СТИНГРЕЙ

- ~~Что такое мобильное приложение~~
- Кому нужен MAST
- Как проверить мобильное приложение без доступа к исходному коду
- Интеграция в CI/CD-процессы

Свидетельство о регистрации в ФИПС: 2020660236
Номер в реестре российского ПО: 7699

STINGRAY

Что не так с мобильными приложениями?

1. Наблюдение показывает, что если к слову «приложение» добавить «мобильное», оно сразу кажется каким-то декоративным и ненастоящим,
к нему начинают относиться несерьезно.

2. Только 18% специалистов ИБ понимают, как работают мобильные приложения, какие угрозы они таят для компании и ее клиентов, и оценивают связанные с ними риски наравне с веб-приложениями и прочим ПО

* Среди компаний, разрабатывающих или заказывающих разработку мобильных приложений, в т.ч. банковский и госсектор

3. Из 120 курсов мобильной разработки ни один не содержит в себе раздел про информационную безопасность, защиту паролей и токенов, опасность deep link-ов, подмену сертификатов и пр.

* первые 120 из поисковой выдачи в российском и зарубежном сегментах

4. Автоматизированные системы разработки мобильных приложений, готовые шаблоны пользовательских интерфейсов, глянцевые кнопки, гипнотизирующие анимации и зеленые галочки авто-тестов мешают понять: вам сделали хорошее приложение или просто красивое

5. Нередко мобильные приложения заказываются у сторонних разработчиков, которые размещают согласованную версию сразу в магазины приложений, не раскрывая код приложения, в отличие от, например, прикладного ПО и веб-приложений.

