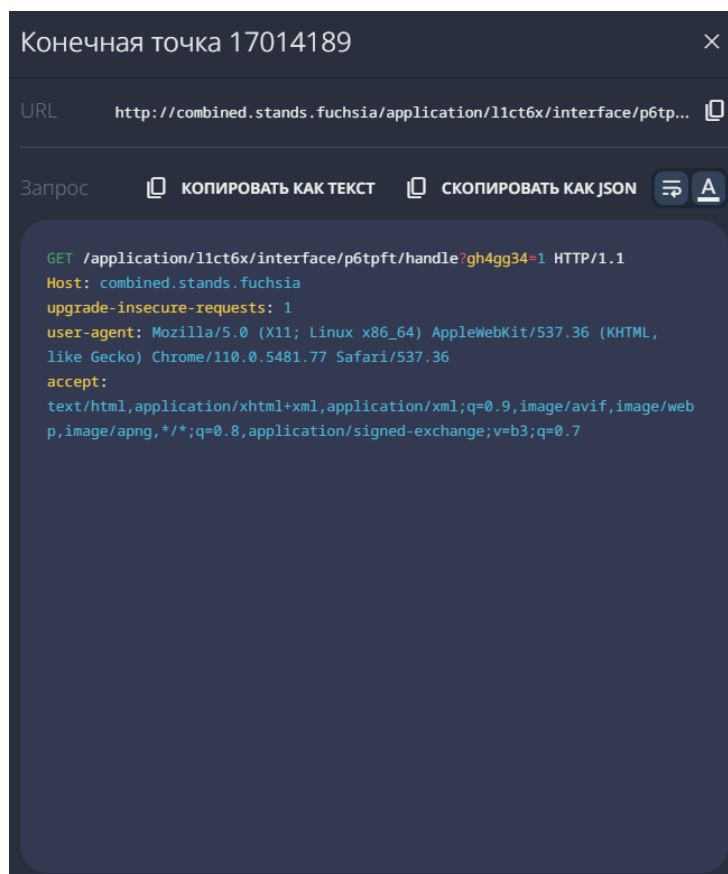
Для просмотра конечных точек и технического отчета необходимо перейти на соответствующие вкладки над сектором «Общая информация» в окне подробной информации о сканировании (см. снимок экрана 40).

На вкладке «Конечные точки» представлен перечень выявленных при сканировании конечных точек и дана краткая информация по каждой из них (см. снимок экрана 52).

Метод	URL	Строка запроса
POST	http://juiceshop.stands.appsecuritest.ru/file-upload	Заголовок: Content-Type: multipart/form-data, Authorization: Bearer UNKNOWN Тело: {"multipart": {"file": "FILE"}}
GET	http://juiceshop.stands.appsecuritest.ru/rest/web3/nftUnlocked	
GET	http://juiceshop.stands.appsecuritest.ru/rest/web3/nftMintList	
GET	http://juiceshop.stands.appsecuritest.ru/api/Challenges/	?key=nftMintChallenge
POST	http://juiceshop.stands.appsecuritest.ru/rest/web3/submitKey	Заголовок: Content-Type: application/json Тело: {"privateKey": "UNKNOWN"}
POST	http://juiceshop.stands.appsecuritest.ru/rest/web3/walletNFTVerify	Заголовок: Content-Type: application/json Тело: {"walletAddress": "UNKNOWN"}
POST	http://juiceshop.stands.appsecuritest.ru/rest/web3/walletExploitAddress	Заголовок: Content-Type: application/json Тело: {"walletAddress": "UNKNOWN"}

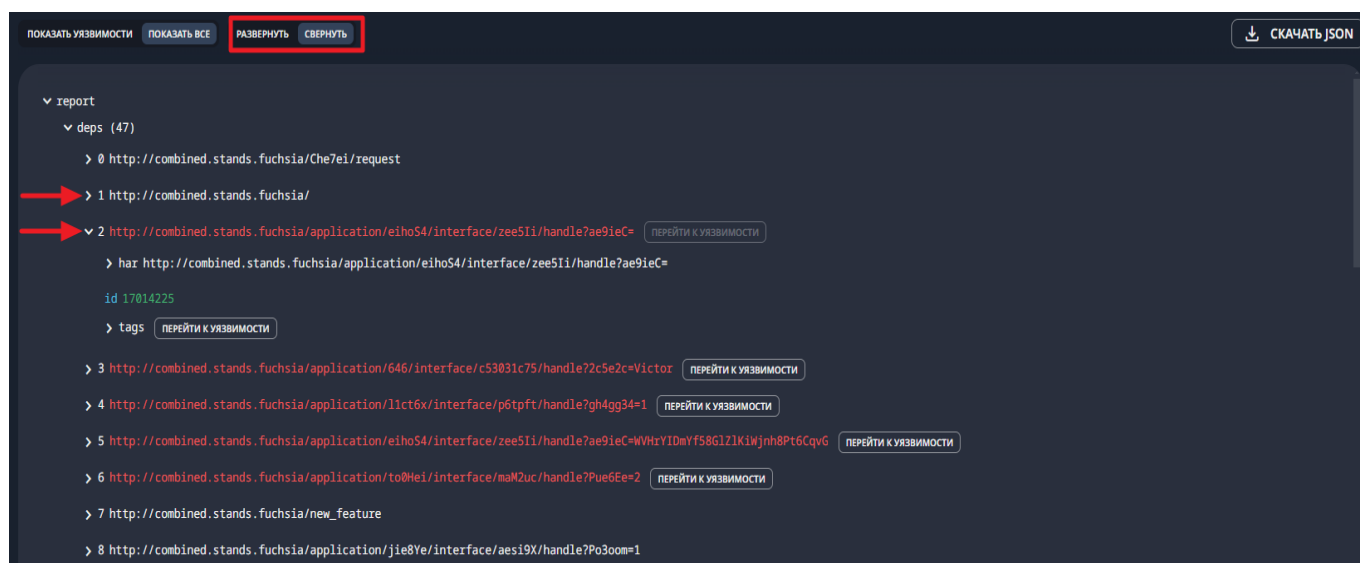
Снимок экрана 52. Вкладка «Конечные точки»

Для просмотра подробной информации о конечной точке необходимо нажать на строку записи. В правой части экрана откроется окно «Конечная точка N», где N – номер конечной точки. В данном окне можно скопировать URL, сведения о конечной точке в виде текста или в формате JSON, а также для удобства просмотра данных воспользоваться кнопками «Перенос строк» и Подсветка кода» (см. снимок экрана 53).



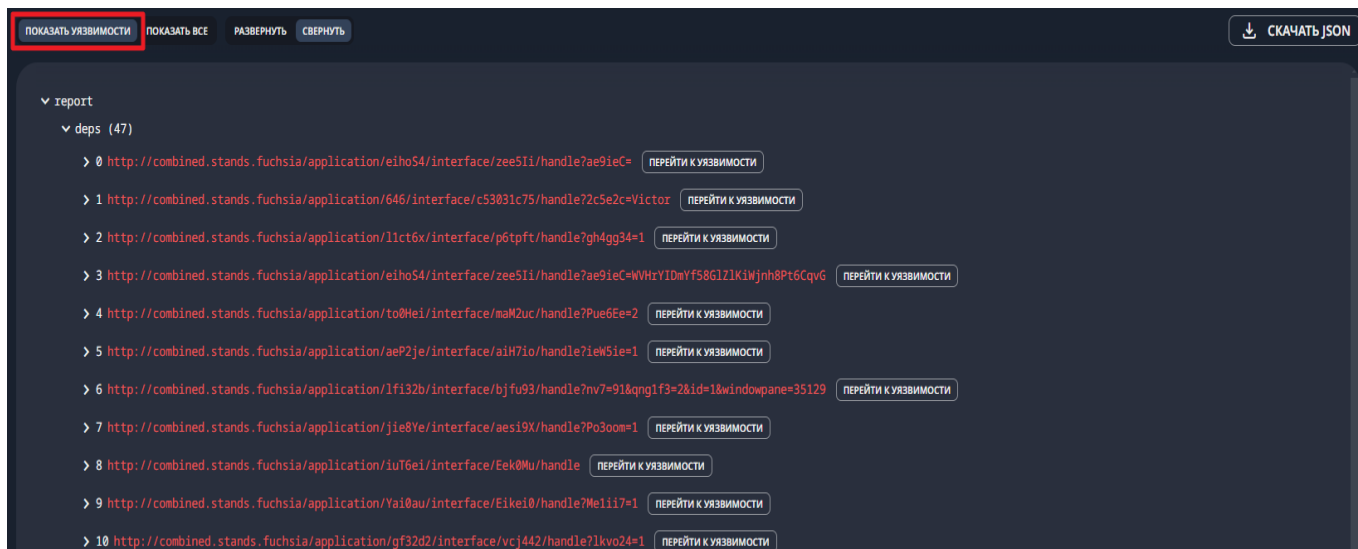
Снимок экрана 53. Окно подробной информации о конечной точке

Технический отчет можно просмотреть, не дожидаясь окончания сканирования. Он скомпонован по ресурсам и точкам входа (deps). Раскрыть и свернуть подробную информацию последовательно можно нажатием на пиктограммы «>» и «▼». Чтобы раскрыть и свернуть подробную информацию сразу полностью следует воспользоваться кнопками «РАЗВЕРНУТЬ» и «СВЕРНУТЬ» (см. снимок экрана 54).



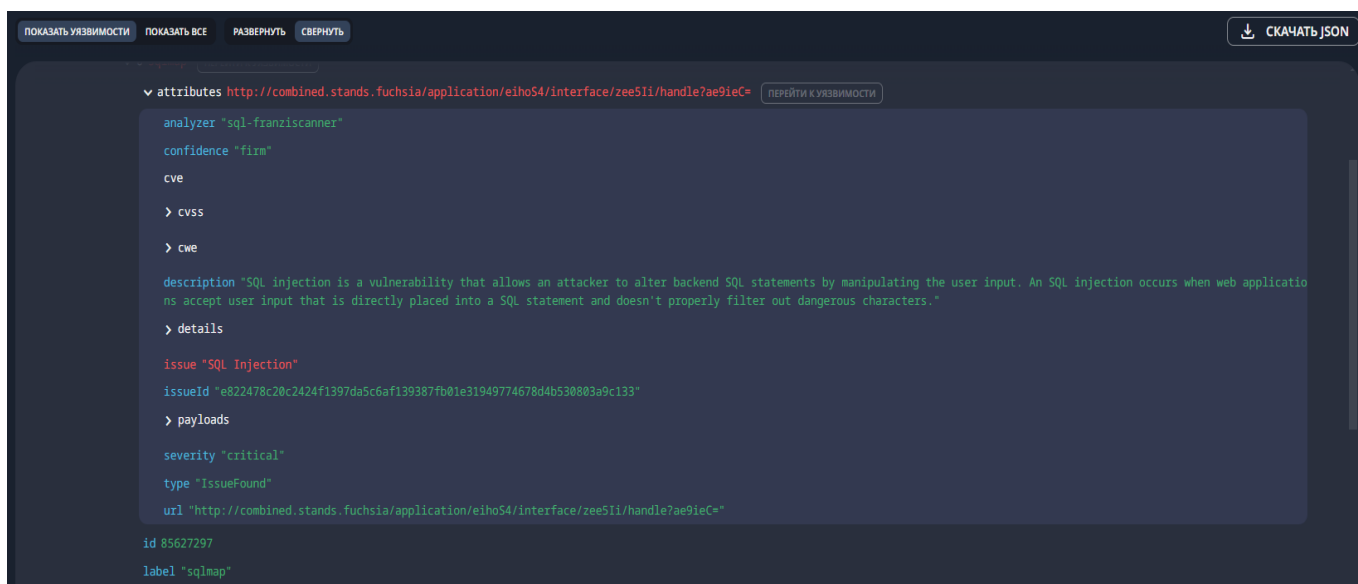
Снимок экрана 54. Окно «Технический отчет»

В этом же окне при нажатии на кнопку «ПОКАЗАТЬ УЯЗВИМОСТИ» отображается список выявленных уязвимостей (см. снимок экрана 55).



Снимок экрана 55. Список только выявленных уязвимостей при нажатии на кнопку «ПОКАЗАТЬ УЯЗВИМОСТИ»

Вне зависимости от положения вышеуказанных кнопок нажатие на кнопку «ПЕРЕЙТИ К УЯЗВИМОСТИ», расположенной в конце адреса ресурса, раскрывает подробную информацию о выявленной уязвимости (см. снимок экрана 56).



Снимок экрана 56. Подробная информация о выявленной уязвимости при нажатии на кнопку «ПЕРЕЙТИ К УЯЗВИМОСТИ»

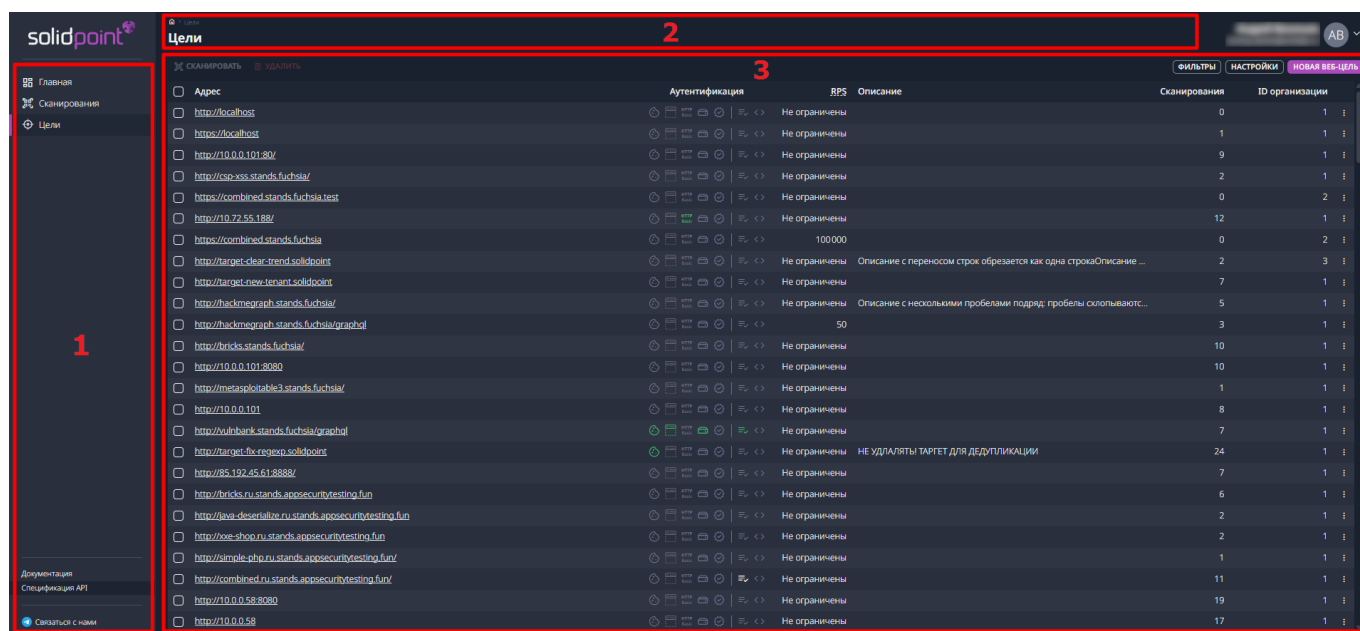
Технический отчет можно скачать в формате «.json». Для этого следует в правом верхнем углу окна нажать кнопку «СКАЧАТЬ JSON» — файл будет загружен в локальное хранилище.

5.3. Окно «Цели»

Окно «Цели» предназначено для создания новой цели сканирования (более подробно см. подраздел 6.1 «Создание цели»), а также управления уже созданными целями.

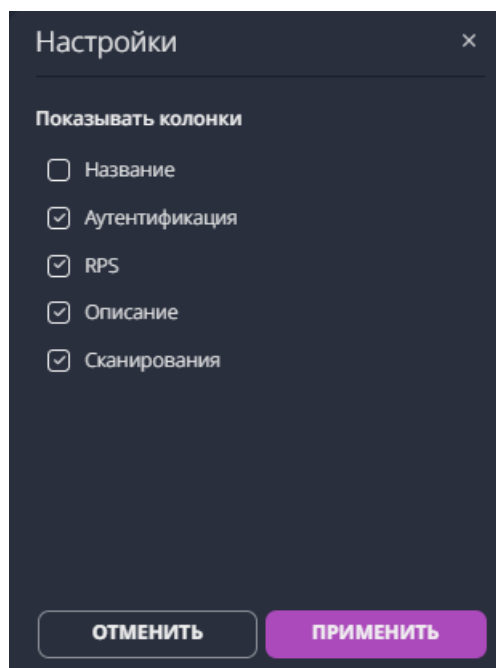
Данное окно содержит три функциональных блока (см. снимок экрана 57):

1. Меню.
2. Заголовок окна с активной иконкой «🏠» в левом верхнем углу для перехода на домашнюю страницу.
3. Список ранее созданных целей в табличном виде с указанием:
 - адреса;
 - типа аутентификации;
 - информации об их ограничениях RPS;
 - описания;
 - количества сканирований цели;
 - ID организации.



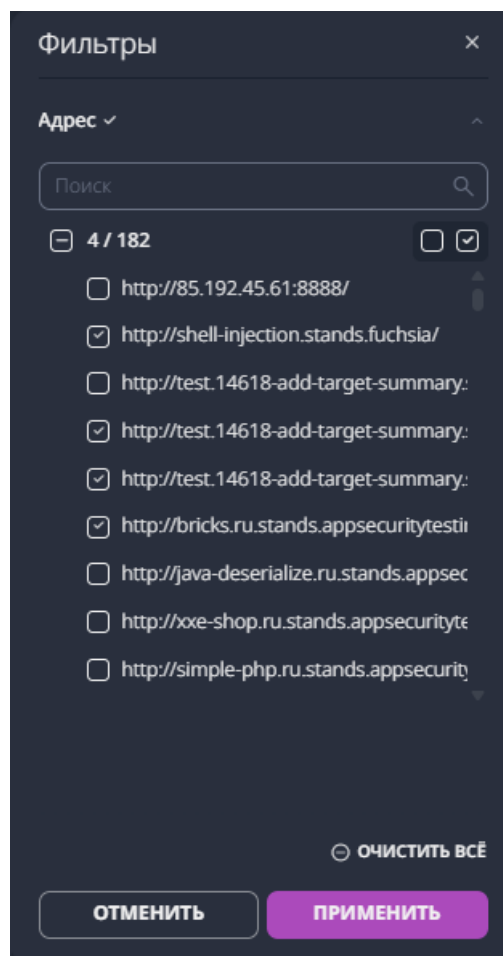
Снимок экрана 57. Окно «Цели»

Для отображения или скрытия колонок можно воспользоваться фильтром, нажав кнопку «Настройки» в правом верхнем углу. В открывшемся окне следует включить/отключить чекбоксы колонок и нажать кнопку «ПРИМЕНИТЬ» (см. снимок экрана 58).



Снимок экрана 58. Фильтр колонок

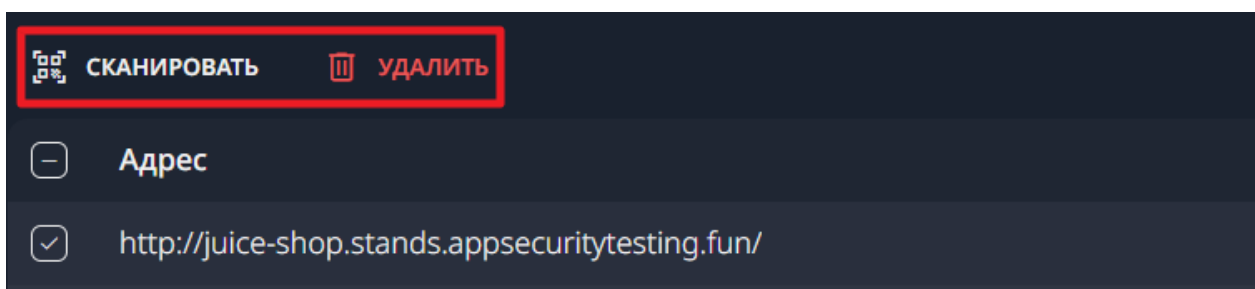
Кнопка «ФИЛЬТРЫ», расположенная в правом верхнем углу, позволяет отфильтровать список целей по адресу. После поиска и включения необходимых чекбоксов следует нажать кнопку «ПРИМЕНИТЬ» (см. снимок экрана 59).



Снимок экрана 59. Фильтр целей

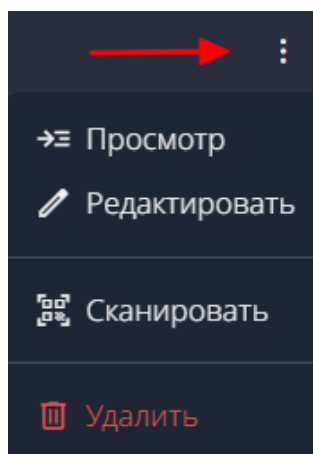
Созданные цели можно сканировать (см. раздел **Ошибка! Источник ссылки не найден.** «Сканирование»), редактировать (см. подраздел 6.3 «Редактирование цели») и удалять (см. подраздел 6.4 «Удаление цели»), а также просмотреть о них подробную информацию (см. подраздел 6.2). Выбрать необходимое действие можно двумя способами:

1. Над списком целей (при включении чекбокса выбранного адреса цели становятся активными кнопки «Сканировать» и «Удалить» (см. снимок экрана 60). Можно выбрать сразу несколько целей.



Снимок экрана 60. Активные кнопки действий при включенном чекбоксе выбранного адреса цели

2. В конце строки адреса цели в контекстном меню, раскрывающимся при нажатии на кнопку «⋮» (см. **Ошибка! Источник ссылки не найден.**).



Снимок экрана 61. Контекстное меню выбранного адреса цели

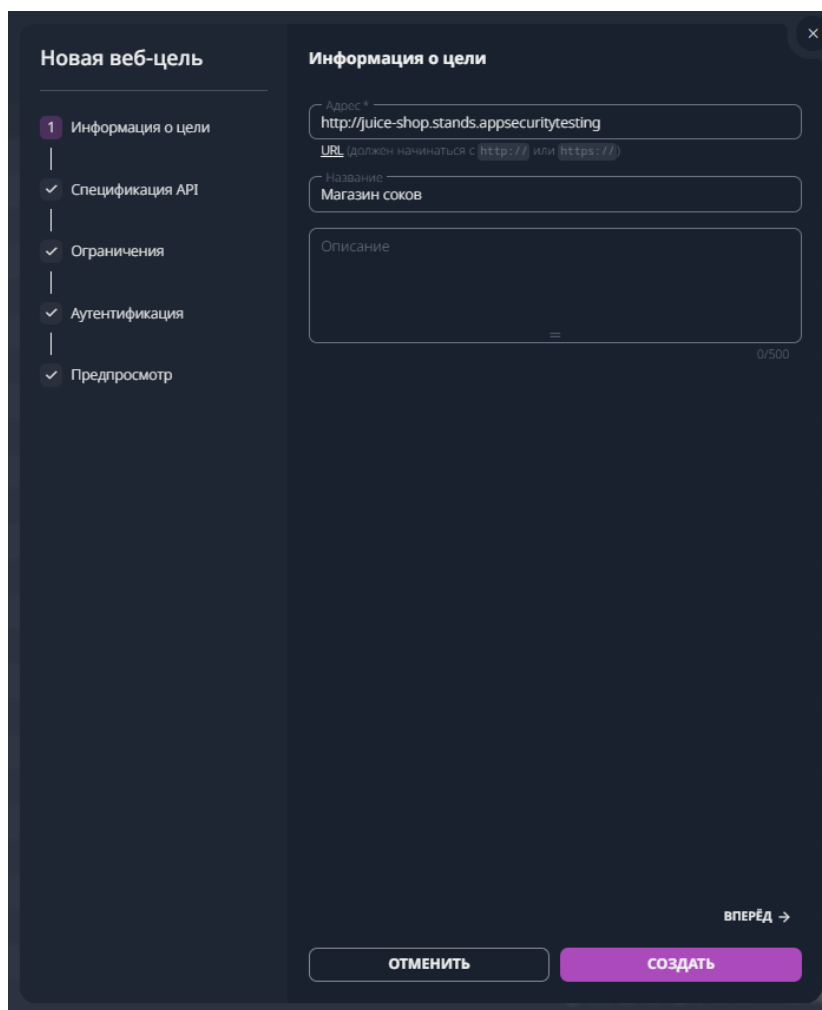
6. ЦЕЛЬ

Цель — это сканируемое приложение с известным URL-адресом и набором заданных настроек.

6.1. Создание цели

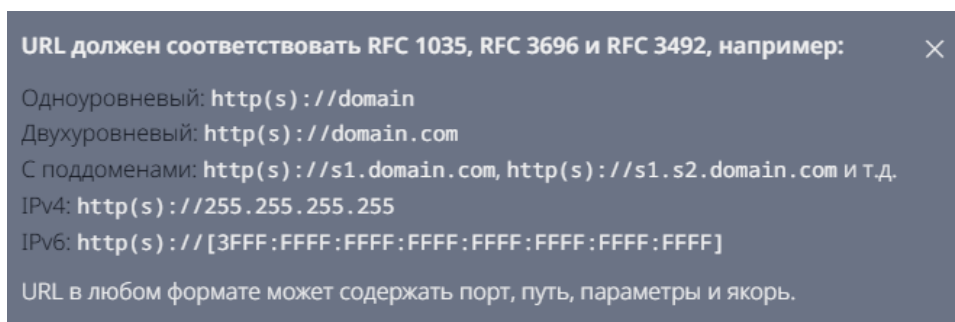
Создание цели сканирования состоит из следующих шагов:

1. В окне «Цели» необходимо нажать кнопку «Новая веб-цель», расположенную в правом верхнем углу (см. снимок экрана 57). Откроется форма «Новая веб-цель» для заполнения данных о цели сканирования.
2. На вкладке «Информация о цели» требуется заполнить обязательное поле «Адрес» (см. снимок экрана 62).

The screenshot shows a dark-themed web application window titled 'Новая веб-цель' (New web target). On the left is a sidebar with a list of tabs: '1 Информация о цели' (1 Target information), '✓ Спецификация API' (API Specification), '✓ Ограничения' (Constraints), '✓ Аутентификация' (Authentication), and '✓ Предпросмотр' (Preview). The main area is titled 'Информация о цели' (Target information) and contains several input fields: 'Адрес *' (Address *) with the value 'http://juice-shop.stands.appsecuritytesting', a note 'URL должен начинаться с http:// или https://', 'Название' (Name) with the value 'Магазин соков' (Juice shop), and a large 'Описание' (Description) text area. At the bottom right of the description area is a character count '0/500'. At the bottom of the form are two buttons: 'ОТМЕНИТЬ' (Cancel) and 'СОЗДАТЬ' (Create). A 'ВПЕРЕД →' (Next) button is also visible near the bottom right.

Снимок экрана 62. Вкладка «Информация о цели»

При этом адрес цели (URL) должен соответствовать стандартам RFC 1035, RFC 3696 и RFC 3492 (см. снимок экрана 63).

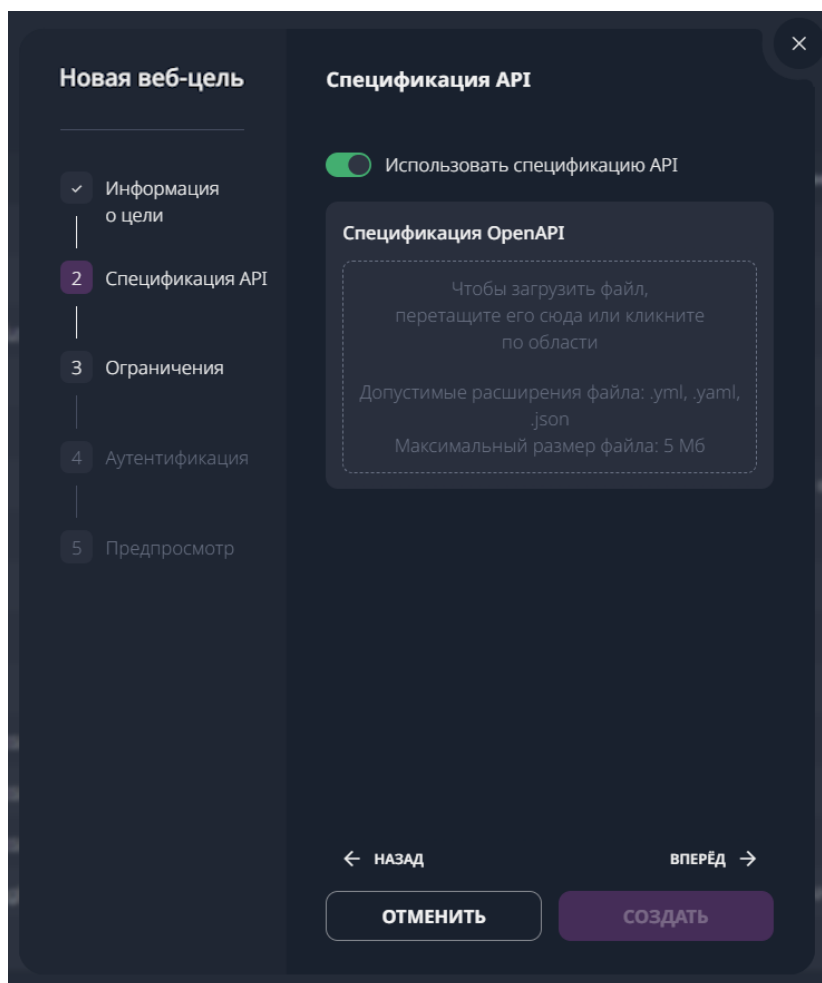


Снимок экрана 63. Стандарты RFC

В поле «Описание» можно добавить информацию о создаваемой цели объемом до 500 символов. Поле заполнять необязательно.

После заполнения полей следует нажать кнопку «ВПЕРЕД» в правом нижнем углу (после заполнения поля «Адрес» цель может быть сохранена нажатием кнопки «СОЗДАТЬ»; далее для ее редактирования доступны все параметры, кроме адреса (см. подраздел 6.3 «Редактирование цели»)).

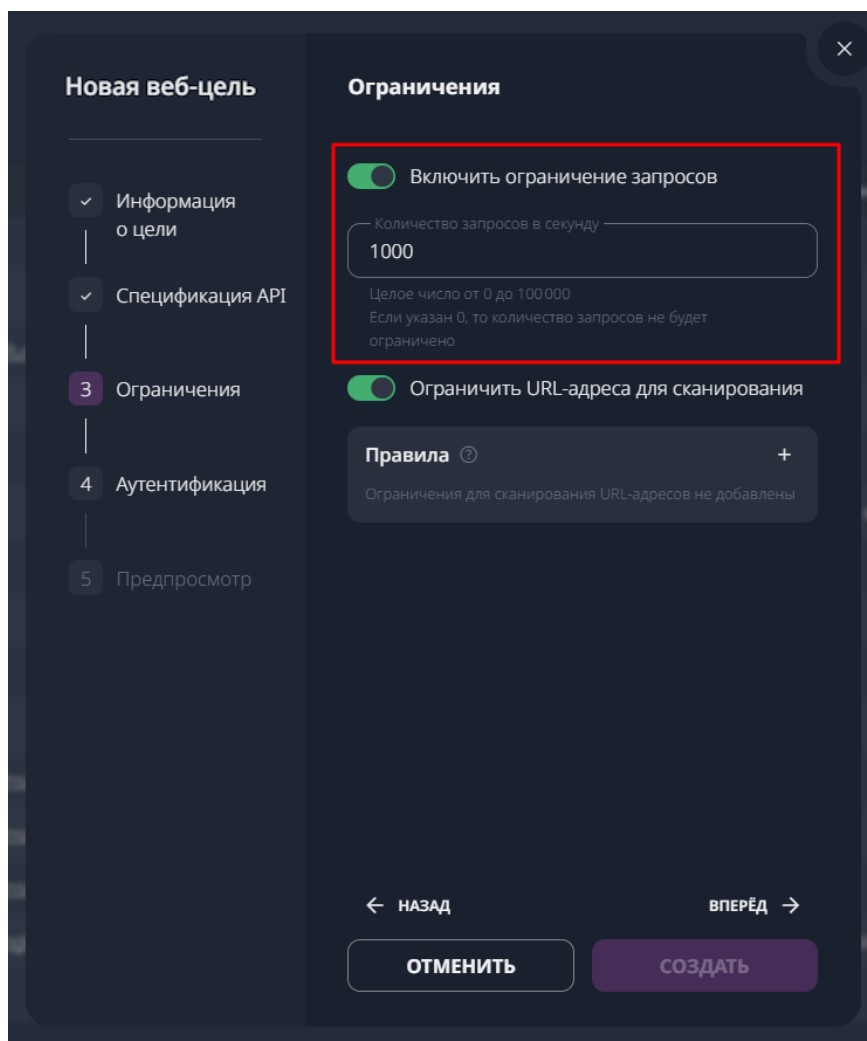
3. На вкладке «Спецификация API» можно добавить спецификацию OpenAPI для сканирования API цели. Для этого следует включить переключатель «Использовать спецификацию API» и в появившуюся область загрузки перетащить из локального хранилища файл или, кликнув по области для загрузки, выбрать его в открывшемся окне проводника (см. снимок экрана 64). Допустимые расширения файла: «.yaml», «.yml» и «.json» размером не более 5 Мб.



