Solar appScreener

Руководство пользователя Solar appScreener модуль анализа состава программного обеспечения (SCA)

Solar appScreener

Версия 3.13.9

Ноябрь 2023

СОДЕРЖАНИЕ

1. ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

Термин	Расшифровка
АРМ	Автоматизированное рабочее место
ОС	Операционная система
ПО	Программное обеспечение
CLI	Command Line Interface – интерфейс командной строки
CLT	Command Line Tool – инструмент командной строки
REST	Representational State Transfer – передача состояния представления
SDLC	System Development Life Cycle – жизненный цикл разработки системы
VCS	Version Control System – система управления версиями

2. ГЛОССАРИЙ

API (Программный интерфейс приложения, Application Programming Interface) — интерфейс, который определяет взаимодействие программы с другой программой.

CI/CD система — система, которая объединяет практики непрерывной интеграции, непрерывной доставки и непрерывного развёртывания. CI/CD системы могут быть встроены в процесс разработки по методике SDLC и SSDLC. Примеры: **TeamCity**, **Jenkins**.

Continuous Delivery (Непрерывная доставка, CD) — практика разработки программного обеспечения, при которой команды производят программное обеспечение в короткие циклы.

Continuous Deployment (Непрерывное развёртывание, CD) — практика разработки программного обеспечения, которая заключается в использовании автоматизированного тестирования для проверки правильности и стабильности изменений в коде для быстрого, автономного развёртывания в производственной среде.

Continuous Integration (Непрерывная интеграция, CI) — практика разработки программного обеспечения, которая заключается в слиянии рабочих копий в общую основную ветвь разработки и выполнении автоматизированных сборок проекта для выявления потенциальных ошибок и решения интеграционных проблем.

ID проекта (Project ID)— первые 6 символов UUID проекта. ID проекта может быть использован при поиске проекта в общем списке проектов, но UUID является полным идентификатором проекта. Пример ID проекта: d4d1e2.

Software Development Lifecycle (SDLC) — методика разработки, которая обеспечивает качество и правильность работы программного обеспечения. Методика SDLC состоит из таких этапов: анализ требований, дизайн системы, разработка, тестирование, эксплуатация, поддержка.

Secure Software Development Lifecycle (Secure SDLC, SSDLC, DevSecOps) — методика разработки программного обеспечения, которая используется организациями для создания безопасных приложений. При SSDLC на каждом этапе SDLC выполняется ряд дополнительных действий по обеспечению безопасности. Например, анализ рисков на этапе анализа требований, оценка рисков на этапе архитектуры, проверка выполнения требований безопасности на этапе тестирования, мониторинг угроз и реагирование на инциденты на этапах эксплуатации и поддержки.

UUID (Universally unique identifier) — 128-битное число, которое используется для идентификации информации. Пример: d4d1e2da-6b82-4350-829b-d3883592f4c8.

Version Control System (VCS, Система контроля версий) — программный инструмент, который служит для записи изменений в файлы и отслеживания изменений, внесённых в код. Примеры: **Git**, **Subversion**.

VCS хостинг — веб-сервис для хостинга проектов и их совместной разработки. Примеры: **GitLab**, **GitHub**, **Bitbucket**.

XPath — язык запросов к элементам XML-документов.

Безопасность приложения (Application security) — набор мер, принимаемых для повышения безопасности приложения, часто путём обнаружения, исправления и предотвращения уязвимостей безопасности.

Интеграция (Integration) — обмен данными между системами с возможной последующей обработкой.

Конфигурационный файл (Configuration file) — файл с настройками приложения.

Система отслеживания ошибок (Bug tracking system, Bug tracker) — программа, разработанная для учёта и контроля ошибок, найденных в программном обеспечении, которая позволяет следить за процессом устранения этих ошибок. Примеры: **Jira**, **Redmine**.

Скрипт (Script) — последовательность команд для автоматического выполнения задачи.

Токен авторизации API (Токен, API authorization token) — набор символов, который предназначен для аутентификации пользователей для выполнения действий в системе без использования пользовательского интерфейса.

3. ВВЕДЕНИЕ

Настоящий документ представляет собой руководство пользователя Solar appScreener модуля анализа состава программного обеспечения (далее модуля SCA).

4. СВЕДЕНИЯ О МОДУЛЕ SCA

4.1. Назначение модуля SCA

Модуль SCA предназначен для выявления уязвимостей в библиотеках с открытым исходным кодом, используемых в коде приложения.

С помощью с помощью модуля SCA можно:

- Обнаруживать и отслеживать компоненты с открытым исходным кодом;
- Выявлять уязвимые зависимости, как прямые, так и транзитивные.

4.2. Описание возможностей

Модуль SCA предоставляет следующие возможности:

- Анализ состава программного обеспечения.
- Мониторинг изменения уровня безопасности приложения.
- Интеграция в процесс разработки.

4.3. Требования к АРМ пользователя

4.3.1. Требования к аппаратному обеспечению

АРМ пользователя модуля SCA должно быть оборудовано персональным компьютером с подключением к внутренней сети компании.

4.3.2. Требования к программному обеспечению

В состав программного обеспечения компьютера для АРМ пользователя Solar appScreener модуль анализа состава программного обеспечения (SCA) должна входить программа-клиент, предоставляющая пользователю возможность навигации и просмотра веб-ресурсов (браузер). Рекомендуемые браузеры (актуальные версии):

- **Mozilla Firefox**;
- **Google Chrome**;
- **Safari**;
- **Internet Explorer**;
- **Microsoft Edge**.

5. ИНТЕРФЕЙС ПОЛЬЗОВАТЕЛЯ

5.1. Авторизация

Ссылка для входа в веб-интерфейс модуля SCA (далее UI) предоставляется администратором. При переходе по ссылке пользователь попадает на страницу авторизации.

Чтобы войти в систему, введите логин и пароль и нажмите кнопку **Войти** (рис. 5.1).

Вход в систему может быть осуществлен с помощью логина (в формате <user> или <user@domain>) и пароля учётной записи **LDAP**. Чтобы настроить доступ с помощью **LDAP**, обратитесь к администратору.

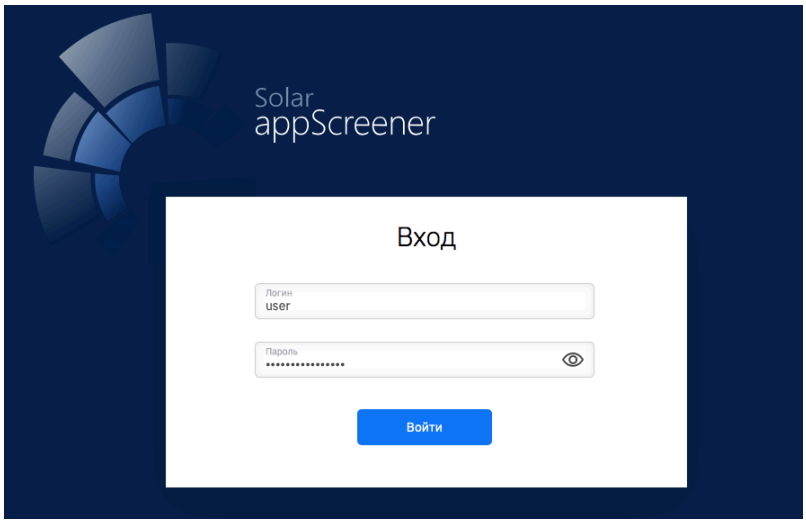

Рис. 5.1: Страница Авторизации

При введении 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 — 5, срок блокировки — 5 часов).

Прежде чем начать работу с модулем SCA, ознакомьтесь с Пользовательским соглашением и нажмите **Принимаю**(рис. 5.2).

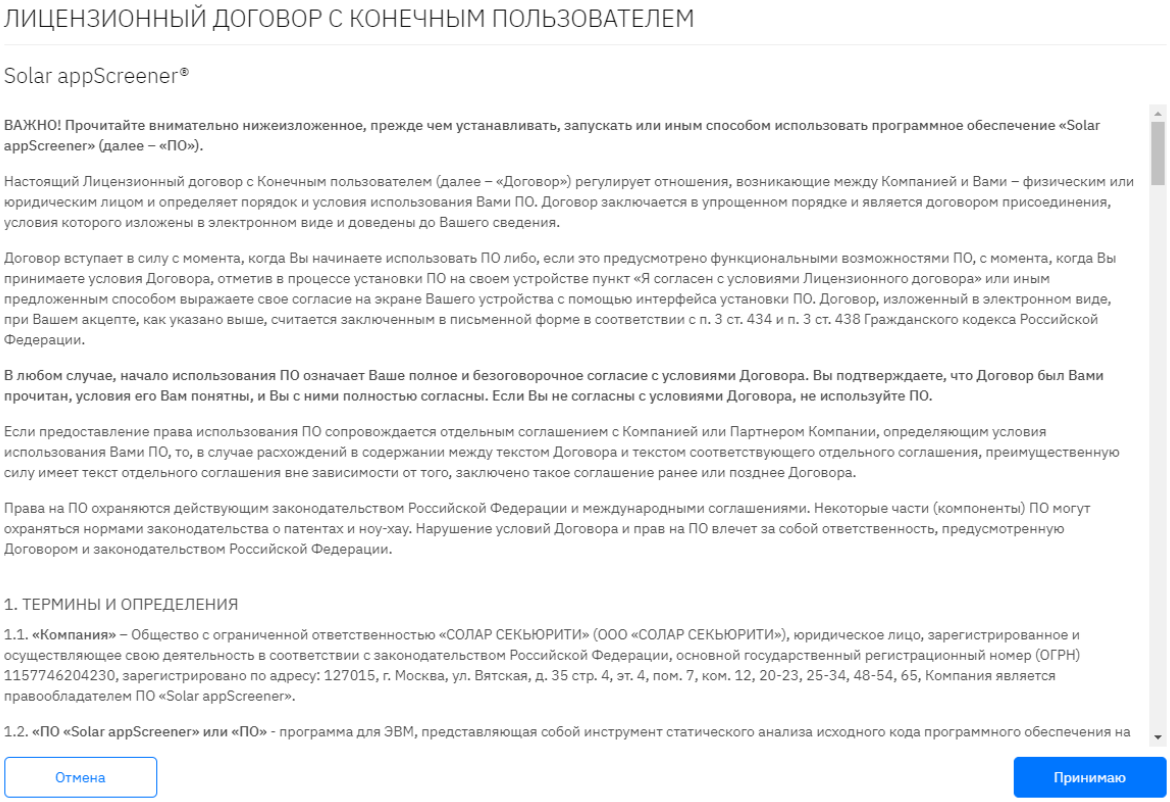

Рис. 5.2: Пользовательское соглашение

После успешного входа в систему отображается краткая инструкция. После просмотра инструкции отображается **Домашняя страница**. Повторный просмотр краткой инструкции доступен на странице **О продукте**.

5.2. Главное меню

В верхней части страницы расположено главное меню, которое предоставляет доступ к разделам **Домашняя страница**, **Проекты**, **Правила и наборы**, **Аналитика**, **О продукте**, **Личный кабинет**.

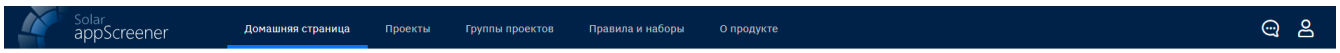

Рис. 5.3: Главное меню

Для доступа к форме обратной связи нажмите  .

5.2.1. Домашняя страница

Домашняя страница (рис. 5.4) предназначена для загрузки и сканирования новых проектов. **Проектом** здесь и далее называется загрузка в модуль SCA приложения и его сканирование с целью выявления уязвимостей. Под **сканированием** следует понимать анализ библиотек с открытым исходным кодом, используемых в приложении на уязвимости. **Уязвимости** — недостатки в коде приложения, которые могут быть использованы злоумышленниками и вызывать нарушение корректной работы

приложения. Подробное описание запуска проекта представлено в разделе Создание проекта.

На **Домашней странице** также можно:

- ознакомиться со списком проектов — отображаются последние 4 проекта с последующей ссылкой на страницу **Проекты** с полным списком проектов;
- увидеть статистику по количеству сканирований с учётом статусов. Нажмите на статус, чтобы посмотреть список соответствующих проектов.

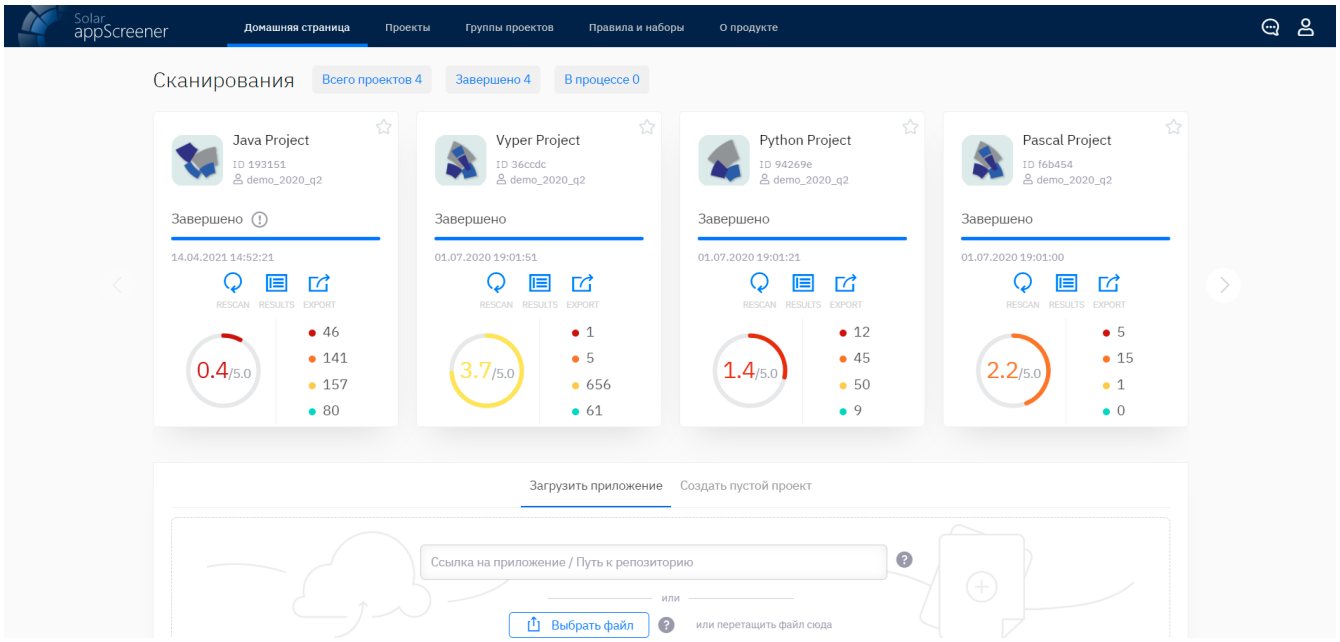

Рис. 5.4: Домашняя страница

5.2.2. Проекты

Страница **Проекты** (рис. 5.5) предназначена для управления проектами. Все проекты представлены в виде списка с краткими характеристиками.

