Платформа для управления уязвимостями и обеспечения безопасности в процессах разработки и DevSecOps “TRON.ASOC v.0.5”

Руководство пользователя

Июнь 2024

Содержание

Введение

Настоящий документ представляет собой руководство пользователя программного комплекса TRON.ASOC

Термины и определения

БДУ	Банк данных угроз безопасности информации
ПО	Программное обеспечение
Уязвимость (Vulnerability)	Уязвимость программного обеспечения — это сбой, изъян или слабое место в программном обеспечении, которое может быть использовано для нарушения функциональности или несанкционированного доступа к ресурсам приложения
ФСТЭК	Федеральная служба по техническому и экспортному контролю
ASOC (Application Security Orchestration and Correlation)	платформы или решения, предназначенные для управления и координации безопасностью приложений. ASOC позволяет автоматизировать процессы обнаружения, анализа и реагирования на угрозы безопасности, связанные с приложениями.
CI/CD	комбинация непрерывной интеграции (continuous integration) и непрерывного развертывания (continuous delivery или continuous deployment) программного обеспечения в процессе разработки. CI/CD объединяет разработку, тестирование и развертывание приложения.
CVE	Common Vulnerabilities and Exposures - база данных общеизвестных уязвимостей информационной безопасности. Каждой уязвимости присваивается идентификационный номер вида CVE-год-номер, описание и ряд общедоступных ссылок с описанием.
DevSecOps	методология разработки программного обеспечения, которая интегрирует практики безопасности (Sec) в процессы разработки и поставки программного обеспечения (DevOps).

NVD	National Vulnerability Database - национальная база данных уязвимостей. Американский правительственный репозиторий данных управления уязвимостями на основе стандартов, представленных с использованием протокола автоматизации содержимого безопасности.
PCI SSC	PCI Security Standards Council - открытое глобальное сообщество, задачи которого включают непрерывное развитие, совершенствование, хранение, распространение и внедрение стандартов безопасности для защиты данных платежных карт.
Security Pipeline	сочетание заданий для непрерывной доставки программного обеспечения, состоит из нескольких состояний или этапов, которые выполняются в последовательности один за другим.
SAST (Static Application Security Testing)	это процесс тестирования приложения на наличие ошибок и уязвимостей в исходном коде с применением статического анализа. Статический анализ может применяться для поиска кода, потенциально содержащего уязвимости
Проект	это сущность, которая создается авторизованным пользователем, чтобы логически объединить весь набор связанных приложений или компонентов, которые разрабатываются или поддерживаются в рамках одной команды или организации, и который нужно проверять на соответствие политикам безопасности компании и качество.

Общие сведения

«TRON.ASOC» - программный продукт для обнаружения и управления уязвимостями, а также обеспечения безопасности в процессах разработки и DevSecOps.

«TRON.ASOC» позволяет осуществлять всесторонний контроль безопасности разрабатываемых проектов, обеспечивая надежную защиту на всех этапах разработки.

«TRON.ASOC» интегрируется с репозиторием Gitlab, реестром образов Nexus и различными инструментами анализа безопасности разрабатываемых продуктов, такими как статический анализатор исходного кода PT Application Inspector и анализатор безопасности контейнеров KCS. Программа управляет проверками исходного кода и образов контейнеров на уязвимости и помогает управлять результатами этих проверок. Интеграция с этими инструментами позволяет настроить сканирование, запускать проверки и консолидировать результаты.

«TRON.ASOC» упрощает работу с найденными при помощи инструментов AST проблемами и уязвимостями, проводя их анализ и группировку для более эффективного управления.

«TRON.ASOC» осуществляет консолидацию и визуализацию данных, предоставляя пользователям наглядную информацию о состоянии безопасности их проектов.

«TRON.ASOC» предлагает удобный пользовательский интерфейс, доступный в современных браузерах на движке Chromium (Google Chrome, Яндекс Браузер, Edge, Safari и т.д.) и Firefox.

«TRON.ASOC» предоставляет возможности для управления сканированиями, включая настройку параметров сканирования, планирование запусков и мониторинг выполнения сканирований.

«TRON.ASOC» позволяет выгружать отчеты по результатам сканирований в формате JSON, что обеспечивает удобство интеграции с другими системами и инструментами анализа данных.

Начало работы в системе

Ссылка для входа в систему предоставляется администратором. При переходе по ссылке пользователь попадает на страницу авторизации.

Чтобы войти в систему, введите логин и пароль и нажмите кнопку Войти.