Снимок экрана 64. Вкладка «Спецификация API»

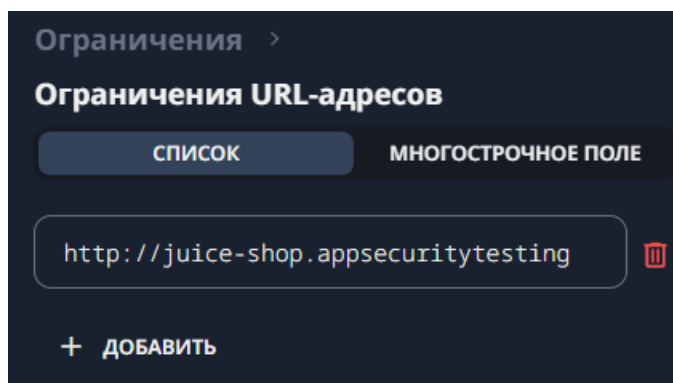
Далее следует нажать кнопку «ВПЕРЕД».

4. Вкладка «Ограничения» предназначена для установки ограничений количества запросов RPS и URL-адресов при сканировании и содержит два переключателя:
 - **Включить ограничение запросов.** Можно указать количество запросов в секунду при сканировании. Максимальное число запросов — 100000. Если указать 0, то количество запросов не будет ограничено (см. снимок экрана 65).



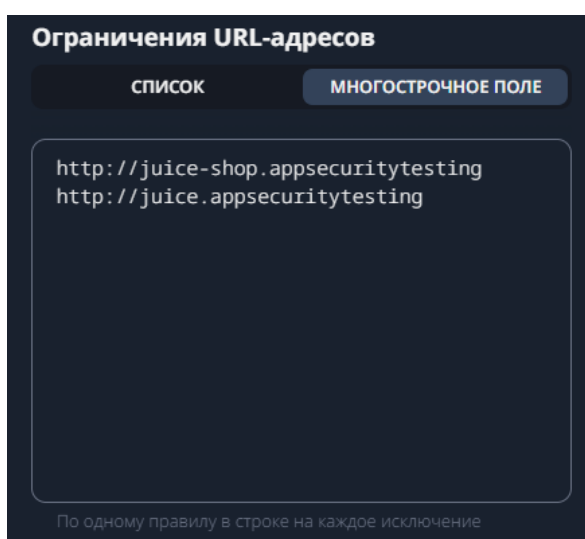
Снимок экрана 65. Переключатель «Включить ограничение запросов»

- **Ограничить URL-адреса для сканирования.** Сканер не будет переходить по ссылкам, попадающим под ограничения. Ограничения можно указать как строку или как регулярное выражение. Для добавления данных ограничений необходимо в правой части поля «Правила» нажать кнопку «+». Откроется окно «Ограничения URL-адресов», содержащее две вкладки:
 - **Список.** Необходимо добавить в поле URL-адрес. Если требуется указать дополнительные URL-адреса, следует нажать кнопку «ДОБАВИТЬ». Чтобы удалить лишнюю строку нужно нажать на иконку «» (см. снимок экрана 66).



Снимок экрана 66. Вкладка «Список»

- **Многострочное поле.** В данном поле следует указывать по одному правилу в строке на каждое исключение (см. снимок экрана 67).

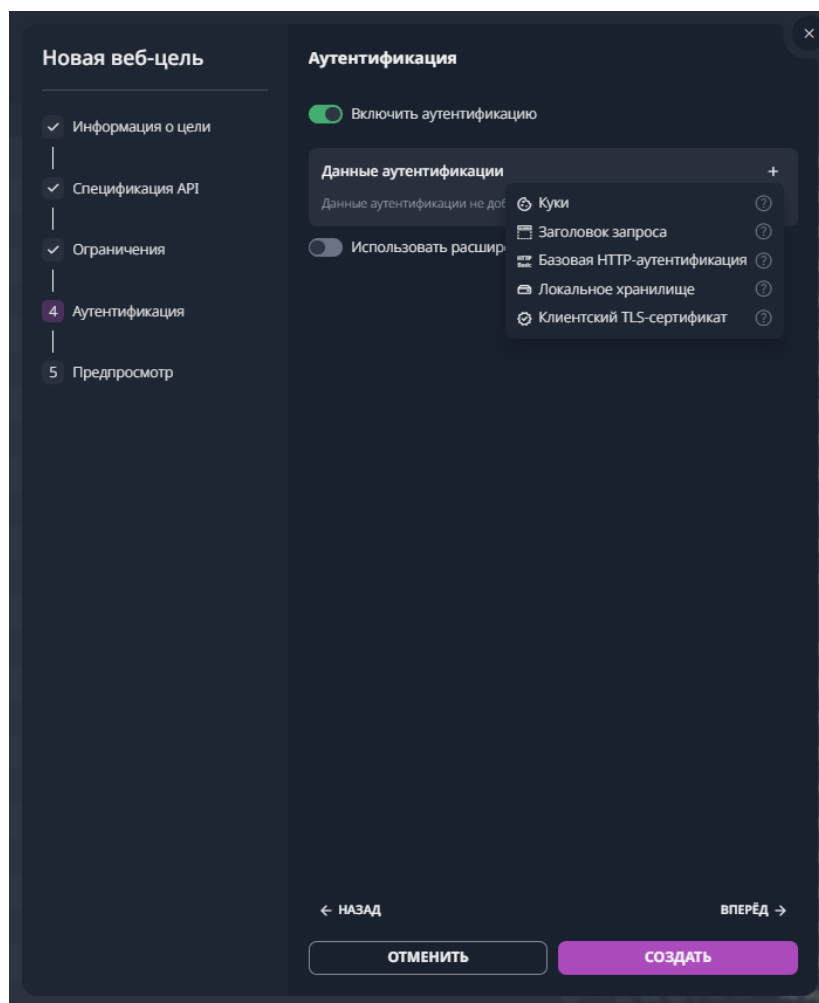


Снимок экрана 67. Вкладка «Многострочное поле»

После установки ограничений необходимо в правом нижнем углу окна нажать кнопки «ПРИМЕНИТЬ», затем «ВПЕРЁД».

- На вкладке «Аутентификация» можно включить аутентификацию и выбрать ее тип для сканирования защищенных авторизацией зон сайта, например личного кабинета (см. п. 5.1), а также установить расширенные параметры механизмов проверки и обновления аутентификации при работе сканера с целью (см. п. 5.2).

- Для выбора типа аутентификации необходимо активировать переключатель «Включить аутентификацию», затем в поле «Данные аутентификации» нажать кнопку «+», чтобы раскрыть контекстное меню (см. снимок экрана 68).



Снимок экрана 68. Вкладка «Аутентификация», поле «Данные аутентификации»

Доступны следующие типы аутентификации:

- **Куки** — тип аутентификации, использующий уникальный идентификатор, отправляемый сервером в веб-браузер пользователя. При выборе данного типа аутентификации откроется форма, в которой поля, помеченные символом «*», являются обязательными для заполнения (см снимок экрана 69). При этом имя хоста допустимо вводить в одном из следующих форматов (см снимок экрана 70):
 - одноуровневый — domain;
 - двухуровневый — domain.com;
 - с поддоменами — s1.domain.com, s1.s2.domain.com и т. д;
 - IPv4 — 255. 255. 255. 255;
 - IPv6 — 3FFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF.

Снимок экрана 69. Аутентификация «Куки»

Снимок экрана 70. Форматы имени хоста

- **Заголовок запроса** — пользовательский заголовок запроса, содержащий токен или набор учетных данных, используемых для проверки личности и уровня авторизации пользователя, делающего запрос (см. снимок экрана 71). Форматы данных имени хоста аналогичны типу аутентификации «Cookie» (см. снимок экрана 70).

Новая веб-цель

- ✓ Информация о цели
- ✓ Спецификация API
- ✓ Ограничения
- 4 Аутентификация**
- 5 Предпросмотр

Аутентификация > Заголовок запроса

URL

Имя хоста Порт

Имя хоста без указания `http://` или `https://`

Путь *

Относительный путь к сканируемому ресурсу (должен начинаться со знака `/`)

Параметры

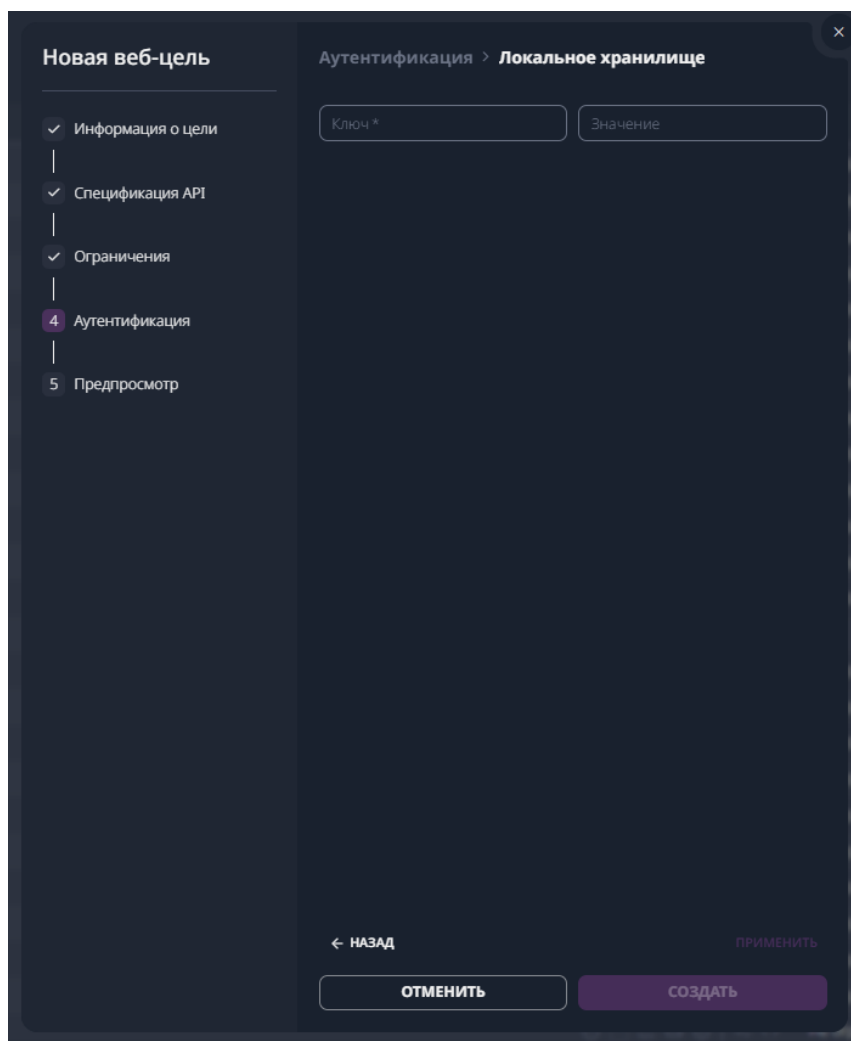
Название * Значение

← НАЗАД ПРИМЕНИТЬ

ОТМЕНИТЬ **СОЗДАТЬ**

Снимок экрана 71. Аутентификация «Заголовок запроса»

- **HTTP Basic Auth** — базовая аутентификация при помощи логина и пароля. Форма заполнения данных для HTTP Basic Auth аналогична форме «Заголовок запроса» (см. снимок экрана 71).
- **Локальное хранилище** — тип аутентификации с использованием сохраненных в локальном хранилище браузера токенов доступа. При выборе данного типа аутентификации откроется форма, в которой поле «Ключ» является обязательным для заполнения.



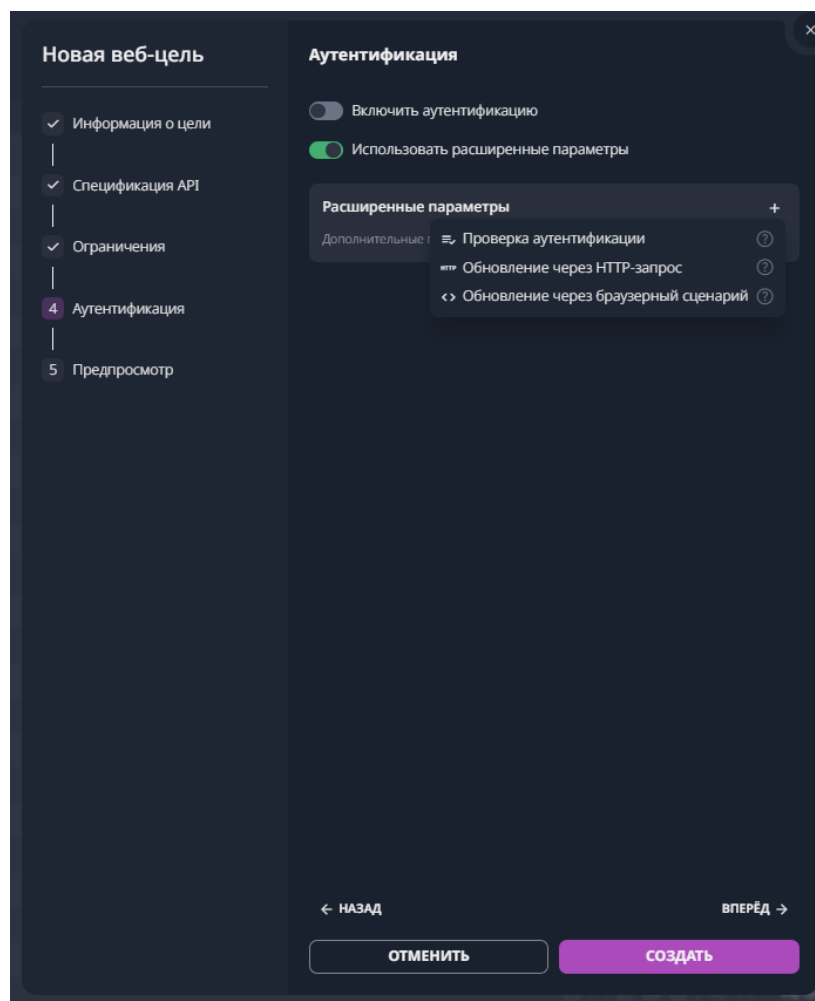
Снимок экрана 72. Аутентификация «Локальное хранилище»

- **Клиентский TLS-сертификат** — аутентификация при помощи клиентского сертификата через протокол TLS с созданием зашифрованного сетевого соединения. При выборе данного типа аутентификации откроется форма, в которой нужно добавить TLS-сертификат в формате «.crt» и ключ к сертификату в формате «.key». Для добавления следует перетащить в области для загрузки из локального хранилища файлы или, кликнув по области для загрузки, выбрать их в открывшемся окне проводника. Максимальный размер каждого файла не более 128 Кб (см. снимок экрана 73).

Снимок экрана 73. Аутентификация «Клиентский TLS-сертификат»

Можно выбрать несколько типов аутентификации. После заполнения необходимых полей в каждом выбранном типе для сохранения настроек следует нажать кнопку «ПРИМЕНИТЬ», расположенную в правом нижнем углу.

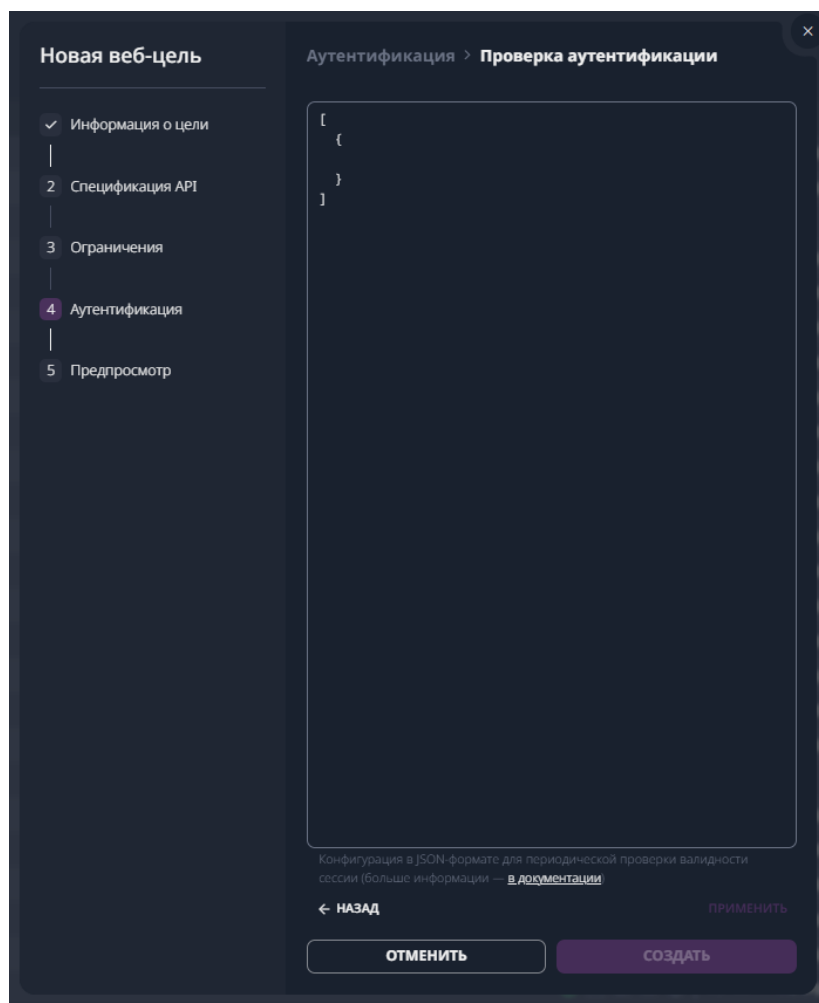
- 5.2. Для установки расширенных параметров механизмов проверки и обновления аутентификации необходимо активировать переключатель «Использовать расширенные параметры», затем в поле «Расширенные параметры» нажать кнопку «+», чтобы раскрыть контекстное меню (см. снимок экрана 74).



Снимок экрана 74. Вкладка «Аутентификация», поле «Расширенные параметры»

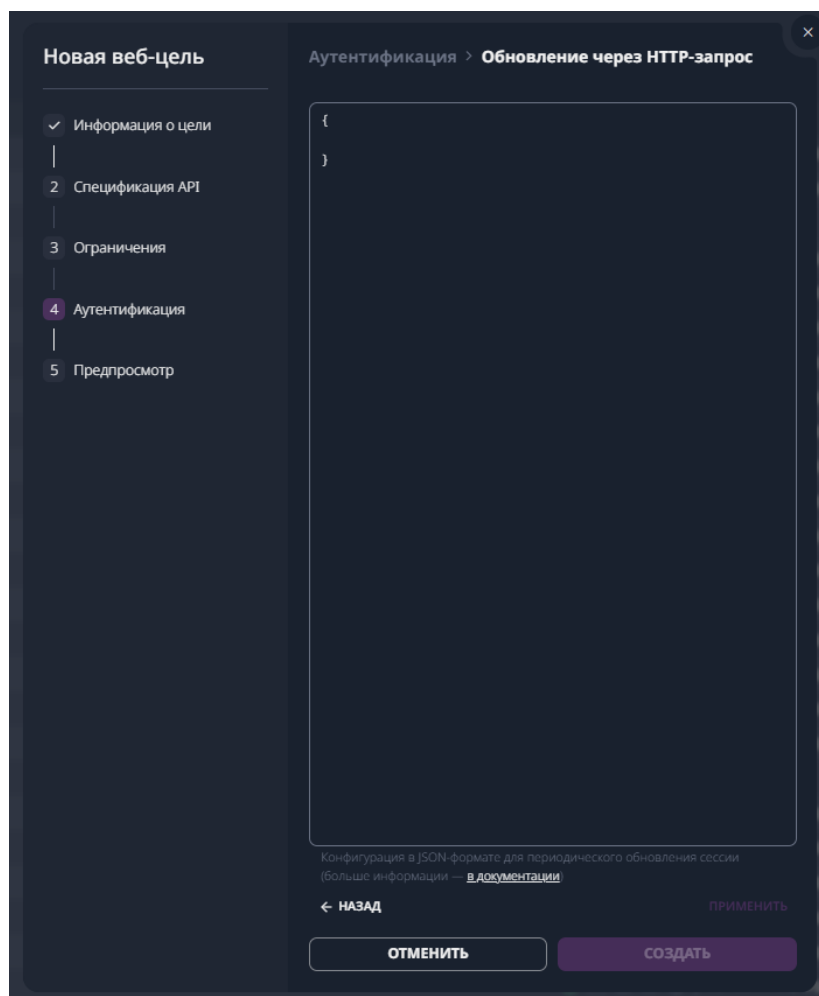
Доступны следующие виды параметров:

- **Проверка аутентификации** — выполняется периодическая проверка действительности сессии, используя описанную в формате JSON конфигурацию. При выборе данного параметра откроется окно «Проверка аутентификации», в поле которого необходимо добавить JSON конфигурацию и нажать кнопку «ПРИМЕНИТЬ», расположенную в правом нижнем углу (см. снимок экрана 75). Данный вид параметра подробно описан в приложении А.1 «Механизм проверки аутентификации», а также в онлайн документации, расположенной по ссылке <https://docs.solidpoint.net/ru/userguide/further-work/web-authentication/#authchecker>.



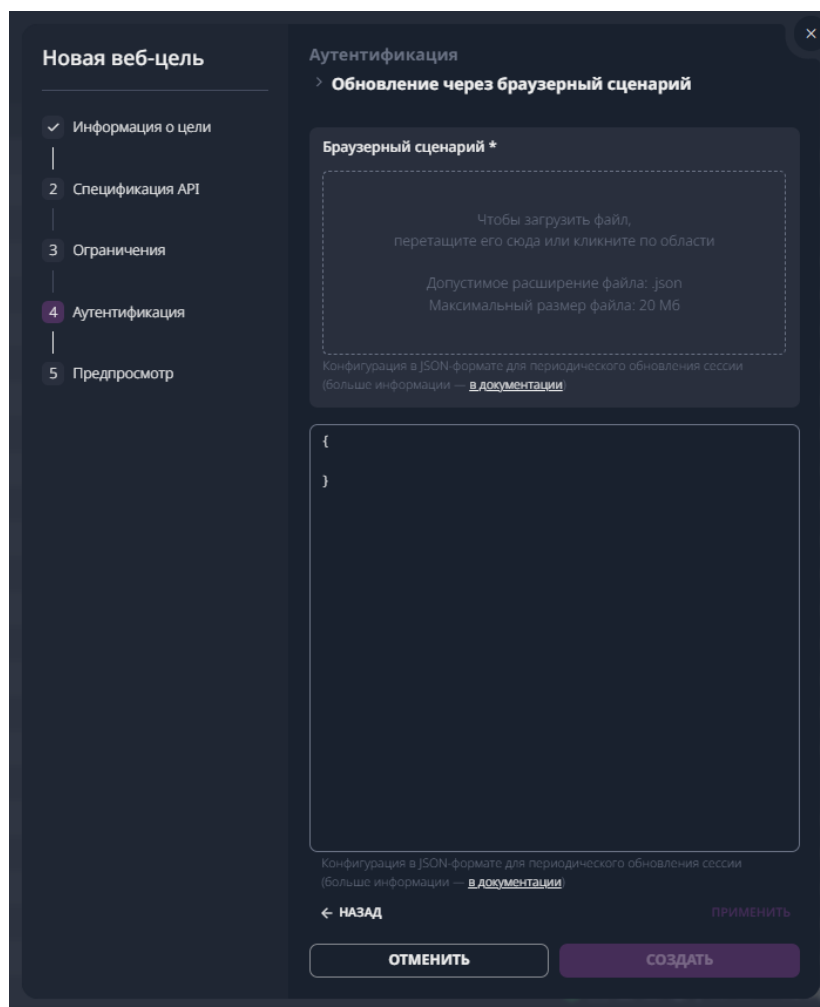
Снимок экрана 75. Окно параметра «Проверка аутентификации»

- **Обновление через HTTP-запрос** — выполняется периодическое обновление сессии, используя описанную в формате JSON конфигурацию. Работает только в сочетании с механизмом проверки аутентификации. При выборе данного параметра откроется окно «Обновление через HTTP-запрос», в поле которого необходимо добавить JSON конфигурацию и нажать кнопку «ПРИМЕНИТЬ», расположенную в правом нижнем углу (см. снимок экрана 76). Данный параметр подробно описан в приложении А.2, а также в онлайн документации по ссылке, расположенной по ссылке <https://docs.solidpoint.net/ru/userguide/further-work/web-authentication/#authrefresher-http>.



Снимок экрана 76. Окно параметра «Обновление через HTTP-запрос»

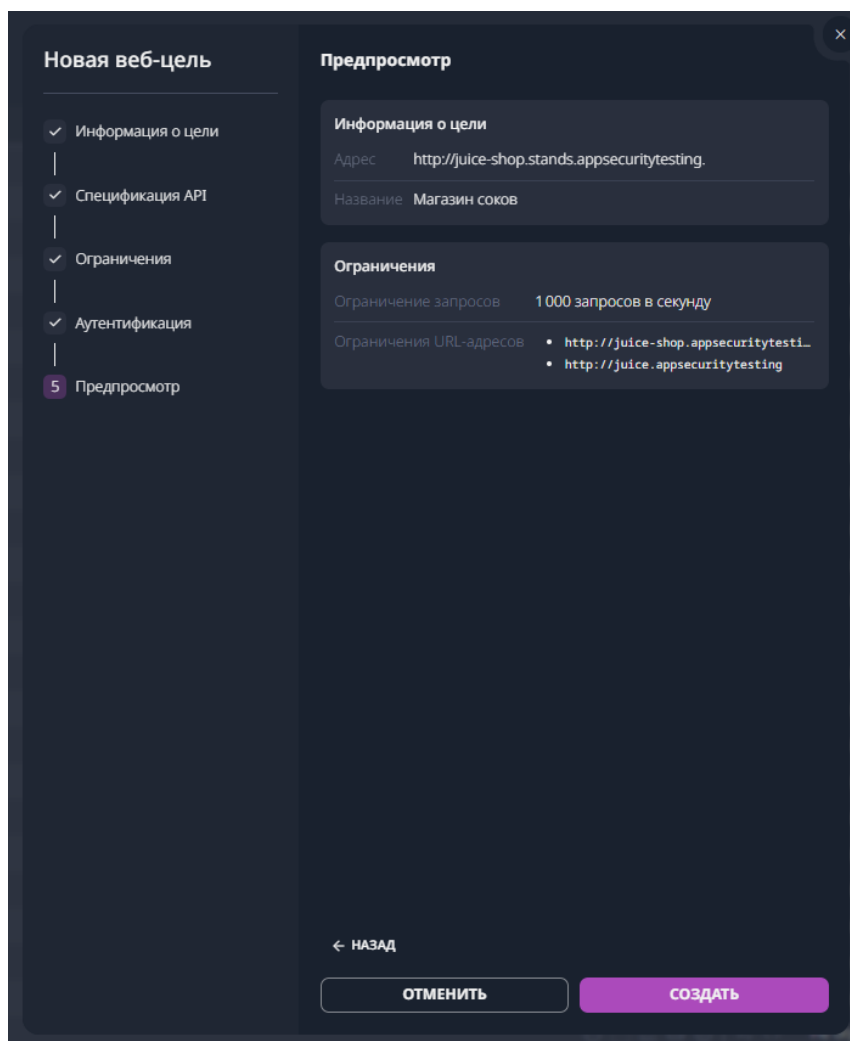
- **Обновление через браузерный сценарий** — выполняется периодическое обновление сессии, используя описанную в формате JSON конфигурацию. Работает только в сочетании с механизмом проверки аутентификации. При выборе данного параметра откроется окно «Обновление через браузерный сценарий», которое содержит два поля (см. снимок экрана 77):
 - «Браузерный сценарий» для загрузки файла записи браузерного сценария (запись браузерного сценария подробно описана в приложении А.3, а также в онлайн документации, расположенной по ссылке <https://docs.solidpoint.net/ru/userguide/further-work/web-authentication/#authrefresher-browser-script-recording>. Для загрузки браузерного сценария необходимо в область загрузки перетащить из локального хранилища файл или, кликнув по области для загрузки, выбрать его в открывшемся окне проводника. Допустимое расширение файла – JSON, максимальный размер файла – 20 Мб.
 - Поле для добавления JSON-конфигурации (подробно описано в приложении А.3, а также в онлайн документации по ссылке, расположенной по ссылке <https://docs.solidpoint.net/ru/userguide/further-work/web-authentication/#authrefresher-browser-script-configuration>).



Снимок экрана 77. Окно параметра «Обновление через браузерный сценарий»

После добавления браузерного сценария следует нажать кнопку «ПРИМЕНИТЬ». Далее необходимо нажать кнопку «ВПЕРЕД».

6. Вкладка «Предпросмотр» является завершающей. На вкладке отображаются все настройки, заданные при создании цели. Если требуется изменить настройки, то следует воспользоваться кнопкой «НАЗАД» до перехода на нужную вкладку либо нажать на название вкладки и внести изменения (см. снимок экрана 78).



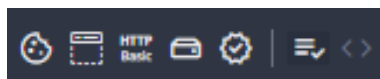
Снимок экрана 78. Вкладка «Предпросмотр»

После того, как все настройки цели заданы, необходимо в правом нижнем углу нажать кнопку «СОЗДАТЬ». Созданная цель появится в списке раздела «Цели». При этом выбранный тип аутентификации (расширенного параметра) будет подсвечиваться в столбце «Аутентификация» строки цели зеленым цветом (см. снимок экрана 79).



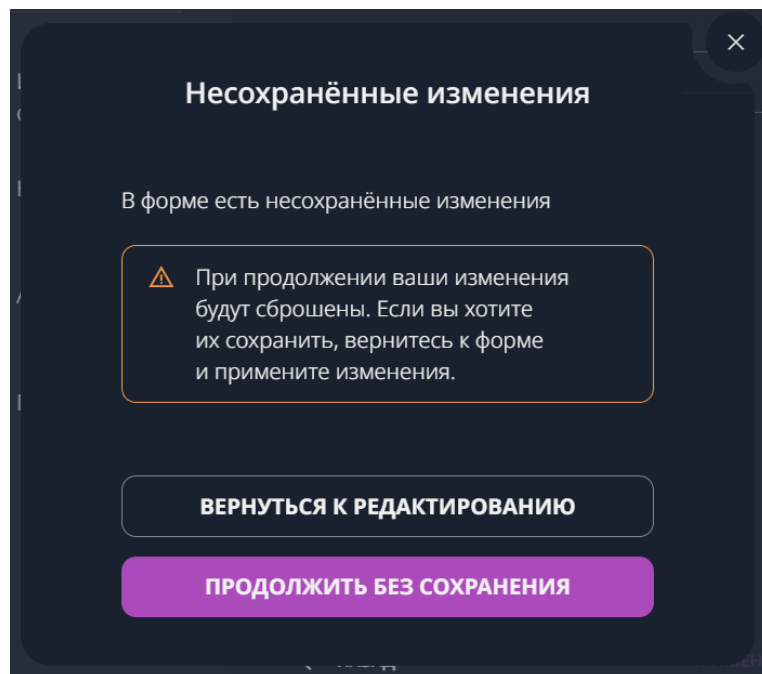
Снимок экрана 79. Выбранная аутентификация (расширенные параметры)

Если аутентификацию (расширенные параметры) выключить с заданными настройками, в том числе при редактировании цели (см. подраздел 6.3 «Редактирование цели»), тип выбранной аутентификации (расширенного параметра) будет подсвечен белым цветом (см. снимок экрана 80).



Снимок экрана 80. Аутентификация (расширенные параметры) выключены с заданными настройками

Примечание. При создании цели в окне «Новая цель» (см. шаги 1 – 6) процесс создания можно прервать на любом этапе, нажав в левом нижнем углу кнопку «ОТМЕНИТЬ» или крестик закрытия окна «✕» в правом верхнем углу. При этом появится окно «Несохранённые изменения», в котором нужно подтвердить намерение нажатием кнопки «ПРОДОЛЖИТЬ БЕЗ СОХРАНЕНИЯ». Кнопка «ВЕРНУТЬСЯ К РЕДАКТИРОВАНИЮ» или крестик «✕» в правом верхнем углу прерывают отмену создания цели (см. Снимок экрана 81).