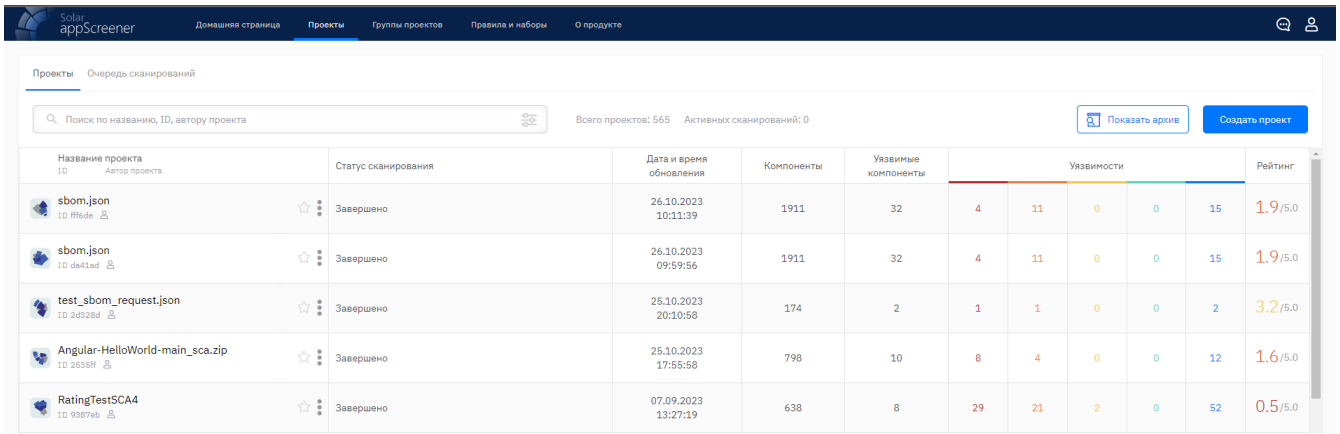

Рис. 5.5: Проекты

Для каждого проекта отображаются следующие данные:

- логотип, название проекта, автор (пользователь, загрузивший проект), ID проекта (первые шесть символов UUID проекта);

Рис. 5.6: Проекты: название

- статус последнего сканирования;

Рис. 5.7: Проекты: статус

- меню действий:
  - копировать UUID проекта;
  - посмотреть подробные результаты последнего сканирования;
  - запустить сканирование;
  - выгрузить отчёт;
  - настроить проект;
  - добавить в группу;
  - архивировать проект.

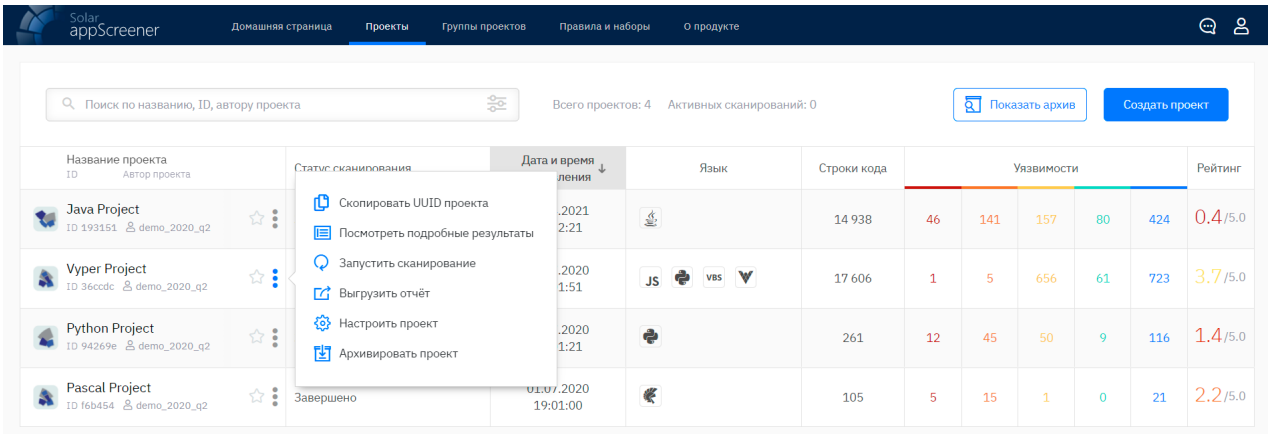

Рис. 5.8: Проекты: действия

- кнопка добавления в Избранное

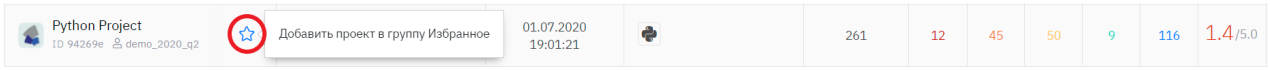

Рис. 5.9: Проекты: добавить в Избранное

- дата и время последнего сканирования;

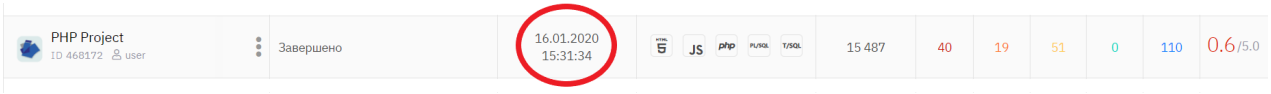

Рис. 5.10: Проекты: дата и время

- компоненты, которые были проанализированы;

!

- количество обнаруженных уязвимых компонент;

!

- количество уязвимостей критического, среднего, низкого и информационного уровней, а также общее количество уязвимостей;

Рис. 5.11: Проекты: количество уязвимостей

- рейтинг приложения.

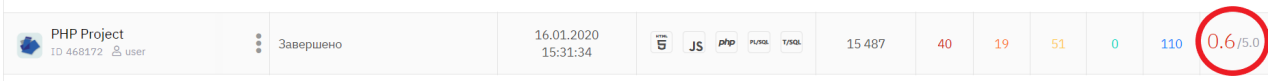

Рис. 5.12: Проекты: рейтинг

В модуле анализа состава программного обеспечения (SCA) уязвимости поделены на четыре категории: критические, среднего уровня, низкого уровня и информационного уровня.

1. Критические уязвимости с большой вероятностью приводят к компрометации конфиденциальных данных и нарушению целостности системы.
2. Уязвимости среднего уровня могут с меньшей вероятностью привести к компрометации конфиденциальных данных и нарушению целостности системы либо являются менее серьёзными нарушениями безопасности.
3. Уязвимости низкого уровня могут стать потенциальной угрозой безопасности.
4. Уязвимости информационного уровня сигнализируют о нарушении хороших практик программирования.

Рейтинг приложения вычисляется исходя из количества критических уязвимостей и уязвимостей среднего уровня. Влияние критических уязвимостей больше, чем влияние уязвимостей среднего уровня, и не учитывает объем кода. Уязвимости среднего уровня учитываются из расчёта их количества на общее число строк исходного кода.

Список можно отсортировать по названию, статусу последнего сканирования, по дате и по рейтингу. Для этого нажмите на соответствующий заголовок, повторное нажатие меняет порядок сортировки (рис. 5.13).

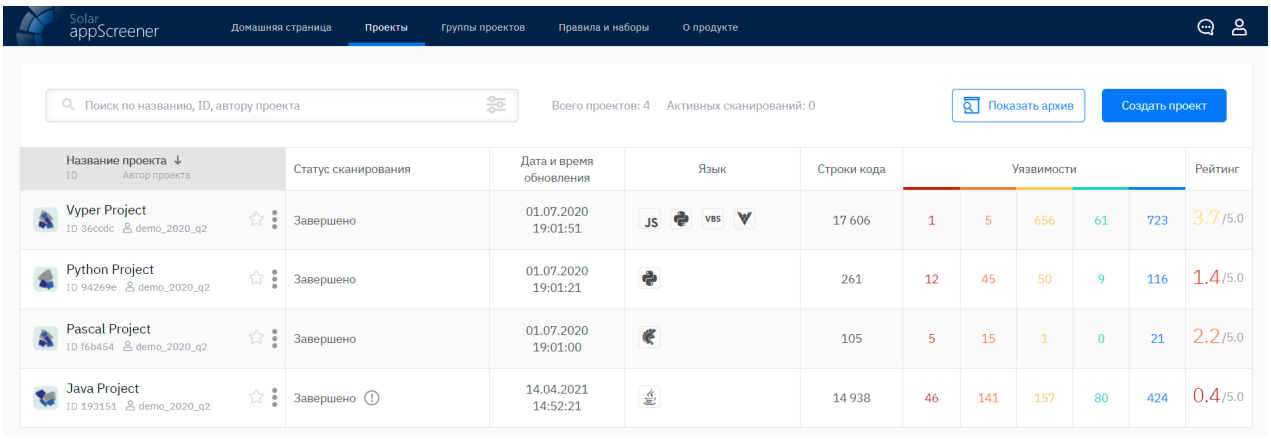

Рис. 5.13: Сортировка по названию

Для скрытия ненужных в данный момент проектов существует возможность архивации. Архивированный проект сохраняется в системе, но становится недоступным для работы. Выберите **Архивировать проект** в меню действий, чтобы добавить проект в архив. Проект, находящийся в архиве, можно найти, нажав **Показать архив** на странице **Проекты**.

Для удобной навигации по проектам предусмотрены поиск и фильтры. Поиск позволяет искать проекты по названию, ID проекта или автору. Чтобы установить фильтры, нажмите на иконку фильтров и настройте один или несколько параметров:

- статус сканирования — выбрать из списка статусы сканирования;
- дата обновления — задать временной диапазон;
- рейтинг — задать диапазон для рейтинга последнего сканирования в проекте;
- количество уязвимостей каждого из уровней критичности — задать диапазон для количества уязвимостей критического, среднего, низкого или информационного уровня.

Чтобы установить фильтры, нажмите на кнопку **Применить**. После применения фильтров в правой части страницы появится количество отобранных проектов и кнопка **Сбросить**. Нажатие на кнопку отменит фильтрацию.

Чтобы перейти на страницу конкретного проекта, нажмите на его название в списке. Подробнее про управление конкретным проектом в разделе Управление проектом.

5.2.2.1. Очередь сканирований

На вкладке **Очередь сканирований** можно управлять очередью сканирований в системе, поднимать/опускать приоритет сканирований. Система поддерживает 4 уровня приоритета сканирований: Низкий, Средний, Высокий и Эксклюзивный. По умолчанию сканирования запускаются со **Средним** приоритетом.

Искать сканирование в очереди можно по ID, названию проекта и автору сканирования.

В основной части страницы находится список всех активных сканирований в системе. Он представлен в виде таблицы со столбцами:

- Название проекта — кликабельно, по клику происходит переход на страницу **Обзор** (при наличии доступа в проект у пользователя);
- Сканирование — первые 6 символов UUID сканирования (по кнопке может быть скопирован целиком) и автор сканирования;
- Дата создания;
- Статус;
- Приоритет.

Все столбцы поддерживают сортировку, по умолчанию отсортированы по приоритету. Сканирования с одинаковым приоритетом сортируются по дате создания: первым отображается и будет просканирован проект, запущенный *раньше*.

Обратите внимание: изменение приоритета сканирования затрагивает только проекты в очереди и не повлияет на прогресс сканирований, которые уже выполняются.

5.2.3. Группы проектов

Проекты в Solar appScreener модуль анализа состава программного обеспечения (SCA) можно объединять в группы. Используя группы, можно выполнять действия с несколькими логически связанными проектами одновременно. Также для групп доступна сводная информация и аналитика. Работать с группами можно в разделе **Группы проектов** (рис. 5.14).

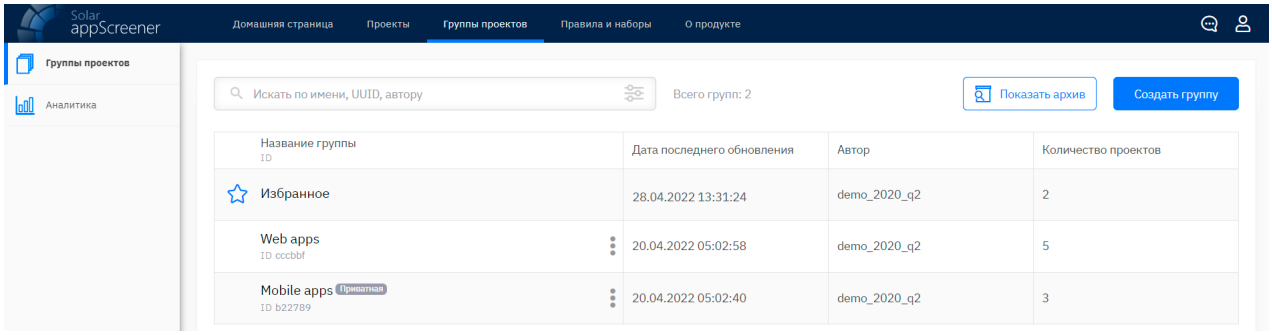

Рис. 5.14: Группы проектов

Список групп отображается в основной части страницы. Для каждой группы отображаются следующие данные:

- название группы;
- ID группы;
- видимость;
- меню действий:
  - копировать UUID группы;
  - проекты — перейти к списку проектов;
  - настроить группу;
  - архивировать группу.
- дата и время обновления;
- автор;
- количество проектов в группе.