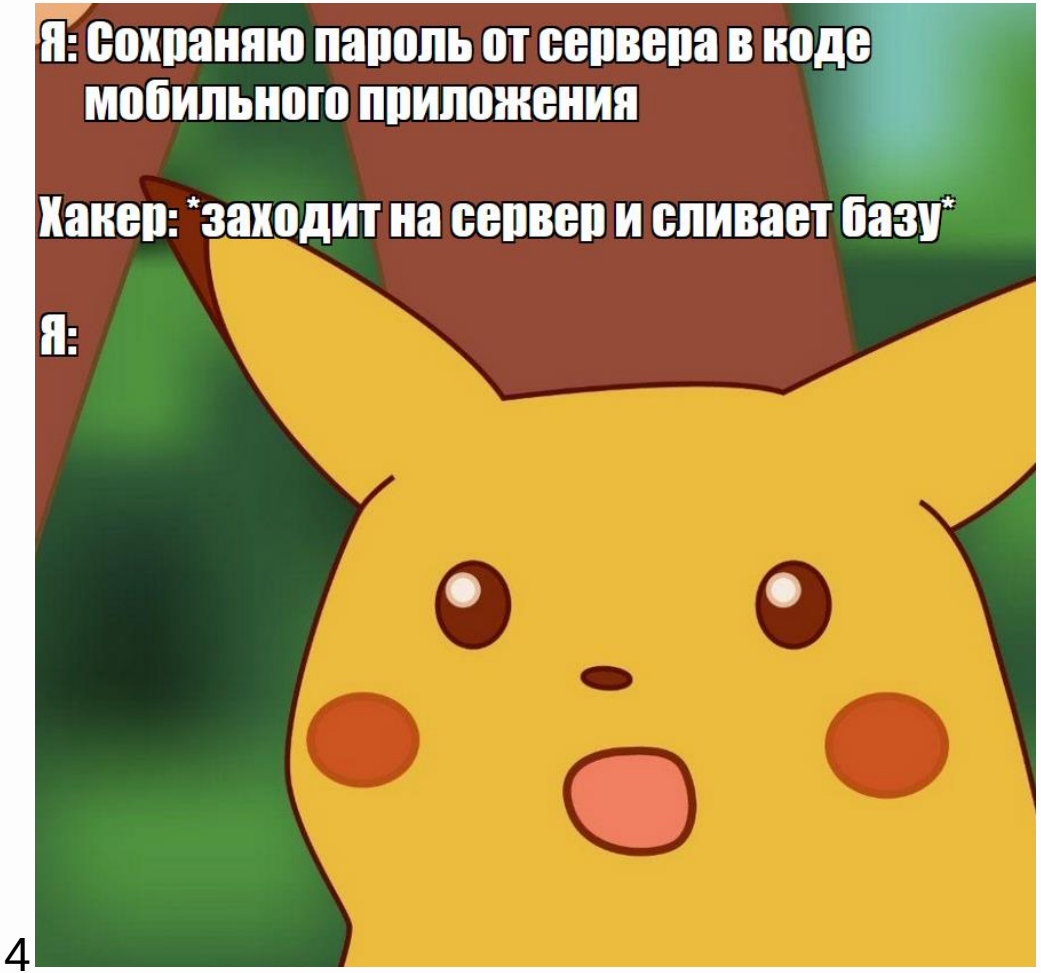
STINGRAY

Почему уязвимы мобильные приложения?

- Устаревшие или непроверенные технологии
- Оишбки в коде
- Халатность при разработке приложений
- Отсутствие контроля со стороны заказчика
- Недостаточные знания разработчиков в области ИБ и отсутствие ответственности аутсорсеров за последствия

STINGRAY

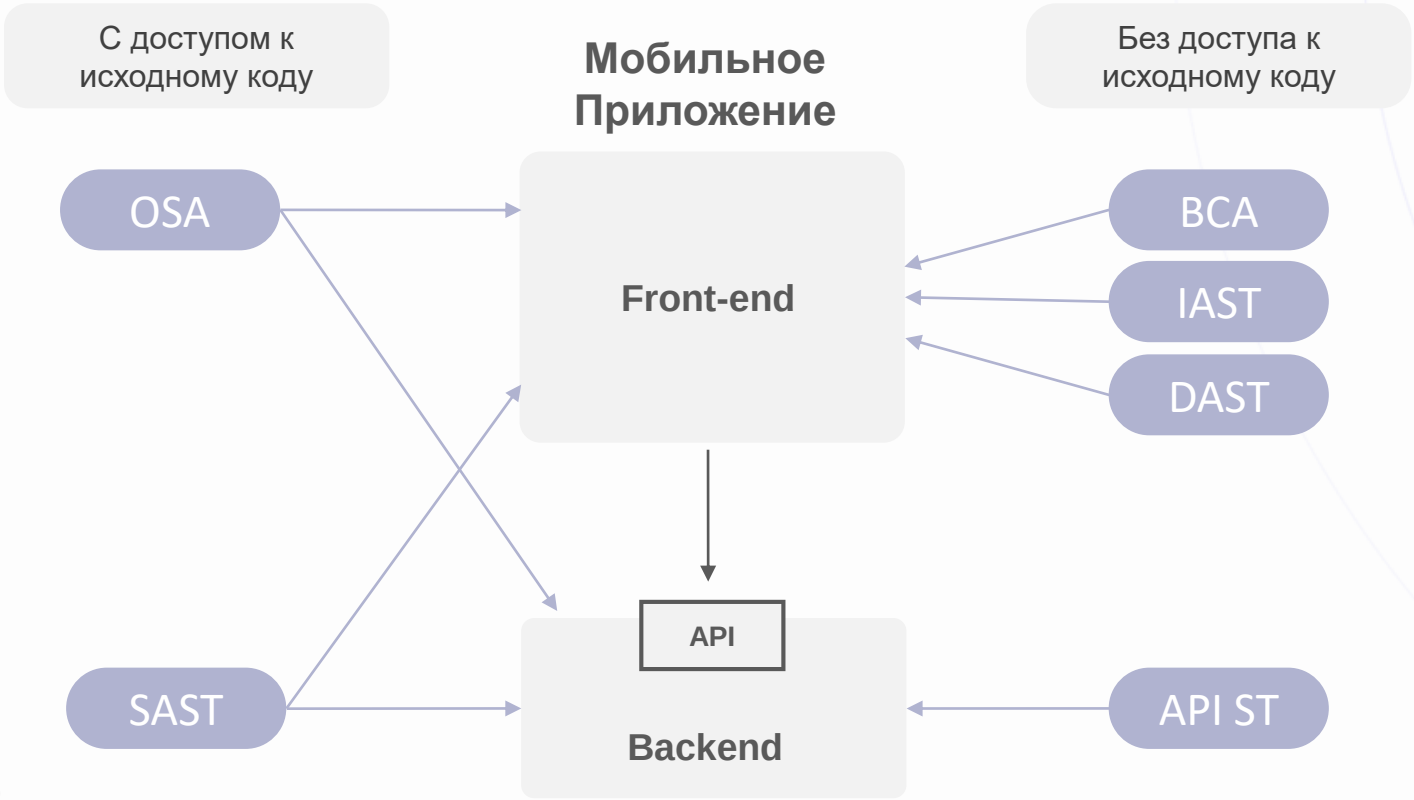
Какие последствия?



