т Отчет о тестировании требований безопасности

|  |  |  |
| --- | --- | --- |
| Наименование приложения | | Coin Keeper |
| Версия | | 2.18.0 |
| Дата проверки | | 02.03.2020 |
| Проверил | | я |
| Конфиденциальная информация | | Логин и пароль пользователя |
| **Требования безопасности** | | **Результат** |
| 1 | Ненадежное хранение данных | - |
| 1.1 | Локальное хранение конфиденциальных данных  STORAGE-1 и STORAGE-2 | нет |
| 1.1.1 | наличие разрешений AndroidManifest.xml для read/write во внешнем хранилище | нет |
| 1.1.2 | наличие прав доступа к файлам MODE\_WORLD\_READABLE или MODE\_WORLD\_WRITABLE | нет |
| 1.1.3 | наличие классов и функций:  SharedPreferences;  FileOutPutStream;  getExternal \*;  getWritableDatabase;  getReadableDatabase;  getCacheDir;  getExternalCacheDirs. | да |
| 1.1.4 | конфигурационные файлы build configs, такие как local.properties, gradle.properties | нет |
| 1.1.5 | файлы ресурсов | да |
| 1.2 | Файлы отчетов (log files) STORAGE-3 | нет |
| 1.3 | Передача конфиденциальных данных третьей стороне STORAGE-4 | Не нашёл |
| 1.4 | Поля ввода конфиденциальных данных STORAGE-5 | Да |
| 1.5 | Безопасность межпроцессного взаимодействия STORAGE-6 | нет |
| 1.6 | Безопасность данных в пользовательском интерфейсе STORAGE-7 | нет |
| 1.7 | Резервное копирование STORAGE-8 | да |
| 1.8 | Приложение скрывает конфиденциальные данные с экрана, когда  находится в фоновом режиме.  STORAGE-9 | нет |
| 1.9 | Приложение не хранит конфиденциальные данные в памяти  дольше, чем необходимо, и полностью удаляет их из памяти после работы с ними. STORAGE-10 | нет |
| 1.10 | Приложение требует от пользователя минимальную настройку  доступа к устройству, такую, как установку пин-кода на устройство. STORAGE-11 | нет |
| 1.11 | Приложение информирует пользователя о персональных данных,  которые оно обрабатывает, а также о лучших практиках безопасности, которым  должен следовать пользователь при использовании приложения. STORAGE-12 | нет |
| 1.12 | ПРОВЕРКА СЕРТИФИКАТОВ X.509  (NETWORK‑3) | Нарушен |
| 1.13 | ПРОВЕРКА SSL PINNING  (NETWORK‑4)  ОШИБКИ PIN-ПРИКРЕПЛЕНИЯ СЕРТИФИКАТОВ | Файл конфигурации отсутствует |
| 1.14 | НАЛИЧИЕ ДОПОЛНИТЕЛЬНОГО КАНАЛА СВЯЗИ  (NETWORK‑5) | Отсутствует |
| 1.15 | SECURITY PROVIDER  (NETWORK‑6) | ProviderInstaller вызывается корректно |
| 1.16 | РЕАЛИЗАЦИЯ АУТЕНТИФИКАЦИИ НА СТОРОНЕ СЕРВЕРА  (AUTH-1) | Дополнительные факторы аутентификации отсутствуют, есть только логин и почта |
| 1.17 | УПРАВЛЕНИЕ СЕАНСОМ С ОТСЛЕЖИВАНИЕМ СОСТОЯНИЯ  (AUTH-2) |  |
| 1.18 | УПРАВЛЕНИЕ СЕАНСОМ БЕЗ ОТСЛЕЖИВАНИЯ СОСТОЯНИЯ  (AUTH-3) |  |
| 1.19 | ТЕСТИРОВАНИЕ ВЫХОДА ПОЛЬЗОВАТЕЛЯ ИЗ СИСТЕМЫ  (AUTH-4) | Код сервера недоступен. Выход из системы выполняется правильно |