Список можно отсортировать. Для этого нажмите на соответствующий заголовок, повторное нажатие меняет порядок сортировки. Для удобной навигации также

предусмотрен поиск и фильтры. Поиск позволяет искать группы проектов по названию, UUID группы или автору. Чтобы установить фильтры, нажмите на иконку фильтров и настройте один или несколько параметров:

- видимость — выбрать публичные или приватные группы;
- количество проектов в группе — можно указать диапазон;
- дата создания;
- дата последнего обновления;
- наличие проектов — добавить проекты, которые должна содержать группа.*

* *Обратите внимание: при выборе нескольких проектов фильтр работает как условие ИЛИ, то есть результаты поиска будут содержать группы проектов с хотя бы одним из указанных проектов.*

Чтобы установить фильтры, нажмите на кнопку **Применить**. После применения фильтров в правой части страницы появится количество отобранных проектов и кнопка **Сбросить**. Нажатие на кнопку отменит фильтрацию.

5.2.3.1. Создание группы проектов

Чтобы создать группу проектов, нажмите **Создать группу**, укажите имя группы и выберите проекты, которые следует в неё включить. Также можно включить проекты из существующих групп. Чтобы группа отображалась у всех пользователей, выберите опцию **Публичная**. После выполнения этих действий нажмите **Сохранить** (рис. 5.15).

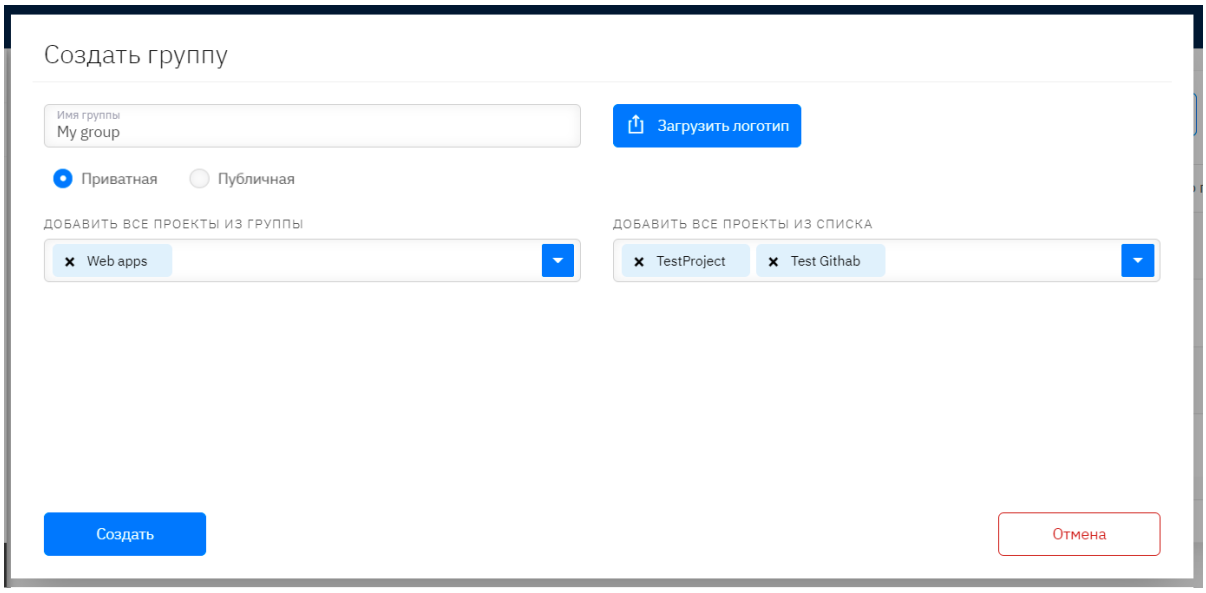

Рис. 5.15: Создание группы проектов

5.2.3.2. Работа с группой проектов

Чтобы перейти к конкретной группе проектов, кликните по её названию в списке групп.

На вкладке **Обзор** представлена общая статистика по сканированиям в группе. Динамику результатов сканирований проектов можно проследить на графиках. В верхней части страницы можно выбрать тип значений (суммарное или среднее) и период

для отображения. Сводная информация по сканированиям представлена в таблице **Статистика группы**.

Действия с проектами в группе доступны на вкладке **Проекты**. Здесь можно просмотреть список всех проектов в группе, добавить/удалить проект или поместить/извлечь проект из архива группы. Обратите внимание: при удалении проекта происходит только его удаление из группы, но не из системы.

Управлять группой и правами пользователей в группе можно во вкладке **Настройки**. В подразделе **Управление группой** можно редактировать данные группы, поместить/извлечь группу из архива или удалить группу. В подразделе **Jira** можно привязать группу проектов модуля SCA к проекту **Jira**.

5.2.3.3. Аналитика

Раздел **Аналитика** предназначен для просмотра общей статистики по всем сканированиям в системе и сравнения результатов анализа по группам.

На вкладке **Результаты** (рис. **??**) можно проследить динамику результатов сканирований проектов. Добавьте группу к статистике, чтобы сравнить результаты. Для просмотра информации по всем проектам, выберите **Все проекты** в списке групп. Аналогично разделу **Статистика группы** тип значений и период для отображения можно настроить. Для каждой из групп на графиках отображаются данные:

- количество сканирований (при отображении суммарного значения) или рейтинг (при отображении среднего значения);
- продолжительность сканирований;
- количество уязвимостей (с учётом уровня критичности).

Для просмотра аналитики по сканированиям перейдите на вкладку **Сканирования**. В таблице отображаются данные о количестве проектов в группе, количестве сканирований и их статусах. Чтобы убрать группу из статистики, нажмите на иконку крестика в конце строки нужной группы.

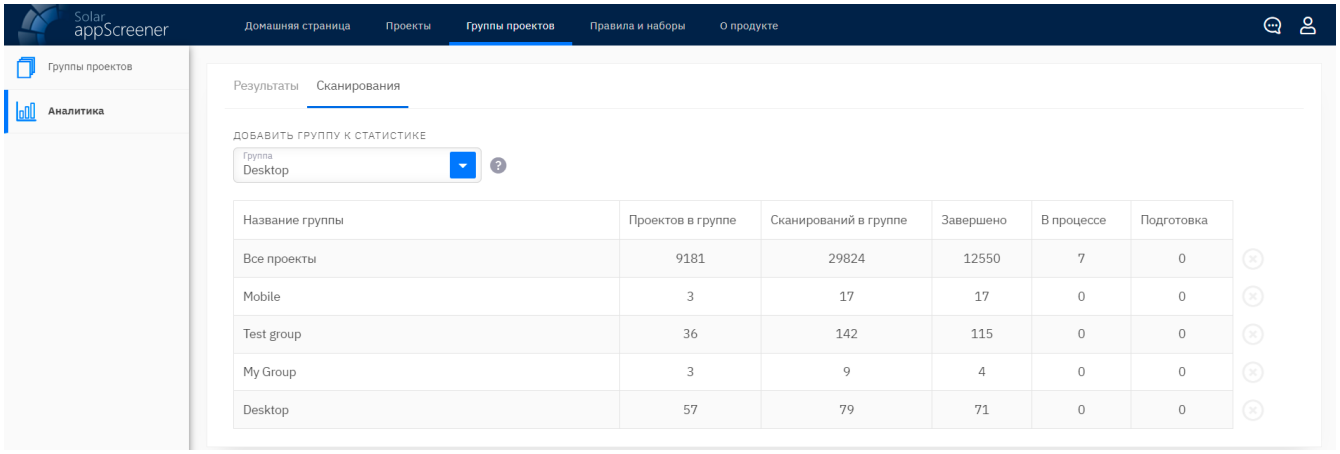

Рис. 5.16: Просмотр статистики по группам проектов

5.2.4. О продукте

Страница **О продукте** (рис. **??**) служит для предоставления пользователю общей информации о работе с Solar appScreener модуль анализа состава программного обеспечения (SCA). В верхней части страницы можно переключаться между следующими разделами:

- Инструкция;
- Общая информация;

В разделе **Инструкция** представлено краткое описание запуска анализа. Из этого раздела можно скачать руководство пользователя и включить/отключить отображение подсказок в интерфейсе.

В разделе **Общая информация** перечисляются основные возможности продукта.

В разделах **Анализ мобильных приложений** и **Анализ веб-приложений** приведены распространенные уязвимости для мобильных и веб-приложений соответственно.

В разделе **Инструкции по настройке WAF** описана возможность генерировать рекомендации по настройке средств защиты периметра.

5.2.5. Личный кабинет

Личный кабинет (рис. 5.17) открывается при наведении курсора на иконку в правом углу верхнего меню. Появляется выпадающее меню с пунктами: **Профиль**, **Настройки**, **Выйти**.

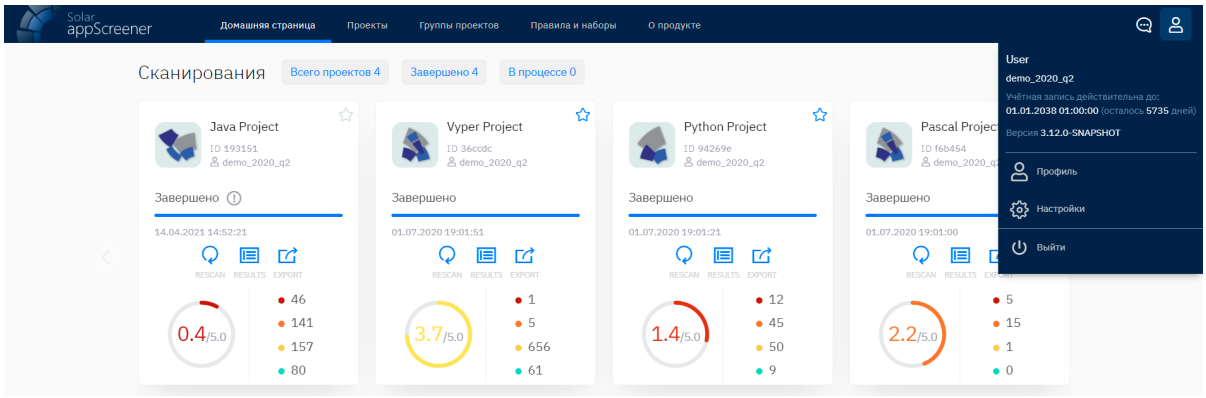

Рис. 5.17: Личный кабинет

5.2.5.1. Профиль

В разделе **Профиль** можно выполнить следующие действия:

- ознакомиться с информацией об учётной записи;
- ознакомиться с информацией об ограничениях лицензии;
- настроить оповещения;
- выбрать язык интерфейса.

Если вы хотите получать почтовые оповещения о завершённых сканированиях, воспользуйтесь переключателем. По желанию к оповещению можно добавить краткую

информацию о результатах сканирования или текст ошибки в случае, если сканирование будет завершено с ошибкой.

5.2.5.2. Настройки доступа

5.2.5.2.1. Токен и пароль

На вкладке **Токен и пароль** можно получить активный токен авторизации и изменить пароль учётной записи.

Токен авторизации предназначен для аутентификации пользователя при выполнении действий в Solar appScreener модуль анализа состава программного обеспечения (SCA) без использования UI. Например, чтобы запускать сканирования напрямую через CLT или автоматизировать действия в системе с помощью скриптов. Чтобы получить токен авторизации API:

1. Нажмите **Создать токен**.
2. Введите пароль учётной записи.
3. Укажите время действия токена.
4. Нажмите **Получить активный токен**.

Токен авторизации появится в соответствующем поле. Ознакомиться с информацией о всех активных токенах можно в таблице.

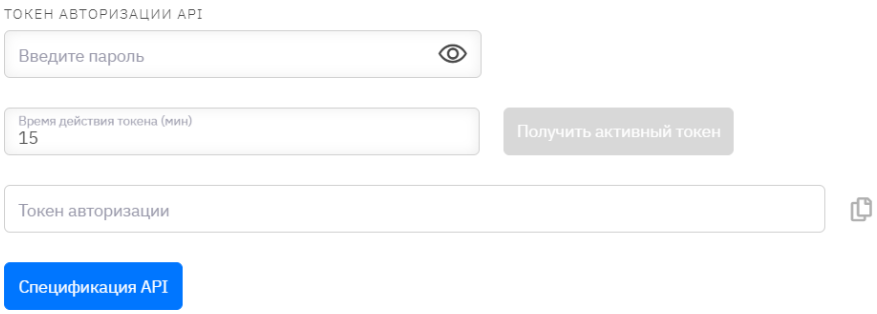

Рис. 5.18: Токен авторизации API

В соответствии с требованиями информационной безопасности **пароль** учётной записи должен регулярно обновляться. Незадолго до истечения срока действия текущего пароля вы получите уведомление.

Для **смены пароля:**

1. Укажите текущий пароль.
2. Укажите новый пароль и повторите его в следующем текстовом поле.
3. Нажмите **Сохранить**.

По истечению срока действия пароля произойдёт автоматический выход из системы на всех устройствах. Для повторного входа требуется установить новый пароль.

5.2.5.2.2. Jira

Для того чтобы привязать аккаунт Jira (рис. 5.19):

1. Введите URL сервера Jira.
2. Введите логин и пароль от аккаунта Jira.
3. Нажмите **Привязать аккаунт**.

В результате этих действий в разделе **Личный кабинет** будет указан привязанный аккаунт Jira. В этом же разделе можно **Отвязать аккаунт** и **Проверить соединение** с Jira.

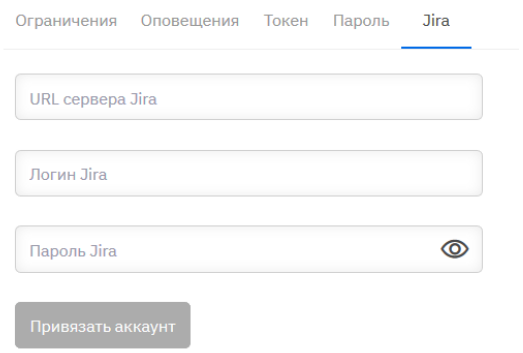

Рис. 5.19: Привязка аккаунта Jira

5.2.5.2.3. Приватный репозиторий

В разделе **Приватный репозиторий** можно работать с учётными данными, необходимыми для анализа файлов из закрытых репозиториев. Сохранённые в разделе учётные записи можно использовать в различных проектах в системе.

Вы можете добавить/редактировать учётные данные 4 типов:

- логин и пароль - укажите имя пользователя и пароль от ресурса, которому требуется аутентификация;
- токен доступа - предоставьте токен, используемый для авторизации на стороннем ресурсе;
- SHH-ключ - предоставьте приватный SSH-ключ (может быть введён вручную или загружен файлом) и при необходимости отредактируйте конфигурацию SSH клиента (доступно только при выключенном переключателе);

Добавленные учётные записи отображаются в виде списка на соответствующих вкладках. Чтобы отредактировать данные или настроить доступ к ним других пользователей системы, выберите нужную учётную запись из списка.