Снимок экрана 81. Окно «Несохраненные изменения»

6.2. Подробная информация о цели

О любой созданной цели можно просмотреть подробную информацию. Для этого следует в списке целей нажать на адрес выбранной цели или на кнопку «⋮» в конце строки адреса цели и в раскрывшемся контекстном меню выбрать пункт «Просмотр» (см. **Ошибка! Источник ссылки не найден.**). Окно подробной информации о цели откроется по умолчанию на вкладке «Обзор»; помимо вкладки «Обзор» окно также содержит вкладки «Сканирования» и «Уязвимости» (см. снимок экрана 82).



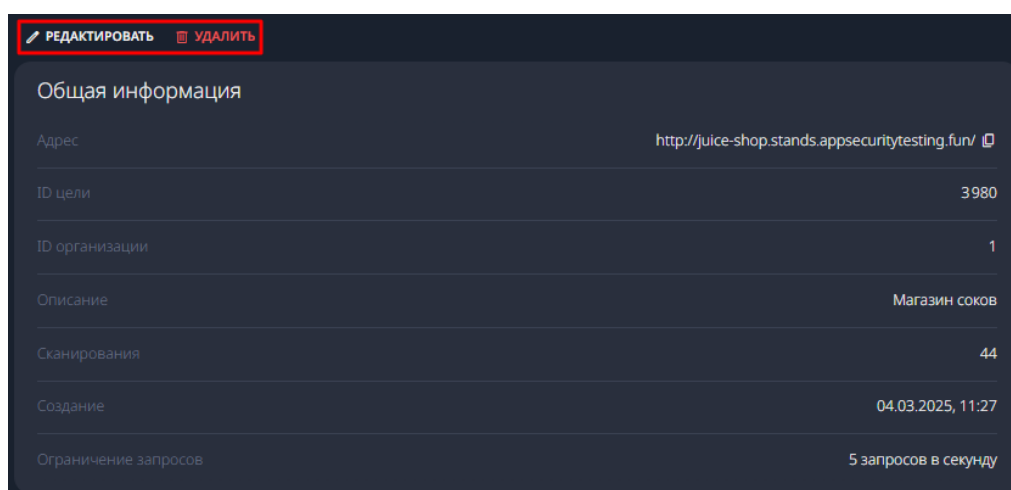
Снимок экрана 82. Вкладка «Обзор», окно подробной информации о цели

6.2.1. Вкладка «Обзор»

Вкладка «Обзор» содержит четыре информационных сектора: «Общая информация», «Данные аутентификации», «Сканирования» и «Уязвимости».

Сектор «Общая информация» содержит данные об (см. снимок экрана 83):

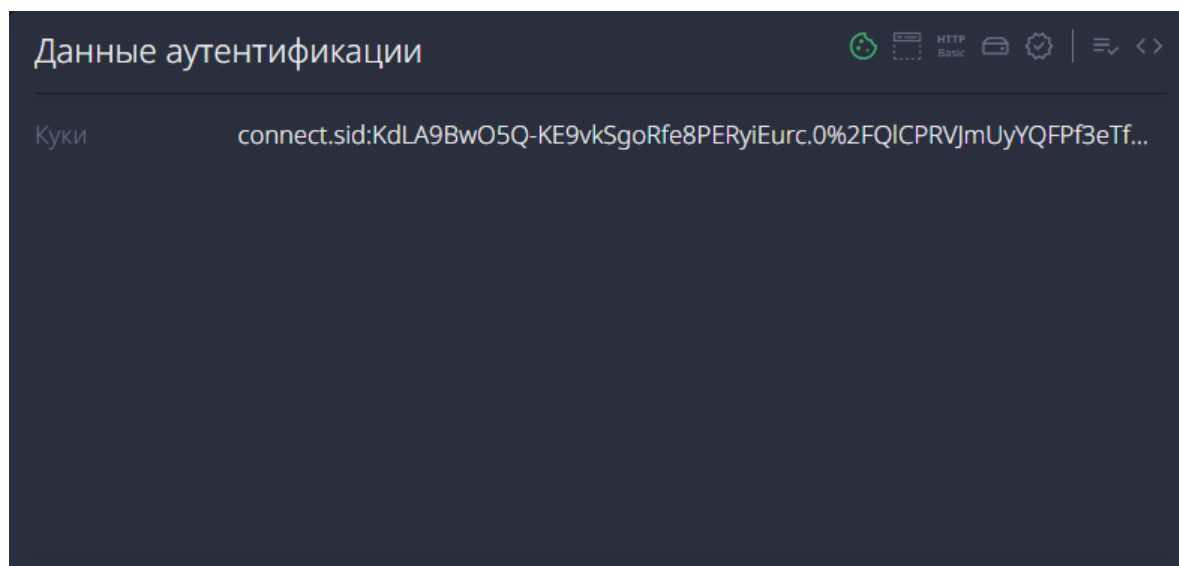
- адресе цели;
- ID цели;
- ID организации;
- описании цели;
- общем количестве сканирований;
- дате создания цели;
- ограничении запросов RPS.



Снимок экрана 83. Сектор общей информации о цели

Над данным сектором расположены кнопки «Редактировать» и «Удалить» для редактирования параметров (см. подраздел 6.3) и удаления цели (см. подраздел 6.4) соответственно.

Сектор «Данные аутентификации» содержит данные о заданных параметрах аутентификации цели (см. снимок экрана 84).



Снимок экрана 84. Сектор данных об аутентификации

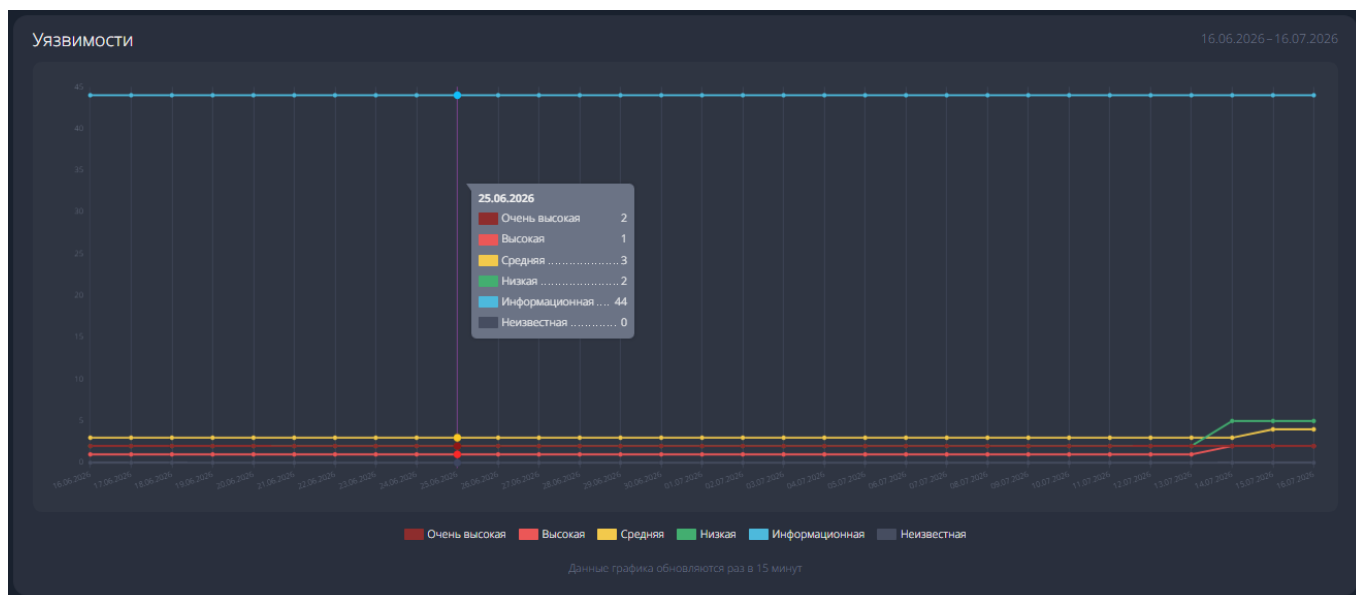
Сектор «Сканирования» содержит данные об общем количестве сканирований цели, а также информацию о количестве сканирований по каждому статусу (см. снимок экрана 85):

- В ожидании;
- В процессе;
- Приостановка;
- Синхронизация;
- Успешно;
- С замечаниями;
- Ошибка;
- Ошибка аутентификации;
- Отменено.

Сканирования (44)		к списку ➔
В ожидании	0	
В процессе	0	
Приостановка	0	
Приостановлено	4	
Синхронизация	0	
Успешно	7	
С замечаниями	2	
Ошибка	4	
Ошибка аутентификации	0	
Отменено	27	

Снимок экрана 85. Сектор подробной информации о сканированиях цели

Сектор «Уязвимости» содержит график найденных уязвимостей всех сканирований цели, отражающий изменение уровня защищённости выбранной цели. График интерактивный, при наведении курсора на любую вертикальную линию появится всплывающее окно с датой сканирования и количеством найденных уязвимостей (см. снимок экрана 86).



Снимок экрана 86. Сектор «Уязвимости»

6.2.2. Вкладка «Сканирования»

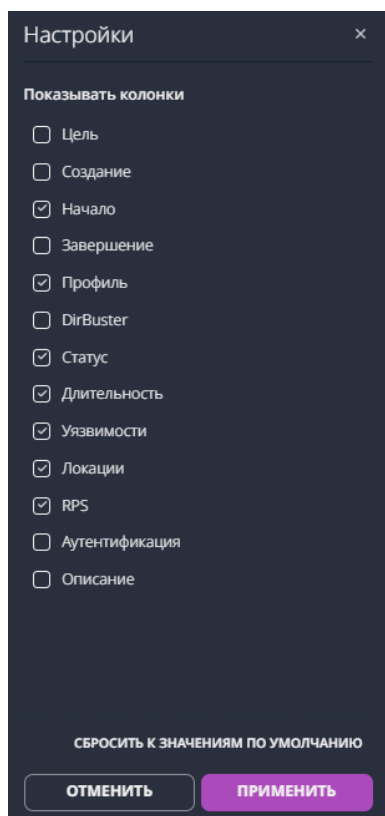
На вкладке «Сканирования» содержится список сканирований выбранной цели (см. снимок экрана 87).

ID	Начало	Профиль	Статус	Длительность	Уязвимости	Локации	ID организации
12395	08.07.2026, 10:04	Полное	Ошибка	1м		0	1
12394	08.07.2026, 10:01	Полное	Ошибка	1м		0	1
11634	10.04.2026, 10:21	Полное	Успешно	2ч 25м	0 0 1 1 12 0	7	1
11548	01.04.2026, 17:24	Полное	Отменено	<1м		5	1
11353	17.03.2026, 18:57	Полное	Приостановлено	99+д		5	1
11349	17.03.2026, 12:05	Полное	Успешно	2ч 19м	0 0 0 1 1 20 0	7	1
10955	13.02.2026, 14:39	Полное	Отменено	<1м		5	1
10625	14.01.2026, 11:15	Полное	Успешно	2ч 6м	0 0 0 5 1 19 0	7	1
10608	13.01.2026, 15:12	Выборочное	Приостановлено	99+д		61	1
10294	19.12.2025, 14:00	Выборочное	Приостановлено	99+д		1	1
10237	17.12.2025, 10:37	Полное	Отменено	3ч 5м	0 0 0 3 3 26 0	243	1
10089	05.12.2025, 17:41	Полное	С замечаниями	>2д	2 0 0 5 1 32 0	243	1
10088	05.12.2025, 17:39	Полное	Отменено	4м		8	1
10083	05.12.2025, 16:49	Полное	Отменено	48м		61	1
9917	21.11.2025, 14:59	Полное	Отменено	<1м		8	1
9640	07.11.2025, 10:05	Полное	Приостановлено	99+д		60	1
9093	26.09.2025, 13:04	Полное	Отменено	46м		243	1
9028	24.09.2025, 9:23	Полное	Отменено	<1м		8	1
8932	17.09.2025, 11:34	Полное	Отменено	1м		8	1
8930	17.09.2025, 11:33	Полное	Отменено	<1м		8	1
8903	15.09.2025, 9:17	Полное	С замечаниями	>1д	1 0 0 5 1 14 0	246	1
8662	29.08.2025, 10:30	Полное	Отменено	1м		9	1
8427	21.08.2025, 10:00	Полное	Отменено	3ч 51м	0 0 0 1 1 17 0	123	1

Снимок экрана 87. Список сканирований выбранной цели

Значения колонок «Начало», «Профиль», «Статус», «Длительность», «Уязвимости», «Локации», «ID организации» и «Кнопка «:» аналогичны значениям колонок в окне «Сканирования» (см. раздел 5.2, п. 3). В колонке «ID» содержится уникальный номер сканирования, в колонке «Цель» — выбранной адрес цели.

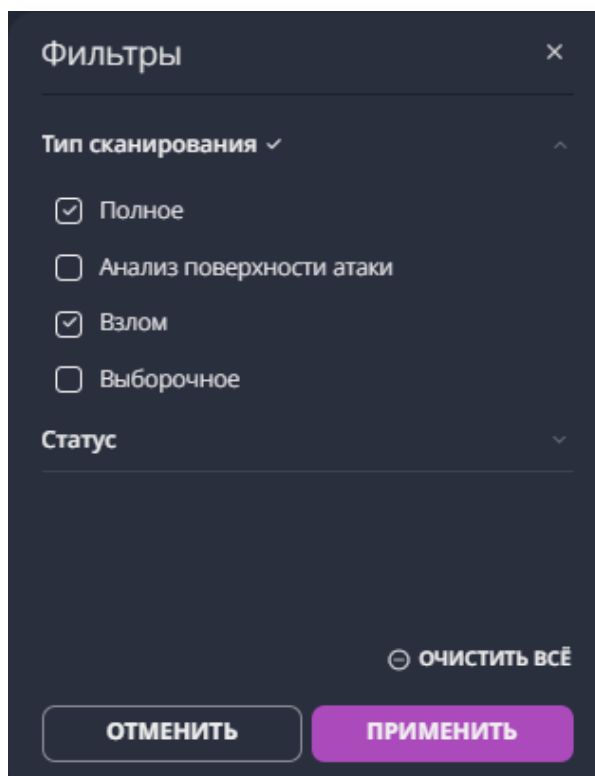
Для отображения или скрытия колонок можно воспользоваться фильтром, нажав кнопку «Настройки» в правом верхнем углу. В открывшемся окне «Настройки» следует включить/отключить чекбоксы соответствующих колонок и нажать кнопку «ПРИМЕНИТЬ». (см. снимок экрана 88).



Снимок экрана 88. Окно «Настройки» для отображения/скрытия колонок

Возможные действия со сканированиями цели («Приостановить», «Возобновить», «Прервать» и «Удалить») осуществляется включением/выключением чекбокса и выбора соответствующих кнопок действий, расположенных под вкладками «Обзор» и «Сканирования», а также пункта контекстного меню в конце строки цели (см. снимок экрана 29). Возможные действия со сканированием в зависимости от его статуса представлены в таблице 14.

Кнопка «ФИЛЬТРЫ», расположенная в правом верхнем углу, позволяет отфильтровать сканирования цели по типу сканирования (см. снимок экрана 89) и статусу (см. снимок экрана 90). После включения необходимых чекбоксов следует нажать кнопку «ПРИМЕНИТЬ».



Фильтры

Тип сканирования ✓

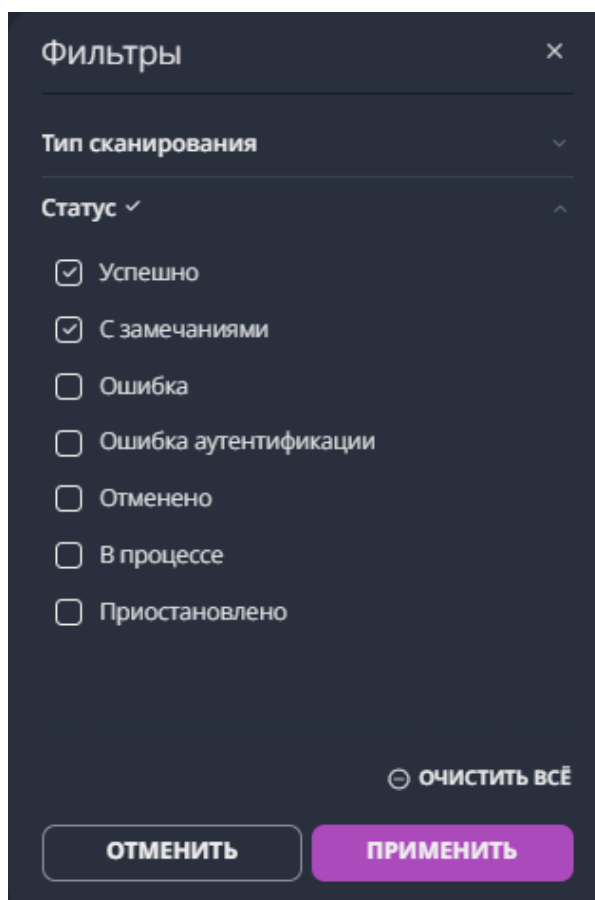
- ☒ Полное
- ☐ Анализ поверхности атаки
- ☒ Взлом
- ☐ Выборочное

Статус

ОЧИСТИТЬ ВСЁ

ОТМЕНИТЬ ПРИМЕНИТЬ

Снимок экрана 89. Окно «Фильтры», поиск по типу сканирования выбранной цели



Фильтры

Тип сканирования

Статус ✓

- ☒ Успешно
- ☒ С замечаниями
- ☐ Ошибка
- ☐ Ошибка аутентификации
- ☐ Отменено
- ☐ В процессе
- ☐ Приостановлено

ОЧИСТИТЬ ВСЁ

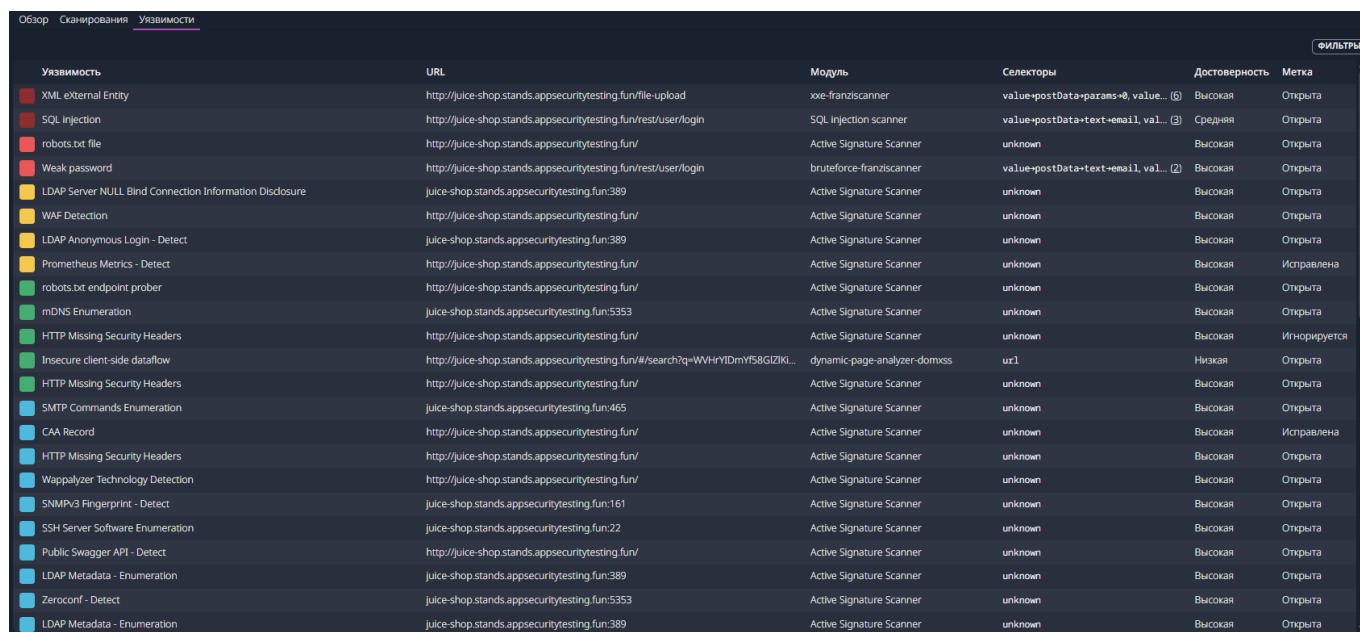
ОТМЕНИТЬ ПРИМЕНИТЬ

Снимок экрана 90. Окно «Фильтры», поиск по статусу сканирования выбранной цели

Кнопка «Сканировать», расположенная в правом верхнем углу, предназначена для запуска нового сканирования.

6.2.3. Вкладка «Уязвимости»

Вкладка «Уязвимости» в целом аналогична такой же вкладке, описанной в подразделе 5.2.1 «Подробная информация о сканировании». На данной отображен список уязвимостей цели всех сканирований в табличном виде (см. снимок экрана 91).



Уязвимость	URL	Модуль	Селекторы	Достоверность	Метка
XML external Entity	http://juice-shop.stands.appsecuritestesting.fun/file-upload	xxe-franziscanner	value+postData+params+0.value... (6)	Высокая	Открыта
SQL Injection	http://juice-shop.stands.appsecuritestesting.fun/rest/user/login	SQL Injection scanner	value+postData+text+email, va1... (3)	Средняя	Открыта
robots.txt file	http://juice-shop.stands.appsecuritestesting.fun/	Active Signature Scanner	unknown	Высокая	Открыта
Weak password	http://juice-shop.stands.appsecuritestesting.fun/rest/user/login	bruteforce-franziscanner	value+postData+text+email, va1... (2)	Высокая	Открыта
LDAP Server NULL Bind Connection Information Disclosure	juice-shop.stands.appsecuritestesting.fun:389	Active Signature Scanner	unknown	Высокая	Открыта
WAF Detection	http://juice-shop.stands.appsecuritestesting.fun/	Active Signature Scanner	unknown	Высокая	Открыта
LDAP Anonymous Login - Detect	juice-shop.stands.appsecuritestesting.fun:389	Active Signature Scanner	unknown	Высокая	Открыта
Prometheus Metrics - Detect	http://juice-shop.stands.appsecuritestesting.fun/	Active Signature Scanner	unknown	Высокая	Исправлена
robots.txt endpoint prober	http://juice-shop.stands.appsecuritestesting.fun/	Active Signature Scanner	unknown	Высокая	Открыта
mDNS Enumeration	juice-shop.stands.appsecuritestesting.fun:5353	Active Signature Scanner	unknown	Высокая	Открыта
HTTP Missing Security Headers	http://juice-shop.stands.appsecuritestesting.fun/	Active Signature Scanner	unknown	Высокая	Игнорируется
Insecure client-side dataflow	http://juice-shop.stands.appsecuritestesting.fun/#search?q=WHYIDmY58GIZIK...	dynamic-page-analyzer-domxss	url	Низкая	Открыта
HTTP Missing Security Headers	http://juice-shop.stands.appsecuritestesting.fun/	Active Signature Scanner	unknown	Высокая	Открыта
SMTP Commands Enumeration	juice-shop.stands.appsecuritestesting.fun:465	Active Signature Scanner	unknown	Высокая	Открыта
CAA Record	http://juice-shop.stands.appsecuritestesting.fun/	Active Signature Scanner	unknown	Высокая	Исправлена
HTTP Missing Security Headers	http://juice-shop.stands.appsecuritestesting.fun/	Active Signature Scanner	unknown	Высокая	Открыта
Wappalizer Technology Detection	http://juice-shop.stands.appsecuritestesting.fun/	Active Signature Scanner	unknown	Высокая	Открыта
SNMPv3 Fingerprint - Detect	juice-shop.stands.appsecuritestesting.fun:161	Active Signature Scanner	unknown	Высокая	Открыта
SSH Server Software Enumeration	juice-shop.stands.appsecuritestesting.fun:22	Active Signature Scanner	unknown	Высокая	Открыта
Public Swagger API - Detect	http://juice-shop.stands.appsecuritestesting.fun/	Active Signature Scanner	unknown	Высокая	Открыта
LDAP Metadata - Enumeration	juice-shop.stands.appsecuritestesting.fun:389	Active Signature Scanner	unknown	Высокая	Открыта
Zeroconf - Detect	juice-shop.stands.appsecuritestesting.fun:5353	Active Signature Scanner	unknown	Высокая	Открыта
LDAP Metadata - Enumeration	juice-shop.stands.appsecuritestesting.fun:389	Active Signature Scanner	unknown	Высокая	Открыта

Снимок экрана 91. Вкладка «Уязвимости»

Список уязвимостей содержит следующие данные:

- Уязвимость;
- URL;
- Модуль;
- Селекторы;
- Достоверность;
- Метка.

Для отображения списка с уязвимостями нужной степени критичности следует воспользоваться кнопкой «ФИЛЬТРЫ», расположенной в верхнем правом углу. В открывшемся окне необходимо включить нужные чекбоксы и нажать внизу кнопку «ПРИМЕНИТЬ» (см. снимок экрана 43).

6.2.4. Вкладка «Стек технологий»

На вкладке «Стек технологий» отображаются технологии, выявленные при сканировании цели (см. снимок экрана 92).

Обзор Сканирования Уязвимости <u>Стек технологий</u>					
Технология	Тип	Категории	Достоверность	URL	Внешняя ⓘ
cdnjs	Программное обеспечение	cdn	Высокая	http://cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js	
cdnjs	Программное обеспечение	cdn	Высокая	http://cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js	
cdnjs	Программное обеспечение	cdn	Высокая	http://juice-shop.stands.appsecuritytesting.fun/	
Cloudflare	Программное обеспечение	cdn	Высокая	http://cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.css	✓
Cloudflare	Программное обеспечение	cdn	Высокая	http://cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js	✓
Cloudflare	Программное обеспечение	cdn	Высокая	http://cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js	✓
Cloudflare	Программное обеспечение	cdn	Высокая	http://juice-shop.stands.appsecuritytesting.fun/	
HTTP/3	Программное обеспечение	miscellaneous	Высокая	http://cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.css	✓
HTTP/3	Программное обеспечение	miscellaneous	Высокая	http://cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js	✓
HTTP/3	Программное обеспечение	miscellaneous	Высокая	http://cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js	✓
jQuery 2.2.4	Программное обеспечение	javascript-libraries	Высокая	http://cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js	
jQuery 2.2.4	Программное обеспечение	javascript-libraries	Высокая	http://juice-shop.stands.appsecuritytesting.fun/	
Module Federation	Программное обеспечение	miscellaneous	Высокая	http://juice-shop.stands.appsecuritytesting.fun/runtime.js	
Nginx 1.22.1	Сервер	web-servers, reverse-proxies	Высокая	http://juice-shop.stands.appsecuritytesting.fun/	✓
Nginx 1.22.1	Сервер	web-servers, reverse-proxies	Высокая	http://juice-shop.stands.appsecuritytesting.fun/runtime.js	✓
Webpack	Программное обеспечение	miscellaneous	Низкая	http://juice-shop.stands.appsecuritytesting.fun/runtime.js	

Снимок экрана 92. Вкладка «Стек технологий»

Список технологий содержит следующие данные:

- Технология;
- Тип;
- Категории;
- Достоверность;
- URL;
- Внешняя.

6.3. Редактирование цели

Для редактирования параметров уже созданной цели следует нажать в конце строки адреса цели кнопку «:» и в раскрывшемся контекстном меню выбрать пункт «Редактировать» (см. **Ошибка! Источник ссылки не найден.**). Откроется окно «Редактирование веб-цели» (см. снимок экрана 93).

Снимок экрана 93. Окно «Редактирование веб-цели»

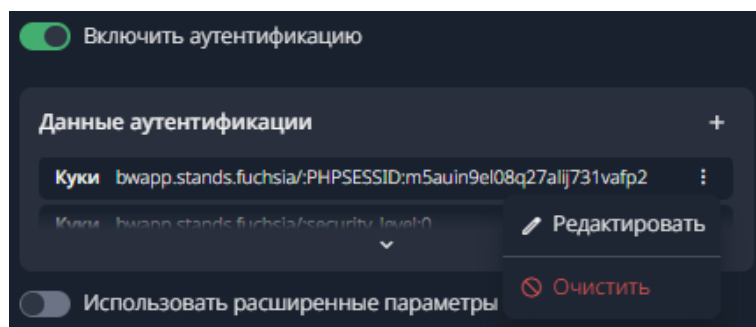
Окно содержит те же вкладки, что и окно «Новая цель». Для изменения параметров следует выбрать нужную вкладку.

На вкладке «Информация о цели» можно изменить описание. Поле «Адрес» не редактируется.

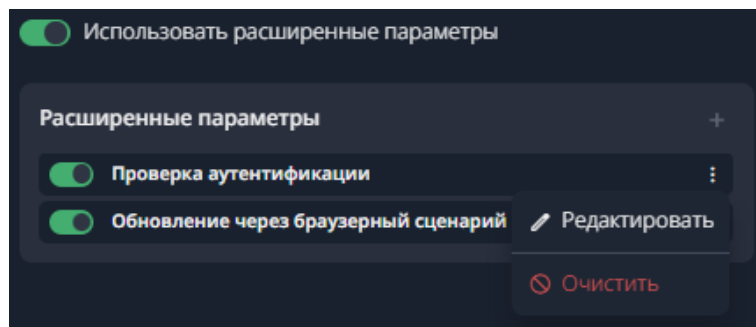
На вкладке «Спецификация API» можно удалить или заменить спецификацию OpenAPI, а также отключить использование данной функциональности.

На вкладке «Ограничения» можно изменить значение настраиваемого параметра RPS, удалить или добавить ограничивающие сканирование URL-адреса, а также отключить использование данных режимов.

На вкладке «Аутентификация» можно отключить использование аутентификации и расширенных параметров, а также изменить или удалить данные этих функциональностей. Для этого в области «Данные аутентификации» или «Расширенные параметры» следует нажать в конце строки нужной аутентификации (параметра) на кнопку «⋮» и в раскрывшемся контекстном меню выбрать пункт «Редактировать» или «Очистить» (см. снимки экрана 94, 95).



Снимок экрана 94. Данные аутентификации



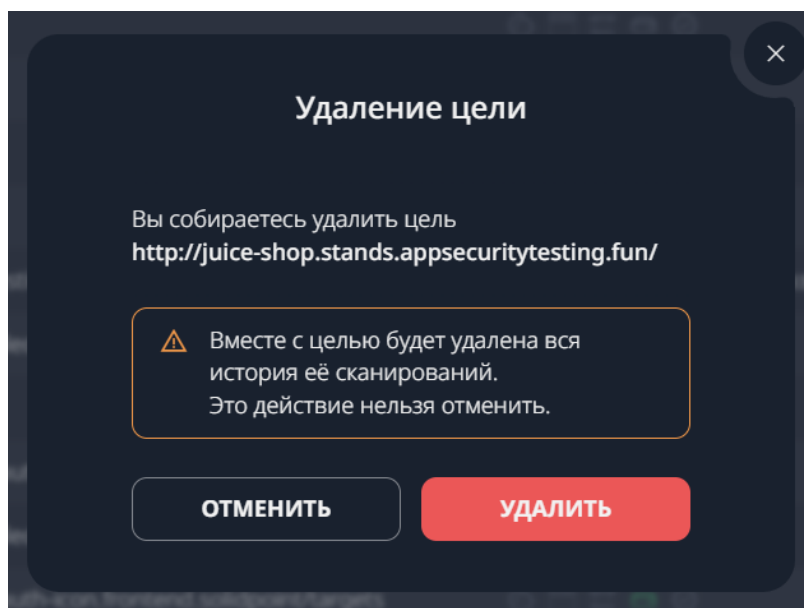
Снимок экрана 95. Расширенные параметры

При выборе пункта «Очистить» тип аутентификации (вид параметра) будет удален из списка. При выборе пункта «Редактировать» откроется окно параметров аутентификации (вида параметра), аналогичное при создании цели, где можно внести изменения (см. снимки экрана 69 – 73 и 75 – 77). Изменение данных требует подтверждения нажатием кнопки «ПРИМЕНИТЬ», как и при создании цели (см. п. 5, подраздела 6.1 «Создание цели»).

После внесения изменений необходимо в правом нижнем углу окна «Изменение цели» нажать кнопку «СОХРАНИТЬ».

6.4. Удаление цели

Для удаления цели необходимо нажать в конце строки адреса цели на кнопку «⋮» и в раскрывшемся меню выбрать пункт «Удалить» (см. п. 2, подраздела 5.3 «Окно «Цели»»). Откроется окно «Удаление цели» (см. снимок экрана 96).



Снимок экрана 96. Окно «Удаление цели»

При нажатии на кнопку «УДАЛИТЬ» цель будет удалена. Для закрытия окна без удаления цели следует нажать кнопку «ОТМЕНИТЬ» или крестик закрытия окна «» в правом верхнем углу.

7. СКАНИРОВАНИЕ

7.1. Создание сканирования

Новое сканирование создается в окне «Сканирования» (см. снимок экрана 23).

