Отчет о тестировании требований безопасности

|  |  |  |
| --- | --- | --- |
| Наименование приложения | | VK mp3 mod |
| Версия | | 91/635 |
| Дата проверки | | 04.03.2020 |
| Проверил | | Фурс Дмитрий |
| Конфиденциальная информация | | Персональные данные пользователей (аудио- и видеозаписи, фото, личные сообщения и т.д.) |
| **Требования безопасности** | | **Результат** |
| 1 | Ненадежное хранение данных | - |
| 1.1 | Локальное хранение конфиденциальных данных  STORAGE-1 и STORAGE-2 | - |
| 1.1.1 | наличие разрешений AndroidManifest.xml для read/write во внешнем хранилище | + |
| 1.1.2 | наличие прав доступа к файлам MODE\_WORLD\_READABLE или MODE\_WORLD\_WRITABLE | - |
| 1.1.3 | наличие классов и функций:  SharedPreferences;  FileOutPutStream;  getExternal \*;  getWritableDatabase;  getReadableDatabase;  getCacheDir;  getExternalCacheDirs. | +  SharedPreferences    FileOutPutStream    getExternal  getWritableDatabase/getReadableDatabase  getCacheDir/getExternalCacheDirs |
| 1.1.4 | конфигурационные файлы build configs, такие как local.properties, gradle.properties | Не удалось получить доступ к файлам, т.к. был доступен лишь apk файл. |
| 1.1.5 | файлы ресурсов | В результате поиска не было найдено никаких подозрительных строк. |
| 1.2 | Файлы отчетов (log files) STORAGE-3 | Используется пакет android.util.Log  Случаев динамического конструирования строки найдено не было. |
| 1.3 | Передача конфиденциальных данных третьей стороне STORAGE-4 | Для работы со сторонними API через http запросы используется библиотека okttp, c помощью которой приложение обращается к VK API для получения информации (аудио- и видеозаписи, фото, личные сообщения и т.д.) |
| 1.4 | Поля ввода конфиденциальных данных STORAGE-5 | При вводе пароля не появляются строки-подсказки, для это поля кэш клавиатуры отключён. |
| 1.5 | Безопасность межпроцессного взаимодействия STORAGE-6 | Нет |
| 1.6 | Безопасность данных в пользовательском интерфейсе STORAGE-7 | Login.xml  EditText для ввода пароля, символы заменяются точками. Аналогично при изменении пароля. |
| 1.7 | Резервное копирование STORAGE-8 | Флага allowBackup не обнаружено |
| 1.8 | Фоновый режим STORAGE-9 | Не установлен FLAG\_SECURE, приложение не скрывает конфиденциальные данные с экрана, когда находиться в фоновом режиме |
| 1.9 | Хранение конфиденциальных данных в памяти  STORAGE-10 | Логин и пароль используются в LoginActivity, а также в активити, предназначенном для смены пароля. Для аутентификации пользователя через http клиент посылается запрос на сервер.      Конфиденциальная информация не очищается из памяти, не используются примитивные типы. |
| 1.10 | Настройка доступа к устройству  STORAGE-11 | Используется Settings.Secure    Использования Device Administration API не найдено |
| 1.11 | Проверка сертификатов  NETWORK-3 | Используется TrustManager и HostnameVerifier |
| 1.12 | Проверка SSL PINNING  NETWORK-4 | Используется NetworkSecurityPolicy    Нет конфигурационного файла для сетевых настроек |
| 1.13 | Наличие дополнительного канала связи  NETWORK-5 | Для входа в приложение, а также для восстановления аккаунта можно использовать только электронную почту/телефон |
| 1.14 | SECURITY PROVIDER  NETWORK-6 | Нет доступа к файлам сборки |
| 1.15 | Ненадёжная аутентификация (на бэкенде)  AUTH-1 | Используется аутентификация только по логину и паролю |
| 1.16 | Управление сеансом с отслеживанием состояния  AUTH-2 | На стороне сервера токены генерируются случайным образом. Не было найдено попыток сохранения информации о токене в хранилище. |
| 1.17 | Управление сеансом без отслеживания состояния  AUTH-3 | Для хранения токенов используется Keystore. |
| 1.18 | Тестирование выхода пользователей из системы  AUTH-4 | Нет доступа к коду сервера. |
| 1.19 | Реализация парольной политики  AUTH-5 | Максимальная длина пароля – 32 символа.  Минимальная длина пароля – 6 символов.  Остальные требования (“обрезка”, использование всех символов, чередование учётных данных) соответствуют требованиям. |
| 1.20 | Защита от перебора данных авторизации AUTH-6 | При большом количестве попыток (6) появляется капча. Блокировка отсутствует. |
| 1.21 | Срок действия токена  AUTH-8 | Время ожидания отсутствует. |
| 1.22 | Двухфакторная аутентификация  AUTH-9  AUTH-10 | Отсутствует двухфакторная аутентификация. |
| 1.23 | Информирование пользователя о действиях с его учётной записью  AUTH-11 | Приложение не информирует пользователя обо всех действиях по входу в систему (с возможностью блокировки определённых устройств). |
| 1.24 | Локальная аутентификация в Android  Подтверждение учётных данных | Используется KeyguardManager |
| 1.25 | Локальная аутентификация в Android  Биометрическая аутентификация | Отсутствует биометрическая аутентификация |
| 1.26 | Требования к криптографии  Проверка использования стандартных криптографических алгоритмов (CRYPTO-2, CRYPTO-3, CRYPTO-4) | Класс Cipher    Класс MessageDigest    Класс Signature    Класс PrivateKey |
| 1.27 | Требования к криптографии  Тестирование генерации случайных чисел (CRYPTO-6) | Используется класс SecureRandom |
| 1.28 | Требования к криптографии  Управление ключами | Не используется AndroidKeyStore |
| 1.29 | Проверка на уязвимости к инъекциям фрагментов | Используется PreferenceActivity |
| 1.30 | Проверка пользовательских URL SCHEMES | Используются параметризованные схемы |
| 1.31 | Проверка безопасной работы приложения при использовании IPC | Есть экспортируемые компоненты, но утечки данных не обнаружено |
| 1.32 | Проверка выполнения JavaScript в WebViews | Не используется WebView |
| 1.33 | Тестирование обработчиков протокола WebView | Не используется WebView |
| 1.34 | Представление Java объектов через WebViews | Не используется WebView |
| 1.35 | Проверка сохранения объектов | Не применяется шифрование |
| 1.36 | Приложение подписано валидным сертификатом  CODE-1 |  |
| 1.37 | Возможность отладки приложения  CODE-2 | Нет флага debuggable и allowBackup |
| 1.38 | Проверка наличия уязвимостей в сторонних библиотеках  CODE-5 | Не используются сторонние библиотеки |
| 1.39 | Проверка обработки исключений  CODE-6, CODE-7 | Конфиденциальная информация не раскрывается в блоках обработки исключений |
| 1.40 | Проверка активации стандартных функций безопасности  CODE-9 |  |