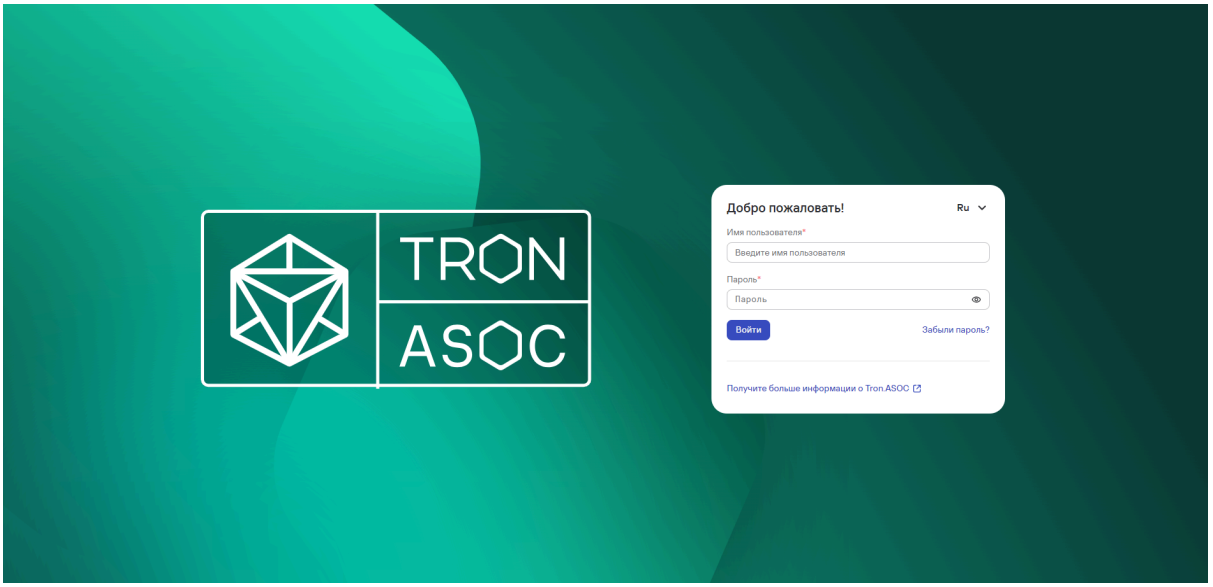

Рис. 1

При вводе неверных учётных данных на экране отобразится сообщение Неверный логин и/или пароль. При превышении числа попыток аутентификации с неверным паролем ваш аккаунт будет временно заблокирован. Количество попыток аутентификации и продолжительность блокировки устанавливается администратором системы (по умолчанию лимит попыток входа — 3, срок блокировки — 1 минута). После успешного входа в систему отображается Домашняя страница.

Домашняя страница

В левой части страницы расположено сайд-бар меню, которое предоставляет доступ к разделам продукта: Аутентификация, Управление доступом, Проекты, Интеграции (вкладки подменю - Инструменты безопасности и Источники сканирования), Конвейер безопасности. Видимость пунктов меню раздела зависит от набора привилегий и прав роли пользователя.

Проекты

Страница Проекты (рис. 2) предназначена для управления проектами. Все созданные и доступные пользователю проекты представлены в виде списка.

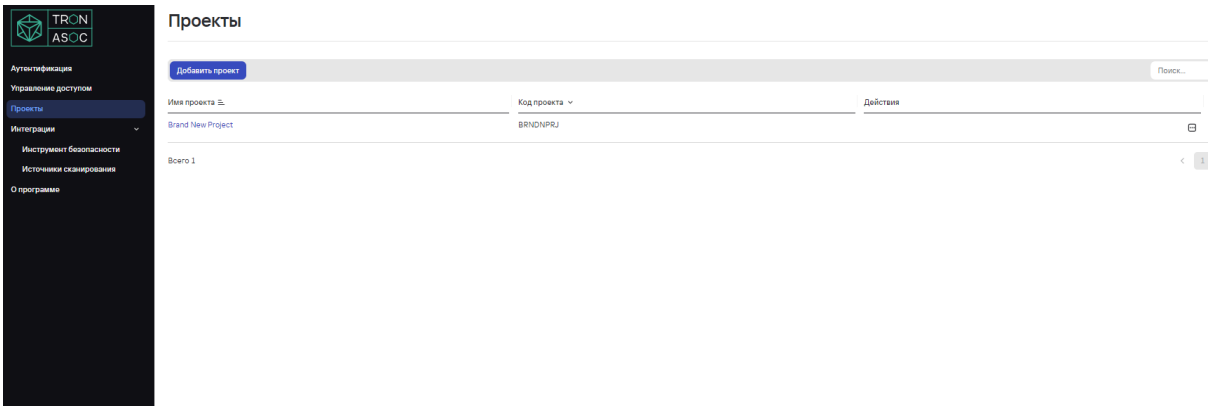

Рис.2

Для каждого проекта отображаются следующие данные: имя проекта, код проекта, доступные действия. В меню действий можно удалить (архивировать) проект и перейти на страницу редактирования проекта.