Сканирование бывает трех типов:

- «Полное» — сканирование всеми доступными модулями. Сканирование может занять продолжительное время.
- «Выборочное» — сканирование выбранными модулями. Для корректной работы модулей взлома поверхность атаки должна быть обнаружена соответствующими модулями.
- «Анализ поверхности атаки» — сканирование модулями анализа поверхности атаки для определения всех конечных точек серверного API в веб-ресурсах без анализа уязвимостей. Полученный результат может использоваться в будущем для других сканирований выбранной цели.

Для создания сканирования необходимо нажать кнопку «**НОВОЕ ВЕБ-СКАНИРОВАНИЕ**», расположенную в правом верхнем углу окна «Сканирования» (см. снимок экрана 97). Откроется окно «Новое сканирование».

Снимок экрана 97. Кнопка «НОВОЕ ВЕБ-СКАНИРОВАНИЕ»

Создание сканирования состоит из четырех шагов (создание сканирования с типами «Полное» и «Анализ поверхности атаки» одинаковое; создание сканирования с типом «Выборочное» отличается и описано в шагах 1.1 – 1.2):

1. На вкладке «Общая информация» посредством прокрутки списка либо через поле поиска необходимо выбрать цель сканирования, включив рядом с ней чекбокс (можно выбрать несколько целей), и нажать кнопку «ВПЕРЁД» (см. снимок экрана 98).

Снимок экрана 98. Вкладка «Общая информация»

Примечание. С помощью поля поиска также можно создать новую цель, добавив ее вручную. Нажатие на кнопку «СОЗДАТЬ ЭТУ ЦЕЛЬ» автоматически создаст цель, которая будет добавлена в список целей как на данной вкладке, так и в разделе «Цели». Созданная таким образом цель не будет иметь дополнительных настроек, однако она доступна для редактирования согласно описанию в подразделе 6.3 «Редактирование цели». После выбора цели можно сразу запустить сканирование, не проходя все шаги до конца, нажав кнопку «СОЗДАТЬ». (см. снимок экрана 99).

Новое веб-сканирование

1 Общая информация

2 Дедупликация

3 Дополнительная информация

4 Экспериментальные параметры

5 Предпросмотр

Общая информация

Профиль сканирования *

Полное

☒ Сканировать с использованием DirBuster

Выберите цели *

Найдите или создайте цель

http://stands.appsecuritytesting.fun

URL (должен начинаться с http:// или https://)

Совпадений не найдено

ОЧИСТИТЬ ПОИСК

СОЗДАТЬ ЭТУ ЦЕЛЬ

ВПЕРЕД →

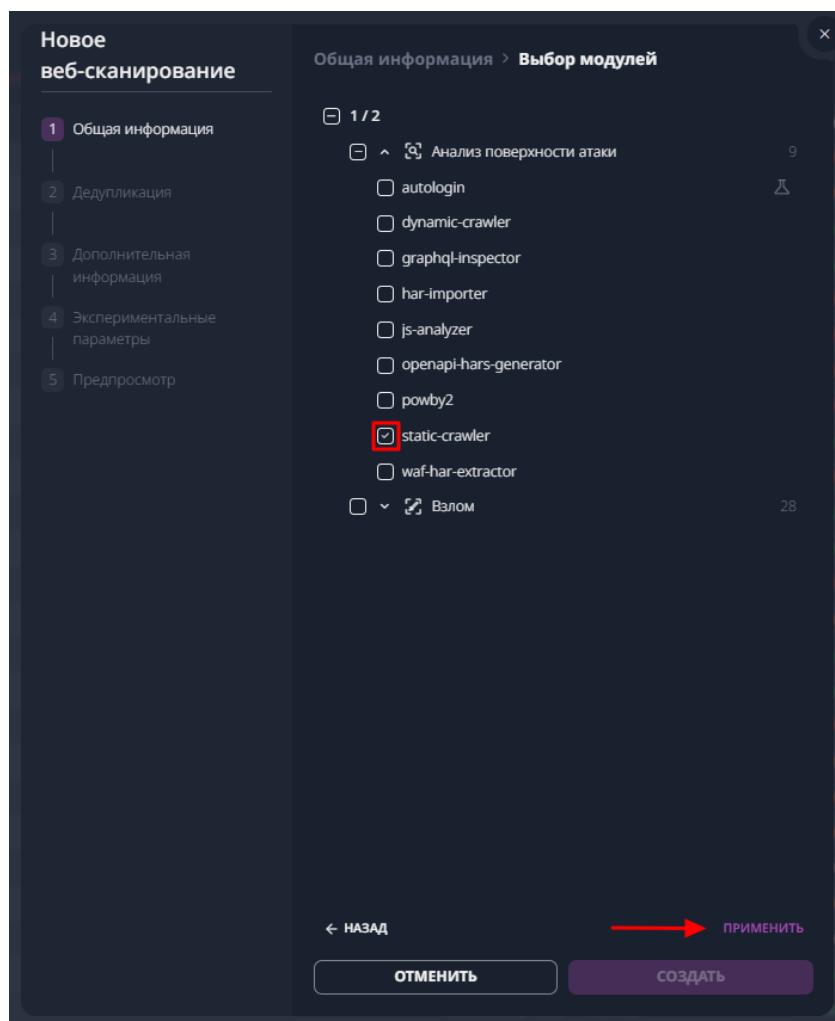
ОТМЕНИТЬ

СОЗДАТЬ

Снимок экрана 99. Вкладка «Общая информация», создание цели

Далее следует в верхней части вкладки в раскрывающемся списке «Профиль сканирования» выбрать тип, а также использование функции «DirBuster» включением (выключением) чекбокса.

- 1.1. При установке выборочного сканирования функция «DirBuster» становится недоступна. Если данная функция необходима, требуется выбрать модуль «static-crawler» в типе сканирования «Анализ поверхности атаки», при этом чекбокс «Сканировать с использованием функции «DirBuster» станет доступным для включения. Чтобы выбрать модуль необходимо в правой части поля «Модули» нажать кнопку «+», в открывшемся окне «Общая информация. Выбор модулей» раскрыть список «Анализ поверхности атаки», включить чекбокс и в правом нижнем углу нажать кнопку «ПРИМЕНИТЬ» (см. снимок экрана 100).



Снимок экрана 100. Окно «Общая информация. Выбор модулей», выбор модуля «static-crawler»

1.2. При необходимости выбора других модулей следует в раскрывающихся списках «Анализ поверхности атаки» и «Взлом» включить соответствующие чекбоксы и нажать кнопку «ПРИМЕНИТЬ» (количество модулей выбранных типов сканирования отобразится в поле «Модули»). Далее необходимо нажать кнопку «ВПЕРЕД». (см. снимок экрана 101).

Новое веб-сканирование

Общая информация

Профиль сканирования *
Выборочное

☒ Сканировать с использованием DirBuster

Модули * (6)
2 4

Выберите цели *

Найдите или создайте цель

1 / 181

- ☐ http://localhost
- ☐ https://localhost
- ☐ http://10.0.0.101:80/
- ☐ http://csp-xss.stands.fuchsia/
- ☐ http://10.72.55.188/
- ☐ http://target-new-tenant.solidpoint
- ☐ http://hackmegraph.stands.fuchsia/
- ☐ http://hackmegraph.stands.fuchsia/graphql
- ☐ http://bricks.stands.fuchsia/
- ☐ http://10.0.0.101:8080
- ☐ http://metasploitable3.stands.fuchsia/
- ☐ http://10.0.0.101
- ☐ http://vulnbank.stands.fuchsia/graphql
- ☐ http://target-fix-regexp.solidpoint

ВПЕРЕД →

ОТМЕНИТЬ СОЗДАТЬ

Снимок экрана 101. Вкладка «Общая информация» с установленными параметрами

Примечание. Если не выбрать ни одного модуля анализа поверхности атаки, модули взлома не отработают должным образом.

- На вкладке «Дедупликация» можно настроить параметры дедупликации, заполнив форму необходимыми данными, после чего нажать кнопку «ВПЕРЕД» (см. снимок экрана 102).

Новое веб-сканирование

- ✓ Общая информация
- 2 Дедупликация**
- 3 Дополнительная информация
- 4 Экспериментальные параметры
- 5 Предпросмотр

Дедупликация

Дедупликация страниц

☒ Включить дедупликацию страниц на основе встроенных алгоритмов

Минимальное число страниц: Целевое число страниц:

Число страниц, при достижении которого начнется дедупликация (0 – моментально) Алгоритм будет объединять дубликаты страниц, стремясь к указанному количеству (0 – не ограничено)

☒ Включить дедупликацию страниц на основе регулярных выражений

Правила +

Правила для дедупликации страниц не добавлены

Дедупликация конечных точек

☒ Включить дедупликацию конечных точек на основе встроенных алгоритмов

Режим:

☒ Включить дедупликацию конечных точек на основе регулярных выражений

Правила +

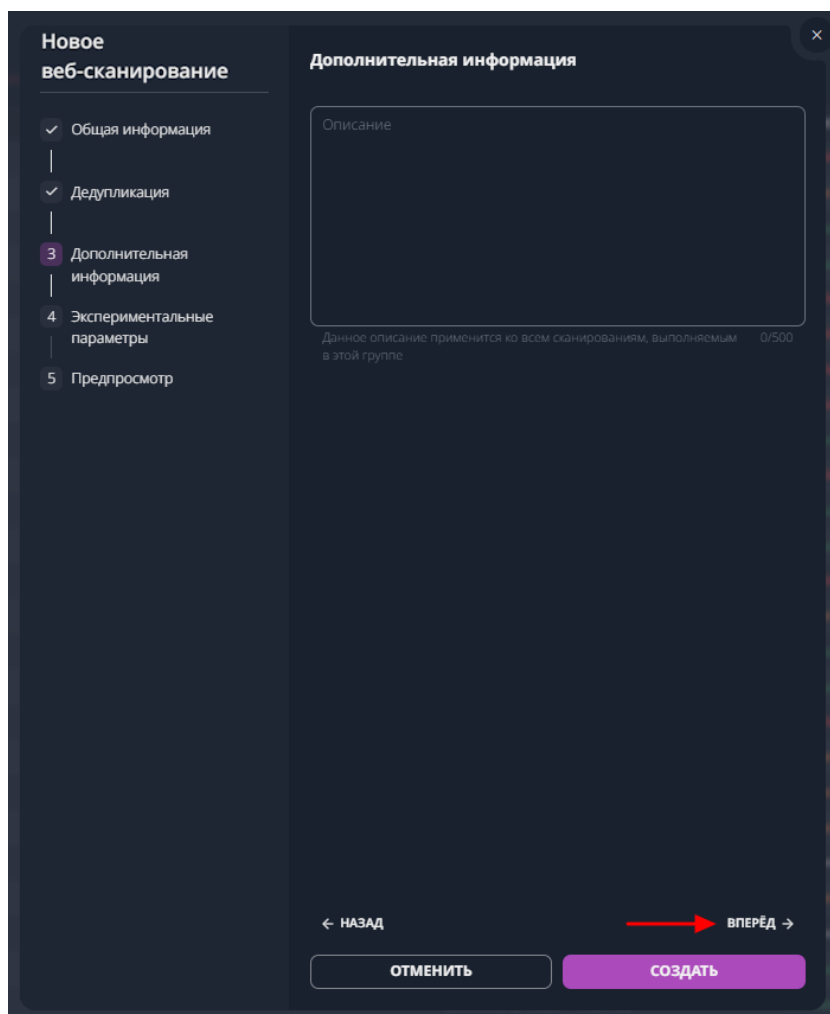
Правила для дедупликации конечных точек не добавлены

← НАЗАД → ВПЕРЕД

ОТМЕНИТЬ СОЗДАТЬ

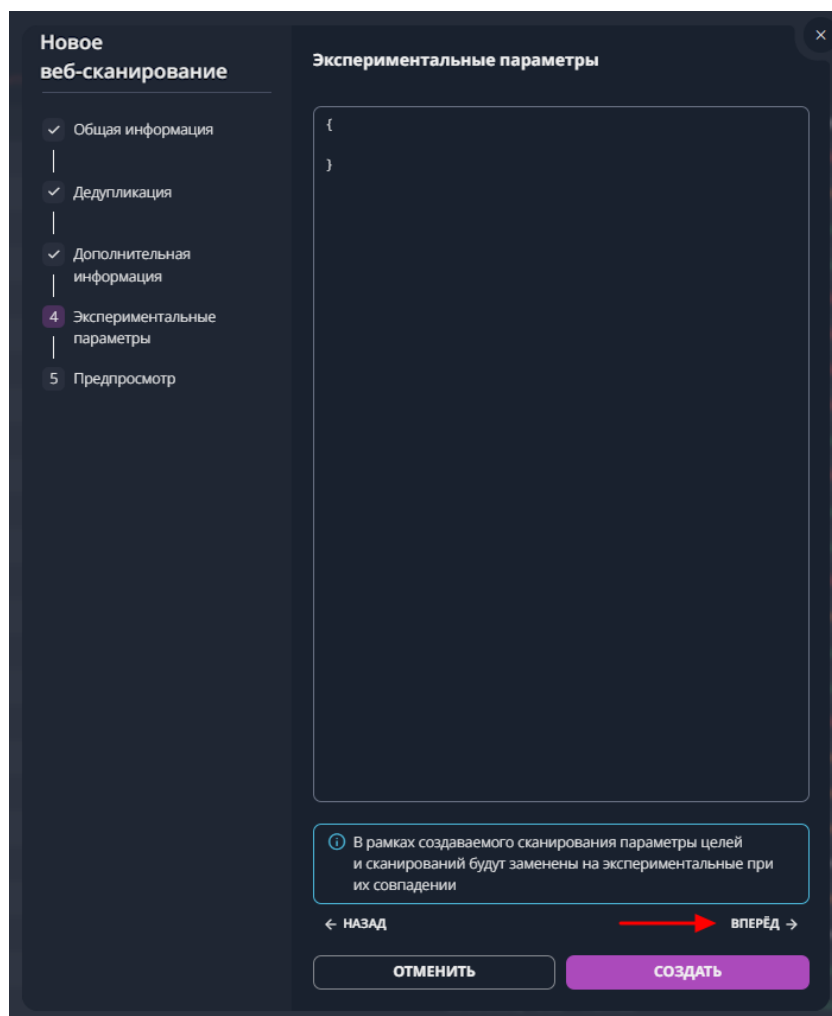
Снимок экрана 102. Вкладка «Дедупликация»

- На вкладке «Дополнительная информация» можно добавить описание (не более 500 символов), которое применится ко всем сканированиям, выполняемым в этой группе (см. снимок экрана 103).



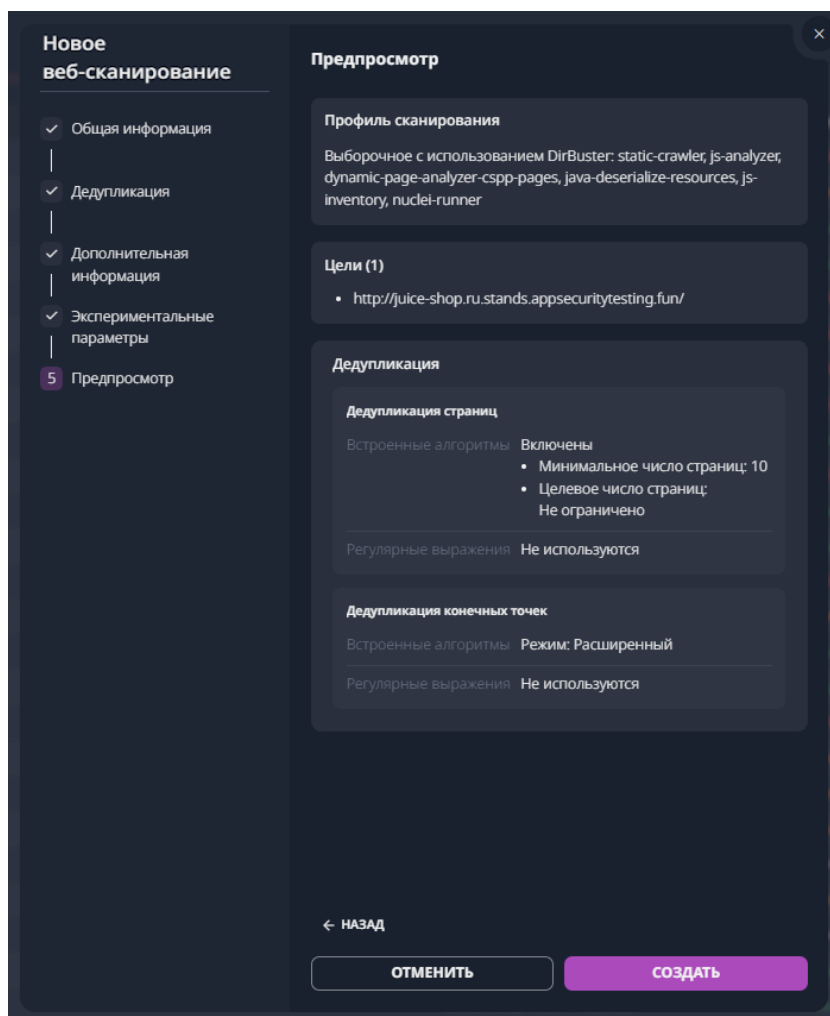
Снимок экрана 103. Вкладка «Дополнительная информация»

4. На вкладке «Экспериментальные параметры», при необходимости, можно добавить экспериментальные параметры (при создании сканирования через веб-интерфейс нельзя задать конфигурацию, не поддерживаемую сканером), затем следует нажать кнопку «ВПЕРЕД» (см. снимок экрана 104).



Снимок экрана 104. Вкладка «Экспериментальные параметры»

- Вкладка «Предпросмотр» является завершающей. На вкладке отображаются все настройки, заданные при создании сканирования. Если требуется изменить настройки, то следует воспользоваться кнопкой «НАЗАД» до перехода на нужную вкладку либо нажать на название вкладки и внести изменения. После установки необходимых параметров необходимо в правом нижнем углу нажать кнопку «СОЗДАТЬ» для запуска сканирования (см. снимок экрана 105).



Снимок экрана 105. Вкладка «Предпросмотр»

Примечание. При создании сканирования (см. шаги 1 – 5) процесс создания можно прервать на любом этапе, нажав в левом нижнем углу кнопку «ОТМЕНИТЬ» или крестик закрытия окна «✕» в правом верхнем углу. При этом появится окно «Несохранённые изменения», в котором нужно подтвердить намерение нажатием кнопки «ПРОДОЛЖИТЬ БЕЗ СОХРАНЕНИЯ». Кнопка «ВЕРНУТЬСЯ К РЕДАКТИРОВАНИЮ» или крестик «✕» в правом верхнем углу прерывают отмену создания сканирования (см. снимок экрана 81).

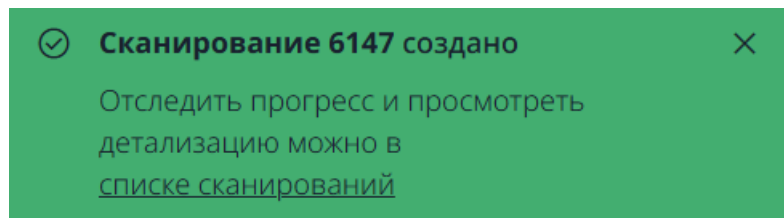
7.2. Запуск сканирования

Сканирование происходит в два последовательных этапа. Сначала задействуются модули анализа поверхности атаки для поиска всех точек входа, затем на основании полученных результатов модули обнаружения недостатков выявляют уязвимости (список модулей сканера SolidPoint DAST представлен в приложении А).

Скорость сканирования зависит от мощности процессора (CPU) и объема оперативной памяти (RAM) машины, на которой развёрнут сканер, а также сложности веб-приложения.

Запустить сканирование цели можно одним из пяти способов:

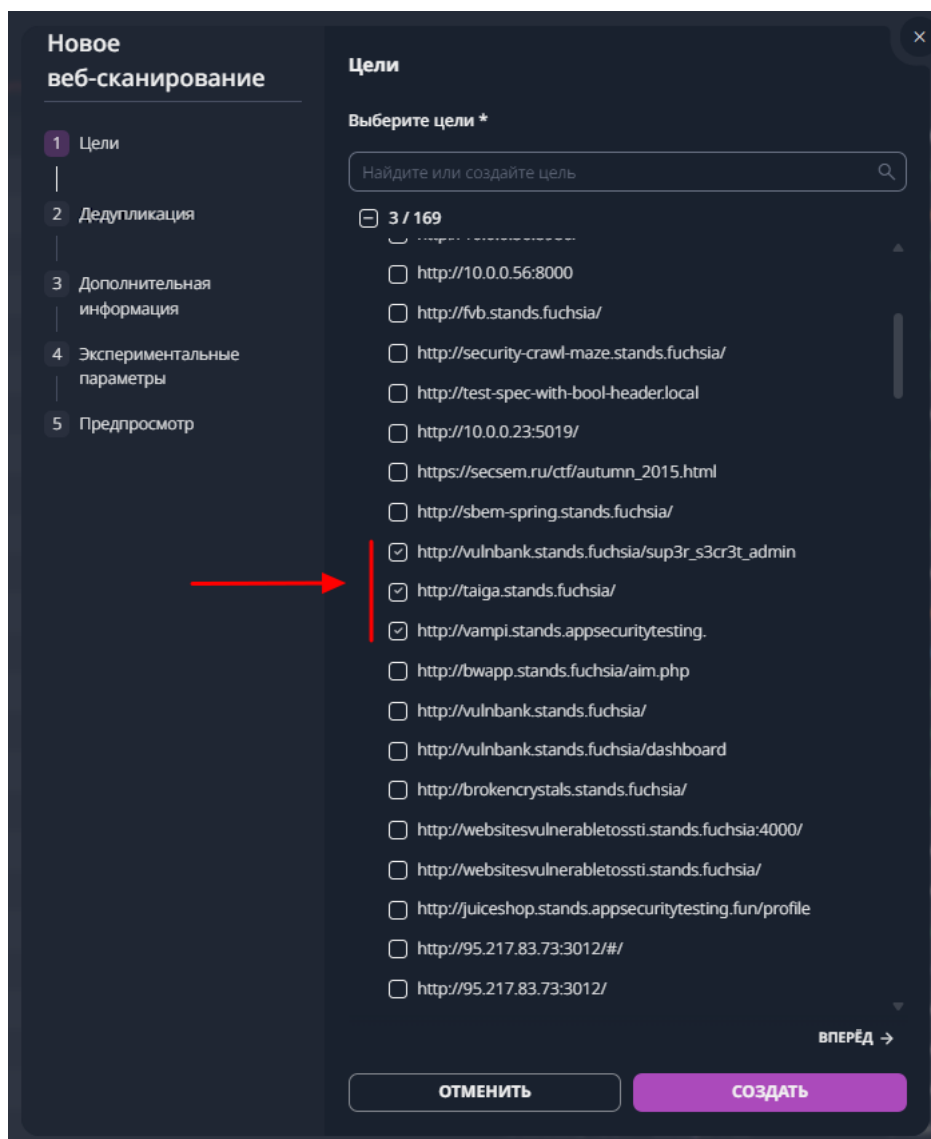
- В окне «Цели» над списком целей нажатием кнопки «Сканировать» после включения чекбокса выбранной цели (см. п. 1 раздела 5.3 «Окно «Цели»»);
- В окне «Цели» нажатием кнопки «Сканировать» в конце строки адреса цели в контекстном меню (см. п. 2, раздела 5.3 «Окно «Цели»»). После запуска сканирования в окне «Цели» в правом нижнем углу экрана появится уведомление о создании сканирования (см. снимок экрана 106).



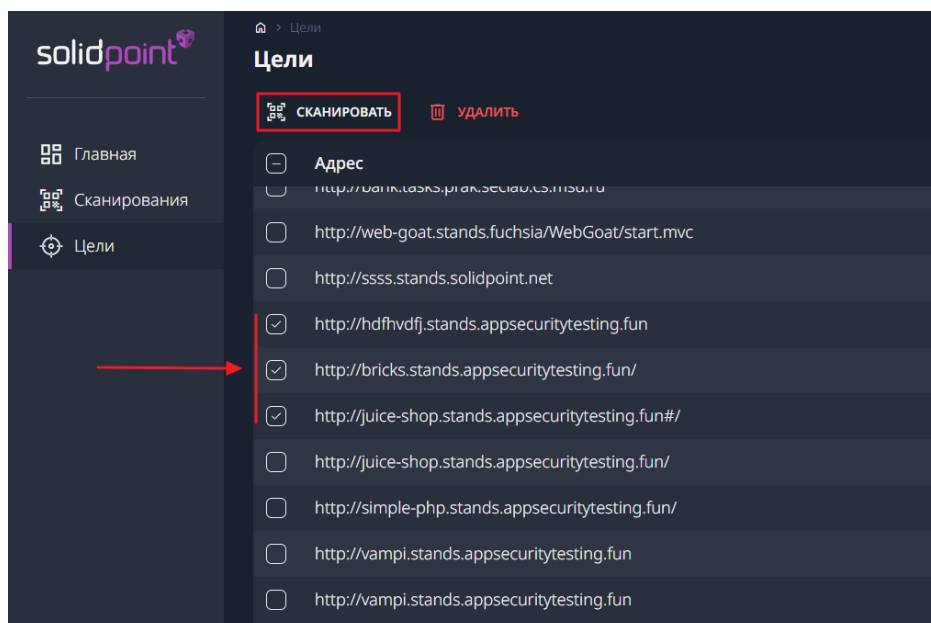
Снимок экрана 106. Уведомление о создании сканирования

- В мастере создания сканирования после выбора цели (см. п. 1, раздела 7.1);
- В мастере создания сканирования после заполнения всех параметров сканирования, на вкладке «Предпросмотр» (см. п. 5, раздела 7.1);
- Посредством API-запроса, согласно спецификации API (отрывается при нажатии надписи «Спецификация API» в нижней части меню сканера).

Можно одновременно запустить сканирование двух и более целей, выбрав в мастере создания сканирования в поле «Выберите цели» (см. снимок экрана 107) или в окне «Цели» (см. снимок экрана 108).

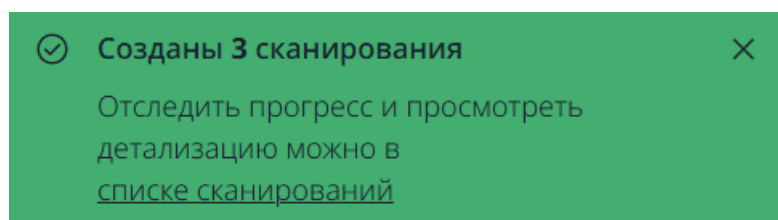


Снимок экрана 107. Запуск нескольких сканирований в мастере создания сканирования



Снимок экрана 108. Запуск нескольких сканирований в окне «Цели»

После запуска сканирований в правом нижнем углу экрана появится уведомление о создании сканирований (см. снимок экрана 109).

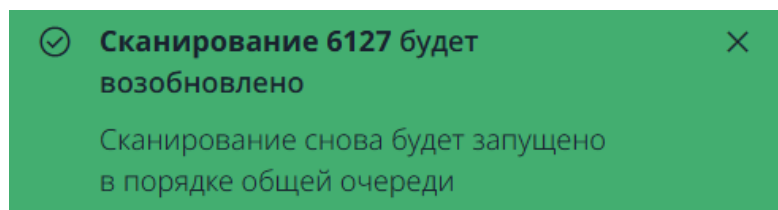


Снимок экрана 109. Уведомление о создании нескольких сканирований

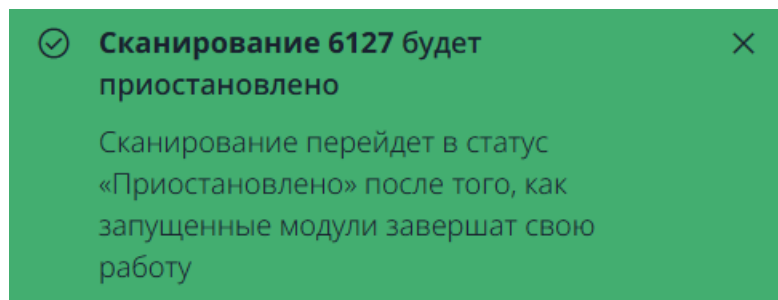
7.3. Управление сканированием

Повторить, приостановить, возобновить, прервать или удалить сканирование, в зависимости от его статуса (см. таблицу 14), можно в окне «Сканирования» (см. п. 1, 2, раздел 5.2 «Окно «Сканирования»»). В секторе «Общая информация» при статусах в «Процессе», «Приостановлено» и «Успешно» сканирование можно прервать, возобновить или повторить, нажав соответствующие кнопки.

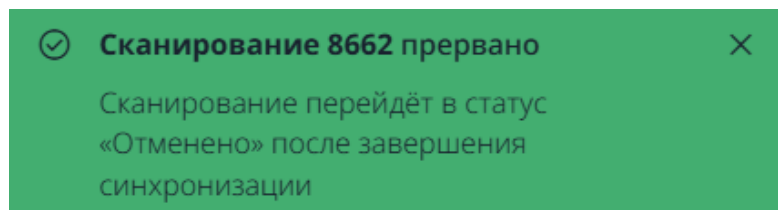
Уведомление о возобновлении (см. снимок экрана 110), приостановке (см. снимок экрана 111), прерывании (см. снимок экрана 112) и удалении (см. снимок экрана 113) сканирования появляются в правом нижнем углу экрана.



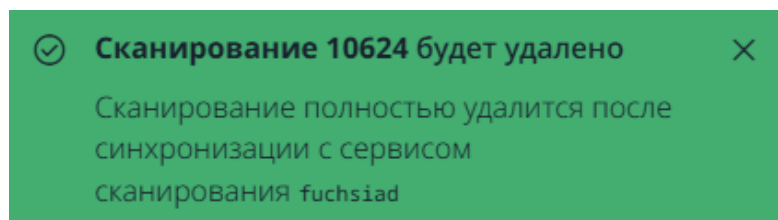
Снимок экрана 110. Уведомление о возобновлении сканирования



Снимок экрана 111. Уведомление о приостановке сканирования

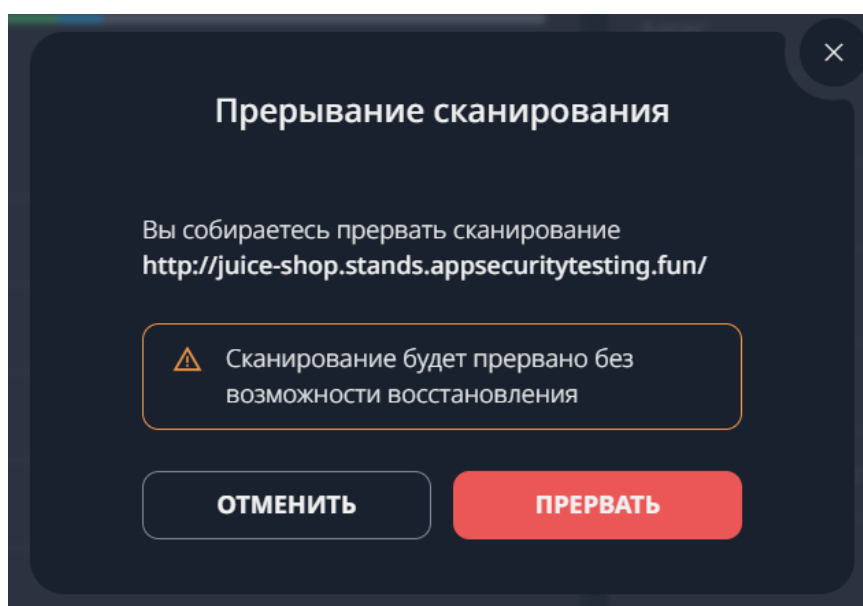


Снимок экрана 112. Уведомление о прерывании сканирования



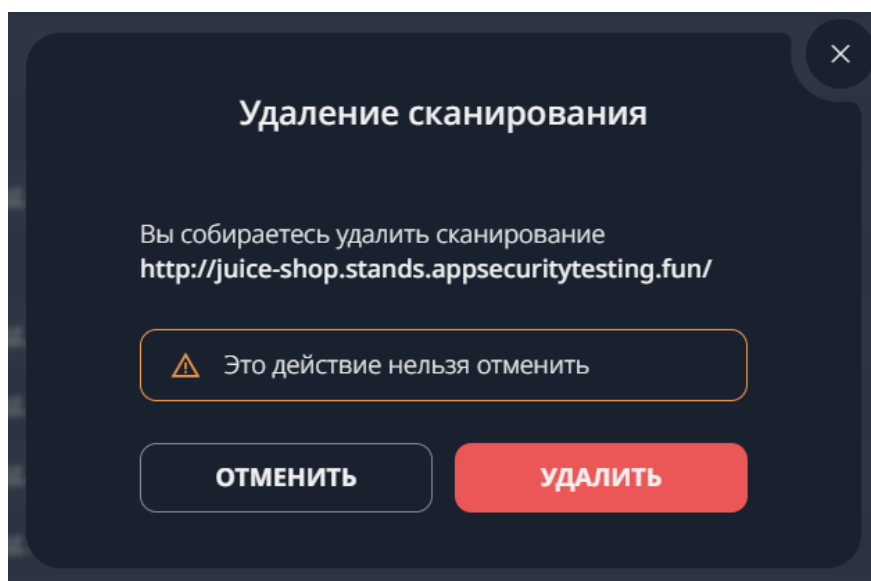
Снимок экрана 113. Уведомление об удалении сканирования

При прерывании сканирования появится окно «Прерывание сканирования», в котором надо подтвердить намерение нажатием кнопки «ПРЕРВАТЬ». Кнопка «ОТМЕНИТЬ» или крестик «» в правом верхнем углу закрывают окно без прерывания сканирования (см. снимок экрана 114).