Данные учётной записи также можно заполнить перед началом сканирования. Выбор опции **Использовать данные при пересканировании проекта** сохранит данные в зашифрованном виде в настройках проекта для последующих сканирований.

Логин и пароль

Чтобы добавить учётные данные этого типа, задайте название записи и укажите имя пользователя и пароль от необходимого ресурса. Также вы можете настроить доступ др

5.2.5.3. Настройки системы

5.2.5.3.1. Сканирование

В подразделе **Сканирование** можно выполнять действия с шаблонами настроек сканирования. Шаблоны позволяют не настраивать конфигурацию сканирования вручную перед каждым запуском, а в один клик выставлять часто используемые настройки для анализа. На странице можно:

- создать шаблон;
- внести изменения в существующие шаблоны;
- выбрать шаблон по умолчанию.

Вы можете самостоятельно выбирать, изменять и удалять значение шаблона по умолчанию для запуска анализа. Если вы ничего не укажете или шаблон будет удалён, вашим шаблоном по умолчанию будет значение, установленное администратором системы. Если администратор не назначит иной шаблон, для запуска сканирования будет использоваться системный шаблон.

Для удобной навигации по шаблонам предусмотрена возможность поиска по названию или автору шаблона.

Создание шаблона настроек сканирования

Чтобы создать шаблон настроек:

1. Нажмите на кнопку **Создать шаблон**. После этого откроется форма создания шаблона настроек.
2. В форме создания шаблона настроек задайте название шаблона.
3. Отметьте чекбокс **Шаблон настроек по умолчанию**, чтобы использовать выбранный шаблон по умолчанию при запуске нового анализа.
4. При необходимости добавьте описание шаблона настроек.
5. Укажите, будет шаблон публичным или приватным. **Публичный шаблон** будет доступен для использования всем пользователям системы. **Приватный шаблон** будет доступен только автору шаблона и администратору системы.
6. Шаблон хранит в себе информацию о конфигурации настроек пунктов следующих блоков:
   - общие настройки;
   - настройки репозитория Git;
   - настройки приватного репозитория;
   - настройки кодировки.
7. Нажмите **Сохранить**. После успешного сохранения система вернёт вас в подраздел **Сканирование**.

Важно обратить внимание:

При дальнейшем обновлении системы настройки старых шаблонов будут переноситься без изменений.

Изменение шаблона настроек сканирования

Чтобы изменить шаблон настроек:

1. Нажмите на название шаблона в списке. После этого откроется форма изменения шаблона настроек.
2. Внесите желаемые изменения.
3. Нажмите **Сохранить**. После успешного сохранения система вернёт вас в подраздел **Сканирование** раздела **Настройки**.

Для удаления шаблона настроек после выполнения шага 2 нажмите кнопку **Удалить**.

Важно обратить внимание:

При редактировании собственного шаблона вы можете изменить любые настройки. При работе с шаблонами других пользователей или системным шаблоном настройки недоступны для редактирования. Вы можете:

- просмотреть шаблон;
- установить выбранный шаблон в качестве шаблона по умолчанию для запуска анализа;
- скопировать настройки шаблона и использовать копию для создания собственного шаблона.

5.2.5.3.2. Экспорт отчёта

В подразделе **Экспорт отчёта** можно выполнять действия с шаблонами настроек экспорта отчёта. Шаблоны позволяют в один клик выставлять часто используемую конфигурацию отчёта. На странице можно:

- создать шаблон;
- внести изменения в существующие шаблоны;
- выбрать шаблон по умолчанию.

Для удобной навигации по шаблонам предусмотрена возможность поиска по названию или автору шаблона.

Создание шаблона экспорта отчёта

Чтобы создать шаблон:

1. Нажмите на кнопку **Создать шаблон**. После этого откроется форма создания шаблона экспорта отчёта.
2. Задайте название шаблона.
3. Отметьте чекбокс **Шаблон экспорта по умолчанию**, чтобы использовать выбранный шаблон по умолчанию при генерации отчёта.
4. При необходимости добавьте описание шаблона настроек.
5. Укажите, будет шаблон публичным или приватным. **Публичный шаблон** будет доступен для использования всем пользователям системы. **Приватный шаблон** будет доступен только автору шаблона и администратору системы.
6. Настройте видимость шаблона в списке на странице **Экспорт отчёта** проекта.
7. Шаблон хранит в себе информацию о конфигурации настроек пунктов отчёта. Подробнее о настройках экспорта см. Экспорт отчёта.
8. Нажмите **Сохранить**. После успешного сохранения система вернёт вас в подраздел **Экспорт отчёта**.

Изменение шаблона экспорта отчёта

Чтобы изменить шаблон экспорта:

1. Нажмите на название шаблона в списке. После этого откроется форма изменения шаблона.
2. Внесите желаемые изменения.
3. Нажмите **Сохранить**. После успешного сохранения система вернёт вас в подраздел **Экспорт отчёта** раздела **Настройки**.

Для удаления шаблона экспорта после выполнения шага 2 нажмите кнопку **Удалить**.

6. ОПИСАНИЕ РАБОТЫ С МОДУЛЕМ АНАЛИЗА СОСТАВА ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ (SCA)

Solar appScreener модуль анализа состава программного обеспечения (SCA) предоставляет возможность сканировать приложения с целью выявления уязвимых компонент и зависимостей в open-source библиотеках в режиме **Анализ состава ПО**.

6.1. Создание проекта

В интерфейсе модуля SCA реализованы следующие способы создания проекта анализа состава ПО:

- запуск сканирования приложения, загруженного с локального компьютера;
- запуск сканирования приложения по ссылке на репозиторий;
- создание пустого проекта, у которого нет сканирований.

6.1.1. Создание пустого проекта

Чтобы создать пустой проект, введите название и нажмите **Создать проект**. При необходимости нажмите **Показать настройки** и установите настройки анализа. Подробнее про настройки анализа в разделе Общие.

В созданном проекте можно настроить интеграции. Подробнее про интеграции в разделе Интеграциz с Jira.

6.1.2. Запуск сканирования

Чтобы запустить новое сканирование в UI:

1. Перейдите на **Домашнюю страницу**.
2. Загрузите проект в виде архива с исходным кодом, ссылки на репозиторий с исходным кодом проекта или SBOM файла в формате Cyclone DX (архив со SBOM файлом или ссылка на SBOM файл в репозитории приведет к ошибке сканирования).
3. Настройте анализ (подробнее о **Настройках** в разделе Настройки).
4. Нажмите **Начать сканирование**.

6.2. Инструкция по сборке SBOM файла

Проекты Swift/Objective-C (cocoapods)

Для проектов, написанных на Swift, Objective-C, можно воспользоваться инструментом **cyclonedx-cocoapods**. Пример команды, с помощью которой можно создать SBOM файл в формате CycloneDX:

```
cyclonedx-cocoapods --path /path/to/project --output /path/to/bom.xml
```

где `--path` путь до проекта, `--output` путь до файла SBOM.

В результате получится файл с расширением `.xml`. Чтобы конвертировать его в `.json`, можно использовать **cyclonedx-cli**. Пример команды для конвертации CycloneDX-XML в CycloneDX-JSON:

```
cyclonedx convert --input-file /path/to/bom.xml --input-format xml --output-file
/path/to/bom.json --output-format json
```

где:

`--input-file` - путь до конвертируемого файла;

`--input-format` - формат исходного файла;

`--output-file` - путь до итогового файла;

`--output-format` - итоговый формат файла.

Обратите внимание: данный генератор не строит дерево транзитивных зависимостей.

Для генерации SBOM файла для многих языков программирования можно воспользоваться инструментом **cdxgen**. Пример команд, с помощью которых можно создать SBOM файл:

Проекты JavaScript

```
cd /path/to/project
```

```
cdxgen -t node.js -o /path/to/sbom.json
```

где `-t` тип проекта, `-o` путь до файла SBOM.

Проекты Java/Scala/Kotlin (Maven/Gradle)

```
cd /path/to/project
```

```
cdxgen -t java -o /path/to/sbom.json
```

Проекты C/C++ (conan)

```
cd /path/to/project
```

```
cdxgen -t c/c++ -o /path/to/sbom.json
```

Обратите внимание: дерево транзитивных зависимостей будет простроено только если зависимости описаны в `conan.lock`.

Проекты PHP (Composer)

```
cd /path/to/project
```

```
cdxgen -t php -o /path/to/sbom.json
```

Проекты Swift (SwiftPM)

```
cd /path/to/project
```

```
cdxgen -t swift -o /path/to/sbom.json
```

Проекты C# (.Net)

```
cd /path/to/project
```

```
cdxgen -t .Net -o /path/to/sbom.json
```

Обратите внимание: дерево транзитивных зависимостей будет сгенерировано только в присутствии файлов `project.assets.json`, `packages.lock.json`.

Проекты на других языках

Список генераторов для разных языков программирования представлен по ссылке. Все генераторы поддерживают формат SBOM CycloneDX.

6.3. Управление проектом

Управление проектом состоит из разделов **Обзор**, **Подробные результаты**, **Сканирования**, **Экспорт отчёта**, **Сравнение сканирований** и **Настройки**. Переключение между этими разделами осуществляется через меню в левой части страницы.

Справа от логотипа проекта отображается ID (первые символы UUID проекта). Чтобы скопировать в буфер полный UUID, нажмите на  .

На страницу **Обзор** можно перейти, нажав на название проекта на странице **Проекты** в разделе **SCA** или на **Домашней странице** (если проект входит в шесть последних запущенных проектов).

На страницы **Подробные результаты** или **Экспорт отчёта** можно перейти, нажав на соответствующие кнопки быстрой навигации на странице **Проекты** или на **Домашней странице** (если проект входит в шесть последних запущенных проектов).

6.3.1. Обзор

В разделе **Обзор** в правом верхнем углу можно выбрать сканирование, для которого будет отображаться статистика по сканированию. Нажмите на иконку  , чтобы отобразились параметры запуска анализа для выбранного сканирования.

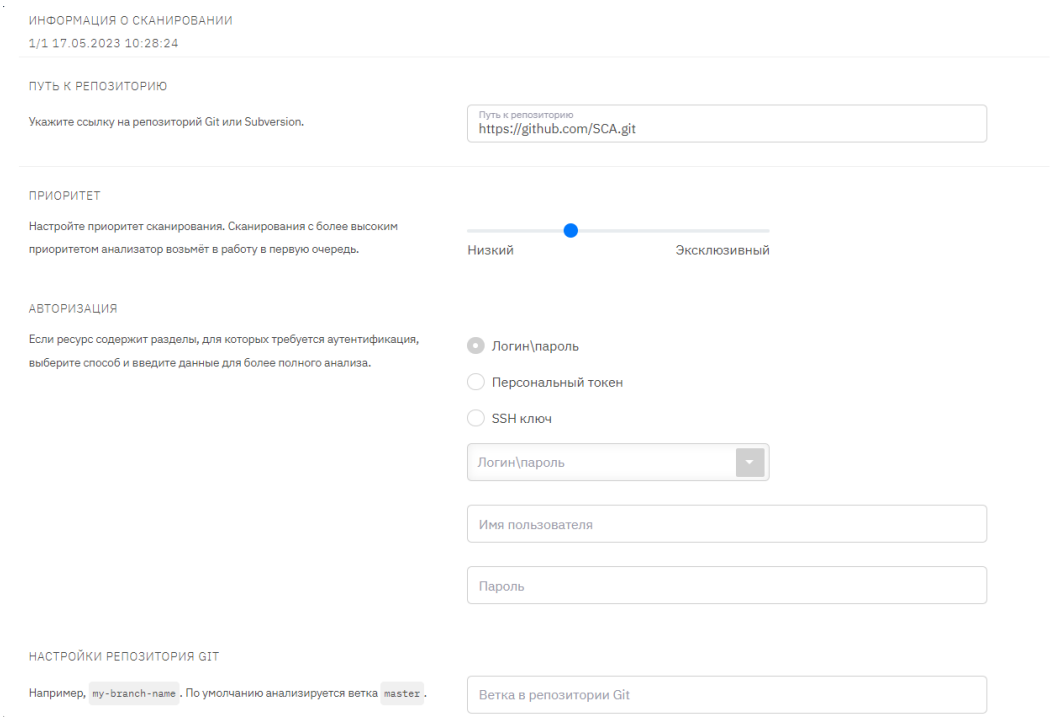

Рис. 6.1: Параметры запуска анализа

На странице **Обзор** представлена следующая информация:

- рейтинг;
- статус сканирования;
- продолжительность сканирования;
- общее количество компонент;
- количество уязвимых компонент;
- графическая информация по сканированию и проекту:
  - диаграмма с количеством уязвимостей каждого уровня критичности в сканировании;
  - график уровня безопасности проекта;
  - график количества уязвимостей в проекте;
  - диаграмма с наиболее уязвимыми компонентами.