Список проектов можно отфильтровать по названию и коду проекта. Чтобы перейти на страницу конкретного проекта, нажмите на Имя проекта в списке.

Создание нового проекта

Чтобы создать новый проект, нажмите кнопку Добавить проект на странице Проекты. На странице создания проекта (рис.3) заполните поля Код проекта, Имя проекта, Описание, опционально можно добавить теги и нажмите кнопку Создать.

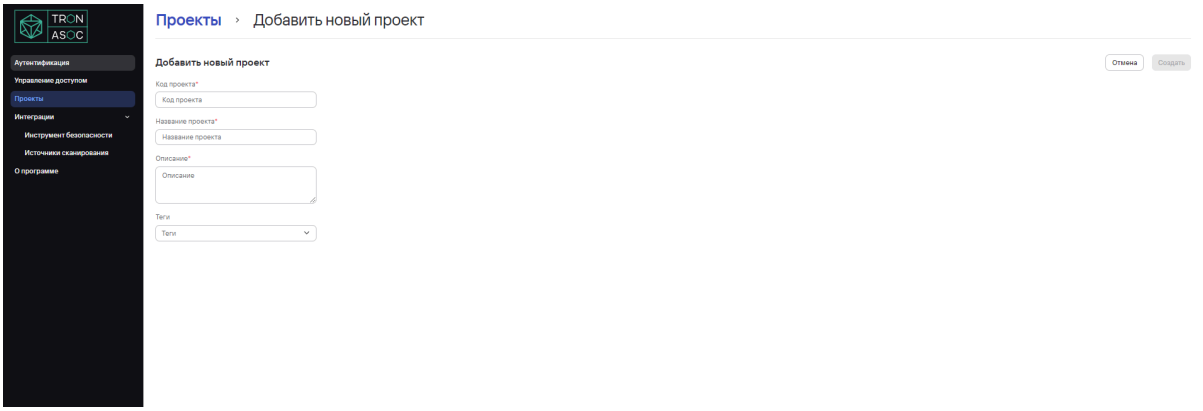

Рис.3

Редактирование проекта

Редактирование проекта доступно по кнопке меню действий в списке проектов. Также, чтобы отредактировать проект, можно перейти на страницу проекта (рис 4), нажав на имя проекта и затем на кнопку Редактировать проект, расположенную в верхнем правом углу. Форма редактирования проекта аналогична форме создания проекта.