Снимок экрана 114. Окно «Прерывание сканирования»

При удалении сканирования появится окно «Удаление сканирования», в котором надо подтвердить намерение нажатием кнопки «УДАЛИТЬ». Кнопка «ОТМЕНИТЬ» или крестик «✕» в правом верхнем углу закрывают окно без удаления сканирования (см. снимок экрана 115).



Снимок экрана 115. Окно «Удаление сканирования»

После подтверждения удаления сканирование будет удалено из списка сканирований.

Для управления сканированиями доступны групповые операции: «Приостановить», «Возобновить», «Прервать» и «Удалить». Чтобы применить действие к нескольким сканированиям, необходимо выбрать их с помощью чекбоксов.

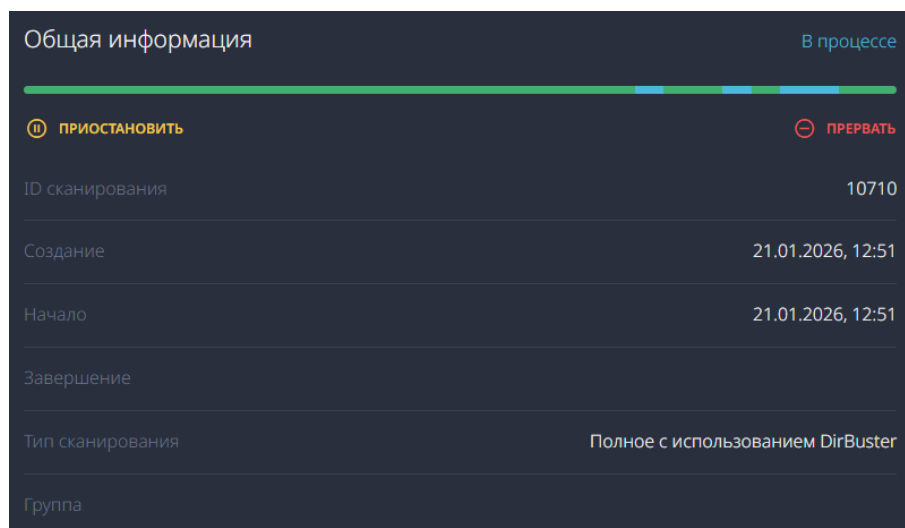
7.4. Процесс сканирования

Запуск сканирования сопровождается его переходом в статус «В ожидании», а затем статус в «В процессе».

Для просмотра подробной информации о процессе сканирования следует нажать на адрес цели. Откроется окно с подробной информацией о сканировании в реальном времени. Информационные секторы в данном окне такие же, как и у завершенных сканирований, описанных в подразделе 5.2.1 «Подробная информация о сканировании».

В верхней части сектора «Общая информация» расположена шкала прогресса работы модулей. Поскольку некоторые модули выполняют сканирование нелинейно, шкала отражает прогресс делением по модулям в реальном времени. Также в секторе «Общая информация» отображаются данные сканирования о (см. снимок экрана 116):

- ID сканирования;
- дате создания сканирования;
- дате и времени начала сканирования;
- дате и времени завершения сканирования;
- типе сканирования;
- группе сканирования.



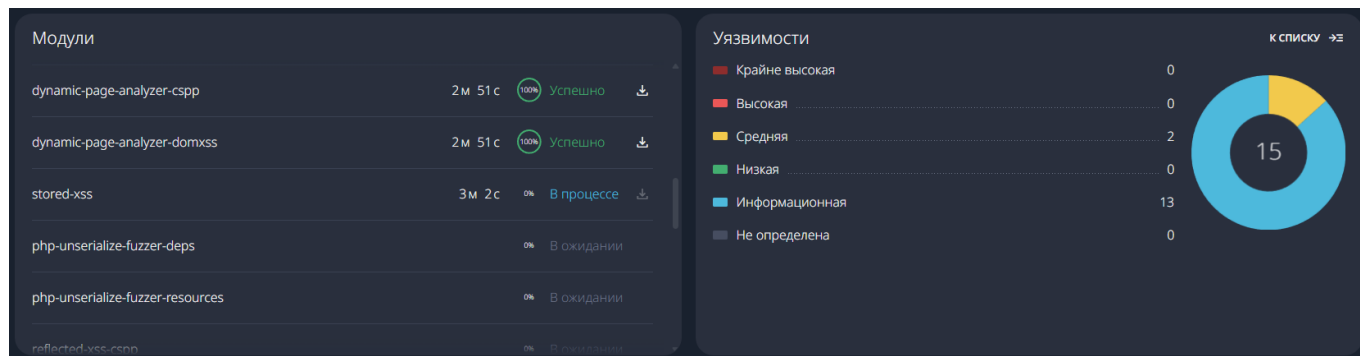
Снимок экрана 116. Сектор «Общая информация» действующего сканирования

В данном секторе можно приостановить или прервать сканирование (см. подраздел 7.3 «Управление сканированием»).

В секторе «Информация о цели» данные в зависимости от статуса сканирования не меняются (см. описание в подразделе 5.2.1 «Подробная информация о сканировании»).

В секторе со статистикой о сканировании данные меняются в течение продолжительности времени сканирования (см. описание в подразделе 5.2.1 «Подробная информация о сканировании»). В случае приостановки сканирования время сканирования не останавливается.

В секторах «Модули» и «Уязвимости» отображаются данные в реальном времени о статусах модулей и найденных уязвимостях (см. снимок экрана 117).



Снимок экрана 117. Секторы «Модули» и «Уязвимости» в момент сканирования

Найденные уязвимости можно просмотреть еще при незаконченном сканировании. Для этого следует нажать кнопку «К СПИСКУ» в правом верхнем углу сектора «Уязвимости» (более подробно о найденных уязвимостях см. в подразделе 5.2.1 «Подробная информация о сканировании»).

Сканирование считается завершенным, когда оно переходит в статусы «Успешно», «С ошибкой», «Замечаниями». Данные статусы будут отображены в секторе «Общая информация» и в списке сканирований окна «Сканирования».

Во время сканирования, а также после его завершения можно просмотреть отчеты «Конечные точки» и «Технический отчет». После завершения сканирования отчет о сканировании как полный, так и краткий, можно сгенерировать в формате файла «.pdf» (подробнее об отчетах см. в подразделе 5.2.2 «Отчеты»).

8. ВЗАИМОДЕЙСТВИЕ С API

Спецификация API сканера SolidPoint DAST расположена по следующим адресам:

- Swagger — <https://ru.cloud.solidpoint.net/swagger>;
- Redocly — <https://ru.cloud.solidpoint.net/redocly>.

8.1. Аутентификация по токenu

Токен создаётся каждый раз при входе в систему. При необходимости, его можно создать с помощью запроса `POST /api/tokens`.

При запросах токен, независимо от способа генерации, может отправляться следующими способами:

- в cookies:

```
curl --location '/api/users/current' --header 'Cookie: auth_token={jwt}'
```

- в заголовке Authorization:

```
curl --location '/api/users/current' --header 'Authorization: Bearer {jwt}'
```

- в заголовке X-Token:

```
curl --location '/api/users/current' --header 'X-Token: {value}'
```

Важно! В cookies и в заголовке Authorization токен передается в формате JWT. Данный формат используется только при логине и создании токена. В остальных случаях необходимо использовать значение value полученной модели токена в заголовке X-Token.

8.2. Примеры обращений к API

8.2.1. Запросы к серверной части

Важно! В последующих примерах в качестве адреса экземпляра сканера используется <https://cloud.solidpoint.net>. При составлении запросов необходимо использовать персональный адрес.

Примеры запросов:

- Указание токена в заголовке X-Token для его последующего использования при аутентификации (подробнее см. в подразделе 8.1 «Аутентификация по токenu»): `curl https://cloud.solidpoint.net/api/scans --header "X-Token: <token>"`;
- Аутентификация через Cookie: `--header 'Cookie: auth_token=jwt'`;
- Аутентификация через токен Bearer: `--header 'Authorization: Bearer jwt'`;
- Изменение пароля для суперадминистратора (однопользовательский режим):

```
curl --location --request PUT \
'https://cloud.solidpoint.net/api/users/current/password' \
--header 'Content-Type: application/json' \
--data '{
  "newPassword": "admin",
```

```
"oldPassword": ""
}'
```

- Вход в систему как суперадминистратор:

```
curl --location --request POST 'https://cloud.solidpoint.net/api/auth/login'
--header 'Content-Type: application/json'
--data-raw '{
  "tenantName": "",
  "email": "admin@fuchsia.local",
  "password": "admin"
}'
```

- Регистрация в системе:

```
curl --location --request POST 'https://cloud.solidpoint.net/api/auth/register'
--header 'Content-Type: application/json'
--data-raw '{
  "tenantName": "",
  "email": "user@test.ru",
  "password": "testuser123",
  "name": "user",
  "companyName": "test",
  "occupation": "test"
}'
```

- Вход в систему:

```
curl --location --request POST 'https://cloud.solidpoint.net/api/auth/login'
--header 'Content-Type: application/json'
--data-raw '{
  "tenantName": "",
  "email": "user@test.ru",
  "password": "testuser123"
}'
```

- Выход из системы:

```
curl --location --request POST 'https://cloud.solidpoint.net/api/auth/logout'
--header 'Cookie: auth_token=jwt'
```

Создание нового тенанта:

```
curl --location --request POST 'https://cloud.solidpoint.net/api/tenants'
--header 'Content-Type: application/json'
--header 'Authorization: Bearer jwt1'
--header 'Cookie: auth_token=jwt2'
--data '{
  "name": "test",
  "hostNameConstraints": ["test"],
  "scanEndpointsIDs": [1]
}'
```

- Добавление или удаление ограничения на имя хоста клиента:

```
curl --location --request PATCH 'https://cloud.solidpoint.net/api/tenants/2/host-name-constraints'
--header 'Content-Type: application/json'
--header 'Cookie: auth_token=jwt'
--data '{
  "add": ["test2", "test3"],
  "delete": ["test"]
}'
```

8.2.2. Запросы к сканеру

Примеры запросов:

- Добавление конечной точки для сканирования:

```
curl --location --request POST 'https://cloud.solidpoint.net/api/scan-endpoints'
--header 'Content-Type: application/json'
--header 'Cookie: auth_token=jwt'
--data '{
  "name": "test",
  "address": "unix:///tmp/fuchsia/fuchsiad.sock"
}'
```

- Обновление конечной точки для сканирования:

```
curl --location --request PATCH 'https://cloud.solidpoint.net/api/scan-endpoints/1'
--header 'Content-Type: application/json'
--header 'Cookie: auth_token=jwt'
--data '{
  "name": "new_name"
}'
```

- Получение конечной точки по ID:

```
curl --location --request GET 'https://cloud.solidpoint.net/api/scan-endpoints/1'
--header 'Cookie: auth_token=jwt'
```

- Получение всех конечных точек:

```
curl --location --request GET 'https://cloud.solidpoint.net/api/scan-endpoints'
--header 'Authorization: Bearer jwt'
--header 'Cookie: auth_token=jwt'
```

- Добавление или удаление конечных точек тенанта:

```
curl --location --request PATCH 'https://cloud.solidpoint.net/api/tenants/2/scan-endpoints'
```

```
--header 'Content-Type: application/json'
--header 'Cookie: auth_token=jwt'
--data '{
  "add": [1],
  "delete": []
}'
```

- Получение тенанта по ID:

```
curl --location --request GET 'https://cloud.solidpoint.net/api/tenants/2'
--header 'Cookie: auth_token=jwt'
```

- Получение списка всех тенантов:

```
curl --location --request GET 'https://cloud.solidpoint.net/api/tenants'
--header 'Cookie: auth_token=jwt'
```

- Получение списка всех пользователей с заданной ролью в определенном тенанте:

```
curl --location --request GET 'https://cloud.solidpoint.net/api/users?role=unknown&tenant=test'
--header 'Cookie: auth_token=jwt'
```

- Добавление пользователя в тенант:

```
curl --location --request POST 'https://cloud.solidpoint.net/api/users'
--header 'Content-Type: application/json'
--header 'Cookie: auth_token=jwt'
--data-raw '{
  "tenantName": "test",
  "email": "user@test.ru",
  "password": "testuser123",
  "name": "user",
  "role": "user",
  "companyName": "test",
  "occupation": "test"
}'
```

- Активация пользователя по ID (возможно указать tenantName вместо tenantID):

```
curl --location --request PUT 'https://cloud.solidpoint.net/api/users/2/activate'
--header 'Content-Type: application/json'
--header 'Cookie: auth_token=jwt'
--data '{
  "role": "user",
  "tenantID": 1
}'
```

- Активация пользователя по email (возможно указать tenantName вместо tenantID):

```
curl --location --request PUT
'https://cloud.solidpoint.net/api/users/user2@test.ru/activate'
--header 'Content-Type: application/json'
--header 'Cookie: auth_token=jwt'
--data '{
    "role": "user",
    "tenantID": 1
}'
```

- Активация всех пользователей:

```
curl --location --request PUT
'https://cloud.solidpoint.net/api/users/activate'
--header 'Content-Type: application/json'
--header 'Cookie: auth_token=jwt'
--data '{
    "role": "user"
}'
```

8.2.3. Работа со сканированиями

Примеры запросов:

- Запуск нового сканирования (можно использовать url вместо targetID):

```
curl --location 'https://cloud.solidpoint.net/api/scans'
--header 'Content-Type: application/json'
--header 'Cookie: auth_token=jwt'
--data '{
    "targetID": 1
}'
```

- Завершение сканирования по ID:

```
curl --location --request PUT
'https://cloud.solidpoint.net/api/scans/cancel/:id'
--header 'Cookie: auth_token=jwt'
```

Примеры работы с параметрами аутентификации сканирований

Работа с параметрами аутентификации сканирований ведется через цели. Примеры:

- Работа с HTTP Basic Auth:

```
curl --location --request PATCH
'https://cloud.solidpoint.net/api/targets/45'
--header 'Content-Type: application/json'
--header 'Cookie: auth_token=jwt'
--data '{
    "appAuth": {
        "httpBasicAuth": [
            {
                "userName": "test2",
```

```

        "password": "qwerty123"
    }
  ]
}
}'

```

- **Работа с Cookies:**

```

curl          --location          --request          PATCH
'https://cloud.solidpoint.net/api/targets/10'
--header 'Content-Type: application/json'
--header 'Cookie: auth_token=jwt'
--data '{
  "appAuth": {
    "cookies": [
      {
        "name": "session",
        "value": "429415c6-ee49-438b-a075-ef5e6fc141c1"
      }
    ]
  }
}'

```

- **Работа с Headers:**

```

curl          --location          --request          PATCH
'https://cloud.solidpoint.net/api/targets/64'
--header 'Content-Type: application/json'
--header 'Cookie: auth_token=jwt'
--data '{
  "appAuth": {
    "headers": [
      {
        "name": "X-Auth-Token",
        "value": "91e58978-d3fd-49ce-857c-a6a17f82118b"
      }
    ]
  }
}'

```

- **Работа с сертификатами:**

```

curl          --location          --request          PATCH
'https://cloud.solidpoint.net/api/targets/70'
--header 'Content-Type: application/json'
--header 'Cookie: auth_token=jwt'
--data '{
  "appAuth": {
    "certificates": [
      {
        "certificate": "crt",
        "key": "key"
      }
    ]
  }
}'

```

```
    ]
  }
}'
```

Если у цели много разных параметров аутентификации, то их можно либо перезаписать, либо обнулить. Это делается с помощью отправки дополнительного параметра `rewriteAppAuth`. Например, у цели есть HTTP Basic Auth и Cookies, а необходимо, чтобы был только сертификат. Тогда нужно отправить только сертификат с дополнительным параметром `rewriteAppAuth`. При обнулении следует отправить только один дополнительный параметр `rewriteAppAuth`. Примеры:

- Перезапись всех параметров аутентификации на сертификат:

```
curl --location --request PATCH 'https://cloud.solidpoint.net/api/targets/70'
--header 'Content-Type: application/json'
--header 'Cookie: auth_token=jwt'
--data '{
  "rewriteAppAuth": true,
  "appAuth": {
    "certificates": [
      {
        "certificate": "...",
        "key": "..."
      }
    ]
  }
}'
```

- Обнуление всех параметров аутентификации цели:

```
curl --location --request PATCH 'https://cloud.solidpoint.net/api/targets/70'
--header 'Content-Type: application/json'
--header 'Cookie: auth_token=jwt'
--data '{
  "rewriteAppAuth": true
}'
```

- Добавление LDAP-аутентификации:

```
curl --location --request POST 'https://cloud.solidpoint.net/api/auth'
--header 'Content-Type: application/json'
--header 'Cookie: auth_token=jwt'
--data '{
  "type": "LDAP",
  "parameters": {
    "label": "ldap",
    "host": "dev.solidwall.io",
    "port": 636,
    "baseDN": "ou=users,dc=solidwall,dc=io",
    "uid": "uid",
    "defaultAttributes": true,
    "tls": true,
  }
}'
```

```

    "roles": {
      "user": "objectClass=inetOrgPerson"
    }
  }
}'

```

- Получение списка всех настроенных аутентификаций:

```

curl --location 'https://cloud.solidpoint.net/api/auth'
--header 'Cookie: auth_token=jwt'

```

- Обновление аутентификации (URL содержит идентификатор записи):

```

curl --location --request PATCH 'https://cloud.solidpoint.net/api/auth/17'
--header 'Content-Type: application/json'
--header 'Cookie: auth_token=jwt'
--data '{
  "disabled": true
}'

```

При обновлении `parameters` их нужно передавать целиком, так как вложенный ключ идет как полное значение.

- Удаление существующей записи (URL содержит идентификатор записи):

```

curl --location --request DELETE 'https://cloud.solidpoint.net/api/auth/17'
--header 'Cookie: auth_token=jwt'

```

Примеры работы со спецификацией для сканирований

Работа со спецификацией для сканирований ведется через цели. Спецификация передается в формате `base64` (... – обозначение в примерах далее). Примеры:

- Создание цели с заданием спецификации:

```

curl --location --request POST 'https://cloud.solidpoint.net/api/targets'
--header 'Content-Type: application/json'
--header 'Cookie: auth_token=jwt'
--data '{
  "url": "https://test.test",
  "specification": {
    "openAPI": {
      "specification": "..."
    },
    "disabled": true
  }
}'

```

- Добавление спецификации в существующую цель:

```

curl --location --request PATCH 'https://cloud.solidpoint.net/api/targets/2'
--header 'Content-Type: application/json'
--header 'Cookie: auth_token=jwt'

```

```
--data '{
  "specification": {
    "openAPI": {
      "specification": "...",
    },
    "disabled": false
  }
}'
```

Параметр `disabled` отвечает за передачу спецификации в сканирование. Если `disabled: true`, то спецификация не будет передана в запрос на сканирование.

Спецификацию цели также можно либо перезаписать, либо обнулить. Это осуществляется с помощью отправки дополнительного параметра `rewriteSpec`. Например, у цели есть несколько спецификаций, а необходимо, чтобы была только одна. В таком случае следует отправить только нужную спецификацию с дополнительным параметром `rewriteSpec`. При обнулении же необходимо отправить только один дополнительный параметр `rewriteSpec`.

Важно! При обнулении параметр `disabled` принимает значение `false`, однако спецификация не подхватится при сканировании, так как она пустая (обнулена).

```
curl --location --request PATCH 'https://cloud.solidpoint.net/api/targets/2'
--header 'Content-Type: application/json'
--header 'Cookie: auth_token=jwt'
--data '{
  "rewriteSpec": true,
  "specification": {
    "openAPI": {
      "specification": "...",
    },
    "disabled": false
  }
}'
```

- Перенос сканирования из тенанта по умолчанию:

```
curl --location --request PATCH 'https://cloud.solidpoint.net/api/scans/replace-tenant'
--header 'Content-Type: application/json'
--header 'Cookie: auth_token=jwt'
--data '{
  "scanIDs": [1218, 1217, 1216, 850, 796, 797],
  "tenantID": 2
}'
```

8.3. Работа с аутентификационными данными цели

8.3.1. Типы аутентификационных данных

Аутентификация — процедура проверки подлинности введённых пользователем данных для подтверждения доступа.

Пользователь может использовать различные типы аутентификационных данных.

Базовая HTTP-аутентификация

«Базовая» схема HTTP-аутентификации определена в документе «RFC 7617». Учетные данные передаются в виде пар «ID пользователя» + «пароль», закодированных с использованием метода Base64.

Заголовки запроса

HTTP-заголовки позволяют клиенту и серверу отправлять дополнительную информацию с запросом или ответом. Они могут содержать описание данных и информацию, необходимую для взаимодействия между клиентом и сервером. В HTTP-заголовке содержится не чувствительное к регистру название, а затем после двоеточия непосредственно значение.

Куки

Куки — это небольшой фрагмент данных, который сервер отправляет браузеру пользователя. Браузер может сохранить этот фрагмент у себя и отправлять на сервер с каждым последующим запросом. С помощью кук можно сохранить любую информацию о состоянии.

TLS-сертификаты

Цифровой сертификат удостоверяет подлинность веб-сайта и позволяет использовать зашифрованное соединение. Использование сертификатов гарантирует, что данные, передаваемые между пользователями и веб-сайтами или между двумя системами, невозможно прочитать сторонним лицам или системам.

Локальное хранилище

Интернет-хранилище — это программные методы и протоколы веб-приложения, используемые для хранения данных в веб-браузере. Оно представляет собой постоянное хранилище данных, похожее на куки, но со значительно большей ёмкостью и без хранения информации в заголовке запроса HTTP. Для локального хранилища характерно сохранение данных после завершения сессии в браузере.

8.3.2. Взаимодействие

Для всех вышеперечисленных типов аутентификационных данных применимы следующие операции:

- добавление;
- обновление;
- запрос;
- удаление.

Эти операции доступны для целей через HTTP API в разделе «Target» по адресу <https://ru.cloud.solidpoint.net/swagger>, а также в панели управления.

Важно! Изменение аутентификационных данных для цели не затрагивает уже имеющиеся сканирования.

8.3.3. Проверка валидности аутентификационных данных

Данная проверка осуществляется с помощью механизма проверки аутентификации. Подробнее с принципами работы и конфигурацией можно ознакомиться в приложении А «Аутентификация в сканируемых приложениях».

8.3.4. Обновление аутентификационных данных

Периодическое обновление сеанса осуществляется двумя механизмами обновления аутентификационных данных:

- с помощью HTTP-запроса (см. приложение А.2 «Обновление аутентификационных данных с помощью HTTP-запроса»);
- с помощью браузерного сценария (см. приложение А.3 «Обновление аутентификационных данных с помощью браузерного сценария»).

8.3.5. Примеры

Добавление конфигурации механизма обновления аутентификационных данных с помощью HTTP-запроса для цели `http://auth-combined.stands.fuchsia` с помощью запроса `PATCH /api/targets/:id`:

```
{
  "authCheckingConfig": {
    "config": {
      "criteria": [
        {
          "interval": "10s",
          "kind": "FAILED",
          "request": {
            "url": "http://auth-combined.stands.fuchsia/health-check"
          },
          "responseConditions": {
            "statusCode": 401
          },
          "rounds": 1
        }
      ]
    },
    "enabled": true
  },
  "regexAuthRefresherConfig": {
    "config": {
      "request": {
        "body": "{\"username\":\"user2\",\"password\":\"password2\"}",
        "headers": {
          "Content-Type": "application/json"
        },
        "method": "POST",
        "url": "http://auth-combined.stands.fuchsia/signin"
      },
      "responseExtractors": [
```

```

    {
      "extractor": "session_token=(.*)"",
      "proxyParams": {
        "cookie": {
          "name": "session_token"
        },
        "hostname": "auth-combined.stands.fuchsia",
        "port": "",
        "scheme": "http"
      }
    }
  ],
  "enabled": true
}

```

Добавление конфигурации механизма обновления аутентификационных данных с помощью браузерного сценария для цели `http://juice-shop.stands.fuchsia` с помощью запроса `PATCH /api/targets/:id`:

```

{
  "authCheckingConfig": {
    "enabled": true,
    "config": {
      "criteria": [
        {
          "kind": "PASSED",
          "request": {
            "url": "http://juice-shop.stands.fuchsia"
          },
          "responseConditions": {
            "statusCode": 200
          }
        }
      ]
    }
  },
  "browserAuthRefresherConfig": {
    "enabled": true,
    "config": {
      "outputExtractors": [
        {
          "type": "TYPE_COOKIE",
          "selectors": ["token"]
        }
      ],
      "loginScript": {
        "inline": "base64_file"
      }
    }
  }
}

```

8.4. Ограничение URL-адресов цели

Список ограничений позволяет блокировать HTTP-запросы к ресурсам из списка. Ограничения описываются через консольный клиент `fuchsiactl` с помощью опции `--url-blacklist`, которая получает на вход регулярное выражение. Данная опция может быть использована повторно в случае, если необходимо задать несколько регулярных выражений.

8.4.1. Конфигурация

Конфигурация ограничений URL-адресов цели представлена в таблице 17.

Таблица 17. Конфигурация ограничений URL-адресов цели

Тип	Допустимые значения	Описание
enabled Логический	true, false	Регулирует использование списка ограничений URL-адресов
list Массив строк	Любые значения, проходящие валидацию	Массив URL-адресов, HTTP-запросы к которым будут заблокированы. Осуществляется валидация значений списка с помощью регулярных выражений

Важно! По умолчанию конфигурация списка ограничений URL-адресов не задана.

8.4.2. Пример

Добавление конфигурации списка ограничений URL-адресов с помощью запроса `PATCH /api/targets/:id`:

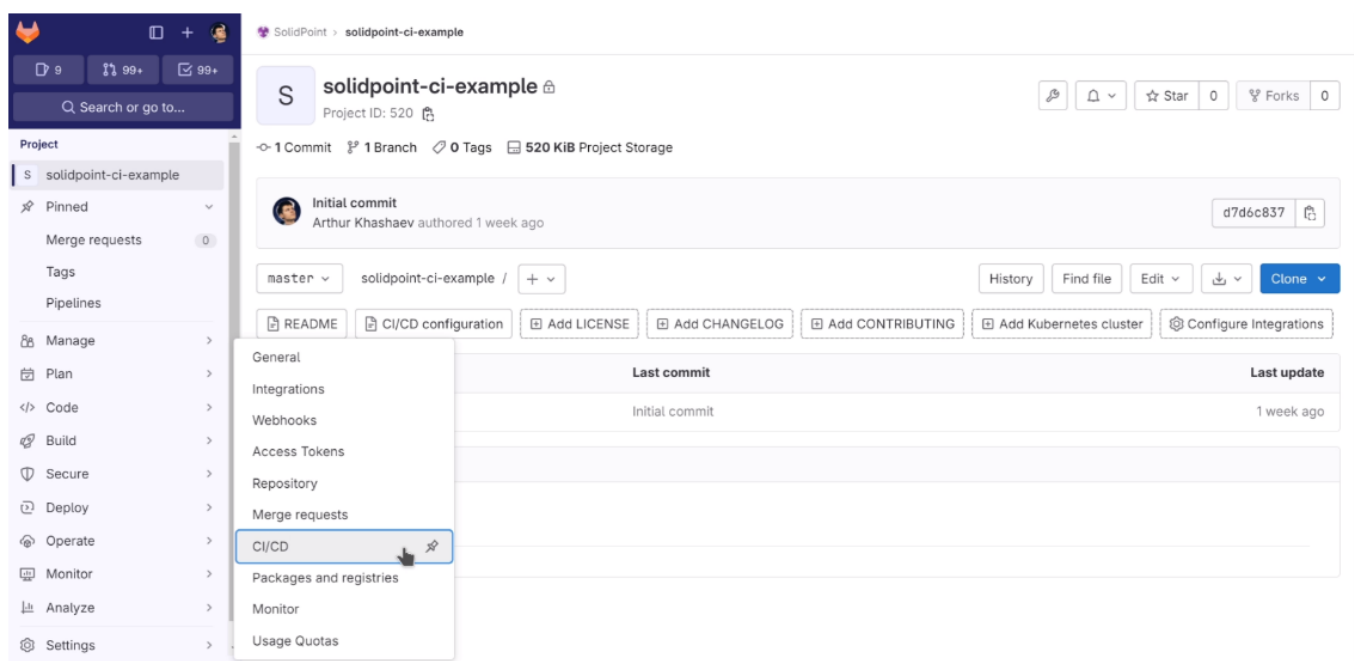
```
{
  "urlRestrictionList": {
    "enabled": true,
    "list": ["test", "test2"]
  }
}
```

9. ВСТРАИВАНИЕ В CI/CD. НАСТРОЙКА СКАНИРОВАНИЯ ВЕБ-ПРИЛОЖЕНИЙ С ПОМОЩЬЮ GITLAB

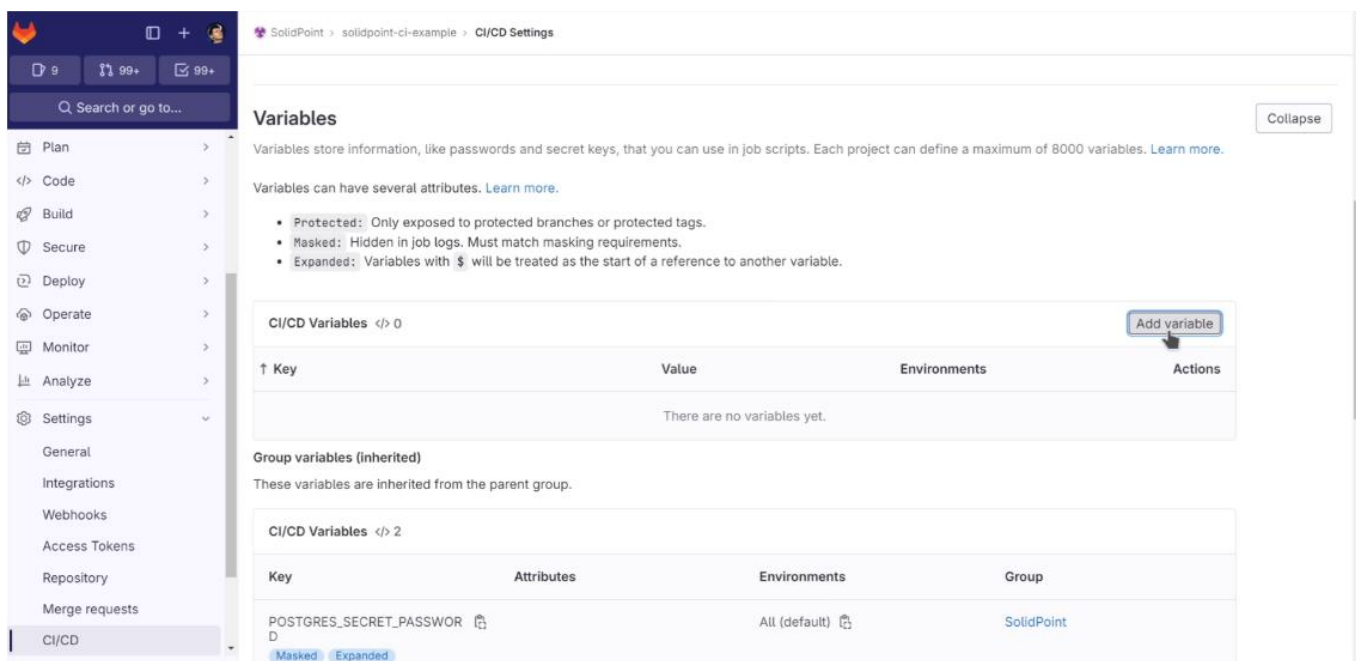
В данном разделе описана настройка в системе GitLab CI. Настройка в других системах выполняется аналогичным образом.

9.1. Добавление переменных окружения

Для добавления переменных окружения в GitLab необходимо выбрать «Настройки» → «CI/CD» → «Переменные» → «Добавить переменную» (см. снимки экрана 118, 119).



