Отчет о тестировании требований безопасности

|  |  |  |
| --- | --- | --- |
| Наименование приложения | | Waking Up |
| Версия | | 1.0.0 |
| Дата проверки | | 11.03.20 |
| Проверил | | Селедцов Денис Евгеньевич |
| Конфиденциальная информация | | Адрес электронной почты. |
| **Требования безопасности** | | **Результат** |
| 1 | Ненадежное хранение данных | - |
| 1.1 | Локальное хранение конфиденциальных данных  STORAGE-1 и STORAGE-2 | SharedPreferences используются, но не хранят какую-либо конфиденциальную  информацию.  SQLite используется лишь сторонними библиотеками (facebook, mixpanel).  Все остальное тоже используется лишь сторонними библиотеками. |
| 1.1.1 | наличие разрешений AndroidManifest.xml для read/write во внешнем хранилище | Данные разрешения присутствуют. |
| 1.1.2 | наличие прав доступа к файлам MODE\_WORLD\_READABLE или MODE\_WORLD\_WRITABLE | Упоминание данных режимов отсутствует. |
| 1.1.3 | наличие классов и функций:  SharedPreferences;  FileOutPutStream;  getExternal \*;  getWritableDatabase;  getReadableDatabase;  getCacheDir;  getExternalCacheDirs. | Упоминаются в сторонних библиотеках. |
| 1.1.4 | конфигурационные файлы build configs, такие как local.properties, gradle.properties | Build configs присутствуют как у сторонних библиотек, так и для основного кода.  Содержит строки:  API\_SECRET = "h4Vi3EN9zcFeBoMBCTHscp6aghbg7GUfEJtqbACHAbV";  APPSFLYER\_DEV\_KEY = "7uX2WBw8h6t4esM5Se3UhY";  BUILD\_TYPE = "release";  DEBUG = false;  MIXPANEL\_API\_TOKEN = "d981b27d9c14fabf1a2cf76603f46a2d";  Properties есть у сторонних библиотек. |
| 1.1.5 | файлы ресурсов | Уже ранее упомянутые:      name="API\_SECRET">h4Vi3EN9zcFeBoMBCTHscp6aghbg7GUfEJtqbACHAbV      name="API\_URL">https://api.wakingup.com      name="APPSFLYER\_DEV\_KEY">7uX2WBw8h6t4esM5Se3UhY      name="MIXPANEL\_API\_TOKEN">d981b27d9c14fabf1a2cf76603f46a2d |
| 1.2 | Файлы отчетов (log files) STORAGE-3 | Логгер и “System.out.println” использовались только в сторонних библиотеках.  В приложении использовался ProGuard, так что весь код связанный с  журналированием мог быть удален. |
| 1.3 | Передача конфиденциальных данных третьей стороне STORAGE-4 | Библиотек много, но они все известные и часто обновляемые. В приложении  Используются последние версии. |
| 1.4 | Поля ввода конфиденциальных данных STORAGE-5 | textNoSuggestions упоминается только раз в searchbar. |
| 1.5 | Безопасность межпроцессного взаимодействия STORAGE-6 | Атрибут exported установлен в false, кроме некоторых библиотек, для которых  Прописано true.  Упоминание permission найдено лишь в разрешениях для приложения, единственно  Не совсем очевидный запрос – на использование камеры, который вроде как не нужен.  Но его используют сторонние библиотеки (facebook, к примеру)  ProtectionLevel нигде не установлен.  ContentProvider используют лишь сторонние библиотеки. |
| 1.6 | Безопасность данных в пользовательском интерфейсе STORAGE-7 | В самом приложении авторизация выполняется путем ввода 4-ех значного  кода из цифр, получаемого при попытке авторизации на почту. Поле ввода кода  представляет из себя 4 большие ячейки, куда требуется ввести цифры. Цифры не  заменяются на \*. После ввода последней цифры автоматически происходит попытка  авторизации в аккаунт.  Атрибут textPassword не найдет. |
| 1.7 | Резервное копирование STORAGE-8 | Резервное копирование разрешено allowBackup="true"  Можно узнать личные данные адреса почты. |
| 1.8 | Скрытие конфиденциальных данных с экрана в фоновом режиме STORAGE-9 | Данные не скрываются при переходе приложения в фоновый режим. |
| 1.9 | Ненадежное хранение данных. STORAGE-10 | Приведенные в презентации алгоритмы хранения данных не найдены. Почти везде  используются строки. Адрес почты  Хранится постоянно и может быть легко извлечен. Вход проводится с помощью пароля,  высылаемого на почту при попытке входа. Следующий раз пароль требуется лишь при  ранее выполненном выходе из аккаунта (опять-таки, получаемый через почту).  Различные API SECRET KEY также хранятся в String и могут быть легко найдены. |
| 1.10 | Требование минимальных настроек доступа STORAGE-11 | Приложение не требует от пользователя каких-либо дополнительных защитных мер и  Не проверяет надежность и безопасность среды. |