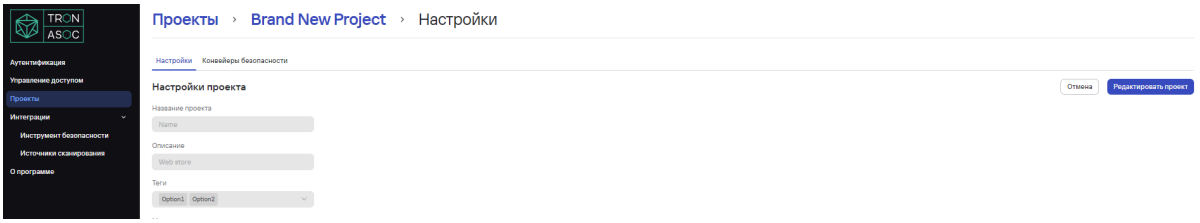

Рис.4а

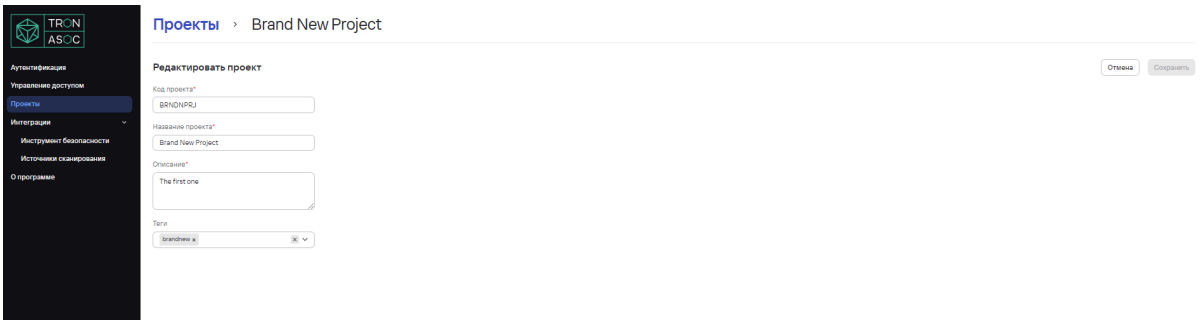

Рис.4б

Можно отредактировать Код проекта, Имя проекта, Описание и Теги. После завершения редактирования, нажмите кнопку Сохранить.

Конвейеры безопасности

В TRON.ASOC каждый Конвейер безопасности привязан к проекту. Конвейер безопасности- это группирующая сущность для Проверок безопасности. У пользователя есть возможность создания новых и настройки доступных ему уже созданных Конвейеров безопасности.
Чтобы начать работу с Конвейерами безопасности, перейдите на страницу Проекты, Имя проекта и откройте вкладку Конвейеры безопасности. Каждый Конвейер безопасности представлен отдельной строкой, которая содержит название и описание конвейера, ссылку на результаты сканирования, содержащиеся внутри конвейера проверки безопасности.

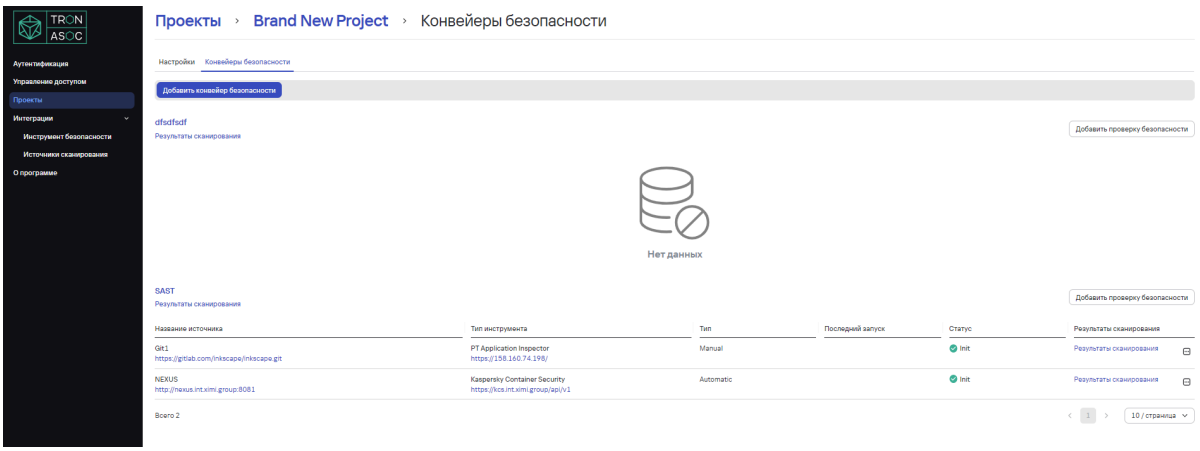

Рис.5

Создание конвейера безопасности

Чтобы создать новый Конвейер безопасности, нажмите на кнопку Добавить конвейер безопасности. На странице создания конвейера безопасности (рис.7) заполните поля Имя и Описание (обязательные поля отмечены звездочкой) и нажмите кнопку Создать.