Снимок экрана 118. Путь к окну для добавления переменных, часть 1



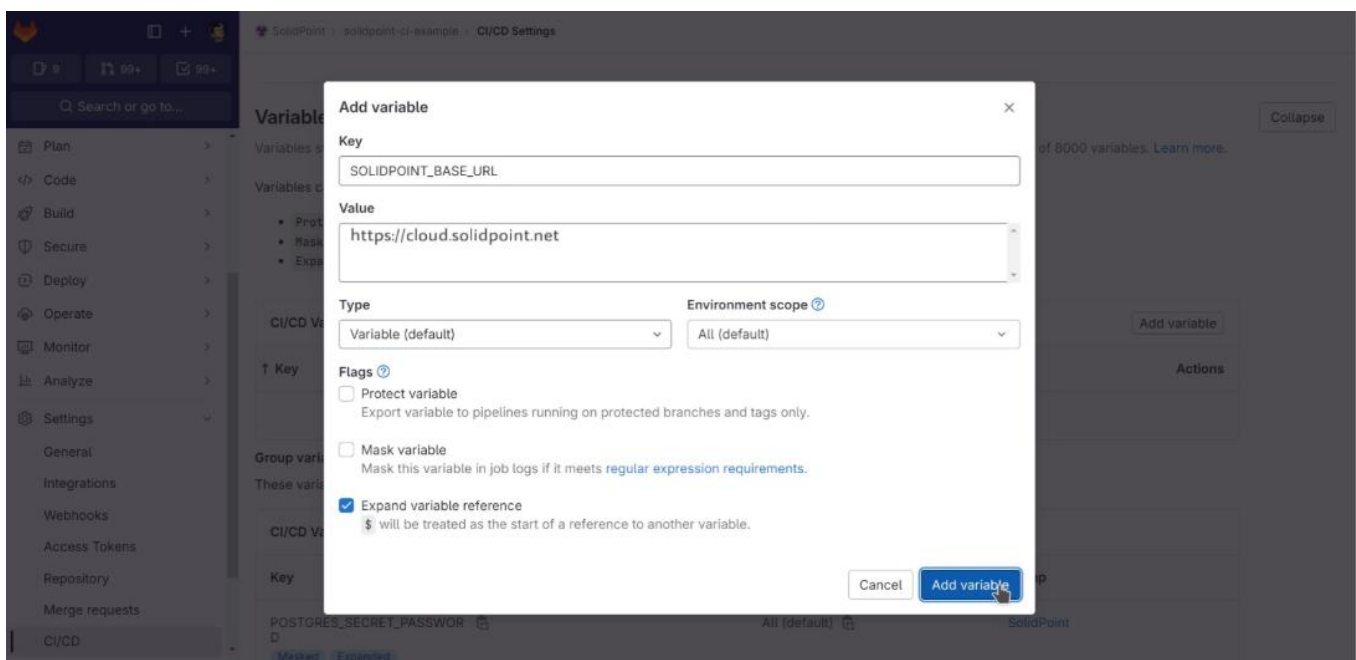
Снимок экрана 119. Путь к окну для добавления переменных, часть 2

Далее в открывшемся окне добавить две переменные:

- адрес сканера;
- секретный токен доступа.

Для добавления адреса сканера нужно (см. снимок экрана 120):

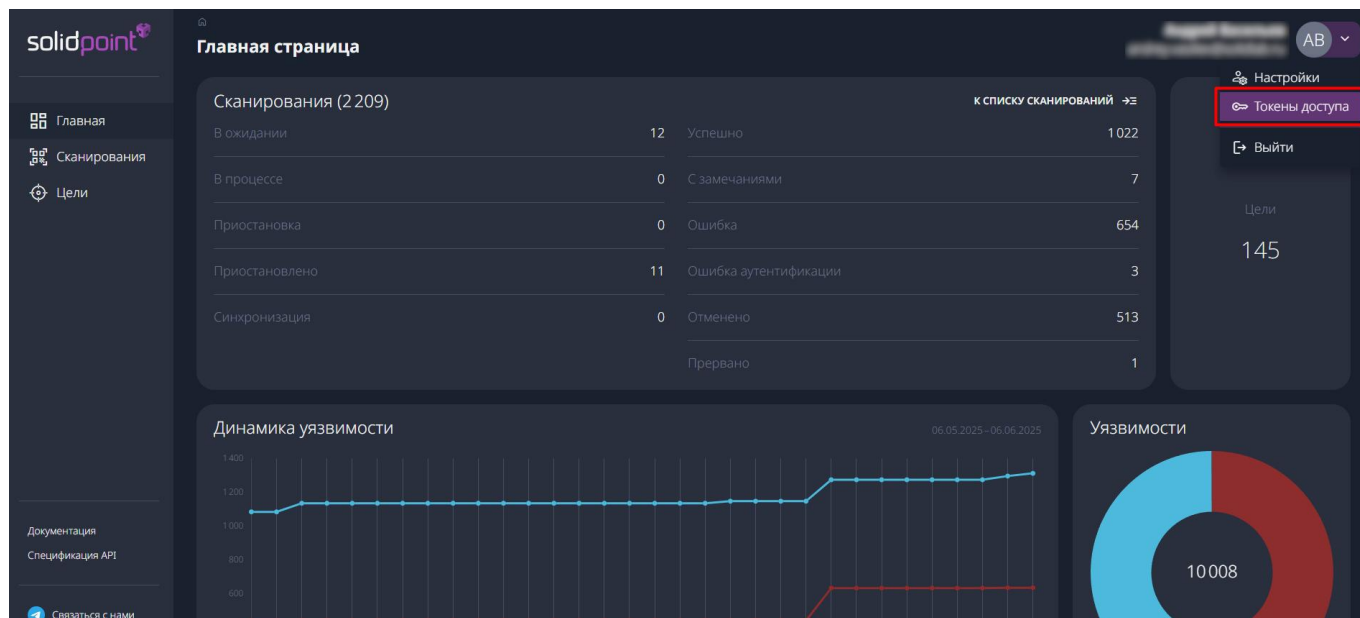
1. В поле «Ключ» указать `SOLIDPOINT_BASE_URL`.
2. В поле «Значение» указать URL сканера, например: <https://cloud.solidpoint.net>.
3. Нажать кнопку «Добавить переменную».



Снимок экрана 120. Добавление адреса сканера

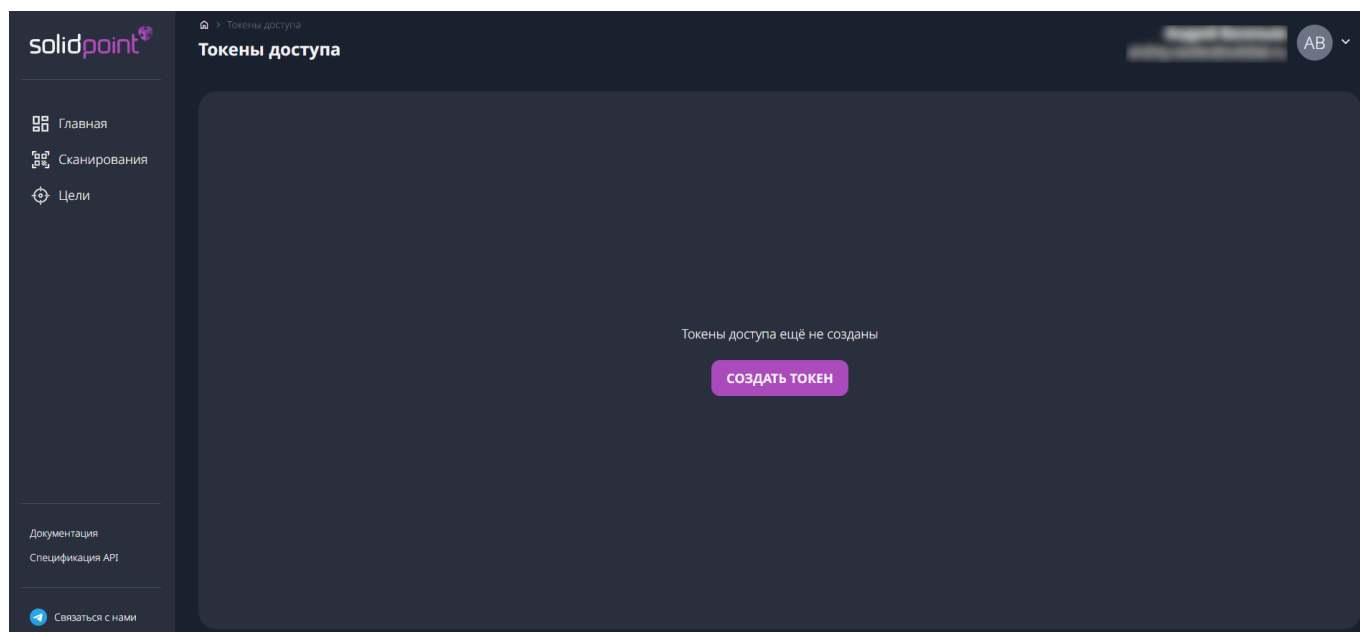
Для добавления секретного токена доступа нужно:

1. Перейти в панель управления.
2. Открыть выпадающее меню рядом с иконкой профиля.
3. Выбрать пункт «Токены доступа» (см. снимок экрана 121).



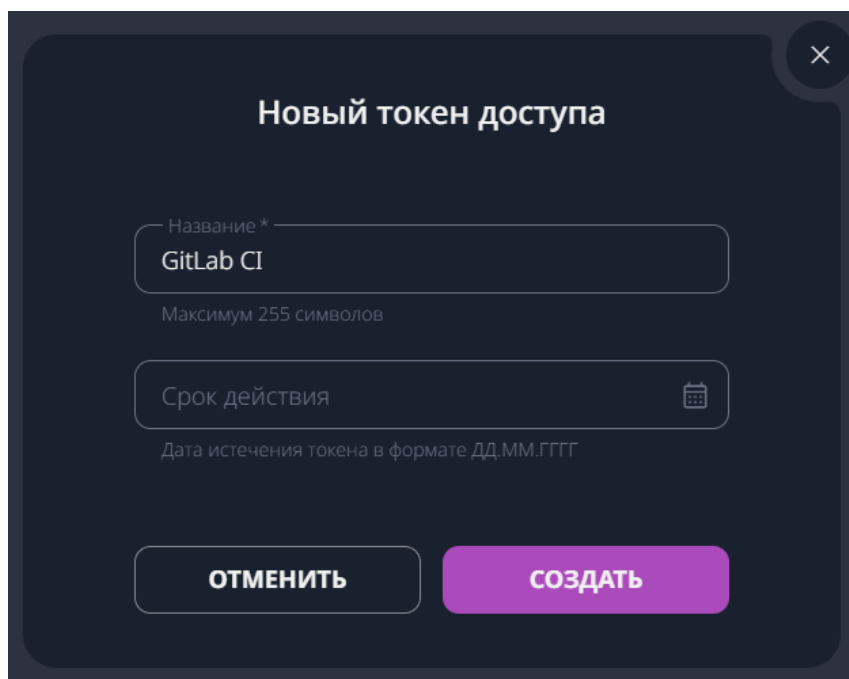
Снимок экрана 121. Пункт «Токены доступа»

4. Нажать кнопку «Создать токен» (см. снимок экрана 122).



Снимок экрана 122. Кнопка «Создать токен»

5. Ввести «GitLab CI» в поле «Название», указать срок действия в соответствующем поле и нажать кнопку «СОЗДАТЬ» (см. снимок экрана 123).



Новый token доступа

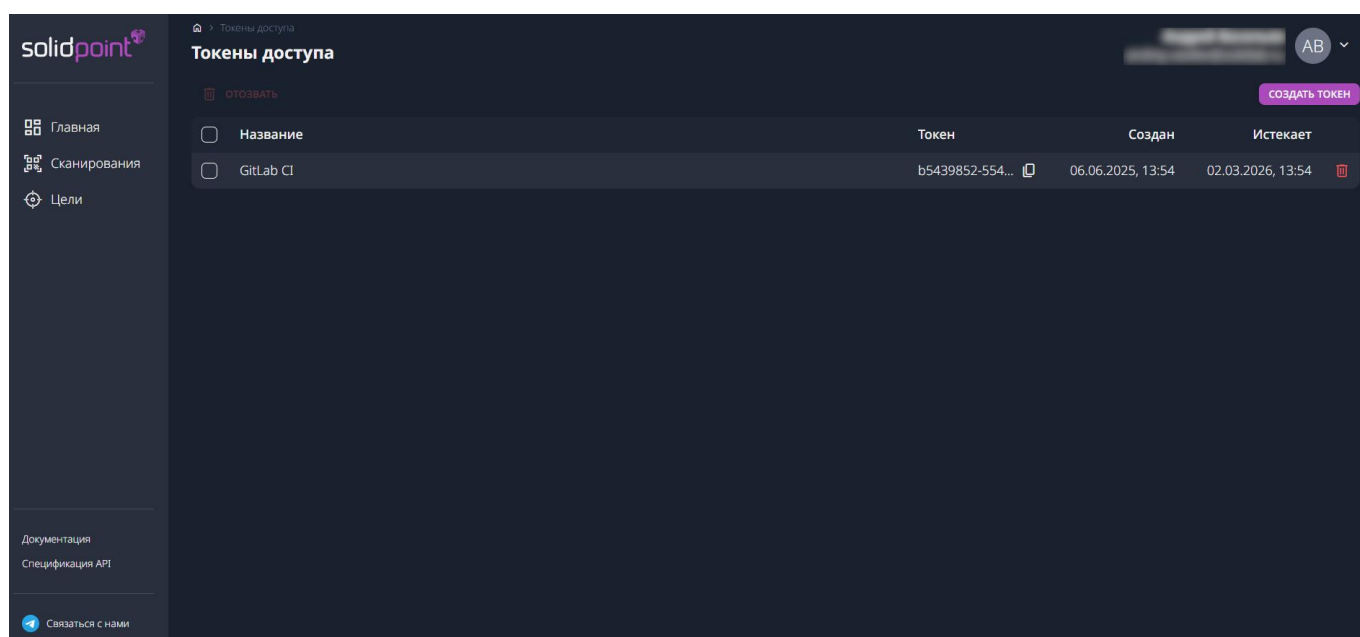
Название *
GitLab CI
Максимум 255 символов

Срок действия
Дата истечения токена в формате ДД.ММ.ГГГГ

ОТМЕНИТЬ СОЗДАТЬ

Снимок экрана 123. Окно «Новый token доступа»

6. Скопировать значение получившегося токена (см. снимок экрана 124).



solidpoint

Токены доступа

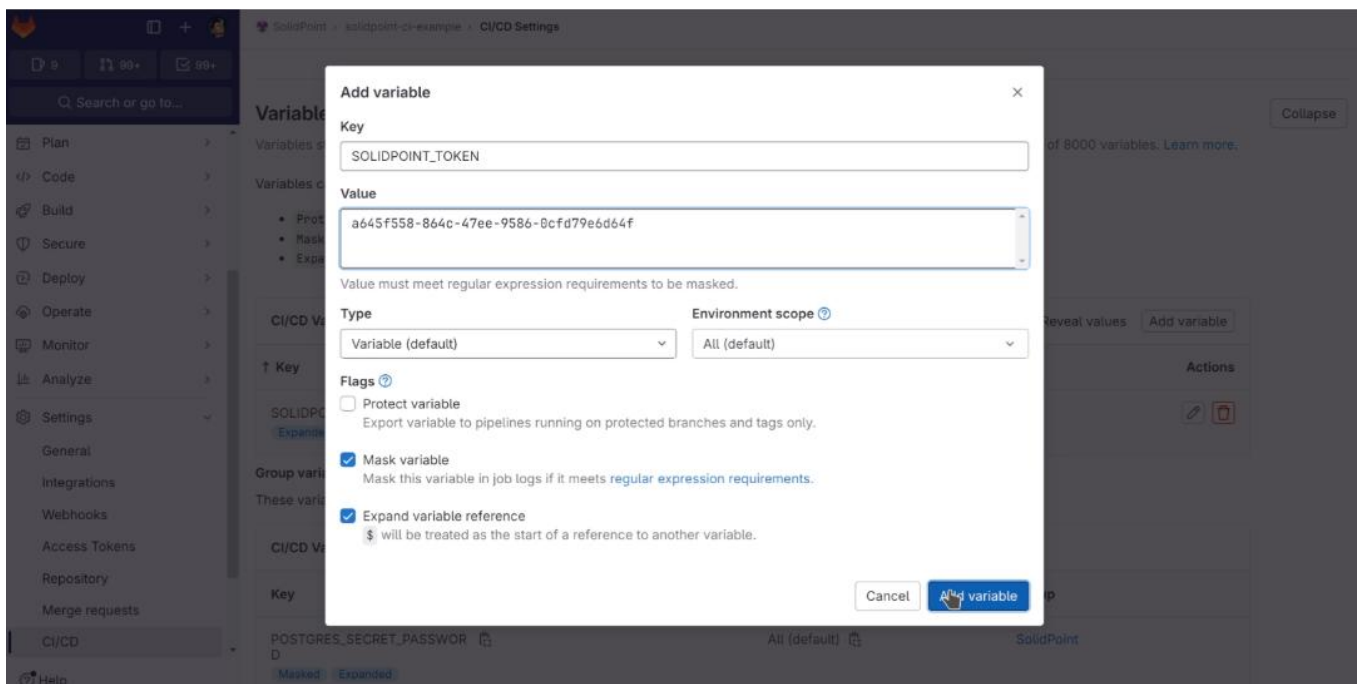
ОТМЕНИТЬ СОЗДАТЬ ТОКЕН

Название	Токен	Создан	Истекает
GitLab CI	b5439852-554...	06.06.2025, 13:54	02.03.2026, 13:54

Документация
Спецификация API
Связаться с нами

Снимок экрана 124. Созданный token доступа

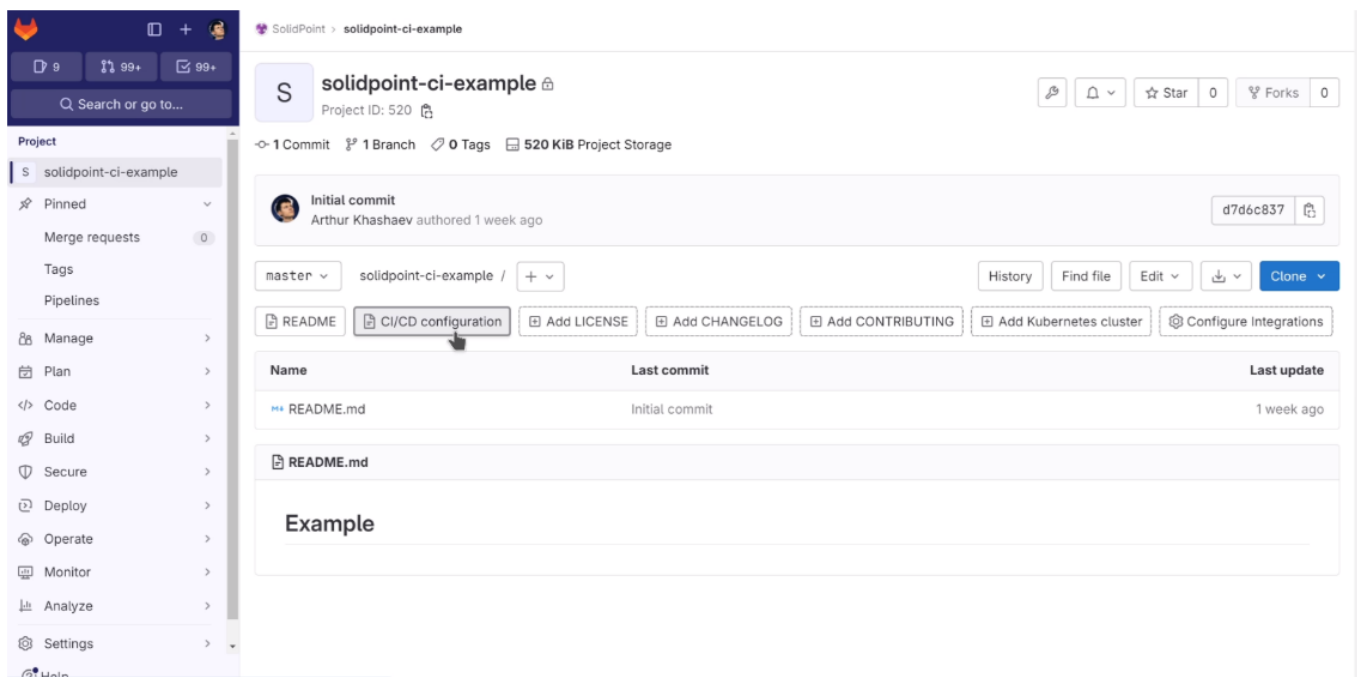
7. Открыть GitLab.
8. В новой переменной в поле «Ключ» указать `SOLIDPOINT_TOKEN`.
9. В поле «Значение» вставить скопированное значение токена.
10. Поставить включить чекбокс «Замаскировать переменную».
11. Нажать кнопку «Добавить переменную» (см. снимок экрана 125).



Снимок экрана 125. Окно добавления переменной

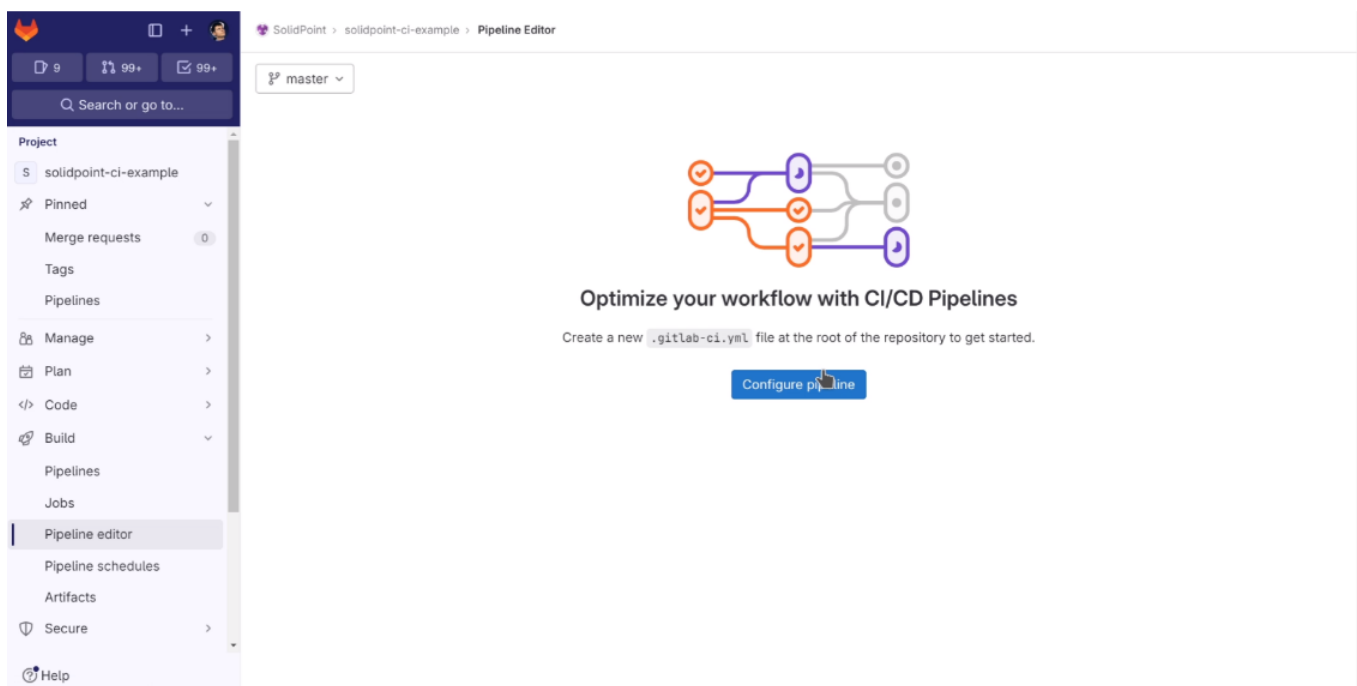
9.2. Настройка конфигурации CI/CD

Для настройки конфигурации необходимо в GitLab CI нажать кнопку «Конфигурация CI/CD» (см. снимок экрана 126).



Снимок экрана 126. Кнопка «Конфигурация CI/CD»

Далее в открывшемся редакторе нажать кнопку «Настроить пайплайн» (см снимок экрана 127).

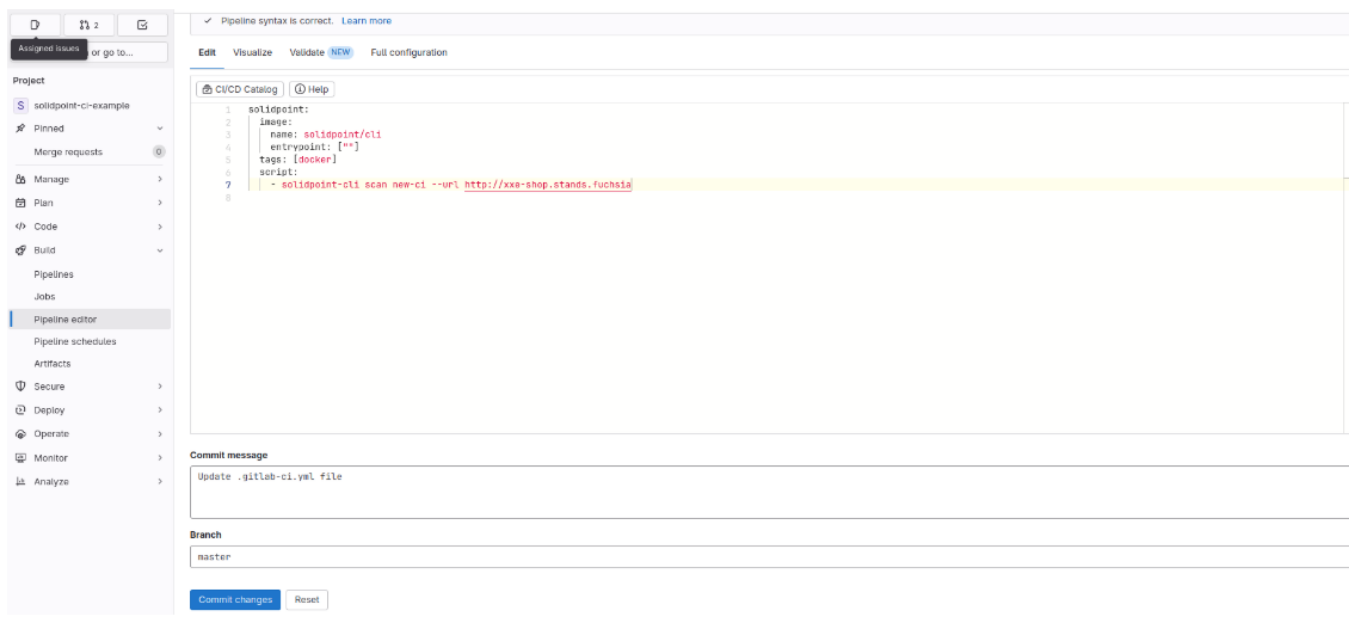


Снимок экрана 127. Кнопка «Настроить пайплайн»

9.2.1. Создание задачи для сканирования

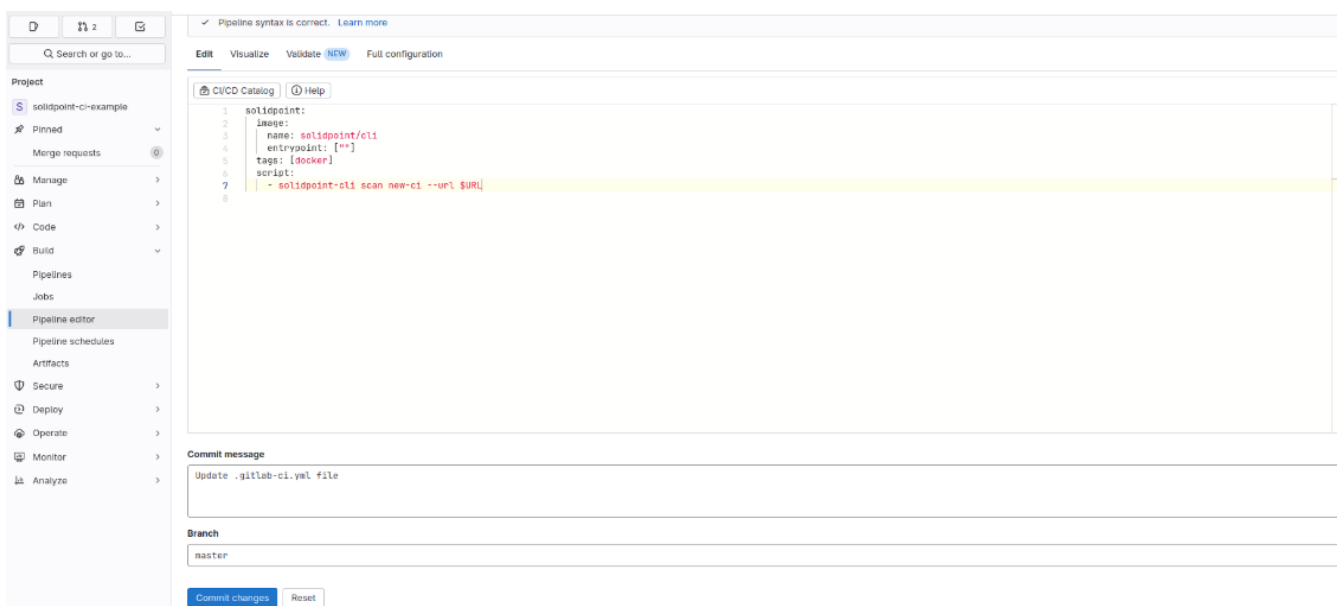
Для создания задачи для сканирования необходимо воспользоваться образом Docker — `solidpoint/cli`. Этот образ должен быть установлен предварительно в GitLab Runner. Для этого вставьте код в редактор для выполнения задачи (см. код ниже и снимок экрана 128).

```
solidpoint:
  image:
    name: solidpoint/cli
    entrypoint: [""]
  tags: [docker]
  script:
    - solidpoint-cli scan new-ci --url http://xe-shop.stands.fuchsia
```



Снимок экрана 128. Код для установки образа

В поле «script» можно по-разному задать адрес для сканирования. В примере выше указан статический адрес. Для задания динамического адреса следует использовать команду `solidpoint-cli scan new-ci --url $URL` (см. снимок экрана 129).

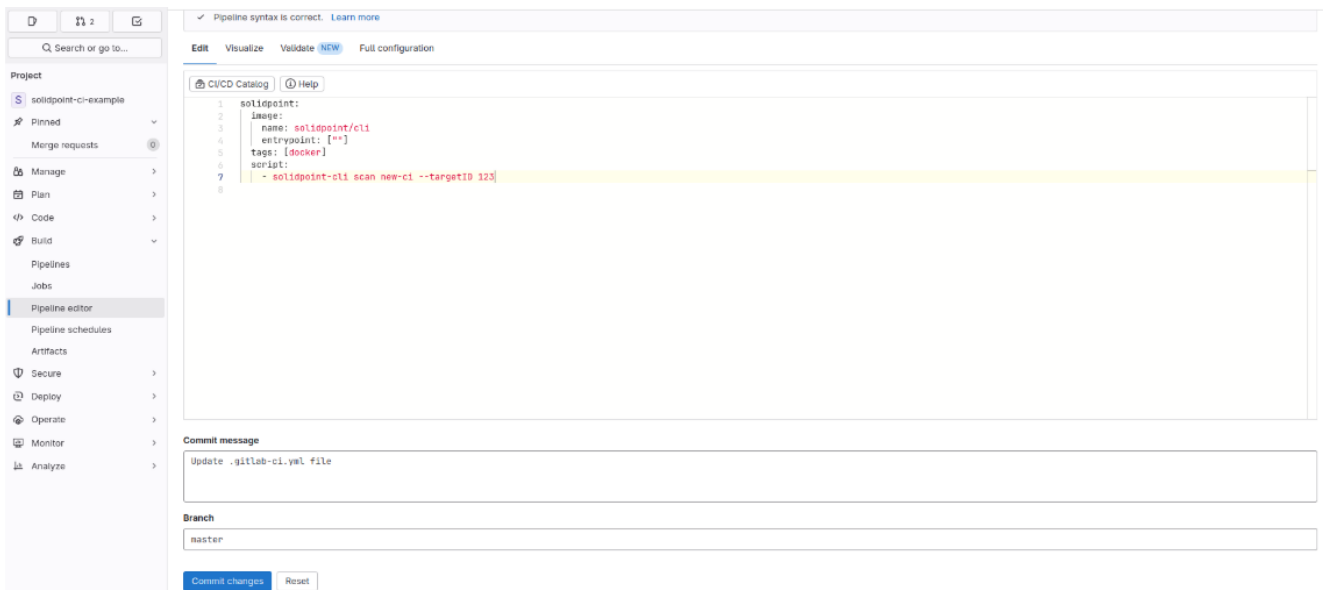


Снимок экрана 129. Задание динамического адреса

Здесь скрипт получает адрес через переменную `$URL`.

