First level header

Some text.

1 Second level header

Some text.

1.1 Third level header

Some text.

1.2 Third level header

Some text.

1.3 Third level header

Some text.

1.3.1 Fourth level header

Fourth level header

Some text.

2 Second level header

2.1 Third level header

Some text.

2.1.1 Fourth level header

Some text.

2.1.2 Fourth level header

Some text.

3 Second level header

Some text.

Third level header

Проект (Project) — верхнеуровневая сущность, внутри которой определяются настройки и профили сканирования для конкретного приложения. На уровне проекта могут быть переопределены правила сканирования, которые будут применяться только для этого проекта. Имя проекта уникально в рамках системы.

First level header

Second level header

Second level header

Third level header

Some text.

Third level header

Fourth level header

Some text.

Fourth level header

Some text.

Fourth level header

Some text.

Third level header

Some text.

Third level header

Some text.

First level header

First level header

Some text.

Second level header

Second level header

Third level header

Проект (Project) — верхнеуровневая сущность, внутри которой определяются настройки и профили сканирования для конкретного приложения. На уровне проекта могут быть переопределены правила сканирования, которые будут применяться только для этого проекта. Имя проекта уникально в рамках системы.

Third level header

Second level header

Second level header

Third level header

Second level header

Third level header

Модуль (Module) — компоненты для сбора различной информации во время сканирования приложения на устройстве (мониторинг системного журнала, использование фай-лов, операции с базой данных и т. д.). Каждый модуль имеет свои уникальные настройки и может быть зависимым от результатов других модулей.

First level header

Second level header

Third level header

Third level header

Тест кейсы (Test cases) — записанный сценарий работы пользователя с приложением. Включает в себя все действия пользователя (нажатия, передаваемый текст, любые взаимодействия с интерфейсом приложения и т. д.). Тест кейс привязывается к конкретному проекту и может быть воспроизведен только в рамках него. Тест кейс запускается только если имя приложения (package_id) при запуске совпадает с именем приложения, для которого был записан тест кейс.

Second level header

Third level header

Сканирование — процесс анализа, во время которого пользователь вручную или система по записанным ранее тест кейсам взаимодействуют с приложением. Во время сканирования система Stingray собирает всю доступную информацию о работе приложения и затем проводит поиск уязвимостей и проверку на соответствие стандартам безопасности.

Third level header

Метод сканирования/запуска — Способ сканирования, определяющий, запускать
ли записанный ранее тест кейс или ожидать ручных операций с приложением. Возможные варианты:

Автоматический — запускает сканирование и запускает выбранный тест кейс.

Ручной — после запуска сканирования необходимо вручную совершать операции с запущенным приложением.

Правила анализа (Rules) — правила анализа, по которым происходит поиск части уязвимостей. Правила представляют собой набор строк или регулярных выражений, которые необходимо искать в собранных данных. Для удобства добавление правил оформлено в виде конструктора, в котором необходимо указать какую строку искать, в результатах каких модулей и в каком месте данных (XML-тэг, значение в JSON и т. д.).
Требование (Requirement) — требования информационной безопасности, на соответствие которому будет проверено приложение. С требованием соотносятся определенные типы дефектов, при нахождении которых в приложении требование будет считаться не выполненным. Требования могут быть сгруппированы в виде категорий или относиться напрямую к стандартам.
Категория (Category) — группировка требований информационной безопасности
по различным признакам.
Стандарт (Standard) — совокупность требований или категорий требований информационной безопасности, на соответствие которым может проверяться приложение. Стандарты могут быть как общемировые, так и внутренние стандарты компании.
Дефекты (Defects) — выявленные во время сканирования дефекты приложения или, по-другому, уязвимости. У

каждого дефекта есть тип, описание и рекомендации по устранению.
Собранные данные (Collected Data) — вся собранная информация о работе приложения за время сканирования. Данные разделены по модулям, каждый из которых отвечает за сбор определенной информации. Эти данные так же можно скачать и проанализировать локально, при желании.
CI/CD (Continuous Integration / Continuous Delivery) — системы для непрерывной интеграции и непрерывных поставок приложения. Примерами таких систем могут быть Jenkins, Teamcity, GitLab CI.
Эмулятор (Emulator) — виртуальный эмулятор имитирующее реальное устройство Android. Характеризуется различной архитектурой и версией операционной системы.