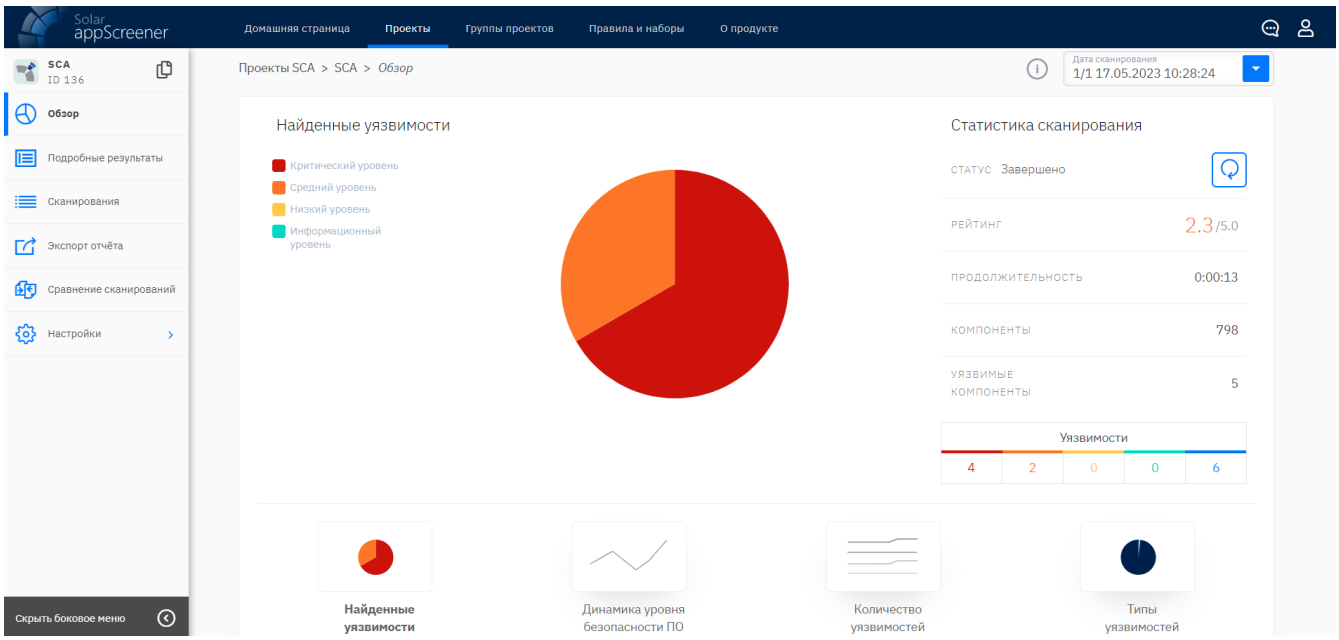

Рис. 6.2: Обзор

Если в данный момент приложение не сканируется, можно запустить новое сканирование, нажав на иконку . Если сканирование находится в процессе анализа, его можно остановить, нажав на иконку .

6.3.2. Подробные результаты

На вкладке **Подробные результаты** отображается информация по каждой из обнаруженных уязвимостей для выбранного сканирования. Переключаться между результатами разных сканирований можно с помощью списка сканирований в правом верхнем углу.

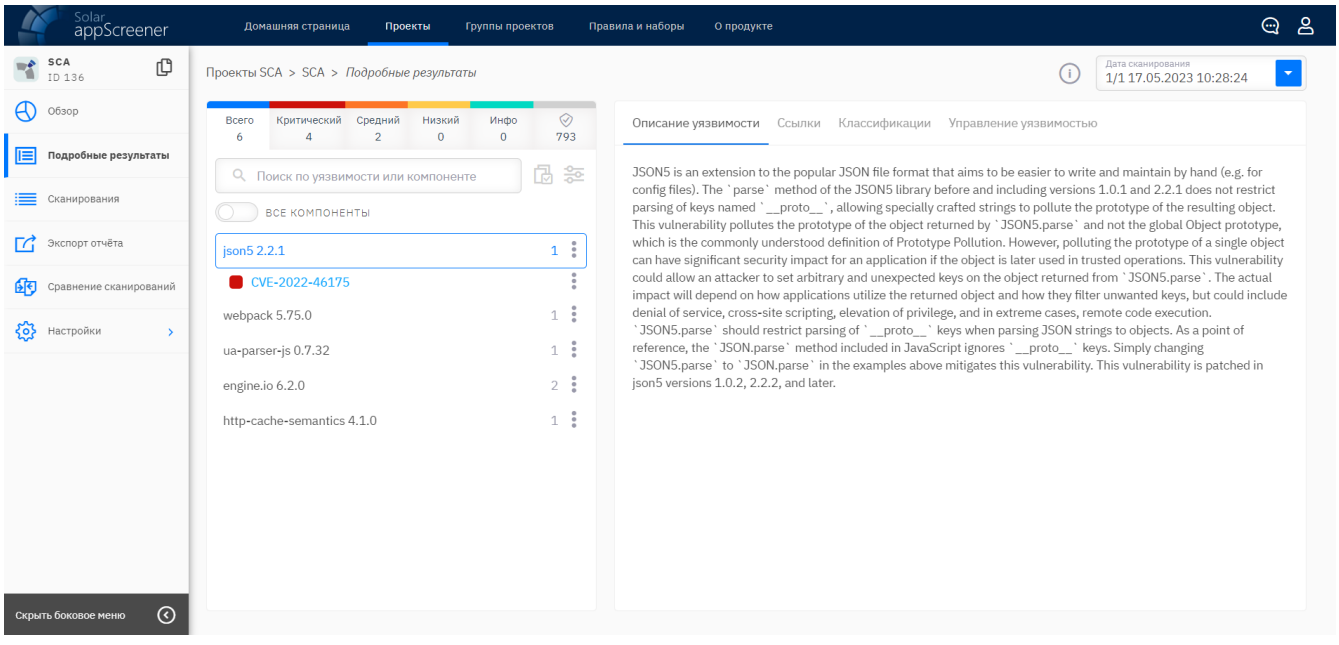

Рис. 6.3: Подробные результаты

В левой части страницы представлен список вхождений уязвимостей, сгруппированный по названию библиотек и версий. Если компонента содержит зависимости, они будут отмечены соответствующими тэгами: **D** для прямых, **T** для транзитивных зависимостей. Связанные зависимости отображаются по наведению курсора на тэг.

В верхнем меню можно выбрать, уязвимости какого уровня требуется отобразить. Для удобной навигации по уязвимостям предусмотрен поиск по названию уязвимости или компоненте, а также фильтры (рис. 6.4).

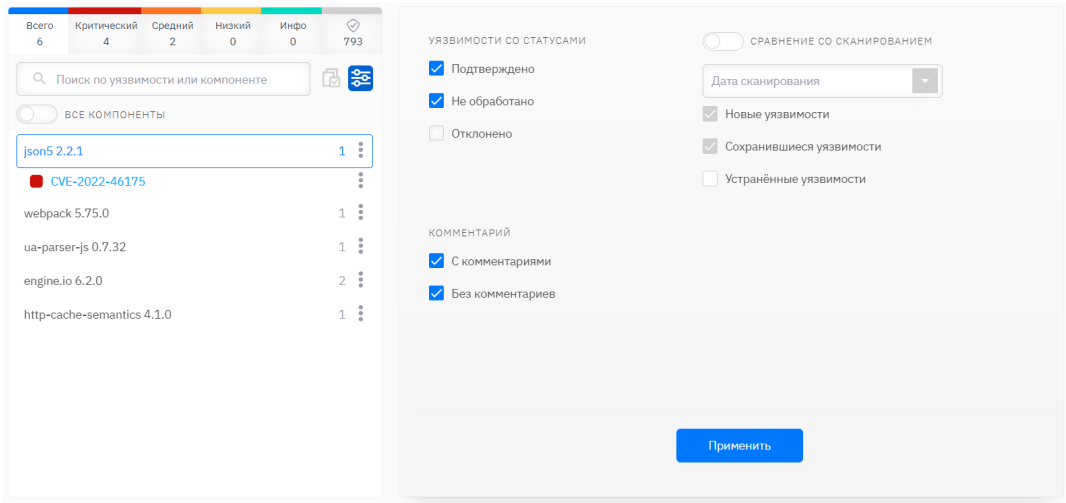

Рис. 6.4: Фильтры результатов

Фильтровать результаты можно по следующим параметрам:

- статусы уязвимостей для отображения:
  - подтверждено;
  - не обработано;
  - отклонено.
- наличие комментария:
  - с комментариями;
  - без комментариев.
- при наличии двух и более успешных сканирований в проекте, можно сравнить текущее сканирование с одним из предшествующих и отобразить уязвимости в соответствии с их статусом. Для этого выберите соответствующие настройки:
  - новые уязвимости — новые уязвимости, по отношению к выбранному из списка сканированию;
  - сохранившиеся уязвимости — уязвимости, обнаруженные в выбранном из списка сканировании и в текущем сканировании;
  - устранённые уязвимости — уязвимости, обнаруженные в выбранном из списка сканировании, но не обнаруженные в текущем сканировании.

Фильтры применяются после нажатия на кнопку **Применить**.

Нажмите на три точки рядом с названием уязвимости, чтобы изменить критичность и статус. При изменении статуса и уровня критичности уязвимости пересчитывается уровень безопасности приложения. Уязвимости со статусом **Отклонено** не учитываются при подсчёте количества уязвимостей и рейтинга безопасности. При пересканировании изменения сохраняются.

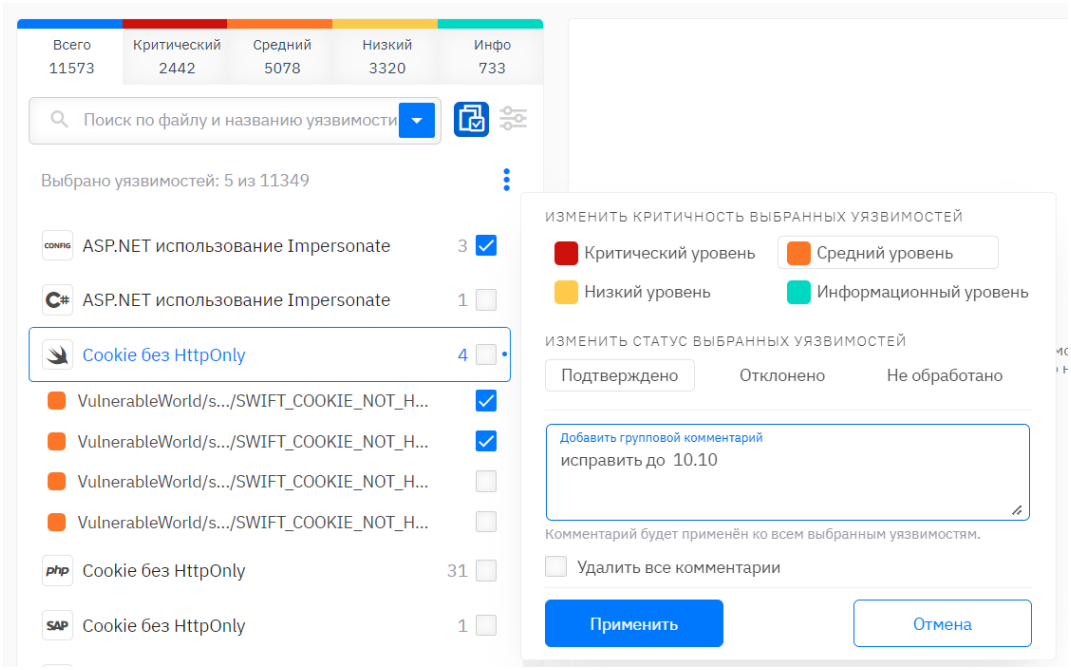

Рис. 6.5: Управление пакетом уязвимостей

После выбора конкретной уязвимости в центральной части страницы отображается следующая информация (рис. 6.6): **Описание уязвимости**, **Ссылки**, **Классификации**, **Управление уязвимостью**.

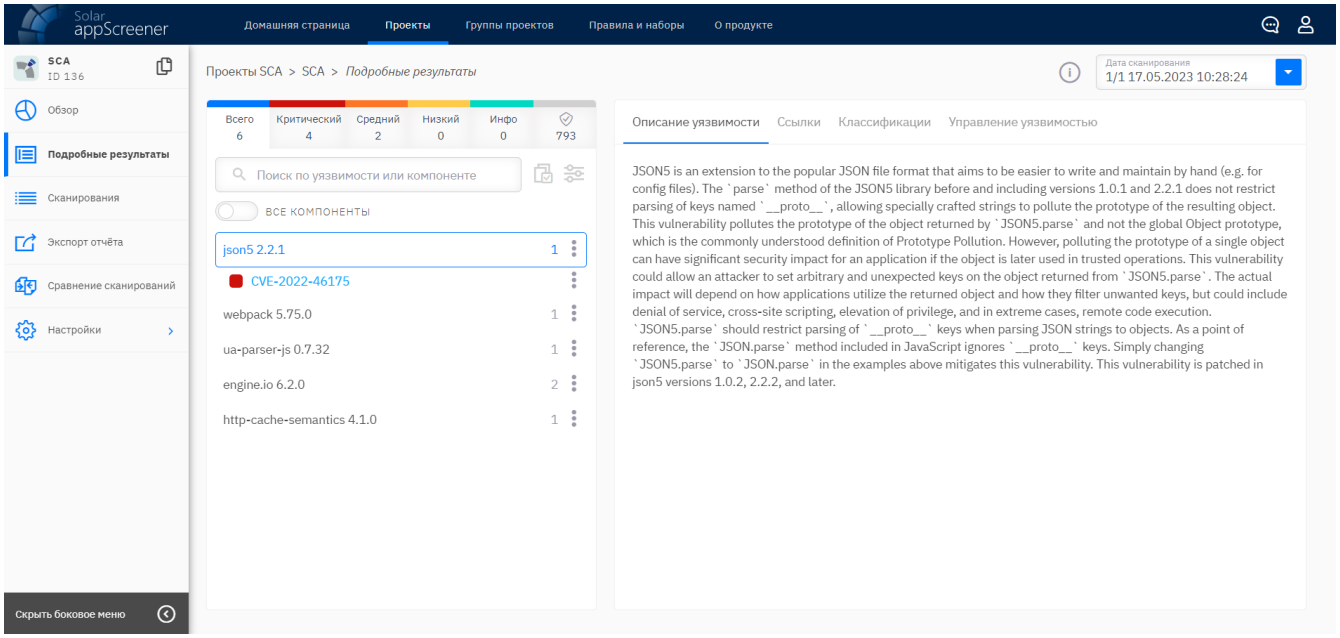

Рис. 6.6: Свойства уязвимости

На вкладке **Управление уязвимостью** (рис. 6.7) можно изменить уровень критичности и статус, добавить комментарий к уязвимости и посмотреть оставленные ранее комментарии.