Альтернативным способом указания адреса для сканирования является задание цели через панель управления. При создании цели ей присваивается уникальный `targetID`. В данном случае скрипт будет иметь следующий вид (см. команду ниже и снимок экрана 130):

```
- solidpoint-cli scan new-ci --targetID 123
```



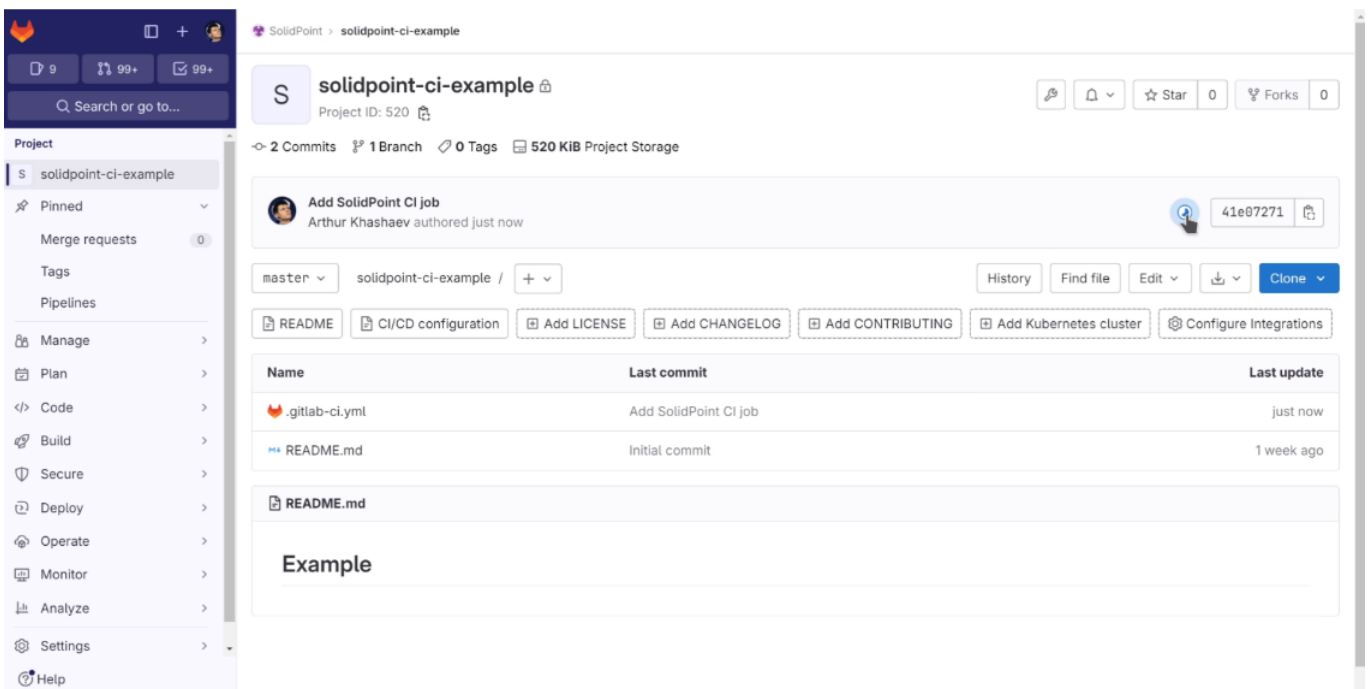
Снимок экрана 130 — Скрипт

Задача готова к выполнению. Для запуска необходимо написать сообщение коммита и нажать кнопку «Commit changes».

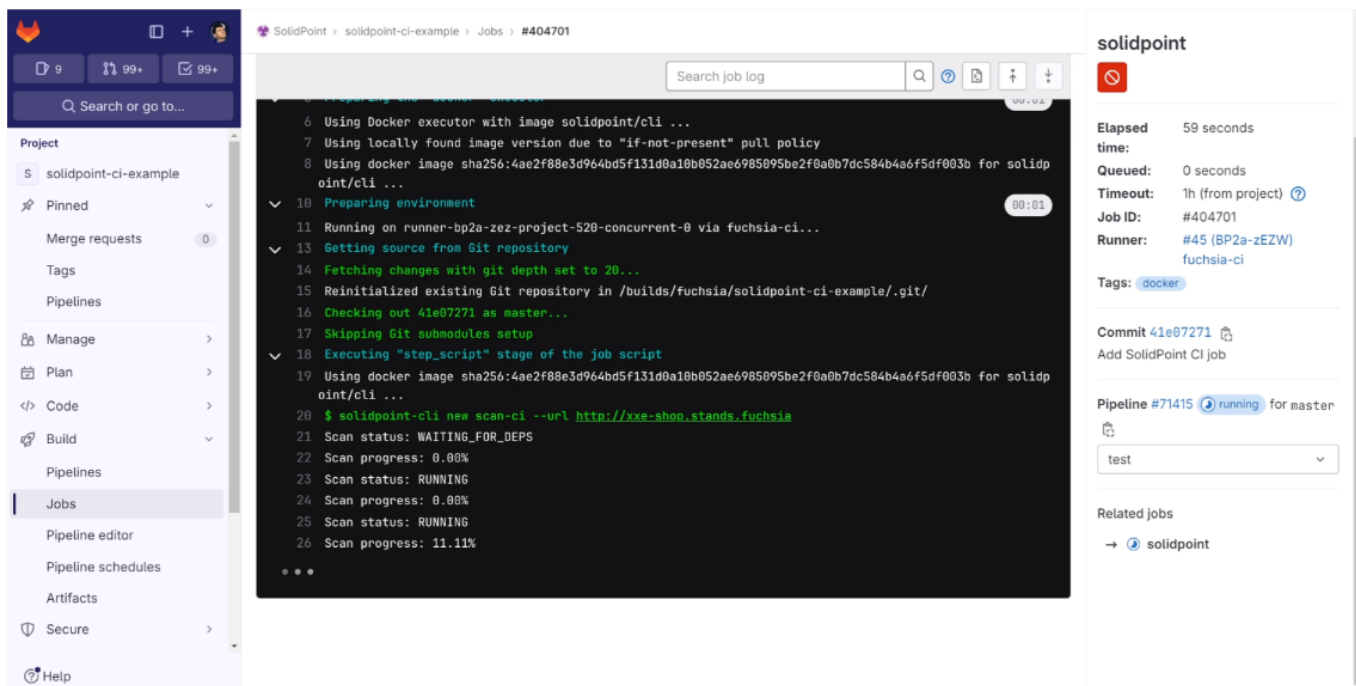
9.3. Просмотр запущенной задачи

Просмотреть выполнение задачи в реальном времени с отслеживанием прогресса и её итоговый результат можно двумя способами:

1. Через интерфейс GitLab (см. снимки экрана 131, 132);

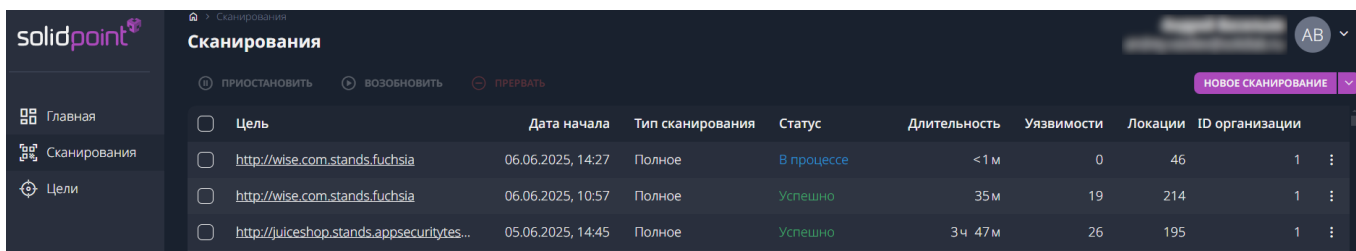


Снимок экрана 131. Интерфейс GitLab

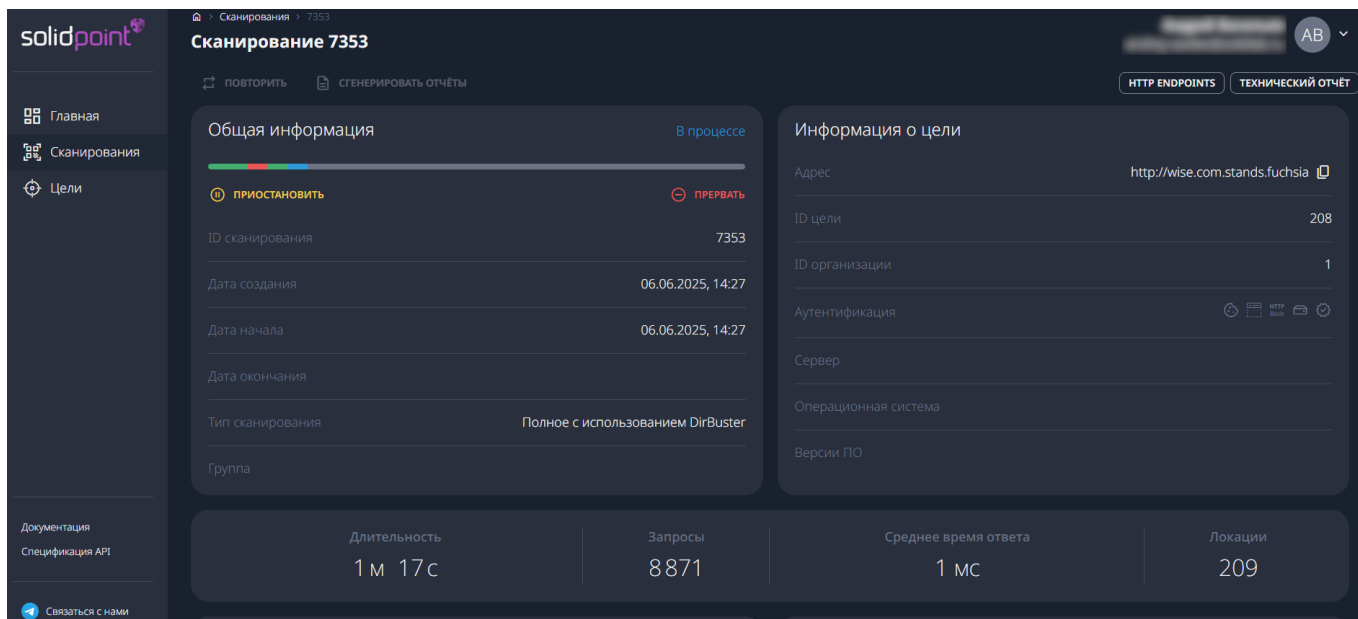


Снимок экрана 132. Интерфейс GitLab 2

2. Через панель управления (см. снимки экрана 133, 134).



Снимок экрана 133. Панель управления



Снимок экрана 134. Панель управления 2

В результате выполнения сканирования, если были выявлены уязвимости, задача возвращает ненулевой код.

ПРИЛОЖЕНИЕ А. АУТЕНТИФИКАЦИЯ В СКАНИРУЕМЫХ ПРИЛОЖЕНИЯХ

А.1. МЕХАНИЗМ ПРОВЕРКИ АУТЕНТИФИКАЦИИ

Механизм проверки аутентификации выполняет периодическую проверку действительности сессии, используя описанную в формате JSON-конфигурацию.

Конфигурация содержит массив критериев проверки действительности сессии. Обязательными полями являются `request`, `responseConditions` с вложенными обязательными полями `url` и `statusCode` соответственно.

Независимо от типа критерия, он считается выполненным тогда и только тогда, когда выполнены все указанные условия. Количество раундов проверки влияет на решение об аутентификации следующим образом:

- критерий имеет вид `PASSED` — аутентификация считается неудачной, если критерий не выполняется `N` раз подряд;
- критерий имеет вид `FAILED` — аутентификация считается неудачной, если критерий выполняется `N` раз подряд.

Поля JSON-конфигурации приведены в таблице 18.

Таблица 18. Поля JSON-конфигурации

Поле	Тип	Значение по умолчанию	Допустимые значения	Описание
<code>kind</code> * ¹	Строка	Не задано	<code>FAILED</code> , <code>PASSED</code>	Показывает, чему соответствует выполнение критерия — пройдена аутентификация или нет
<code>request.url</code> *	Строка	Не задано	—	Абсолютный URL-адрес проверочного запроса
<code>request.method</code>	Строка	<code>GET</code>	<code>GET</code> , <code>HEAD</code> , <code>OPTIONS</code> , <code>TRACE</code> , <code>PUT</code> , <code>DELETE</code> , <code>POST</code> , <code>PATCH</code> , <code>CONNECT</code>	Содержит метод проверочного запроса
<code>request.headers</code>	Объект	Не задано	—	Заголовки проверочного запроса в формате ключ-значение (<code>"Content-Type": "application/json"</code>)
<code>request.body</code>	Строка	Не задано	—	Тело проверочного запроса

¹ Поля, помеченные звездочкой, обязательны для заполнения.

Поле	Тип	Значение по умолчанию	Допустимые значения	Описание
request.timeout	Строка	10s	Любое число с указанием единицы измерения времени s	Тайм-аут HTTP-запроса для проверки сеанса в секундах, например: 0.5s, 1s, 10s
request.ignoreRedirects	Логический	false	–	Регулирует, должен ли механизм игнорировать переадресации и останавливаться при первом ответе
responseConditions.statusCode*	Целое число	Не задано	–	HTTP-статус проверочного ответа. Не равно – критерий не выполнен
responseConditions.body	Строка	Не задано	–	Регулярное выражение для соответствия тела проверочного ответа. Несоответствующее регулярное выражение — критерий не выполнен
responseConditions.headers	Объект	Не задано	–	Содержит пары (name, regex) для сопоставления заголовков проверочных ответов. Любое несоответствие — критерий не выполнен
interval	Строка	10s	Любое число с указанием единицы измерения времени s	Временной интервал между проверками критерия. Использует секунды с дробной частью, например: 0.5s, 1s, 10s
rounds	Целое число	5	–	Количество проверок критериев, гарантирующих, что аутентификация не выполнена

Пример конфигурации:

```
[
  {
    "kind": "PASSED",
    "request": {
```

```

    "url": "http://api.e-shop.com/profile"
  },
  "responseConditions": {
    "statusCode": 200,
    "headers": {
      "Content-Type": "application/json"
    }
  },
  "interval": "7s",
  "rounds": 3
},
{
  "kind": "FAILED",
  "request": {
    "url": "http://api.e-shop.com/"
  },
  "responseConditions": {
    "statusCode": 200,
    "body": ".*Unauthorized.*"
  },
  "interval": "1s",
  "rounds": 7
},
{
  "kind": "FAILED",
  "request": {
    "url": "http://api.e-shop.com/"
  },
  "responseConditions": {
    "statusCode": 403
  },
  "interval": "1s",
  "rounds": 7
},
{
  "kind": "PASSED",
  "request": {
    "method": "POST",
    "url": "http://api.e-shop.com/endpoint/",
    "headers": {
      "Content-Type": "application/json"
    },
    "body": "{\"data\": \"here\"}"
  },
  "responseConditions": {
    "statusCode": 200
  }
}
]

```

А.2. ОБНОВЛЕНИЕ АУТЕНТИФИКАЦИОННЫХ ДАННЫХ С ПОМОЩЬЮ HTTP-ЗАПРОСА

Данный механизм выполняет периодическое обновление сеанса, используя описанную в формате JSON-конфигурацию и HTTP-запрос. Работает только в сочетании с механизмом проверки аутентификации.

Конфигурация описывает способ выполнения HTTP-запроса на обновление сеанса в любом из его проявлений, а также способ настройки новых параметров аутентификации с обновленными данными.

Поля JSON конфигурации с использованием HTTP-запросов приведены в таблице 19.

Таблица 19. Поля JSON-конфигурации с использованием HTTP-запросов

Поле	Тип	Значение по умолчанию	Допустимые значения	Описание
request.url* ²	Строка	Не задано	—	Абсолютный URL-адрес конечной точки обновления сеанса. Это поле обязательно для заполнения
request.method	Строка	GET	GET, HEAD, OPTIONS, TRACE, PUT, DELETE, POST, PATCH, CONNECT	HTTP-метод конечной точки обновления сеанса
request.headers	Объект	Не задано	—	Содержит пары "key": "value", в которых указаны дополнительные заголовки для добавления в запрос на обновление сеанса, если это необходимо
request.body	Строка	Не задано	—	Строковое представление тела HTTP-запроса для обновления сеанса
request.timeout	Строка	10s	Любое число с указанием единицы измерения времени s	Тайм-аут HTTP-запроса для обновления сеанса в секундах, например: 0.5s, 1s, 10s
responseExtractors*	Массив	Не задано	—	Способ обработки ответа конечной точки для обновления сеанса. Каждый элемент массива описывает одну и только одну стратегию извлечения
responseExtractors[].extractor*	Строка	Не задано	—	Регулярное выражение в формате RE2, результатом обработки которого будут извлеченные данные для текущего элемента массива responseExtractors. Для каждого заголовка регулярное выражение ищет соответствия в теле ответа и в заголовках ответа, представленных в

² Поля, помеченные звездочкой, обязательны для заполнения.

Поле	Тип	Значение по умолчанию	Допустимые значения	Описание
				строковом формате Header-Key: Header-Value. Поиск идёт до первого совпадения, после чего останавливается
responseExtractors[].proxyParams	Объект	Не задано	–	Описание механизма аутентификации, который будет добавлен после успешного извлечения данных. Возможные ключи для аутентификации: cookie, header, httpAuth, jsonReplacer. Это поле является взаимоисключающим с responseExtractors[].placeholderVariableName
responseExtractors[].proxyParams.cookie	Объект	Не задано	–	Допустимые ключи: schema, hostname, port, path, name
responseExtractors[].proxyParams.header	Объект	Не задано	–	Допустимые ключи: schema, hostname, port, path, name
responseExtractors[].proxyParams.httpAuth	Объект	Не задано	–	Допустимые ключи: schema, hostname, port, path, username
responseExtractors[].proxyParams.jsonReplacer	Объект	Не задано	–	Допустимые ключи: schema, hostname, port, path
responseExtractors[].proxyParams.[cookie,header,httpAuth,jsonReplacer].schema	Строка	Из базового URL-адреса	–	Схема (сетевой протокол), используемая для аутентификации в сканируемом приложении
responseExtractors[].proxyParams.[cookie,header,httpAuth,jsonReplacer].hostname	Строка	Из базового URL-адреса	–	Имя хоста в любом допустимом варианте: домен (в т. ч. с поддоменами), IPv4 или IPv6
responseExtractors[].proxyParams.[cookie,header,httpAuth].path	Строка	Из базового URL-адреса	–	Путь для аутентификации в сканируемом приложении
responseExtractors[].proxyParams.[cookie,head	Строка	Из базового URL-адреса	"0"–"65535"	Номер порта для аутентификации в сканируемом приложении

Поле	Тип	Значение по умолчанию	Допустимые значения	Описание
er,httpAuth,json Replacer].port				
responseExtractors[].proxyParams.[cookie, header].name*	Строка	Не задано	—	Название заголовка или имя файла Cookie, значения которых будут заменены извлеченными данными
responseExtractors[].proxyParams.httpAuth.username*	Строка	Не задано	—	Имя пользователя для базовой HTTP-аутентификации, пароль которого будет заменен извлеченными данными
responseExtractors[].proxyParams.jsonReplacer.path*	Строка	Из базового URL-адреса	—	Путь к ключам в формате JSON для изменения значения с помощью извлечённых данных
responseExtractors[].placeholderVariableName	Строка	Не задано	—	Имя ключа, по которому будут храниться извлечённые данные. Эти данные будут использоваться во время следующего запроса на обновление сеанса в шаблонной части HTTP-запроса, соответствующей упомянутому ранее ключу. Пример использования: изменение токена обновления после каждого обновления сеанса. Это поле является взаимоисключающим с responseExtractors[].proxyParams
responseExtractors[].valueTransformationTemplate	Строка	Не задано	—	Описывает контекст, в соответствующую плейсхолдеру {{ .Matched }} шаблонную часть которого подставляются извлеченные данные. Этот контекст отображается в HTTP-запросе на обновление сессии в плейсхолдере, соответствующем значению responseExtractors[].placeholderVariableName. Пример использования: извлеченные данные должны использоваться в заголовке Authorization, но значение возвращается без префикса Bearer. Контекст будет выглядеть как Bearer {{ .Matched }}
placeholdersInitValues	Объект	Не задано	—	Содержит пары "key": "value", которые будут использоваться при заполнении вариативных частей HTTP-запроса в полях объекта request. Все пары ключ-значение должны быть заполнены начальными значениями, которые будут использоваться при первом запросе обновления сеанса. Для остальных запросов на обновление сеанса

Поле	Тип	Значение по умолчанию	Допустимые значения	Описание
				значения будут переписаны с помощью извлеченных данных с соответствующим ключом responseExtractors[].placeholderVariableName
dropHooksBeforeRefreshRequest	Логический	false	true, false	Указывает, следует ли удалять данные аутентификации (механизм аутентификации, добавленный после успешного извлечения данных) перед выполнением следующего HTTP-запроса на обновление
retryOptions.maxRetries	Целое положительное число	Не задано	–	Количество попыток обновления аутентификации. В случае отсутствия поля retryOptions в конфигурации по умолчанию совершается только одна попытка обновления
retryOptions.delay	Строка	Не задано	Любое число с указанием единицы измерения времени s	Частота попыток обновления аутентификации, выраженная в секундах (например, 10s). В случае отсутствия поля retryOptions в конфигурации по умолчанию совершается только одна попытка обновления

Примеры конфигурации:

1. Пример 1:

```

{
  "request": {
    "url": "http://example.com/login",
    "method": "POST",
    "body": "login=admin&password=secretpass"
  },
  "responseExtractors": [
    {
      "extractor": "Set-Cookie:.*session_token=(.*);",
      "proxyParams": {
        "cookie": {
          "name": "session_token"
        }
      }
    }
  ]
}

```

2. Пример 2:

```

{
  "request": {
    "url": "http://api.example.com/refresh-with-token",
    "method": "POST",
    "body": "{\"authData\": {\"refreshToken\": \"{{ .RefreshToken }}\"}}",
  },
  "responseExtractors": [
    {
      "extractor": "{\"token\": \"(.*)\"}",
      "proxyParams": {
        "header": {
          "name": "X-Auth",
          "hostname": "api.example.com"
        }
      }
    },
    {
      "extractor": "\"authData\": {\"refreshToken\": \"(.*)\"}",
      "placeholderVariableName": "RefreshToken"
    }
  ],
  "placeholdersInitValues": {
    "RefreshToken": "c2712990-ec19-414b-8be0-8a66e9271253"
  }
}

```

3. Пример 3:

```

{
  "request": {
    "url": "http://example.com/refresh-with-token",
    "method": "POST",
    "body": "{\"authData\": {\"refreshToken\": \"{{ .RefreshToken }}\"}}",
  },
  "responseExtractors": [
    {
      "extractor": "{\"token\": \"(.*)\"}",
      "proxyParams": {
        "header": {
          "name": "Authorization"
        }
      }
    },
    {
      "valueTransformationTemplate": "Bearer {{ .Matched }}"
    }
  ],
  {
    "extractor": "\"authData\": {\"refreshToken\": \"(.*)\"}",
    "placeholderVariableName": "RefreshToken"
  }
],
  "placeholdersInitValues": {
    "RefreshToken": "c2712990-ec19-414b-8be0-8a66e9271253"
  }
}

```

А.3. ОБНОВЛЕНИЕ АУТЕНТИФИКАЦИОННЫХ ДАННЫХ С ПОМОЩЬЮ БРАУЗЕРНОГО СЦЕНАРИЯ

Данный механизм выполняет периодическое обновление сеанса, используя описанную в формате JSON-конфигурацию и браузерный сценарий, записанный с помощью Chrome DevTools Recorder. Сущность, называемая браузерным аутентификатором, исполняет браузерный сценарий, затем передает сканеру состояние Cookie и локального или сессионного хранилища браузера на момент завершения сценария. В конфигурационном файле необходимо описать, каким образом полученные Cookie и локальное или сессионное хранилище будут использоваться в обновленных аутентификационных данных. Работает только в сочетании с механизмом проверки аутентификации. Является взаимоисключающим с механизмом обновления аутентификационных данных с помощью HTTP-запроса.

Конфигурация

Конфигурация регулирует исполнение браузерного сценария и описывает способ настройки новых параметров аутентификации с обновленными данными.

Поля JSON-конфигурации с использованием браузерного сценария приведены в таблице 20.

Таблица 20. Поля JSON-конфигурации с использованием браузерного сценария

Поле	Тип	Значение по умолчанию	Допустимые значения	Описание
browserAuthenticatorName	Строка	fuchsia-browser-authenticator	—	Базовое имя исполняемого файла браузерного аутентификатора. Рекомендуется не заполнять это поле и использовать значение по умолчанию
loginScript	Объект	Не задано	—	Содержит объект, описывающий браузерный сценарий. При запуске сканирования через fuchsiactl рекомендуется не заполнять это поле и использовать флаг --file=@browserAuthenticator:loginScript@/path/to/script.json. Запуск сканирования через HTTP API возможен только с ключом, указывающим на расположение файла. При запуске через интерфейс SolidPoint это поле заполняется путём загрузки файла скрипта в параметрах сканируемой цели
outputExtractors* ³	Массив объектов	Не задано	—	Способ обработки новых Cookie и локального хранилища для обновления сеанса. Каждый элемент массива описывает одну и только одну стратегию извлечения данных

³ Поля, помеченные звездочкой, обязательны для заполнения.

Поле	Тип	Значение по умолчанию	Допустимые значения	Описание
outputExtractors[].type*	Строка	Не задано	"TYPE_COOKIE", "TYPE_LOCAL_STORAGE"	Тип источника данных
outputExtractors[].selectors	Массив строк	Не задано	–	Массив имен Cookie или ключей локального хранилища, которые должны присутствовать у браузерного аутентификатора после исполнения браузерного сценария. Если массив непустой, то при отсутствии хотя бы одного из его элементов в выводе браузерного аутентификатора обновление аутентификационных данных будет считаться неуспешным. Является обязательным полем, если задано поле outputExtractors[].extractSelectorsOnly
outputExtractors[].extractSelectorsOnly	Логический	false	true, false	Флаг, сигнализирующий о том, стоит ли брать из вывода браузерного аутентификатора все данные или же только те, что соответствовали селекторам. Значение true является допустимым только в случае, когда массив output_extractors[].selectors не пуст
outputExtractors[].proxyParams	Объект	Зависит от типа источника данных	–	Описание механизма аутентификации, который будет добавлен после успешного извлечения данных. Это поле может быть задано, только если значение поля outputExtractors[].type указано как "TYPE_LOCAL_STORAGE". Если данный параметр пуст, для этого типа будет создан механизм аутентификации, использующий всё обновлённое локальное хранилище (с точностью до outputExtractors[].selectors и outputExtractors[].extractSelectorsOnly) с целью передать содержимое браузерным модулям. Если поле outputExtractors[].type указано как "TYPE_COOKIE", то извлечённые Cookie автоматически создают новый механизм аутентификации, добавляющий их в аутентификационные данные с учётом свойств Domain и Path.

Поле	Тип	Значение по умолчанию	Допустимые значения	Описание
				Во всех остальных случаях поле допускает ключи cookie, header, httpAuth и jsonReplacer
outputExtractors[[]].proxyParams.[cookie, header].name*	Строка	Не задано	–	Название заголовка или имя Cookie, значения которых будут заменены извлеченными данными
outputExtractors[[]].proxyParams.httpAuth.username*	Строка	Не задано	–	Имя пользователя для базовой HTTP-аутентификации, для которого извлечённые данные будут заменены паролем
outputExtractors[[]].proxyParams.jsonReplacer.path*	Строка	Не задано	–	Указывает путь для замены значений в JSON-телах исходящих запросов сканера. Применяется только при одновременном соблюдении следующих условий: Тело запроса полностью представлено в формате JSON; Указанный JSON-путь существует в структуре. Если условия выполнены, то значение по указанному пути заменяется на данные из извлеченного источника
responseExtractors[[]].valueTransformationTemplate	Строка	Не задано	–	Поддерживается только при одновременном соблюдении следующих условий: Значение поля outputExtractors[[]].type указано как "TYPE_LOCAL_STORAGE", Поле outputExtractors[[]].proxyParams не является пустым. В поле указывается шаблон, в контексте которого с помощью go text/template будут обрабатываться извлеченные значения. Результатом является строка, подставляемая в поле outputExtractors[[]].proxyParams. В качестве плейсхолдеров выступают ключи извлечённых из локального хранилища пар. Например, извлеченный по ключу токен "authToken" необходимо подставить в заголовок следующим образом: Authorization: Bearer <token>. Тогда данное поле примет значение Bearer: {{.authToken}}, а outputExtractors[[]].proxyParams будет

Поле	Тип	Значение по умолчанию	Допустимые значения	Описание
				содержать объект {"header": {"name": "Authorization"}}. Можно использовать более одного плейсхолдера. Настоятельно рекомендуется использовать форму {{ index . "some-name" }} для передачи в шаблонную строку, потому что для шаблонизатора, например, «—» является служебным символом, поэтому в форме Bearer: {{ .some-name }} шаблон не будет успешно обработан
retryOptions.maxRetries	Целое положительное число	Не задано	—	Количество попыток обновления аутентификации. В случае отсутствия поля retryOptions в конфигурации по умолчанию совершается только одна попытка обновления
retryOptions.delay	Строка	Не задано	Любое число с указанием единицы измерения времени s	Частота попыток обновления аутентификации, выраженная в секундах (например, 10s). В случае отсутствия поля retryOptions в конфигурации по умолчанию совершается только одна попытка обновления
totpConfig.seed*	Строка	Не задано	Последовательность символов	Секретный ключ шифрования TOTP-кодов
totpConfig.algorithm*	Перечислимый тип	1	TOTP_ALGORITHM_UNSPECIFIED или 0; TOTP_ALGORITHM_SHA1 или 1; TOTP_ALGORITHM_SHA256 или 2; TOTP_ALGORITHM_SHA512 или 3	Алгоритм шифрования
totpConfig.digits*	Целое положительное число	6	—	Количество цифр, содержащихся в TOTP-коде
totpConfig.period*	Целое положительное	30	—	Период обновления TOTP-кодов в секундах

Поле	Тип	Значение по умолчанию	Допустимые значения	Описание
	целое число			

Примеры конфигурации:

1. Извлечение всех Cookie при наличии среди них хотя бы одного с именем `token` (если нет ни одного с именем `token` — неудача):

```
{
  "output_extractors": [
    {
      "type": "TYPE_COOKIE",
      "selectors": ["token"]
    }
  ]
}
```

2. Извлечение Cookie с именем «`token`», если он присутствует (если отсутствует — неудача):

```
{
  "output_extractors": [
    {
      "type": "TYPE_COOKIE",
      "selectors": ["token"],
      "extract_selectors_only": true
    }
  ]
}
```

3. Извлечение всех Cookie. Извлечение локального хранилища и его передача браузерным модулям. Извлечение из локального хранилища значений по ключам `token_secret_name` и `token` и передача их в заголовок `Authorization` в соответствии с шаблоном. Неудача для всего обновления, если хотя бы одно значение не нашлось:

```
{
  "output_extractors": [
    {
      "type": "TYPE_COOKIE"
    },
    {
      "type": "TYPE_LOCAL_STORAGE"
    },
    {
      "type": "TYPE_LOCAL_STORAGE",
      "selectors": ["token_secret_name", "token"],
      "extractSelectorsOnly": true,
      "proxy_params": {
        "hostname": "example.com",

```

```

    "scheme": "https",
    "port": "443",
    "header": {
        "name": "Authorization"
    },
    "value_transformation_template": "Bearer {{ .token_secret_name }}|{{ .token }}"
  }
}
]
}

```

4. Извлечение всех Cookie. Извлечение из сессионного хранилища значений по ключам `token_secret_name` и `token` и передача их в заголовок `Authorization` в соответствии с шаблоном. Неудача для всего обновления, если хотя бы одно значение не нашлось:

```

{
  "outputExtractors": [
    {
      "type": "TYPE_COOKIE"
    },
    {
      "type": "TYPE_SESSION_STORAGE"
    },
    {
      "type": "TYPE_SESSION_STORAGE",
      "selectors": ["token_secret_name", "token"],
      "extractSelectorsOnly": true,
      "proxyParams": {
        "hostname": "example.com",
        "scheme": "https",
        "port": "443",
        "header": {
          "name": "Authorization"
        }
      },
      "valueTransformationTemplate": "Bearer {{ .token_secret_name }}|{{ .token }}"
    }
  ]
}