О продукте

4 Назначение

Stingray (Система) — это решение для поиска уязвимостей и автоматизации регрессионного тестирования информационной безопасности в мобильных приложениях с использованием технологий машинного обучения (Machine Learning).
Основной особенностью, отличающей систему Stingray, является уникальный механизм создания автоматических тест кейсов, которые воспроизводятся и адаптируются к изменению интерфейса приложения без участия пользователя, что существенно сокращает затраты человеческих ресурсов на тестирование, поиск уязвимостей и позволяет реализовать процесс тестирования безопасности в рамках непрерывного процесса разработки (DevOps). При всей сложности внутри, для пользователя запись тест кейса выглядит, как обычная работа с приложением, нет необходимости в написании скриптов или как-то по-особенному собирать приложение, просто пройдите необходимые шаги в приложении, как если бы оно было установлено на вашем мобильном устройстве.
Система поддерживает технологии байт код анализа (BCA), динамического (DAST) и ин-терактивного (IAST) тестирования, сбор и предоставление полной информации о работе приложения на устройстве.
Система способна обнаруживать более 40 типов уязвимостей и производить проверку на соответствие регуляторным и индустриальным требованиям информационной безопас-ности: GDPR, PCI DSS, СТО БР ИББС, OWASP Mobile Top-10, OWASP MASVS, а также позволяет создавать свои внутренние стандарты безопасности.

5 Возможности

Различные режимы сканирования

В системе Stingray существует несколько режимов анализа безопасности приложений, которые подходят для различных сценариев тестирования. Ручной анализ для разового тестирования приложения и автоматический режим для встраивания в процесс разработки.

Гибкое изменение правил анализа

Изменяйте правила анализа под ваше приложение, чтобы получить максимальную эффективность при нахождении дефектов. Компоненты системы, отвечающие за сбор данных представлены в виде модулей с простой и понятной конфигурацией. Модификация правил сделана в виде конструктора, благодаря которому изменение не займет много времени.

Встраивание в процесс CI/CD

Помимо полноценного REST API, предусмотрены интеграции в системы дистрибуции мобильных приложений. Максимальная гибкость и разнообразие настроек позволяет использовать систему Stingray в том процессе, который уже построен для разработки приложения, и информировать разработчиков о наличии уязвимостей еще на этапе первых сборок.

Проверка на соответствие стандартам безопасности

При анализе приложения Вы получите не только описание и рекомендации о выявленных уязвимостях, всю собранную информацию о работе приложения, но и детальный отчет о соответствии вашего приложения всем актуальным мировым стандартам Информационной Безопасности.

Вся собранная информация о работе приложения

Все данные, собранные во время работы приложения на устройстве, сохраняются, струк-турируются, анализируются в процессе выявления уязвимостей и предоставляются в ка-честве артефактов сканирования.

Детальные рекомендации о выявленных уязвимостях

Stingray позволяет обнаруживать более 40 типов уязвимостей, технология базируется на наблюдении за поведением приложения на устройстве во время различных режимов сканирования.
После всех этапов анализа, выявленные в ходе работы приложения уязвимости отобра-жаются в интерфейсе с подробной информацией о месте возникновения, критичности, детальными рекомендациями по исправлению и, самое главное, недопущению подобных уязвимостей в дальнейшем.
Рекомендации постоянно обновляются новыми способами защиты и лучшими мировыми практиками. Ваши разработчики всегда будут в курсе самых надежных методов защиты приложения!

Уникальный механизм автоматизации регрессионного тестирования

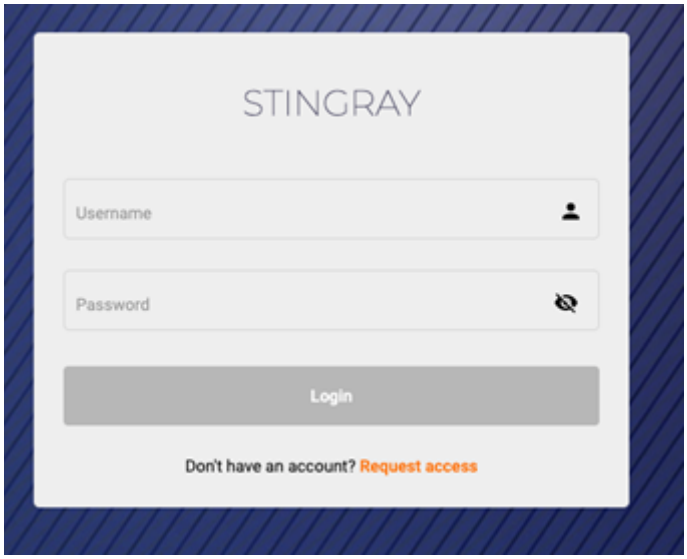
Для автоматизации тестирования в системе Stingray разработан уникальный меха-низм записи, воспроизведения и адаптации тест кейсов. Механизм основан на глубокой интеграции с операционной системой и методах машинного обучения. При всей сложно-сти внутри, для пользователя запись тест кейса выглядит, как обычная работа с приложением, не нужно писать скрипты или как-то по-особенному собирать приложение, просто пройдите необходимые шаги в приложении, как если бы оно было установлено на Ва-шем мобильном устройстве.

Работа с приложением

6 Аутентификация пользователя

Ссылка для доступа к веб-интерфейсу Stingray (GUI) должна быть предоставлена администратором. Перейдите по ссылке, чтобы открыть окно аутентификации.

Для входа в систему введите имя пользователя (логин) и пароль, а затем нажмите кнопку Login.