| 1.20 | РЕАЛИЗАЦИЯ ПАРОЛЬНОЙ ПОЛИТИКИ  (AUTH-5) | +минимальная длина пароля не менее 8 символов;  − максимальная длина пароля не более 128 символов;  + не происходит «обрезка» паролей. Убедитесь, что каждый символ, который вводит пользователь, действительно включен в пароль;  + разрешено использование всех символов, включая юникод и пробелы. Не должно быть правил составления пароля, ограничивающих тип разрешенных символов;  − обеспечивается чередование учетных данных. |
| 1.21 | ЗАЩИТА ОТ ПЕРЕБОРА ДАННЫХ АВТОРИЗАЦИИ  (AUTH-6) | Счётчик попыток отсутствует |
| 1.22 | СРОК ДЕЙСТВИЯ ТОКЕНА  (AUTH-8) | Тайм аут сеанса отсутствует |
| 1.23 | ДВУХФАКТОРНАЯ АУТЕНТИФИКАЦИЯ  (AUTH-9, AUTH-10) | Отсутствует |
| 1.24 | ИНФОРМИРОВАНИЕ ПОЛЬЗОВАТЕЛЯ О ДЕЙСТВИЯХ С ЕГО  УЧЕТНОЙ ЗАПИСЬЮ  (AUTH-11) | Отсутствует |
| 1.25 | ЛОКАЛЬНАЯ АУТЕНТИФИКАЦИЯ В ANDROID  ПОДТВЕРЖДЕНИЕ УЧЕТНЫХ ДАННЫХ | Отсутствует |
| 1.26 | ЛОКАЛЬНАЯ АУТЕНТИФИКАЦИЯ В ANDROID  БИОМЕТРИЧЕСКАЯ АУТЕНТИФИКАЦИЯ  FINGERPRINTMANAGER | Отсутствует |
| 1.27 | ТРЕБОВАНИЯ К КРИПТОГРАФИИ  ПРОВЕРКА ИСПОЛЬЗОВАНИЯ СТАНДАРТНЫХ КРИПТОГРАФИЧЕСКИХ  АЛГОРИТМОВ (CRYPTO-2, CRYPTO-3, CRYPTO-4) | Используются классы и интерфейсы: Cipher, Mac, MessageDigest, Signature, пакеты java.security.\* и javax.crypto.\*. |
| 1.28 | ТРЕБОВАНИЯ К КРИПТОГРАФИИ  ТЕСТИРОВАНИЕ ГЕНЕРАЦИИ СЛУЧАЙНЫХ ЧИСЕЛ (CRYPTO-6) | Класс Random используется в приложении для других целей. |
| 1.29 | ТРЕБОВАНИЯ К КРИПТОГРАФИИ  УПРАВЛЕНИЕ КЛЮЧАМИ | AndroidKeyStore не используется. |
| 1.30 | ПРОВЕРКА НА УЯЗВИМОСТИ К ИНЪЕКЦИЯМ ФРАГМЕНТОВ  (PLATFORM-2) | Активити, расширяющие класс PreferenceActivity отсутсвуют. |
| 1.31 | ПРОВЕРКА ПОЛЬЗОВАТЕЛЬСКИХ URL  SCHEMES (PLATFORM-3) | Пользовательские схемы URL не определены |
| 1.32 | ПРОВЕРКА БЕЗОПАСНОЙ РАБОТЫ ПРИЛОЖЕНИЯ  ПРИ ИСПОЛЬЗОВАНИИ IPC (PLATFORM-4) | Есть exported сервисы, но утечки данных нет. |
| 1.33 | ПРОВЕРКА ВЫПОЛНЕНИЯ JAVASCRIPT В WEBVIEWS  (PLATFORM-5) | WebView отсутствует |
| 1.34 | ТЕСТИРОВАНИЕ ОБРАБОТЧИКОВ ПРОТОКОЛА  WEBVIEW (PLATFORM-6) | WebView отсутствует |
| 1.35 | ПРЕДОСТАВЛЕНИЕ JAVA ОБЪЕКТОВ ЧЕРЕЗ  WEBVIEWS (PLATFORM-7) | WebView отсутствует |
| 1.36 | ПРОВЕРКА СОХРАНЕНИЯ ОБЪЕКТОВ  (PLATFORM-8) | Сохранение объекта не используется для хранения  конфиденциальной информации на устройстве |
| 1.37 | ПРИЛОЖЕНИЕ ПОДПИСАНО ВАЛИДНЫМ  СЕРТИФИКАТОМ (CODE-1) | Релизная сборка подписана с использованием всех трех схем |
| 1.38 | ВОЗМОЖНОСТЬ ОТЛАДКИ ПРИЛОЖЕНИЯ (CODE-2) | Возможность отладки отсутствует. |
| 1.39 | ПРОВЕРКА НАЛИЧИЯ УЯЗВИМОСТЕЙ В  СТОРОННИХ БИБЛИОТЕКАХ (CODE-5) |  |
| 1.40 | ПРОВЕРКА ОБРАБОТКИ ИСКЛЮЧЕНИЙ  (CODE-6, CODE-7) | Приложение не предоставляет конфиденциальную информацию при  обработке исключений в своем пользовательском интерфейсе или в логах. |
| 1.41 | ПРОВЕРКА АКТИВАЦИИ СТАНДАРТНЫХ ФУНКЦИЙ  БЕЗОПАСНОСТИ (CODE-9) |  |
| 1.42 | ПРОВЕРКА ОБНАРУЖЕНИЯ РУТОВАННОГО  УСТРОЙСТВА (RESILIENCE-1) |  |
| 1.43 | ПРОВЕРКА ЦЕЛОСТНОСТИ ФАЙЛОВ  (RESILIENCE-3) | Приложение не использует механизмы проверки целостности. |
| 1.44 | ПРОВЕРКА ИСПОЛЬЗОВАНИЯ ОБФУСКАЦИИ  (RESILIENCE-9) | Приложение не использует механизмы обфускации. |