```

5. Использование TOTP-кодов, состоящих из 6 цифр, с периодом обновления 30с и алгоритмом шифрования SHA1:

```

{
  "totpConfig": {
    "seed": "IFTXE3SPOEYVURT2MRYGI52TKJ4HC3KH",
    "digits": 6,
    "period": 30,
    "algorithm": "TOTP_ALGORITHM_SHA1"
  }
}

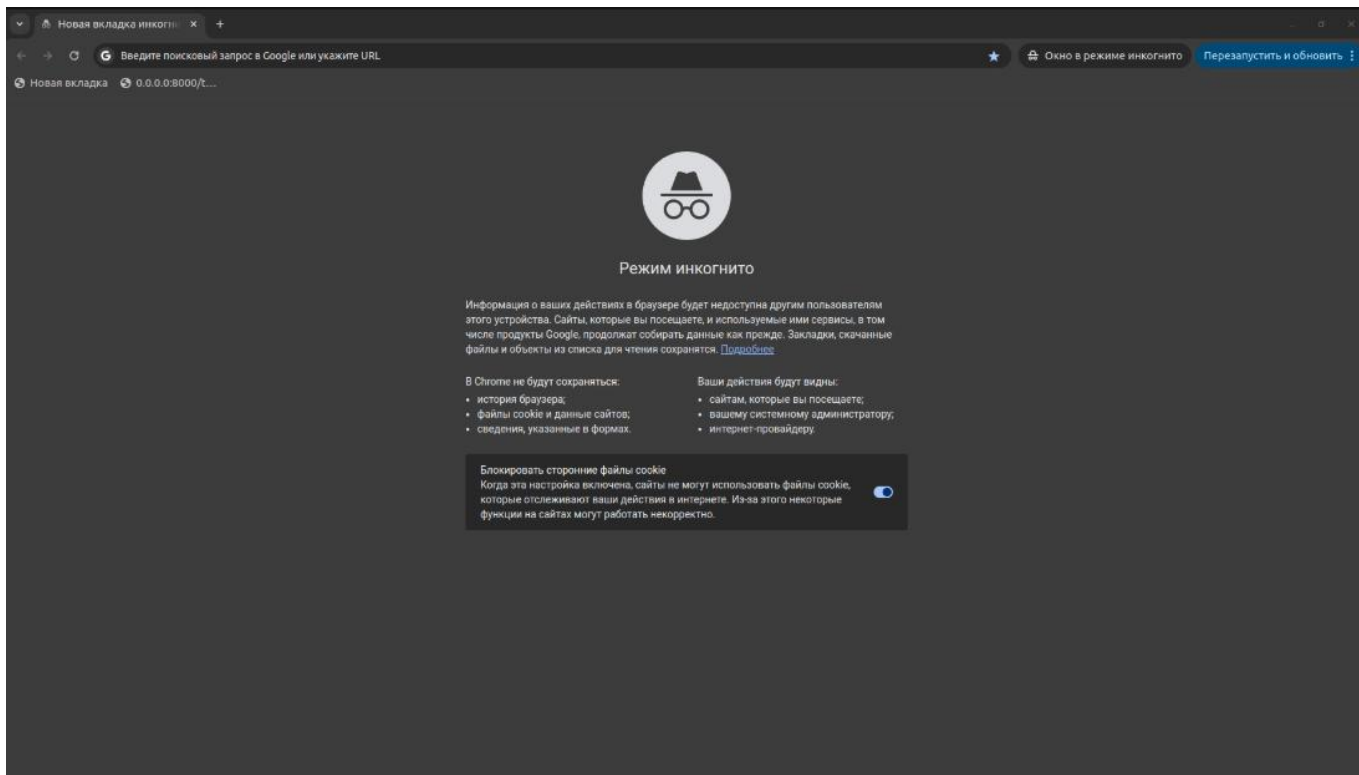
```

}

Запись браузерного сценария

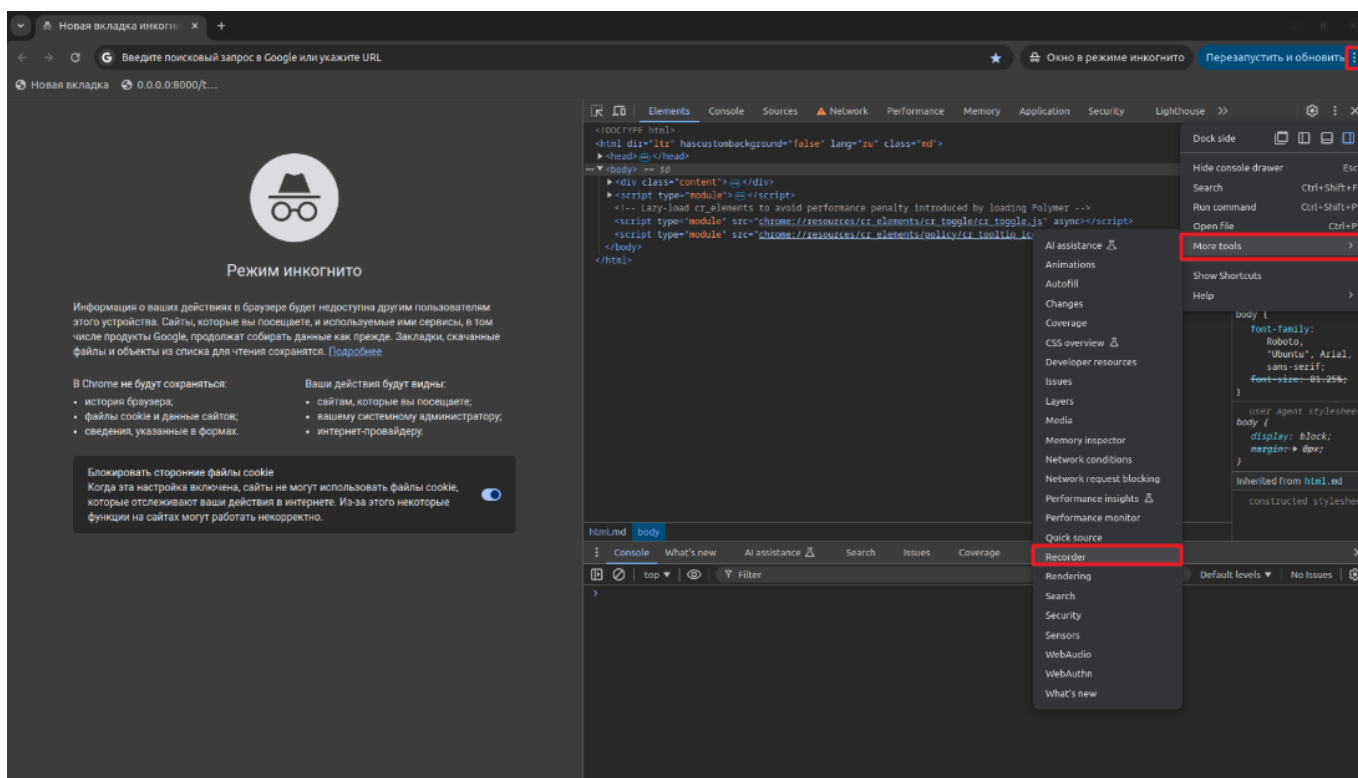
В качестве демонстрационного примера используется адрес <http://juiceshop.stands.appsecuritytesting.fun/>. Для записи браузерного сценария потребуется браузер «Google Chrome». Последовательность действий следующая:

1. Открыть браузер «Google Chrome» в режиме инкогнито (см. снимок экрана 135).



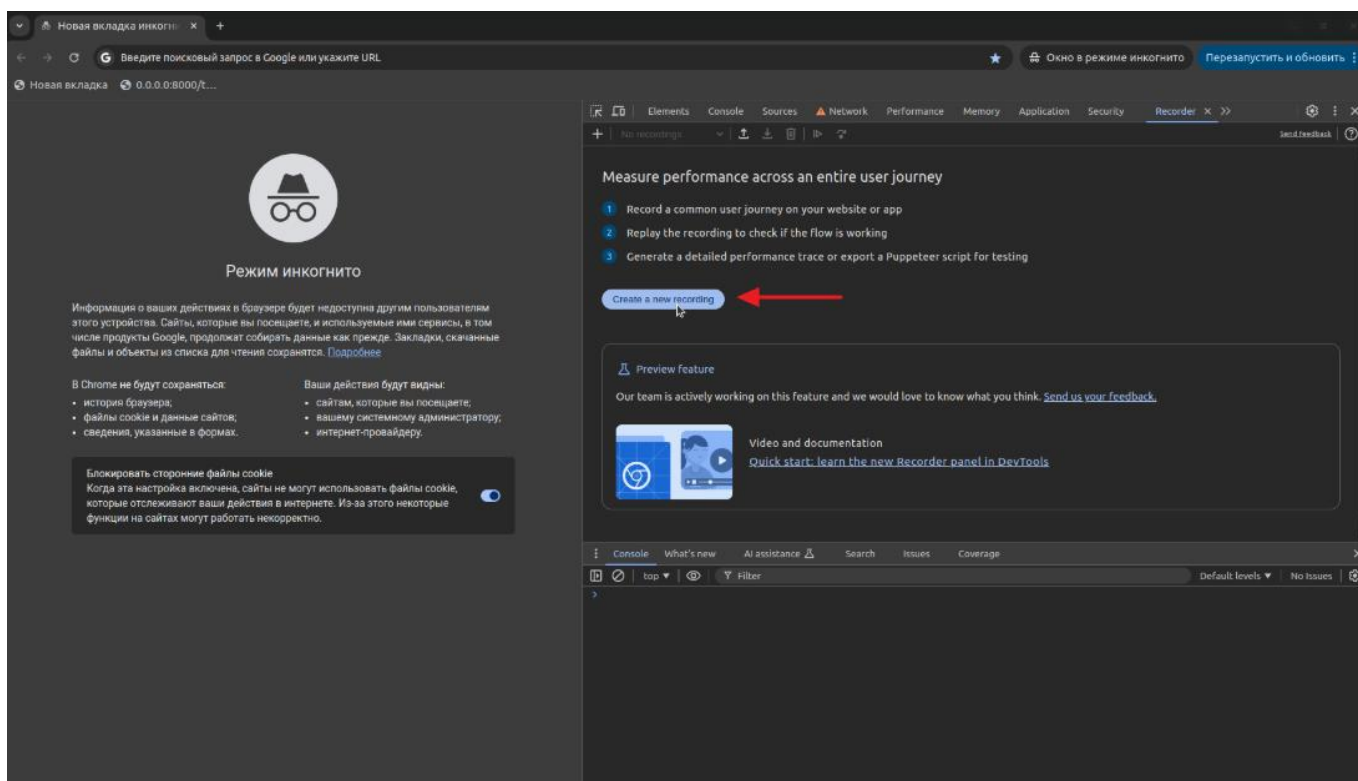
Снимок экрана 135. Режим инкогнито

2. На клавиатуре нажать клавишу «F12» для открытия панели «Chrome Developer Tools», затем нажать пиктограмму «⋮» в правом верхнем углу, далее в выпадающих меню последовательно выбрать пункты «More Tools» и «Recorder» (см. снимок экрана 136).



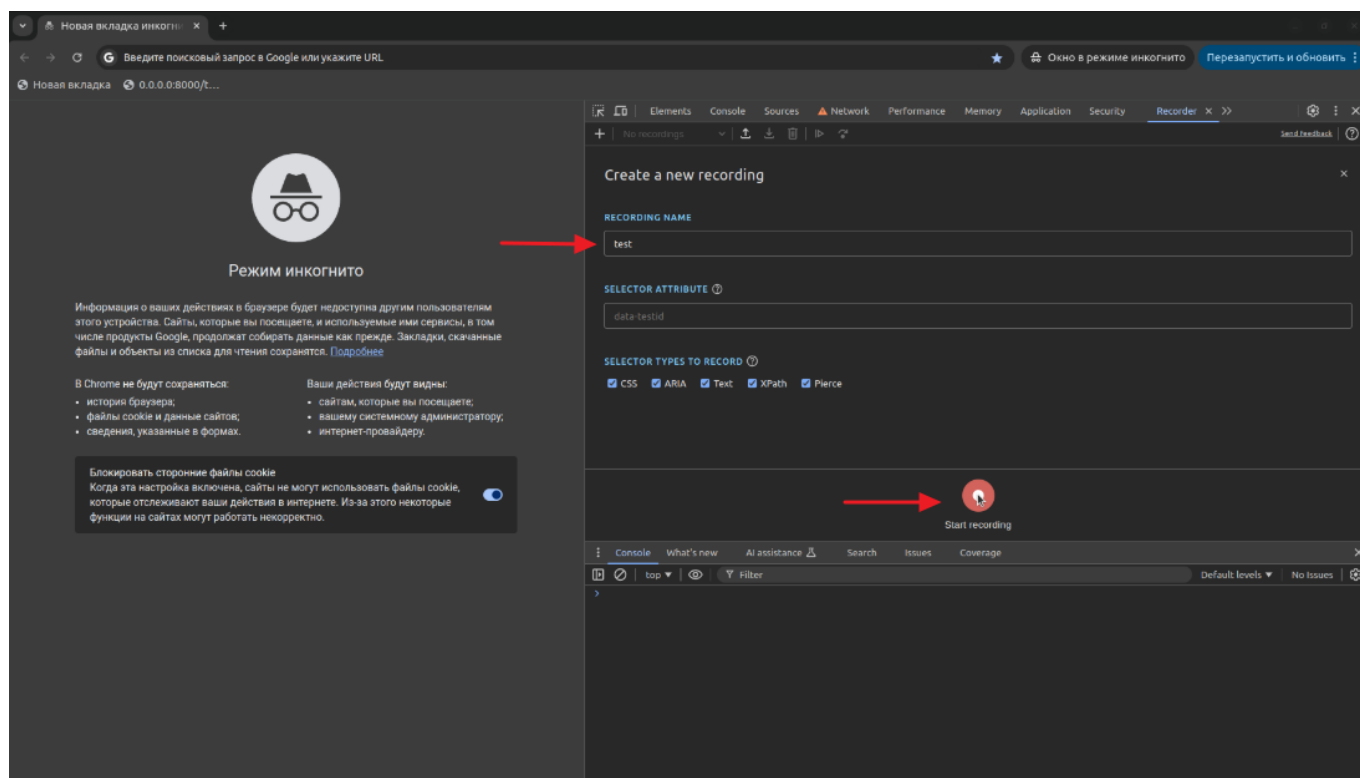
Снимок экрана 136. Панель «Инструменты разработчика», пункт «Recorder»

3. Нажать кнопку «Create a new recording» (см. снимок экрана 137).



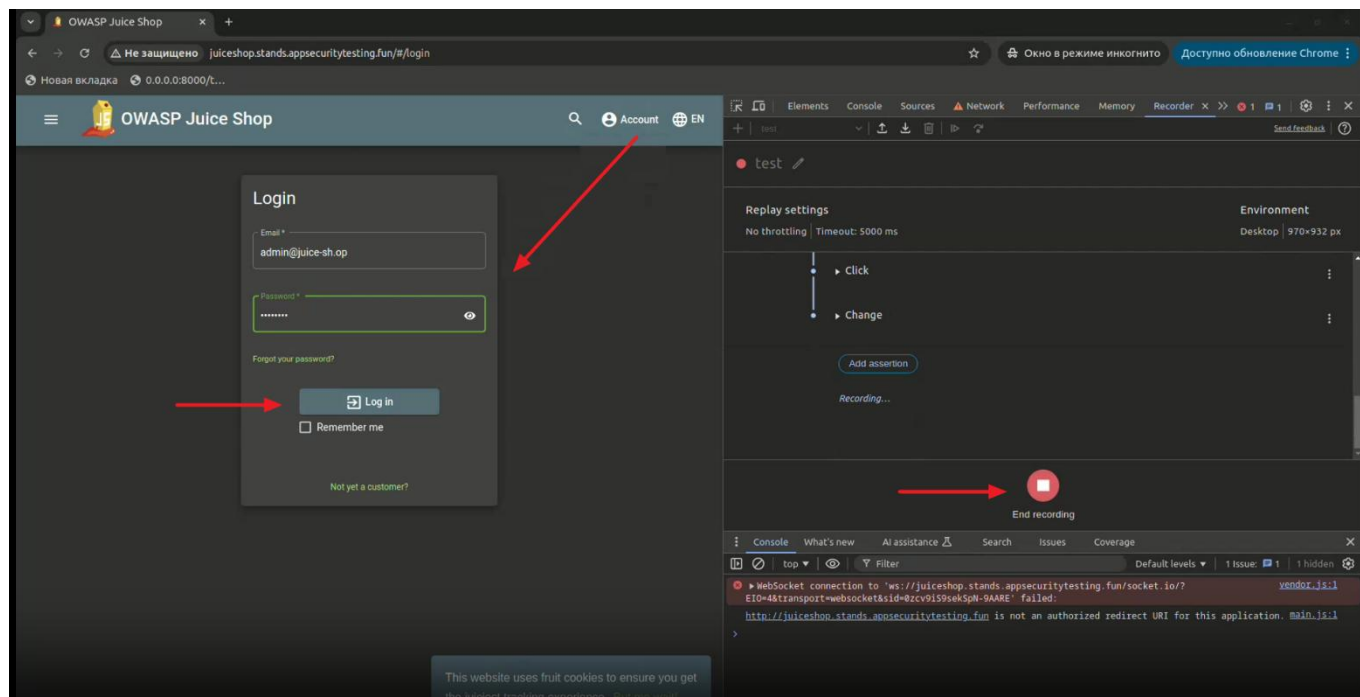
Снимок экрана 137. Кнопка «Create a new recording»

4. В поле «RECORDING NAME» ввести имя для будущего сценария и нажать кнопку «Start recording» (см. снимок экрана 138).



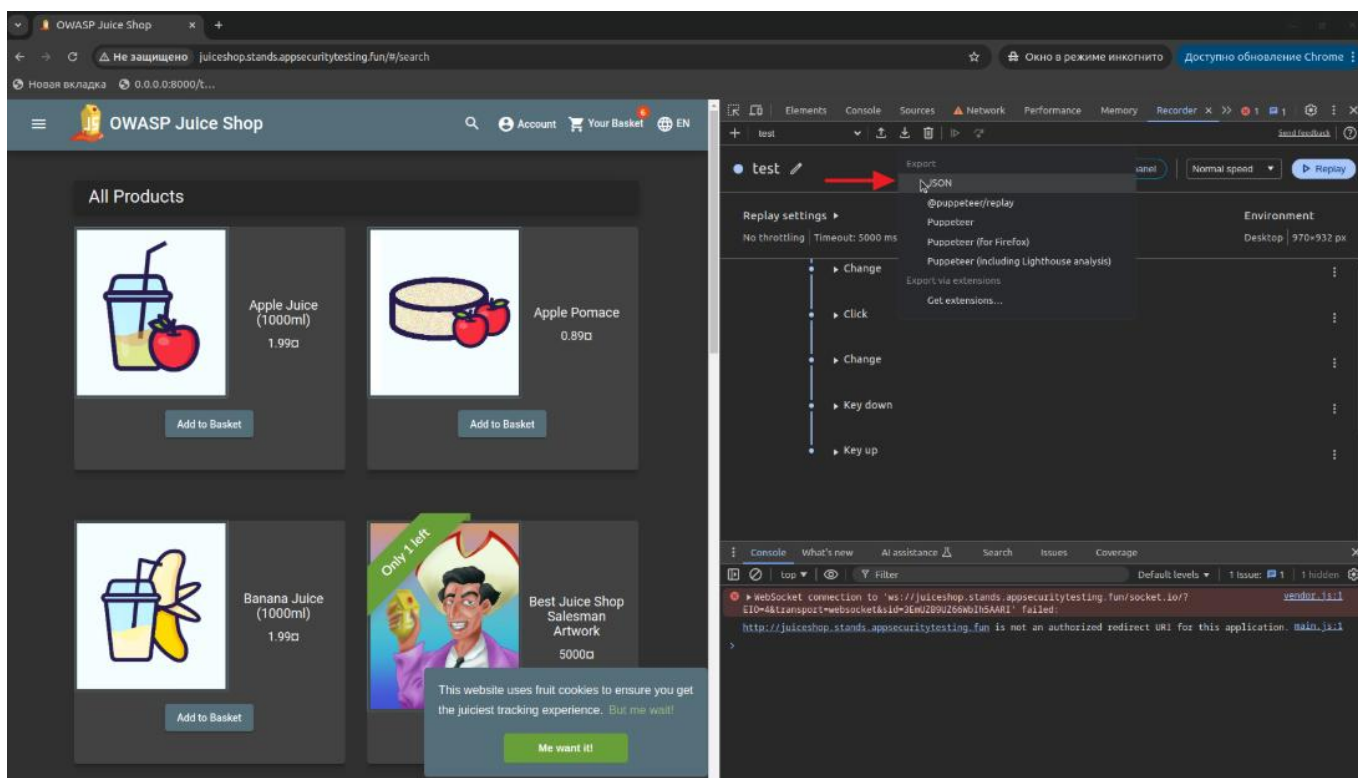
Снимок экрана 138. Поле «RECORDING NAME», кнопка «Start recording»

5. Перейти на страницу аутентификации, ввести необходимые учётные данные, войти в систему и нажать кнопку «End recording» (см. снимок экрана 139).



Снимок экрана 139. Ввод учетных данных, кнопка «End recording»

6. Экспортировать полученную запись в формате JSON (см. снимок экрана 140).



Снимок экрана 140. Экспорт полученной записи в формате JSON

7. Если в ходе записи сценария использовались TOTP-коды, необходимо отредактировать полученную запись, заменив использованные коды на плейсхолдеры <<TOTP_CODE>> для целого кода или <<TOTP_DIGIT_i>> ($i \geq 1$) при пошаговом вводе для каждой цифры.

Полученный файл — это браузерный сценарий, необходимый для обновления аутентификационных данных сканирования.

ПРИЛОЖЕНИЕ Б. МОДУЛИ СКАНИРОВАНИЯ СКАНЕРА SOLIDPOINT DAST

SolidPoint DAST способен анализировать как веб-приложения и API (см. приложение Б.1 «Анализ веб-приложений или API»), так и сети (см. приложение Б.2 «Анализ сетей»).

Б.1. АНАЛИЗ ВЕБ-ПРИЛОЖЕНИЙ ИЛИ API

Список модулей анализа поверхности атаки представлен в таблице 21.

Таблица 21. Модули анализа поверхности атаки

Имя модуля	Методы анализа поверхности атаки	Описание
autologin	Автоматическая аутентификация с помощью форм	Экспериментальный модуль, расширяющий поверхность атаки. Анализирует страницы на наличие форм входа и выполняет попытки аутентификации
dynamic-crawler	Динамический веб-краулинг	Поисковый модуль, выявляющий точки входа посредством динамического взаимодействия с интерфейсами веб-приложения с использованием управляемого браузера
graphql-inspector	Выявление конечных точек GraphQL	Модуль, который отправляет специфичные для GraphQL HTTP-запросы с целью выявления конечных точек GraphQL
har-importer	Импорт HAR-файлов	Модуль, экспортирующий конечные точки из HAR-файлов. Модуль принимает на вход браузерные HAR-файлы и файлы, содержащие массив (типа JSON и NDJSON) описаний HTTP-запросов в расширенном формате HAR
js-analyzer	Анализ клиентского JavaScript-кода	Модуль, выявляющий серверные точки входа при помощи анализа клиентского JavaScript-кода
openapi-hars-generator	Импорт спецификации OpenAPI	Модуль, экспортирующий точки входа из OpenAPI-спецификации
powby2	Недостатки, описанные сигнатурами Powby2	Модуль пассивного сканирования, который анализирует ресурсы, находящиеся в базе данных, и сопоставляет их с сигнатурами
static-crawler	Статический веб-краулинг и DirBuster (слепой перебор серверных точек доступа по словарю)	Поисковый модуль, который обходит веб-ресурсы и анализирует HTML-разметку, не производя открытие и рендеринг страницы. В рамках модуля есть возможность включения и отключения функции DirBuster
waf-har-extractor	Интеграция с SolidWall WAF	Модуль, экспортирующий точки входа из SolidWall WAF
Не задано	Пассивный сигнатурный анализ	Модуль пассивно анализирует HTTP-ответы, получаемые во время сканирования, и сопоставляет их с сигнатурами. Является частью сканера Fuchsia, не

Имя модуля	Методы анализа поверхности атаки	Описание
		имеет собственного имени и не имеет активной задачи в очереди модулей при сканировании. В настоящий момент по умолчанию модуль выключен и доступен для использования только через прямой запрос или консольный клиент fuchsiactl

Список модулей обнаружения недостатков⁴ представлен в таблице 22.

Таблица 22. Модули, обнаруживающие недостатки

Имя модуля	Обнаруживаемые недостатки	Описание
bruteforce	Подбираемые учетные записи	Модуль выявляет в системе учётные записи, имеющие слабые данные для входа, с помощью перебора по словарю. Помимо встроенного, также имеется возможность использовать пользовательский словарь. В настоящий момент поддержка пользовательского словаря реализована только для fuchsiactl
cors-franziscanner	Некорректная настройка CORS (совместное использование ресурсов между разными источниками)	Экспериментальный модуль выявляет недостатки настройки CORS, которые позволяют несанкционированным веб-страницам получать доступ к ресурсам приложения. Недостатки выявляются путём отправки запросов с различными значениями заголовка Origin и анализом CORS-заголовков в HTTP-ответах
cspp-scanner	Client-Side Prototype Pollution (клиентское загрязнение прототипа)	Модуль выявляет указанный недостаток при помощи динамической проверки выполнения JavaScript-кода на странице приложения в веб-браузере
dynamic-page-analyzer-domxss	DOM XSS	Модуль при помощи динамического анализа ищет потоки данных, которые могут привести к DOM XSS
dynamic-page-analyzer-cspp	Client-Side Prototype Pollution (клиентское загрязнение прототипа)	Модуль при помощи динамического анализа ищет потоки данных, которые могут привести к Client-Side Prototype Pollution
file-upload-scanner	Уязвимости загрузки файлов	Модуль выявляет недостатки, связанные с загрузкой файлов на веб-сервер. Обнаруживаются следующие уязвимости: Исполнение произвольного PHP-кода. Уязвимости, связанные с обработчиком изображений ImageMagick.

⁴ Термин «недостаток» понимается в широком смысле и включает в себя в том числе уязвимости и атаки.

Имя модуля	Обнаруживаемые недостатки	Описание
		Reflected XSS (модуль загружает HTML страницу и анализирует содержащийся текст)
idor-franziscanner	IDOR	Экспериментальный модуль выявляет указанный недостаток при помощи выделения потенциально небезопасных параметров и отправки запросов с подстановкой значений разных форматов в такие параметры. В результате работы осуществляются попытки сравнения структур полученных ответов и извлечения из них конфиденциальных данных
java-deserialize	Небезопасная десериализация в Java	Модуль выявляет указанный недостаток для веб-приложений на языке Java, используя сериализованные объекты, найденные при помощи модуля zvlom-serialize
nosql	NoSQL-инъекции	Модуль выявляет недостатки, возникающие при попадании пользовательских данных в контекст команд баз данных NoSQL из-за недостаточной или некорректной фильтрации. Валидация уязвимости осуществляется двумя способами: HTTP-ответ содержит ошибки NoSQL. Отправляется несколько HTTP-запросов с противоположными по смыслу операторами NoSQL и выявляются различия в полученных ответах
nuclei-runner	Недостатки, описанные сигнатурами Nuclei	Модуль активного сканирования, который использует сигнатуры в формате YAML и может сканировать различные протоколы
nuclei-runner-deps	Недостатки, описанные расширенными сигнатурами Nuclei	Модуль активного сканирования выявленных конечных точек, использующий расширенные шаблоны Nuclei. Для указанных конечных точек модуль позволяет задать условия запуска анализа
path-traversal-scanner	Path Traversal	Модуль выявляет недостаток, заключающийся в доступе к произвольным файлам и директориям на сервере, где запущено веб-приложение. Наличие уязвимости выявляется при попытке поиска содержимого стандартных для разных операционных систем файлов в HTTP-ответах
php-unserialize-fuzzer	Небезопасная десериализация в PHP	Модуль выявляет указанный недостаток для веб-приложений на языке PHP, используя сериализованные объекты, найденные при помощи модуля zvlom-serialize
reflected-xss	Reflected XSS (отраженный межсайтовый скриптинг)	Модуль выявляет указанный недостаток при помощи динамической проверки выполнения JavaScript-кода на странице приложения в веб-браузере

Имя модуля	Обнаруживаемые недостатки	Описание
reflected-xss-cspp	Reflected XSS (отраженный межсайтовый скриптинг)	Модуль выявляет указанный недостаток на основании результата работы модуля cspp-scanner
shell-injection-scanner	Shell-инъекции	Модуль выявляет указанный тип недостатка при помощи внедрения shell-команд с различными вариациями выхода из контекста данных в контекст команд. Валидация уязвимости происходит при помощи сетевого взаимодействия и поиска результата вывода команды в теле HTTP-ответа
sql-franziscanner	SQL-инъекции	Модуль выявляет недостатки, возникающие, когда пользовательские данные попадают в инструкцию SQL без должной фильтрации. Модуль выявляет указанный недостаток следующими способами: Слепые boolean-based проверки. Слепые проверки на основе времени HTTP-ответа. Проверки на основе ошибок. Проверки с помощью запросов, использующих UNION. Проверки с помощью составных запросов; Взаимодействие out-of-band
sql-injection-scanner	SQL-инъекции	Модуль выявляет указанный недостаток следующими способами: Взаимодействие out-of-band; Delay-based проверки. Busy wait проверки. Проверка добавлением кавычек
ssti-franziscanner	SSTI (инъекция шаблонов на стороне сканера)	Модуль выявляет недостатки, возникающие, когда веб-приложение некорректно обрабатывает пользовательский ввод в серверных шаблонах. Недостатки выявляются следующими способами: Взаимодействие out-of-band. Поиск результатов выполнения команд в телах HTTP-ответов. Выявление на основе времени HTTP-ответа
stored-xss	Stored XSS (хранимый межсайтовый скриптинг)	Модуль выявляет указанный недостаток при помощи двухэтапного обхода приложения и динамической проверки выполнения JavaScript-кода на странице приложения в веб-браузере
xxe-franziscanner	XXE (XML eXternal Entity attack – инъекция внешних сущностей XML)	Модуль выявляет недостатки приложения, которое анализирует входные данные XML. Недостаток возникает, когда входные данные XML, содержащие ссылку на внешнюю сущность, обрабатываются слабо сконфигурированным

Имя модуля	Обнаруживаемые недостатки	Описание
		анализатором XML. Недостатки выявляются следующими способами: Взаимодействие out-of-band. Поиск в HTTP-ответах содержимого стандартных для различных операционных систем файлов, подключенных как внешняя сущность в отправляемый на сервер XML-документ. Использование local DTDs техники
zvlom-serialize	Контролируемые сериализованные данные	Модуль выполняет поиск сериализованных объектов в ответе сервера. Умеет выявлять сериализованные объекты, которые могут быть закодированы как единой строкой, так и цепочкой из нескольких кодировок или алгоритмов сжатия. Выполняет поиск объектов, сериализованных в приложениях, использующих PHP, Python (Pickle), Ruby, Java, .NET и прочие технологии

Б.2. АНАЛИЗ СЕТЕЙ

Список модулей анализа поверхности атаки представлен в таблице 23.

Таблица 23. Модули анализа поверхности атаки сетей

Имя модуля	Методы анализа поверхности атаки	Описание
tcp-port-scanner	Выявление открытых TCP-портов	Модуль, который для указанной сети осуществляет поиск открытых TCP-портов
udp-port-scanner	Поиск и определение типов UDP-сервисов	Модуль, который для указанной сети осуществляет поиск и определение UDP-сервисов, используя цифровые отпечатки
tcp-port-fingerprinter	Определение типов сервисов	Модуль, который на основании результата работы модуля tcp-port-scanner определяет типы обнаруженных сервисов, используя цифровые отпечатки

ПРИЛОЖЕНИЕ В. ЖУРНАЛИРОВАНИЕ

Для записи истории событий, выявления и анализа ошибок и сбоев в сканере SolidPoint DAST используется система журналирования. Журналы имеют различные виды, которые описаны в таблице 24.

Таблица 24. Виды журналов

Вид	Способы просмотра	Описание
Журналы сервисов	Для Debian: утилита <code>journalctl</code> . Для Docker Compose: команда <code>docker logs</code>	Хранят записи о событиях и состояниях компонентов сканера
Журналы сканирования	Команда <code>fuchsiactl logs</code>	Хранят записи о событиях модулей <code>fuchsiad</code>
Журнал аудита	Запрос <code>GET /api/audit-log</code> в спецификации API ⁵	Хранит записи о взаимодействиях серверной части с другими компонентами или пользователем

⁵ Просмотр журнала аудита по спецификации API доступен по следующим адресам:

- Swagger — <https://ru.cloud.solidpoint.net/swagger> (Audit log);
- Redocly — <https://ru.cloud.solidpoint.net/redocly> (Audit log).