| 1.11 | Информирование пользователя STORAGE-12 | Приложение не информирует пользователя о персональных данных и о практиках  Безопасности. |
| 1.12 | Конфиденциальные данные в локальной памяти STORAGE-13 | Конфиденциальные данных хранятся локально в памяти телефона (почта), пароль же  динамический, и в памяти не хранится. |
| 1.13 | Шифрование локальных данных STORAGE-14 | Локальные данные никаким образом не шифруются и хранятся в памяти в виде строк,  которые можно легко прочитать. |
| 1.14 | Стирание локального хранилища STORAGE-15 | Локальное хранилище после многочисленных бесплодных попыток входа не стирается. |
| 2 | Ненадежная передача данных. | - |
| 2.1 | Проверка сертификатов X.509 NETWORK‑3 | Cоздание TrustManager в классе WebSocketOkhttp c использованием аннотации @SuppressLint({"TrustAllX509TrustManager"}).  Метод с созданием TrustManager с аннатацией @SuppressLint({"TrustAllX509TrustManager"}). |
| 2.2 | Проверка SSL pinning NETWORK-4 | Файлы для анализа отсутствуют. |
| 2.3 | Наличие дополнительного канала связи NETWORK‑5 | Способов восстановления аккаунта нету, т.к. используется лишь почта, а пароль присылается на нее при входе в аккаунт. |
| 2.4 | Security Provider  NETWORK‑6 | Файлы сборки не достал, но google play services используются. |
| 3 | Ненадежная аутентификация. |  |
| 3.1 | Реализация аутентификации на стороне сервера AUTH-1 | - |
| 3.2 | Управление сеансом с отслеживанием состояния AUTH-2 | - |
| 3.3 | Управление сеансом без отслеживания состояния AUTH-3 | - |
| 3.4 | Тестирование выхода пользователя из системы  AUTH-4 | Нету тестирования. Выход выполняется только по запросу пользователя. |
| 3.5 | Реализация парольной политики  AUTH-5 | Пароль высылается на почту при попытке входа. Пароль четырёхзначный, действует 15 минут. |
| 3.6 | Защита от перебора данных авторизации AUTH-6 | - |
| 3.7 | Срок действия токена AUTH-8 | Вход из аккаунта автоматически не выполняется по истечению времени. |
| 3.8 | Двухфакторная аутентификация AUTH-9 AUTH-10 | Двухфакторная аутентификация отсутствует. |
| 3.9 | Информирование пользователя о действиях с его учетной записью AUTH-11 | Уведомления о попытке входа приходят на почту вместе с паролем. |
|  | Локальная аутентификация в Android. Подтверждение учетных данных. | Ничего не требует в случае, если не заходить в него на протяжении нескольких дней/недель/месяцев. |
|  | Локальная аутентификация в Android. Биометрическая аутентификация FingerprintManager. | Биометрия отсутствует. |
| 4 | Требования к криптографии |  |
| 4.1 | Проверка использования стандартных криптографических алгоритмов CRYPTO-2 CRYPTO-3 CRYPTO-4 | Все найденные использования MessageDigest используются для получения md5 хешей строк. |
| 4.2 | Тестирование генерации случайных чисел CRYPTO-6 | Были найдены следующие использования небезопастного генератора случайных чисел:   * RandomGeneratedInputStream – поток случайных байт. Использований не найдено. * FirebaseMessagingMasterService – используется при реагировании на сообщение, упоминания были. |
| 4.3 | Управление ключами | Во всех найденных случаях генерации ключей они сохраняются в AndroidKeyStore. |
| 5 | Требования к взаимодействию с операционной системой |  |
| 5.1 | Проверка на уязвимости к инъекциям фрагментов PLATFORM-2 | Exported Activities, которые расширяли бы класс PreferenceActivity не найдены. |
| 5.2 | Проверка пользовательских URL Schemes PLATFORM-3 | Пользовательские URL не играют в приложении большой роли и угрозы безопасности не несут. |
| 5.3 | Проверка безопасной работы приложения при использовании IPC PLATFORM-4 | - |
| 5.4 | Проверка выполнения JavaScript в WebViews PLATFORM-5 | JS не отыгрывает в важных ситуациях и угрозы представлять не должен. |
| 5.5 | Тестирование обработчиков протокола WebView PLATFORM-6 | * Не найдено использований setAllowContentAccess. * Не найдено использований setAllowFileAccess. * Не найдено использований setAllowFileAccessFromFileURLs. * Не найдено использований setAllowUniversalAccessFromFileURLs. |
| 5.6 | предоставление Java объектов через WebViews PLATFORM-7 | Упоминания метода addJavascriptInterface не найдены. |
| 5.7 | Проверка сохранения объектов  PLATFORM-8 | Объекты с конфиденциальной информацией не сохраняются. |