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. |