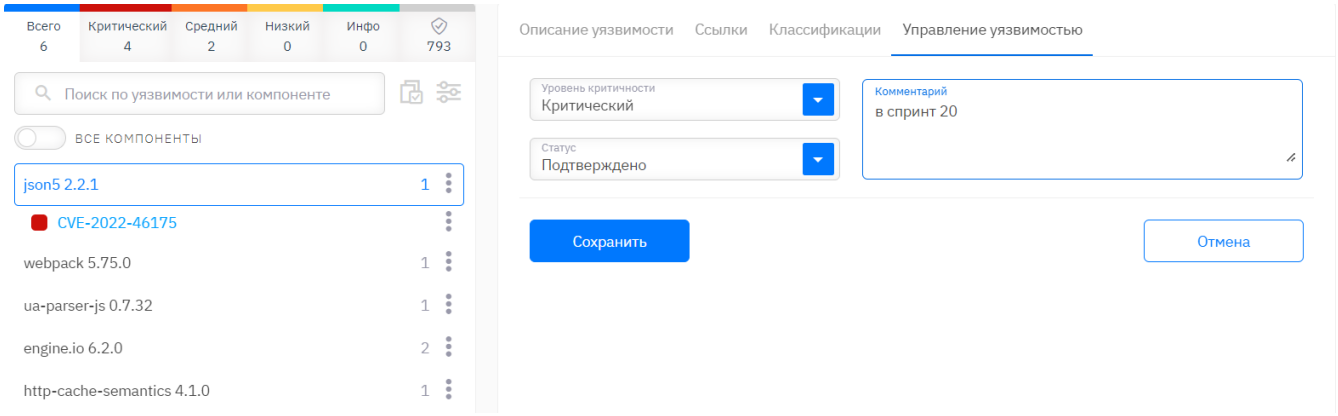

Рис. 6.7: Управление уязвимостью

6.3.3. Сканирования

Раздел **Сканирования** предназначен для управления сканированиями в рамках одного проекта. Для каждого сканирования отображаются следующие данные:

- дата и время сканирования, при нажатии на иконку ⓘ отображается информация о параметрах запуска анализа;
- меню действий:
  - выгрузить отчёт;
  - архивировать сканирование;
  - удалить сканирование.
- статус сканирования;
- продолжительность сканирования;
- общее количество компонент;
- количество уязвимых компонент;
- количество уязвимостей критического, среднего, низкого и информационного уровня;
- рейтинг приложения.

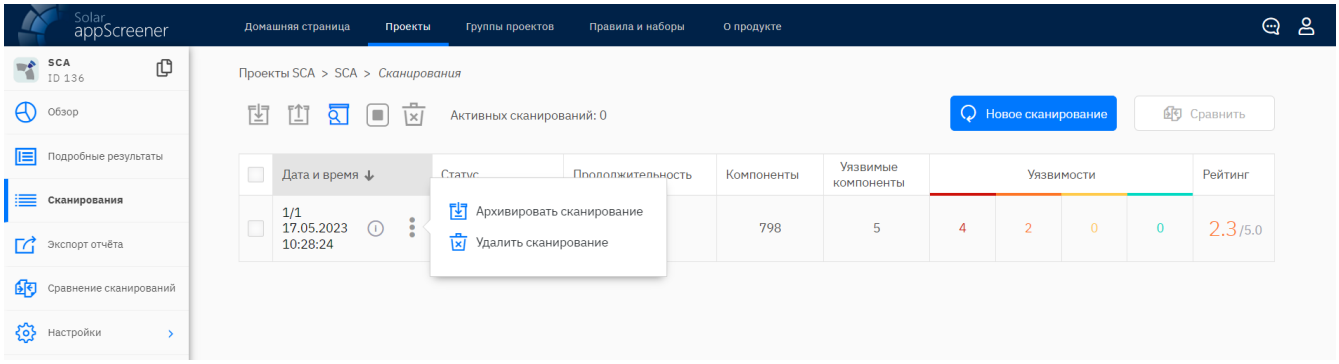

Рис. 6.8: Сканирования

Список можно сортировать по дате сканирования, продолжительности сканирования или

рейтингу, общему количеству компонент или уязвимым компонентам. Для этого нажмите на соответствующий заголовок, повторное нажатие меняет порядок сортировки.

Сравнить результаты двух выбранных сканирований можно, нажав на кнопку **Сравнить**. Сканирования, которые находятся в архиве, можно скрыть из списка, нажав на **Скрыть архив**, или отображать в списке, нажав на **Показать архив**.

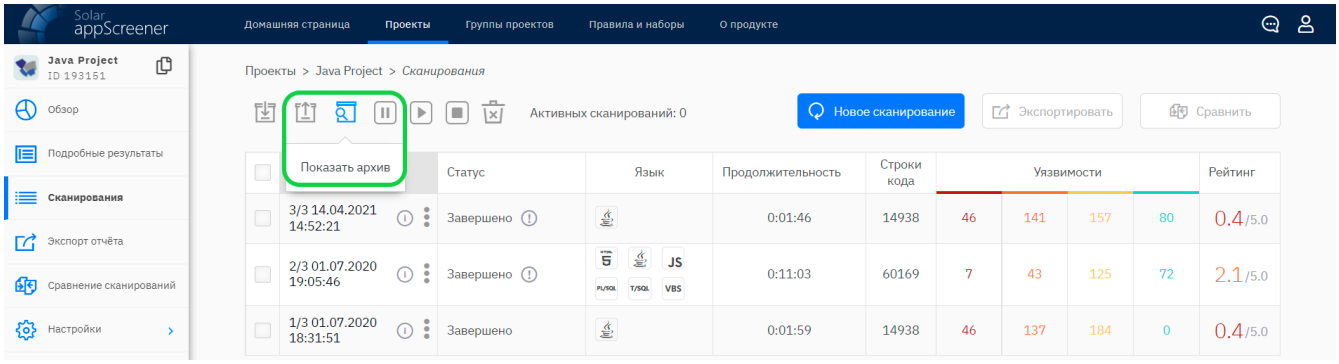

Рис. 6.9: Показать/Скрыть архив

Для проведения повторного сканирования в рамках одного проекта нажмите **Новое сканирование**.

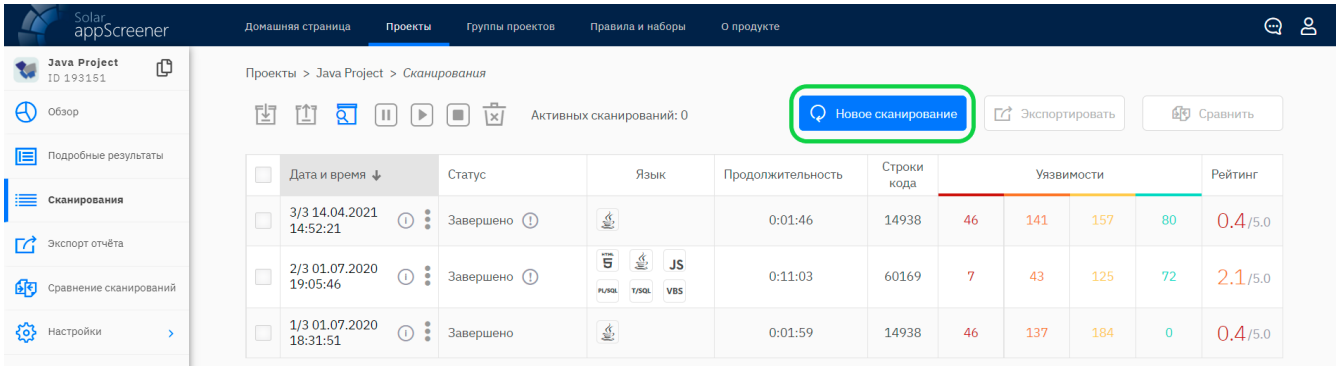

Рис. 6.10: Новое сканирование

В модуле SCA можно запустить сразу несколько сканирований в одном проекте с разными настройками. Отслеживать статусы сканирований можно в графе **Статус**.

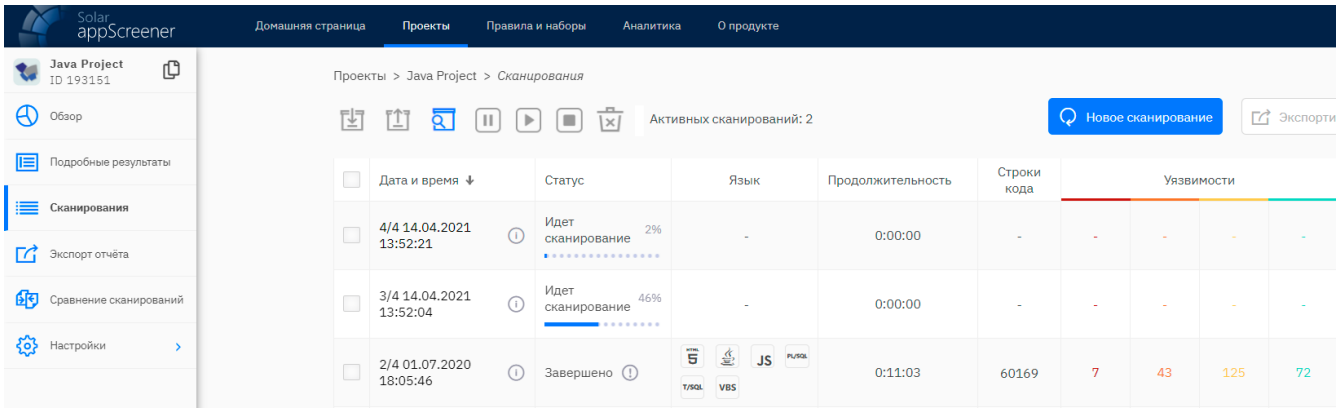

Рис. 6.11: Очередь сканирований

6.3.4. Экспорт отчёта

В разделе **Экспорт отчёта** можно выгрузить результаты сканирования в отчёт в формате PDF, CSV или DOCX. Выберите один из готовых шаблонов настроек или задайте информацию для экспорта вручную.

Настройки отчёта включают следующие блоки:

- сканирования;
- сравнить со сканированием;
- информация о проекте;
- информация о сканировании;
- фильтр уязвимостей;
- список уязвимостей;
- подробные результаты;
- общие настройки отчёта.

Сканирования

Для экспорта отчёта выберите одно или несколько сканирований. Чтобы получить только сводную информацию по проекту, удалите все сканирования из списка.

Сравнить со сканированием

Выберите одно сканирование, чтобы опция **Сравнить со сканированием** стала доступна. В отчёт будут включены таблица сравнения, график и статистика по новым, сохранившимся и устранённым уязвимостям.

Выберите статусы уязвимостей (новые, сохранившиеся и/или устранённые) и укажите количество вхождений каждой уязвимости.

Информация о проекте

В отчёт можно включить динамику уровня безопасности и историю сканирований.

Информация о сканировании

По умолчанию будет добавлена статистика сканирования: статус, рейтинг, продолжительность, количество компонент и уязвимостей.

Выберите дополнительную информацию о сканировании:

- диаграмма найденных уязвимостей;
- диаграмма уязвимых компонент;
- настройки запуска сканирования.

Фильтр уязвимостей

Выберите уязвимости по уровню критичности и типу, а также компоненты для отображения.

Список уязвимостей

Выберите статусы уязвимостей и задайте количество их вхождений.

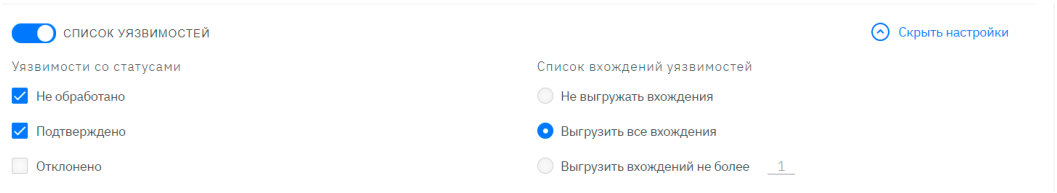

Рис. 6.12: Список уязвимостей

Подробные результаты

По умолчанию для уязвимостей будут добавлены описание, рекомендации по устранению, ссылки. Также можно настроить:

- статусы уязвимостей: **Не обработано**, **Подтверждено**, **Отклонено** (подробнее в разделе Подробные результаты);
- количество уязвимостей компоненты;
- отображение комментариев.

Общие настройки отчёта

Выберите язык, формат отчёта и при необходимости включите в него настройки экспорта и оглавление. Также можно настроить отображение статусов уязвимостей в отчёте и установить пользовательский логотип.

Обратите внимание:

Для корректного отображения данных CSV-отчёта в **Microsoft Excel** необходимо вручную выбрать в выпадающем списке **Обнаружение типов данных** опцию **Не обнаруживать типы данных** во время импорта файла. Настройка отображения статусов уязвимостей недоступна для этого формата.

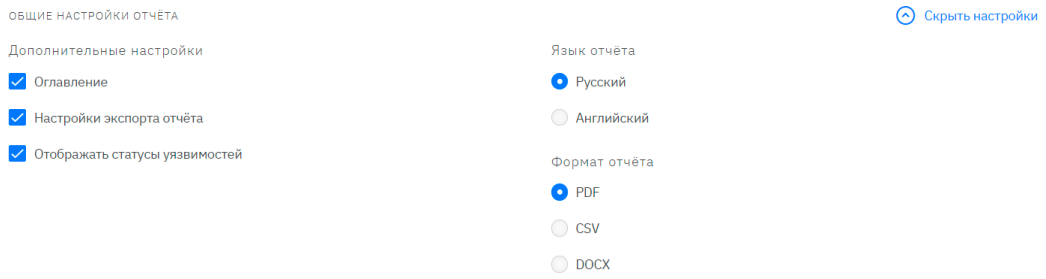

Рис. 6.13: Общие настройки отчёта

Чтобы скачать отчёт, нажмите **Скачать**.

Чтобы отправить отчёт по почте, нажмите **Отправить по e-mail**. В открывшейся форме укажите список адресов получателей и при необходимости отредактируйте текст письма.

6.3.5. Сравнение сканирований

В разделе **Сравнение сканирований** можно производить сравнение результатов сканирований. Чтобы сравнить результаты, выберите два сканирования в верхней части страницы. На странице отобразится количество устраненных, новых и сохранившихся уязвимостей на графике и в таблице. Также будет представлена таблица со сравнением

по дате сканирования, продолжительности, общему количеству и количеству уязвимых компонент, количеству уязвимостей с учётом уровня критичности и рейтингу.