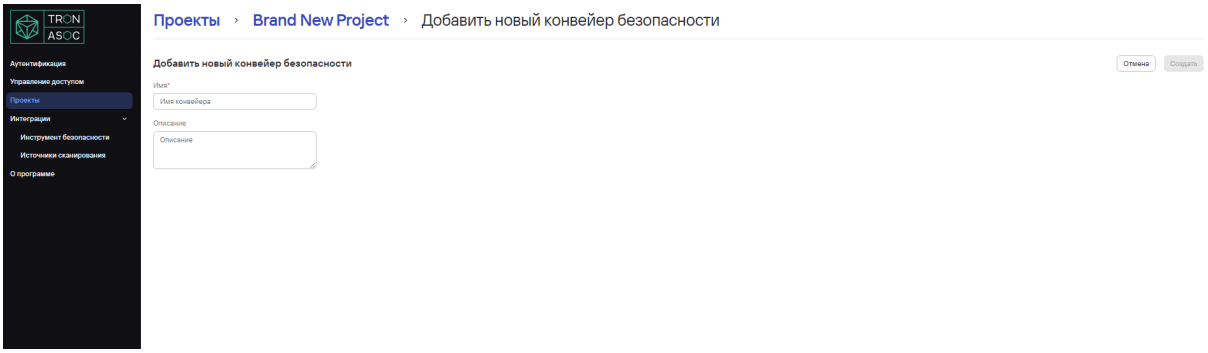

Рис. 6

На странице Конвейеров безопасности (рис.5) можно создавать и управлять Проверками безопасности. Проверка безопасности - это сущность, которая может объединять в себе связку инструмента сканирования и источника. Она используется для запуска сканирования безопасности, а также для получения результатов сканирований. На странице Конвейеров безопасности также можно увидеть название каждой проверки безопасности, используемый в проверке инструменты безопасности и источники, тип проверки (ручной или автоматический), время последнего запуска, статус, ссылку на результаты сканирования.

Проверка безопасности

Создание проверки безопасности

Чтобы добавить новую проверку безопасности, нажмите кнопку Добавить проверку безопасности в нужном Конвейере безопасности (выбор кнопки в строке с названием нужного конвейера).

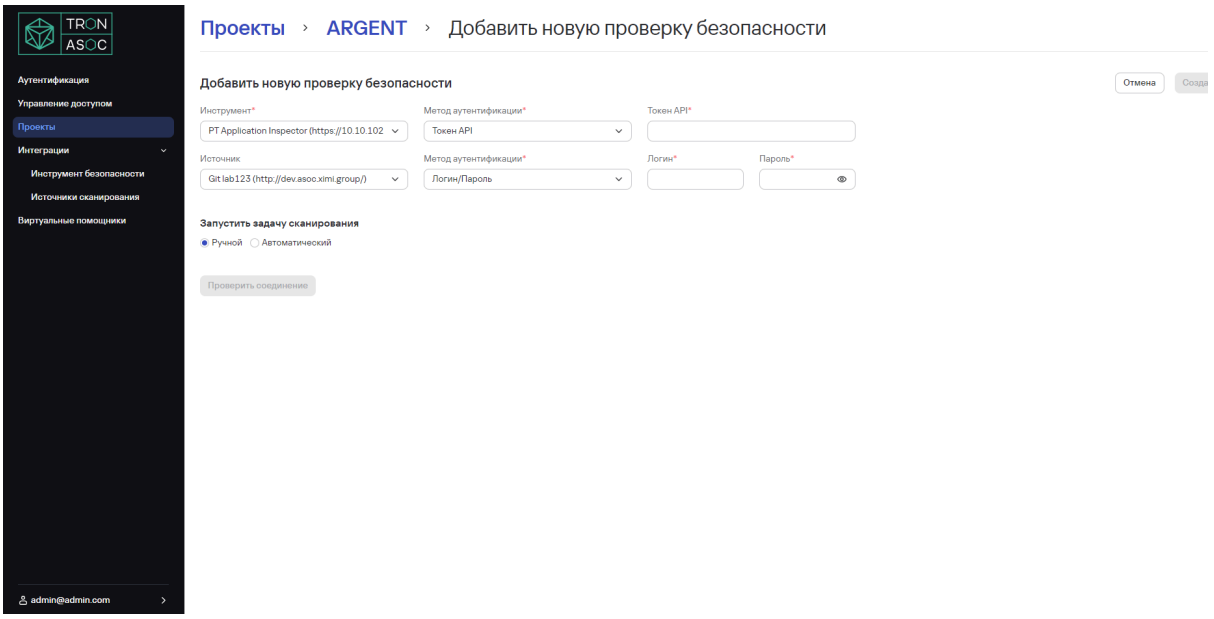

Рис. 7

Для настройки проверки безопасности выбор инструмента безопасности является обязательным. Если при создании интеграции с инструментом безопасности администратор не указал метод аутентификации, то при добавлении инструмента в Проверку безопасности поле выбора метода аутентификации является обязательным. Если вы выбрали метод аутентификации, введите данные для аутентификации в соответствующие поля (могут меняться в зависимости от метода: токен API, логин/пароль).
Пользователь может также добавить источник (объект) сканирования. Если при создании интеграции с источником администратор не указал метод аутентификации, то при добавлении источника в Проверку безопасности поле выбора метода аутентификации является обязательным. Если вы выбрали метод аутентификации, введите данные для аутентификации в соответствующие поля (могут меняться в зависимости от метода: токен API, логин/пароль).
Если заполнены все необходимые поля (инструмент безопасности, источник, методы аутентификации), можно проверить соединение с инструментами, нажав на кнопку Проверить соединение.