- Атака на пользователей и администраторов вашего приложения, кража данных, подмена контента и самого приложения, перенаправление на вредоносные веб-сайты, списание бонусов и денежных средств, запуск шпионского и вредоносного кода на мобильных устройствах от имени вашего приложения.
- Использование найденных в приложении ключей, сертификатов, паролей, токенов, контактов, адресов для атаки на вашу сеть, хранилища кода, облачную инфраструктуру.
- Продвинутые атаки на ваш API с дополнительной информацией, полученной из мобильного приложения.
- Репутационные потери, падение стоимости акций, всеобщее высмеивание и порицание.

STINGRAY

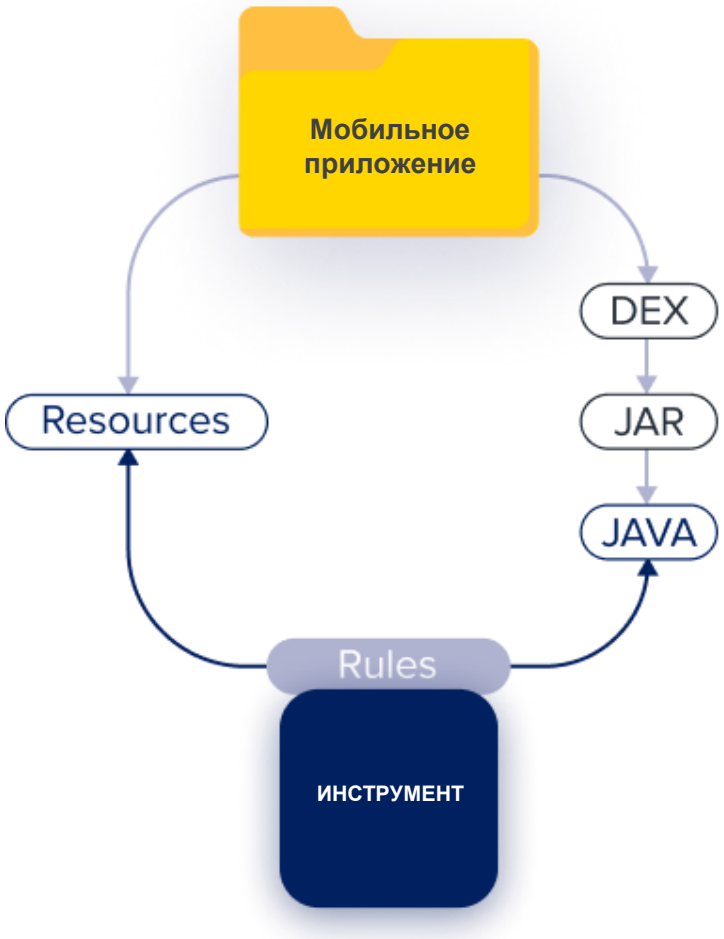
Практики MAST – Mobile Application Security Testing



Все практики MAST можно разделить на две группы:

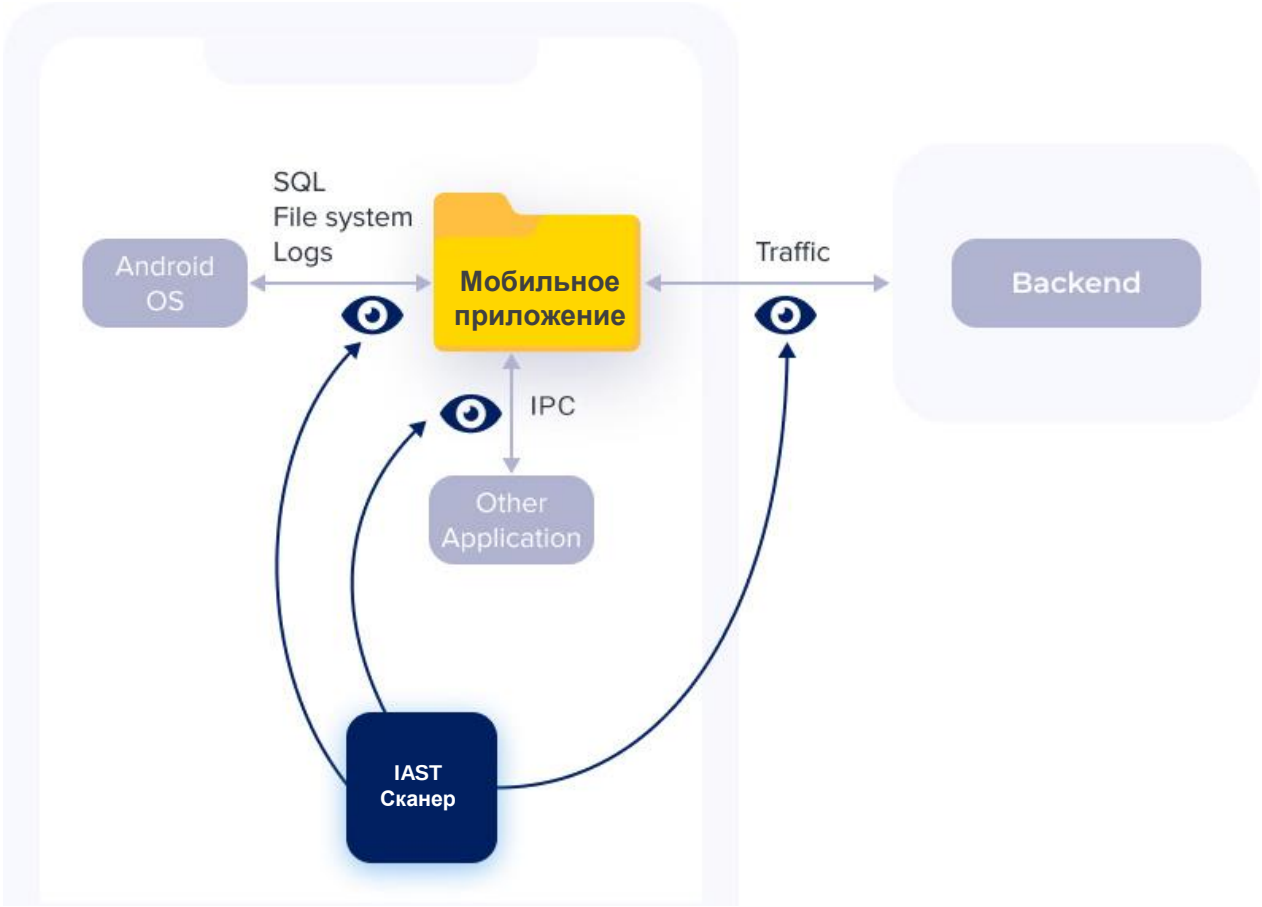
1. Когда доступен исходный код.

2. Когда нет доступа к исходному коду, а есть только готовое приложение.



BCA – Bytecode Analysis

BCA полезен для проверки окончательной версии приложения, чтобы убедиться, что она собрана корректно и, как минимум, включает в себя только файлы и конфигурацию, необходимые для работы, в сборке нет никаких лишних файлов и данных.