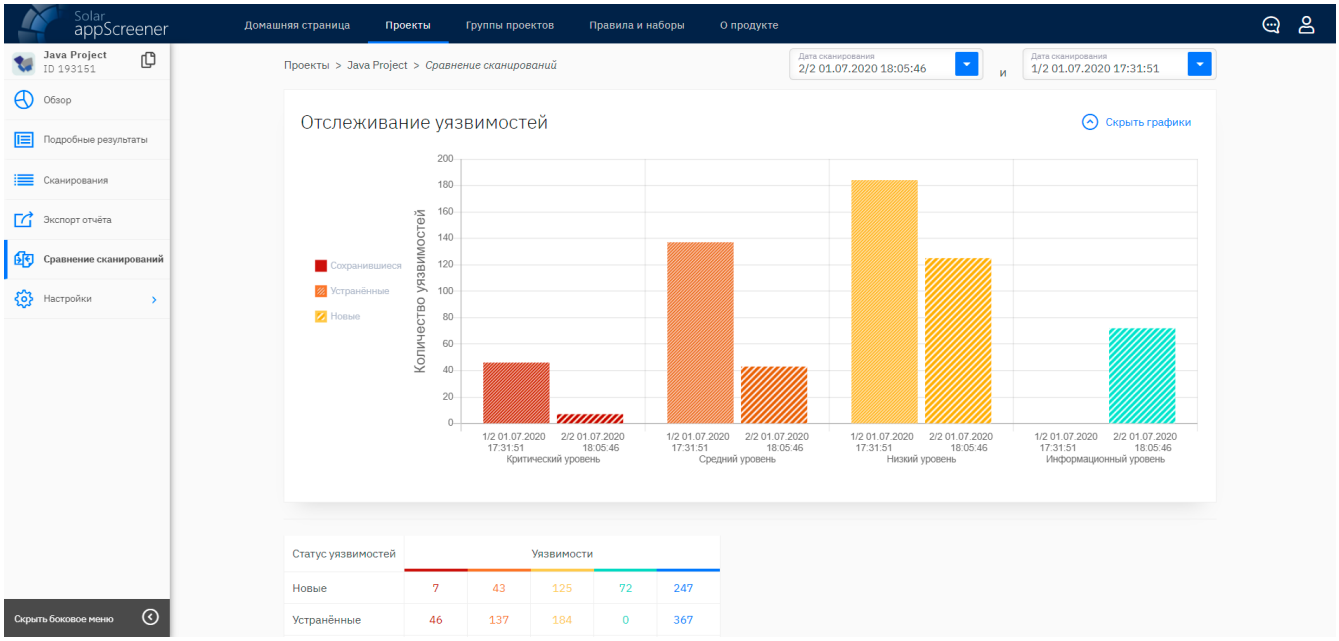

Рис. 6.14: Сравнение сканирований

6.3.6. Настройки

В разделе **Настройки** отображаются настройки проекта. В этом разделе можно работать с сущностями: **Общие**, **Права пользователей**, **Автоматическое сканирование** и **Управление проектом**.

6.3.6.1. Общие

В подразделе **Общие** (рис. 6.15) можно задать настройки для последующих сканирований:

- указать ссылку на репозиторий Git или Subversion;
- задать приоритет сканирования;
- выбрать способ авторизации и заполнить необходимые данные для ресурсов, требующих аутентификации;
- указать ветку для сканирования в Git-репозитории.

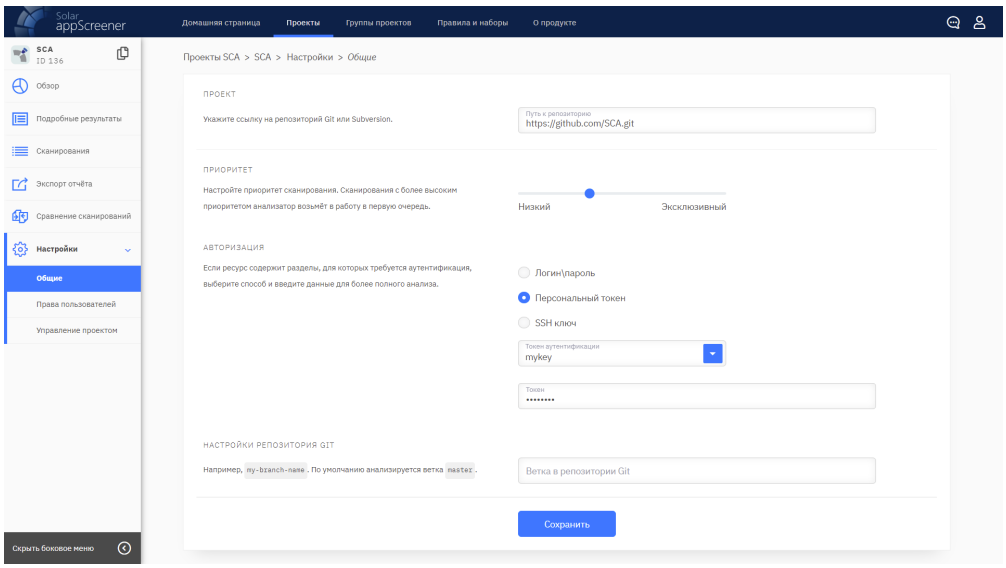

Рис. 6.15: Общие

В подразделе **Права пользователей** можно быстро выдать доступ к проекту другим пользователям системы и настроить их права в проекте.

6.3.6.2. Права пользователей

В подразделе **Права пользователей** можно быстро выдать доступ к проекту другим пользователям системы и настроить их права в проекте. Чтобы настроить права конкретного пользователя, кликните по его логину в списке.

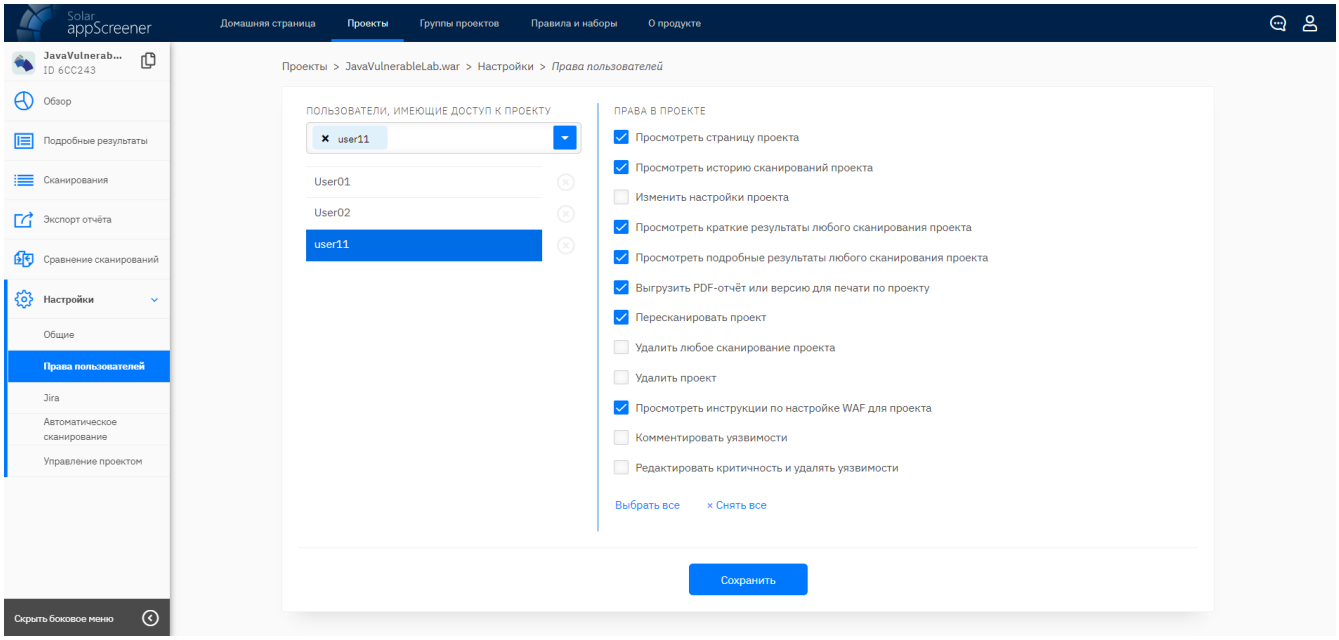

Рис. 6.16: Права пользователей

6.3.6.3. Таск-менеджер

Во вкладке **Jira** можно привязывать проекты в **Jira** к проекту модуля SCA. (подробнее см. раздел Как привязать проект модуля SCA к проекту в Jira).

6.3.6.4. Управление проектом

В подразделе **Управление проектом** можно редактировать данные проекта, а также архивировать или удалить проект. Архивированные проекты продолжают храниться в системе. Чтобы удалить проект без возможности восстановления, нажмите **Удалить проект** и подтвердите действие.

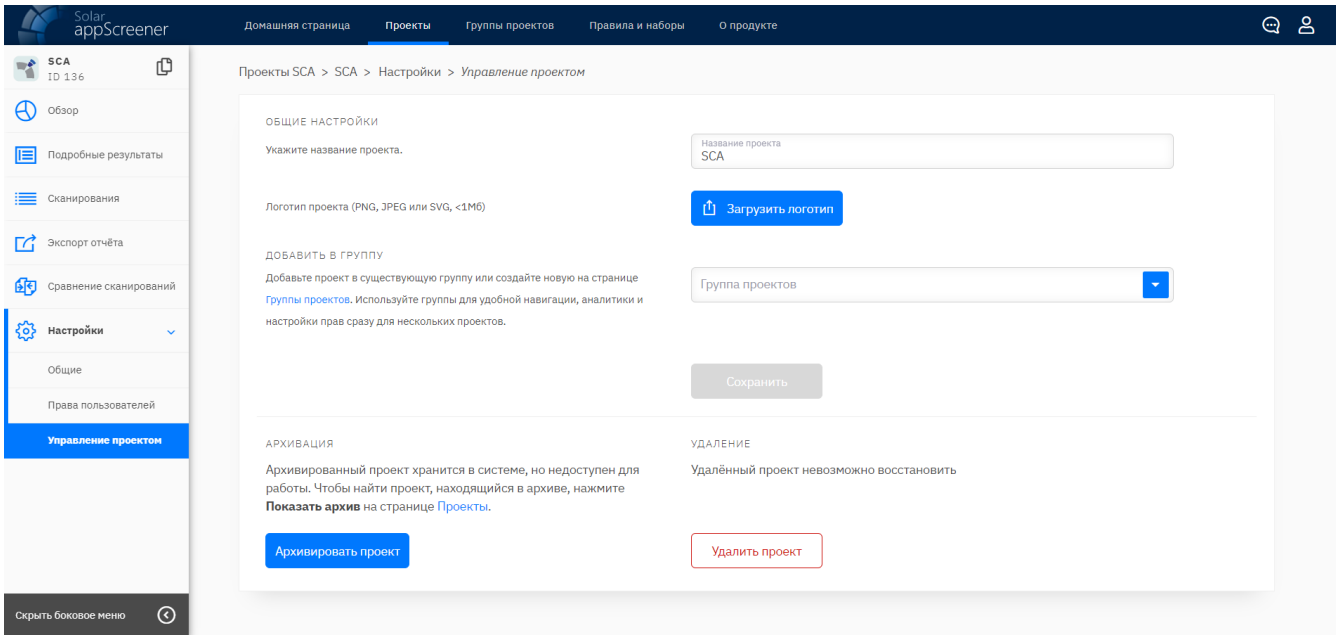

Рис. 6.17: Управление проектом

6.4. Работа с API

Доступ к функциональности модуля SCA также доступен через API. Web-интерфейс спецификации API реализован с помощью Swagger Codegen. Для доступа к API:

1. Перейдите в раздел **Личный кабинет** > **Настройки доступа** > **Токен и пароль**.
2. Нажмите **Создать токен**.
3. Введите пароль учётной записи.
4. Укажите время действия токена.
5. Нажмите **Получить активный токен** и скопируйте значение в буфер.
6. Нажмите **Спецификация API**.
7. На открывшейся странице вставьте значение токена в поле **Enter token here**.
8. Нажмите **Explore**.

6.4.1. Запуск сканирования

Чтобы запустить сканирование из API:

1. Кликните по кнопке **/scan/start** в разделе **Scan**.
2. Нажмите **Try it out**.
3. В теле запроса выберите файл для анализа или укажите ссылку на проект и добавьте настройки сканирования.
4. Нажмите **Execute**.

Пример метода для запуска сканирования из **приватного репозитория**:

```
curl -k -X POST "https://YOUR_SERVER/app/api/v1/scan/start" -H "accept:
application/json" -H "Authorization: Bearer TOKEN" -H "Content-Type:
multipart/form-data" -F "branch=BRANCH" -F "analyzeJsLibs=" -F "ruleSet=" -F
"checkboxNoBuild=" -F "name=" -F "repoPassword=PASSWORD" -F
"saveRepoCredentials=" -F "sourceEncoding=" -F "checkboxUseUserPatterns=" -F
"visualStudio=" -F "checkboxAnalyzeLibs=" -F "repoLogin=LOGIN" -F "saveFile=" -F
"incremental=" -F "languages=" -F "fileSelector=**/*" -F "uuid=" -F
"link=WEB_URL" -F "nameEncoding=" -F "preset="
```

Пример метода для запуска сканирования **архива с локального компьютера**:

```
curl -k -X POST "https://YOUR_SERVER/app/api/v1/scan/start" -H "accept:
application/json" -H "Authorization: Bearer TOKEN" -H "Content-Type:
multipart/form-data" -F "branch=" -F "analyzeJsLibs=" -F "ruleSet=" -F
"checkboxNoBuild=" -F "name=" -F "repoPassword=" -F "saveRepoCredentials=true"
-F "sourceEncoding=" -F "checkboxUseUserPatterns=" -F "visualStudio=" -F
"checkboxAnalyzeLibs=" -F "repoLogin=" -F "saveFile=" -F "incremental=" -F
"link=" -F "languages=" -F "fileSelector=**/*" -F "uuid=" -F
"file=PATH_TO_THE_FILE;type=application/x-msdownload" -F "nameEncoding=" -F
"preset="
```

Получить **статус сканирования**:

```
curl -k -X GET "https://YOUR_SERVER/app/api/v1/scans/SCAN_UUID/compact" -H
"accept: application/json" -H "Authorization: Bearer TOKEN"
```

6.4.2. Выгрузка отчёта

Чтобы выгрузить отчёт сканирования проекта через API:

1. Перейдите в раздел **Report**.
2. Выберите способ получения отчёта: скачать (**/report/file/**) или получить на почту (**/report/email/**).
3. Нажмите **Try it out**.
4. В теле запроса введите UUID нужного проекта и сканирования и укажите настройки отчёта.
5. Нажмите **Execute**.