Есть возможность выбрать тип запуска сканирования (ручной или автоматический) и периодичность и время запуска сканирования при выборе автоматического запуска.

Редактирование проверки безопасности

Чтобы отредактировать проверку безопасности, нажмите на Имя в списке доступных проверок безопасности. Форма редактирования аналогична форме создания новой проверки безопасности, но на форме редактирования есть блок Конечная точка API проверки безопасности.В случае использования внешних скриптов используйте эту конечную точку API для отправки результатов сканирования инструмента.

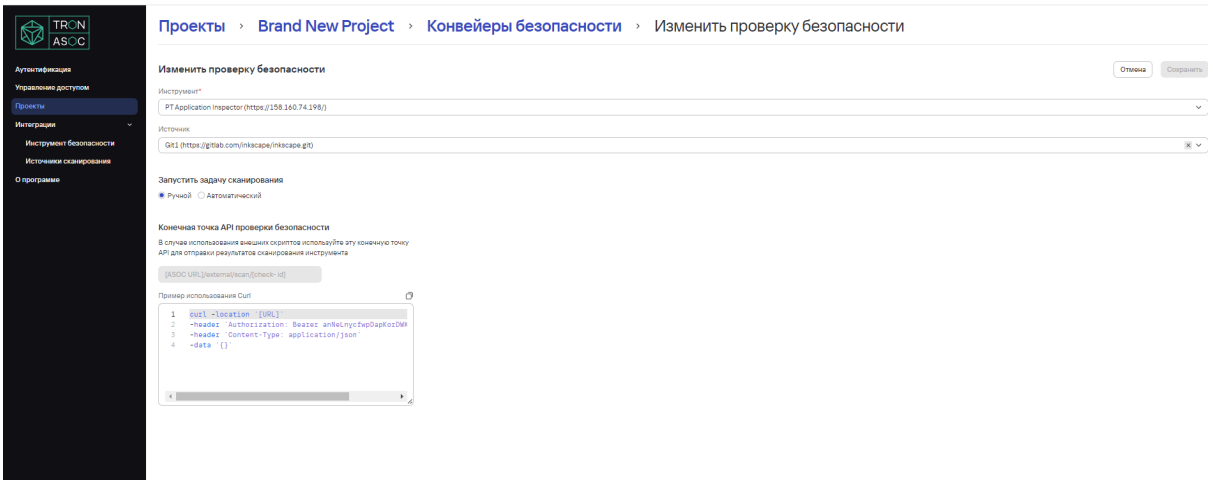

Рис. 9

Запуск сканирования

Запуск проверки безопасности производится вручную. Чтобы запустить сканирование, нажмите кнопку “Начать проверку” в той Проверке безопасности, которую вы хотите запустить. Запущенная проверка получает статус In progress. После успешного завершения проверка переходит в статус Done. Общее максимальное время работы цикла сканирования - по умолчанию 1 час. Если цикл достиг максимального времени работы, то проверка переходит в статус Failed и процесс завершается. Статус Failed также назначается, если что-то пошло не так на каком-либо из шагов сканирования.

Остановка сканирования

Сканирование в статусе In Progress можно остановить из интерфейса в соответствующей Проверке безопасности. Чтобы остановить выполнение проверки безопасности, нажмите на кнопку “Остановить сканирование”.

Результаты сканирований

Результат успешного сканирования можно просмотреть как для всего проекта, так и для отдельного конвейера безопасности и отдельной проверки безопасности.
Результаты сканирования содержат информацию о найденных уязвимостях, ошибках безопасности и других проблемах. Когда выполнение проверки безопасности завершается, результаты проверки импортируются из инструментов AST. Результаты сканирования безопасности собираются и упорядочиваются. Каждый инструмент AST создает отчет по безопасности во время каждого запуска тестирования безопасности. Система позволяет выгружать отчеты по результатам сканирований в формате JSON, что обеспечивает удобство интеграции с другими системами и инструментами анализа данных.
В каждом результате сканирования содержится сводный результат по успешному запуску:

- количество найденных уязвимостей (всего + по степени критичности),
- время поиска
- ошибки, если были
- объект сканирования
- количество проверенных файлов (компонентов)
- количество файлов (компонентов) с уязвимостями.