IAST - Interactive Application Security Testing

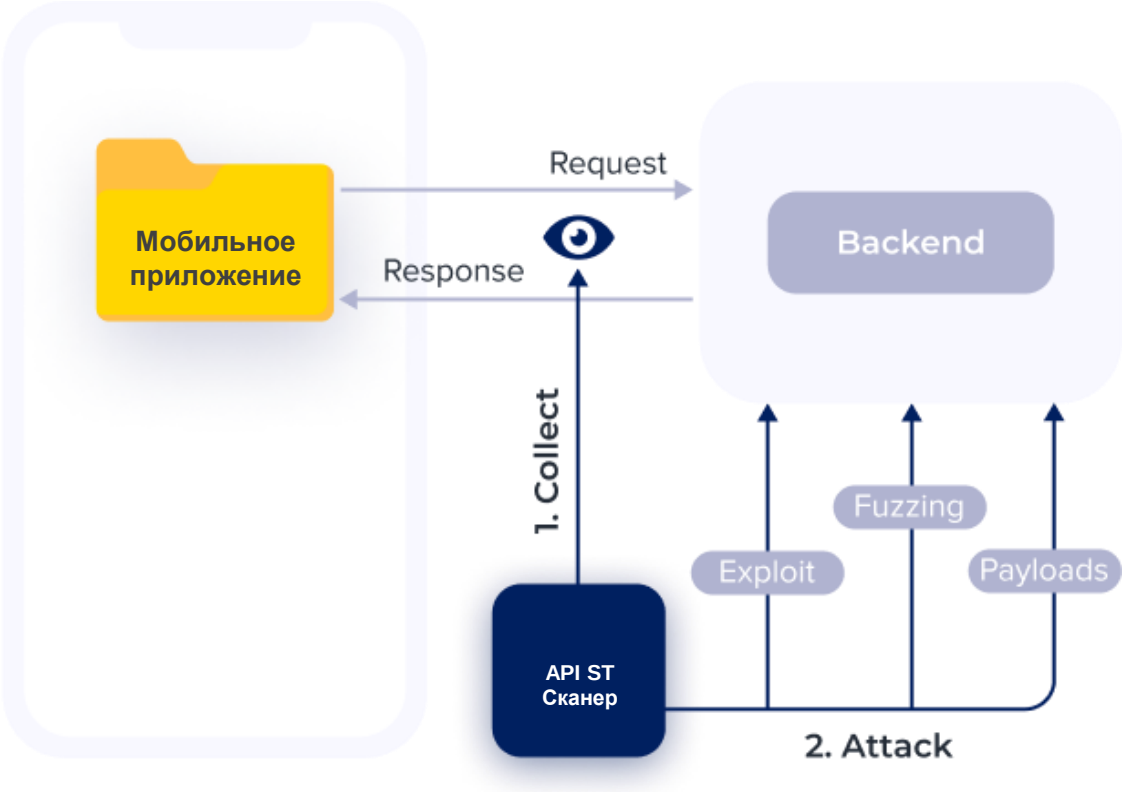
Практика IAST построена на основе наблюдения за поведением приложения, как оно взаимодействует с операционной системой, приложениями, вашим API.

Благодаря этому, можно идентифицировать и определить всю конфиденциальную информацию, с которой работает приложение, и понять, как она обрабатывается и хранится.

DAST - Dynamic Application Security Testing

Практика DAST нацелена на поиск уязвимостей, которые могут быть реализованы без root / jailbreak доступа и основаны на специфике используемых в приложении способов взаимодействия со сторонними приложениями.

Другими словами – это эмуляция злоумышленника, который представляет собой приложение, установленное рядом с вашим.



API ST - API Security Testing

Тестирование безопасности API (API ST) применяется для тестирования серверной части мобильных приложений (API).

Можно считать эту практику частью DAST для серверной части, но чтобы не путаться в аббревиатурах, в безопасности мобильных приложений применяется понятие API Security Testing.

STINGRAY

Важность динамического анализа

При работе с запущенным приложением можно анализировать его меняющееся состояние, реакции на поступающие данные и накапливающиеся ошибки логики обработки пользовательских действий.

Подтверждение уязвимостей

При помощи динамического анализа можно подтвердить уязвимости, выявленные другими практиками и определить, какие из них на самом деле эксплуатируемые.