Получить **отчёт в формате PDF**:

```
curl -k -X POST "https://YOUR_SERVER/app/api/v1/report/file" -H "accept:
application/octet-stream" -H "Authorization: Bearer TOKEN" -H "Content-Type:
```

```
application/json" -d "{\"projectUuid\":\"PROJECT_UUID\",\"scanUuids\":
[\"SCAN_UUID\"],\"exportSettings\":{\"uuid\":\"string\",\"projectInfoSettings\":
{\"securityLevelDynamics\":true,\"vulnNumberDynamics\":true,\"scanHistory\":0},\
"sort\":\"CR\",\"scanInfoSettings\":
{\"included\":true,\"foundVulnChart\":true,\"typeVulnChart\":true,\"langStats\":
true,\"fileStats\":true,\"scanErrorInfo\":true,\"scanSettings\":true},\
"filterSettings\":
{\"critical\":true,\"medium\":true,\"low\":true,\"info\":true,\"standardLibs\":
true,\"classFiles\":true,\"waf\":true,\"jira\":true,\"fuzzy\":
{\"included\":true,\"critical\":0,\"medium\":0,\"low\":0,\"info\":0,\
"percentile\":0,\"mode\":\"TRUE\"},\"lang\":\"ru\"},\"tableSettings\":
{\"included\":true,\"entriesSettings\":
{\"notProcessed\":true,\"confirmed\":true,\"rejected\":true},\"entryNum\":0},\
"detailedResultsSettings\":{\"included\":true,\"entriesSettings\":
{\"notProcessed\":true,\"confirmed\":true,\"rejected\":true},\"entryNum\":0,\
"comment\":true,\"jiraInfo\":true,\"traceNum\":0,\"sourceCodeNum\":0},\
"wafSettings\":{\"included\":true,\"entriesSettings\":
{\"notProcessed\":true,\"confirmed\":true,\"rejected\":true},\"imperva\":true,\"
mod\":true,\"f5\":true},\"generalSettings\":
{\"reportSettings\":true,\"contents\":true,\"locale\":\"ru\",\"format\":\"PDF\"}
},\"comparisonSettings\":
{\"included\":false,\"scanUuid\":\"string\",\"newIssue\":true,\"saved\":true,\
"fixed\":true,\"entryNum\":0,\"scanSettings\":true}}" > PATH_TO_THE_FILE
```

6.5. Интеграция Solar appScreener модуль анализа состава программного обеспечения (SCA) с Jira

Solar appScreener модуль анализа состава программного обеспечения (SCA) использует для интеграции **Jira REST API v2**.

6.5.1. Как привязать проект в Solar appScreener модуль анализа состава программного обеспечения (SCA) к проекту в Jira

Для того чтобы привязать проект в модуле SCA к проекту в Jira:

1. Перейдите на страницу **Проекты**.
2. Выберите проект и перейдите на вкладку **Jira** в разделе **Настройки**.
3. Нажмите на кнопку **Привязать проект**.

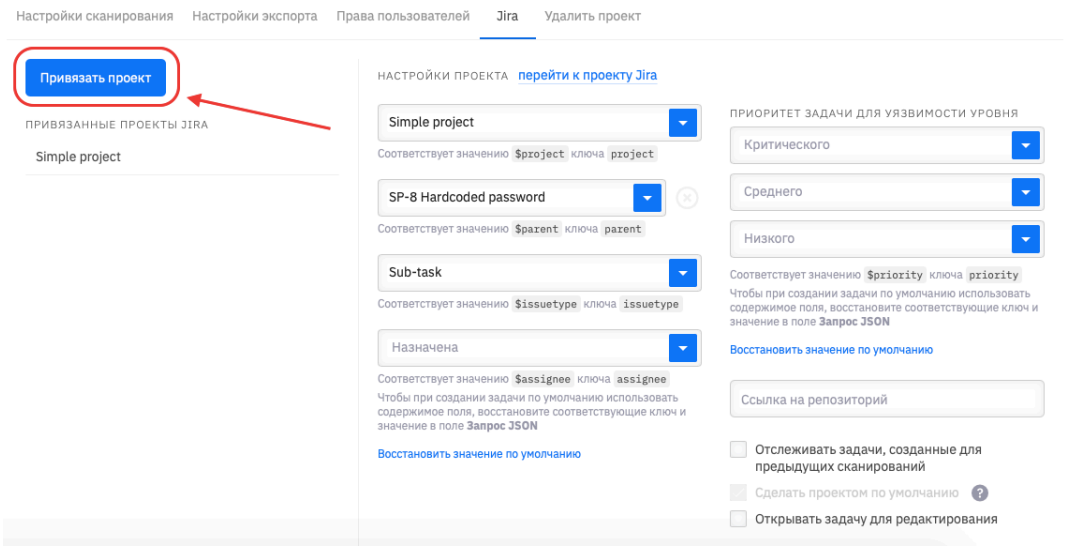

Рис. 6.18: Привязать проект Jira

4. Выберите из списка проект Jira и тип задачи по умолчанию при создании новых задач Jira.
5. Укажите опциональные значения формы, которые также будут использоваться по умолчанию при создании новых задач в Jira.
6. Настройте автоматическое создание задач в Jira по результатам сканирования, если необходимо.

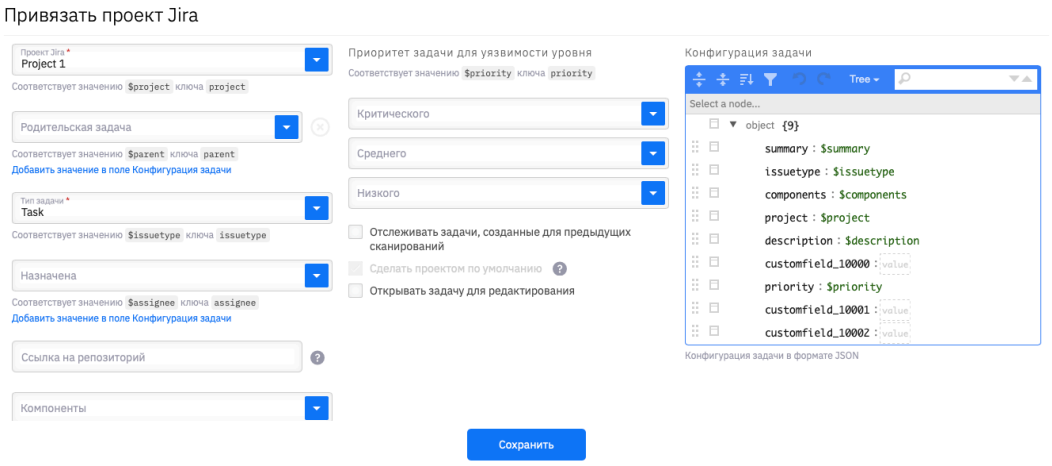

Рис. 6.19: Настроить параметры проекта Jira

Чтобы настроить уже привязанный проект, выберите его из списка и отредактируйте поля формы.

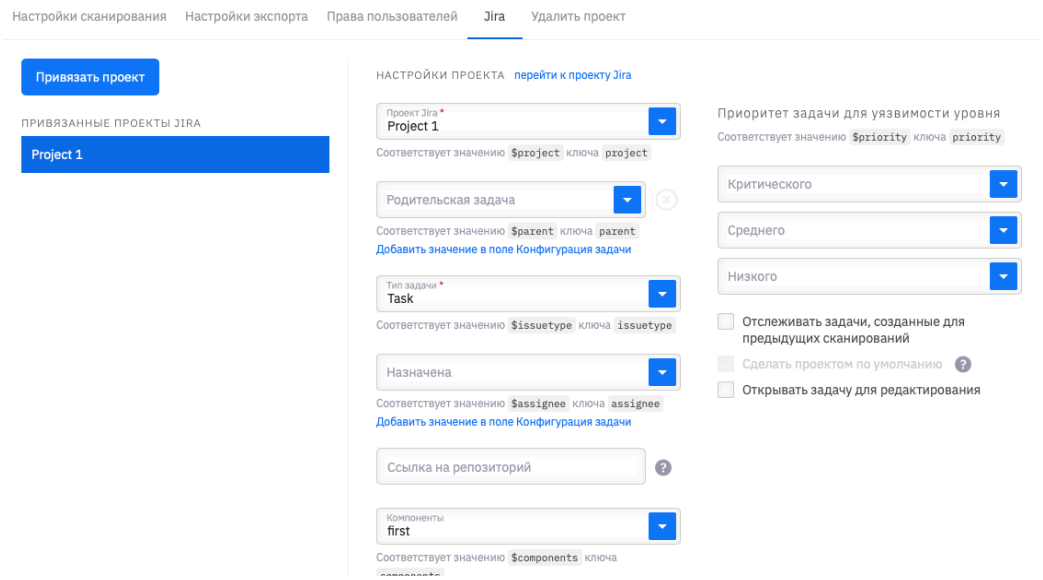

Рис. 6.20: Изменить параметры проекта Jira

6.5.2. Создание задачи в Jira

Если проект в модуле SCA привязан к проекту в Jira, через интерфейс модуля SCA можно создавать задачи в Jira. Для этого выполните действия:

1. Перейдите в раздел **Подробные результаты**.
2. Выберите конкретную уязвимость.
3. Перейдите на вкладку **Jira**, которая располагается в правой нижней части страницы (на данной вкладке отображается список уже созданных задач в Jira).
4. Нажмите на кнопку **Создать задачу**.

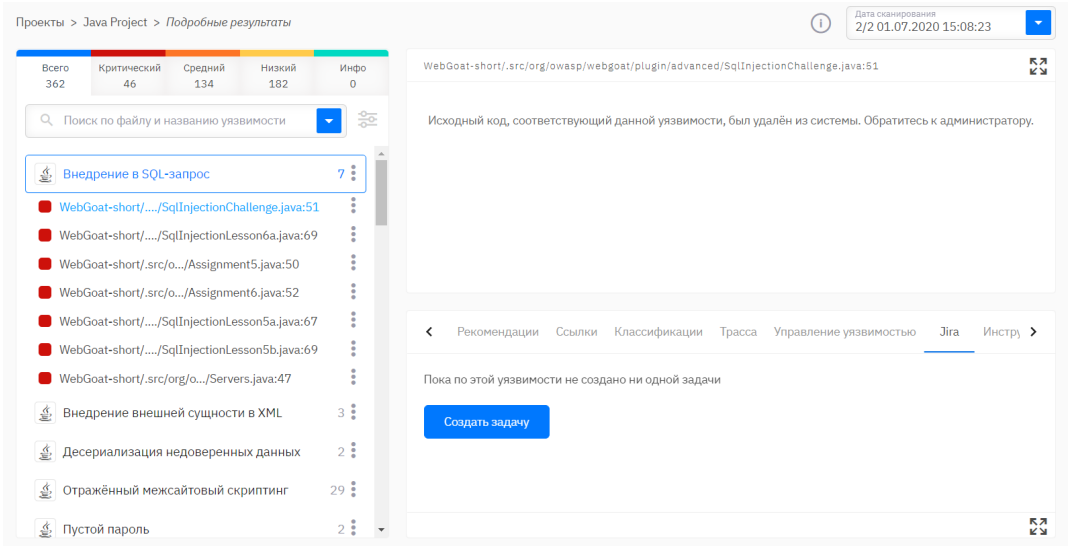

Рис. 6.21: Создать задачу в Jira

5. Укажите проект, родительскую задачу (опционально), тип задачи, компоненты (опционально), тему задачи, приоритет (опционально), кому назначена задача (опционально), описание задачи в формате Jira (опционально).

6. Если в задаче есть другие обязательные поля, для них в поле **Конфигурация задачи** будут сгенерированы пары ключ и значение. Явно укажите значение, которое необходимо задать в задаче.
7. Нажмите на кнопку **Создать**.

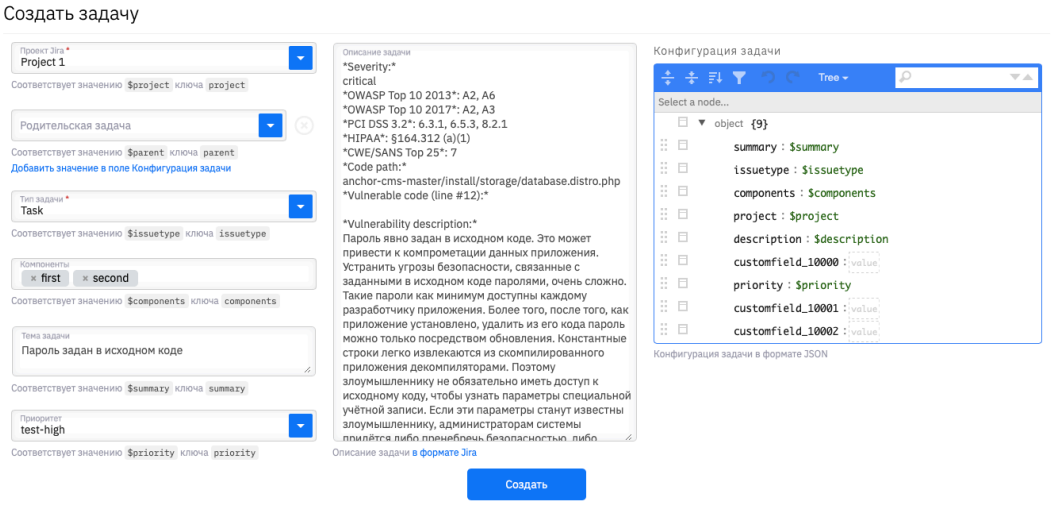

Рис. 6.22: Параметры задачи в Jira

В результате этих действий создается задача в Jira. Для просмотра задачи в Jira кликните на название задачи в списке. Для удаления задачи из интерфейса модуля SCA нажмите на кнопку удаления.

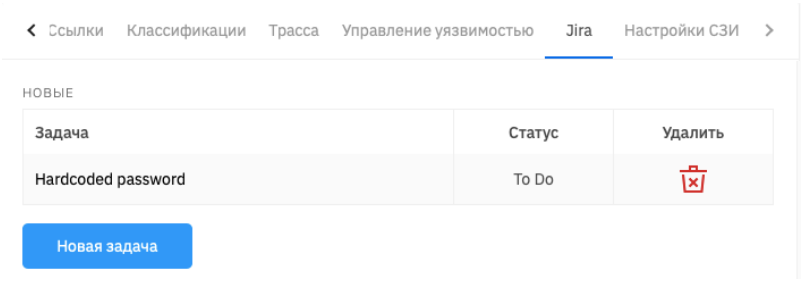

Рис. 6.23: Список задач в Jira