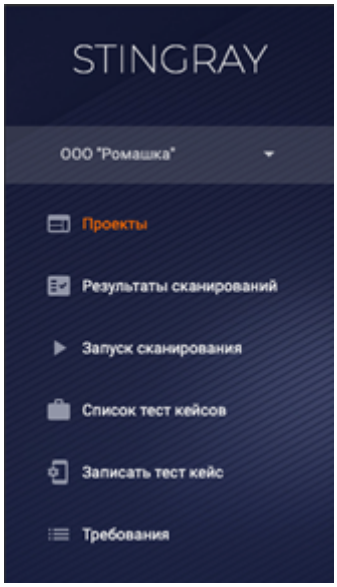


Окно аутентификации

Если учетные данные введены неправильно, будет отображено сообщение о неверном имени пользователя или пароле.

7 Основное меню

В левой части экрана расположено меню с основными экранами системы: Проекты, Результаты сканирований, Запуск сканирования, Список тест кейсов, Записать тест кейс, Требования.



Основное меню

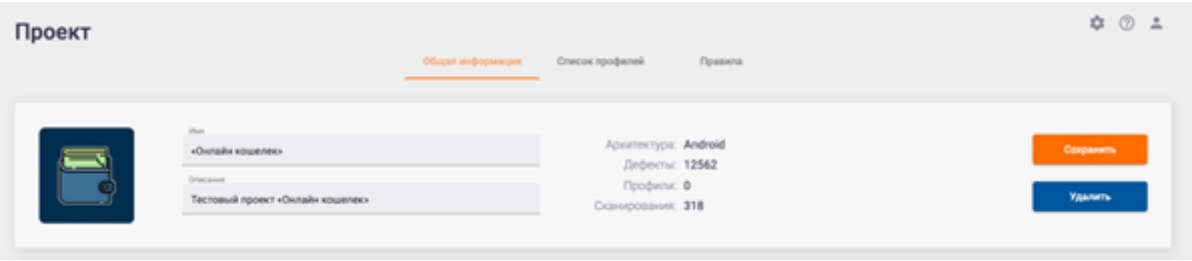
8 Проекты

8.1 Информация проекта

На первой вкладке Проект представлена общая информация по проекту, включающая в себя:

- Аватар проекта.
- Имя.
- Описание.
- Архитектура проекта (Android или iOS).
- Количество дефектов, найденных за время существования проекта.
- Количество сканирований в рамках проекта.

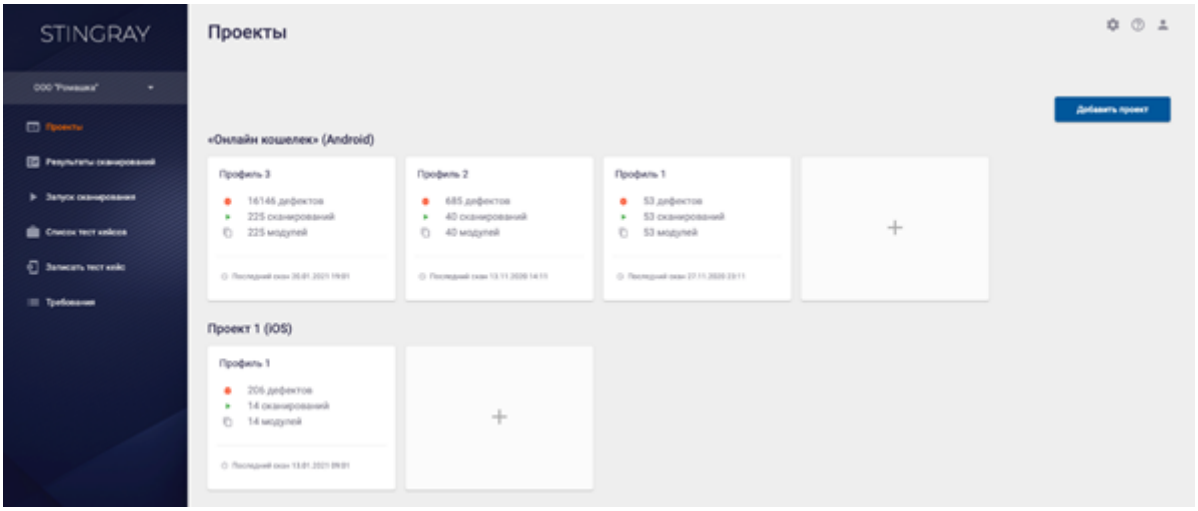
Количество настроенных профилей сканирования.



«Проект» — «Общая Информация»

8.1 Список проектов

На странице Проекты указаны все существующие в системе проекты (их архитектура) и их профили сканирования. На данной странице можно получить краткую информацию о количестве найденных дефектов за все время существования проекта, количество про-веденных сканирований и информацию о включенных модулях. Так же можно добавить новый Проект или добавить новый профиль сканирования для существующего Проекта.



Страница «Проекты»

По нажатию на имя Проекта открывается страница Проекты с тремя вкладками: Общая информация, Список профилей, Правила.