Обнаружение уязвимостей

При динамическом анализе выявляются уязвимости, которые невозможно определить другими практиками.

Работа без исходного кода

Динамический анализ работает без необходимости доступа к исходному коду и анализирует поведение работающего приложения на устройстве.

STINGRAY

Как это делает Стингрей?

STINGRAY

Автоматизация тестирования

ЗАПИСЬ

Система записывает все действия пользователя и отклик приложения на эти действия, и на основе записи формирует сценарий проверки.

Либо специалист, проверяющий приложение, предоставляет готовый сценарий в формате Appium

ВОСПРОИЗВЕДЕНИЕ

Система воспроизводит записанные автотесты, анализирует, привели ли действия к ожидаемым результатам и, при необходимости, отправляет тесты на адаптацию.

АДАПТАЦИЯ

С помощью методов машинного обучения и интеграции с операционной системой Стингрей производит адаптацию автотеста под изменения элементов интерфейса без перезаписи теста.

STINGRAY

Автоматические проверки

Дамп архива приложения
Расшифровка приложения, дамп запущенного приложения из памяти.

Анализ поведения
Activity/Intent для Android. Отслеживание сообщений и взаимодействия с соседними приложениями и сервисами.

Анализ сетевой активности
Перехват HTTP/HTTPs/WebSocket, сбор информации о конечных точках, анализ передаваемых данных.

Анализ систем защиты
Проверка на изменение поведения приложения в зависимости от того, запущено оно на эмуляторе или нет

Анализ файлов, баз данных, системного журнала и дампа памяти приложения
Сбор баз данных, которые используются в приложении (включая зашифрованные базы данных), анализ запросов и ответов.

Анализ файлов, которые использует приложение во время своей работы.

Анализ изменений памяти приложения во время работы.

Анализ записей системного журнала.

Анализ сборки (SAST)
Декомпиляция исходного кода приложения, проверка на обфускацию, анализ качества конфигурации и сборки.

Поиск чувствительной информации
Поиск ключей, имен пользователей и паролей, сертификатов, токенов, введенных данных.

+ рекурсивный поиск найденной и производной информации по всем источникам данных.

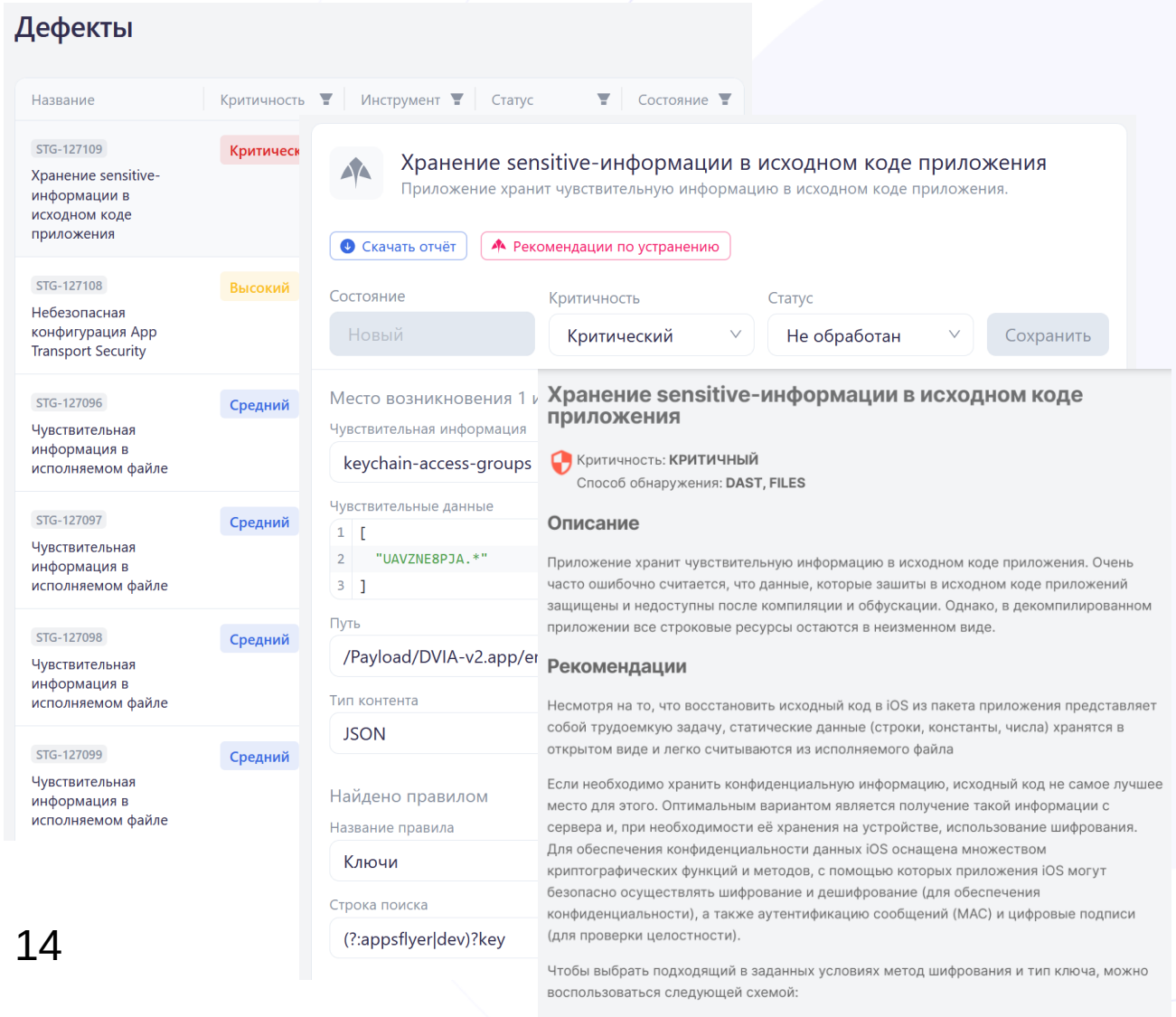
Поиск уязвимостей

Обнаружение уязвимостей, связанных с небезопасным хранением и передачей данных, небезопасной аутентификацией, слабой криптостойкостью.

Анализ поведения приложения на различные входные данные: пользовательский ввод, deep links.

STINGRAY

Отчеты о найденных дефектах



Найденные дефекты складываются в удобный список карточек с обозначением уровня критичности, полной информацией о деталях, а также ссылками на собственную базу данных инструкций по устранению.

Каждое сканирование формирует собственный список найденных дефектов, чтобы вы могли сравнить результаты между собой.

Список можно выгрузить в виде PDF-отчета для предоставления аудиторам.

STINGRAY

Проверка на соответствие требованиям

Найденные дефекты распределяются по пунктам стандартов, чтобы можно было легко проверить, каким стандартам и почему не соответствует ваше приложение:

- MASVS
- OWASP Mobile Top 10
- PCI DSS 4.0
- PCI Software Security Framework
- ОУД4
- ГОСТ-57580

STINGRAY

Сканирование на эмуляторах и живых устройствах

Приложения запускаются на ферме из эмуляторов и специально подготовленных устройствах на базе iOS и Android.

Вместе с отчетом и собранными данными предоставляется запись с экрана устройства для анализа поведения UI и отработки всех этапов сценария автоматизированного тестирования.

Установка платформы и проведение сканирований возможны как в облаке Стингрей, так и в сети заказчика.

STINGRAY

Интеграции

Стингрей обеспечивает интеграцию со многими инструментами DevOps:
CI / CD, дефект-трекерами, системами дистрибуции и другими инструментами

а также возможность проверки публикуемых приложений по расписанию.

STINGRAY

Что делать дальше:

Зайдите на сайт продукта и познакомьтесь с деталями

https://stingray-mobile.ru/

Дождитесь письма с приглашением на демо

Покажем продукт живьем, объясним, как запускаются сканирования, познакомим с отчетами и интеграциями, ответим на технические вопросы, запланируем тест.

Если остались вопросы

@MRCRRA

Или пишите на почту:
dm@afi-d.ru

Или звоните:
7 495 223 35 33
8 800 550 52 23