Протокол аудита безопасности для мобильного приложения

ИНК-Портал

Оглавление

[1. О документе 2](#_Toc92115497)

[2. Список используемого ПО 2](#_Toc92115498)

[3. M1: Обход архитектурных ограничений (Improper Platform Usage) 2](#_Toc92115499)

[3.1. Описание 2](#_Toc92115500)

[3.2. Протокол проведения 2](#_Toc92115501)

[3.3. Выводы 2](#_Toc92115502)

[4. M2: Небезопасное хранение данных (Insecure Data Storage) 2](#_Toc92115503)

[5. M3: Небезопасная передача данных (Insecure Communication) 2](#_Toc92115504)

[6. M4: Небезопасная аутентификация (Insecure Authentication) 2](#_Toc92115505)

[7. M5: Слабая криптостойкость (Insufficient Cryptography) 2](#_Toc92115506)

[8. M6: Небезопасная авторизация (Insecure Authorization) 2](#_Toc92115507)

[9. M7: Контроль содержимого приложения (Client Code Quality) 2](#_Toc92115508)

[10. M8: Модификация данных (Code Tampering) 2](#_Toc92115509)

[11. M9: Анализ исходного кода (Reverse Engineering) 2](#_Toc92115510)

[12. M10: Скрытый функционал (Extraneous Functionality) 2](#_Toc92115511)

# О документе

В документе приведены протоколы выводов утилит, согласно стандарту международной организации [OWASP](https://ru.wikipedia.org/wiki/OWASP) Mobile Security Testing Guide. Все материалы открыты доступны для исследователей и инженеров по безопастности по ссылке <https://github.com/OWASP/owasp-mstg>. Таблица 1 содержит историю изменений в документе.

Таблица 1

|  |  |
| --- | --- |
| **Номер редакции** | **Комментарии** |
| 0.1 | Начальная версия |

# Список используемого ПО

# M1: Обход архитектурных ограничений (Improper Platform Usage)

## Описание

В данном требование необходимо проверить отсутствие адреса сервера для подключения

## Протокол проведения

Lorem ipsum

## Выводы

Lorem ipsum

# M2: Небезопасное хранение данных (Insecure Data Storage)

# M3: Небезопасная передача данных (Insecure Communication)

# M4: Небезопасная аутентификация (Insecure Authentication)

# M5: Слабая криптостойкость (Insufficient Cryptography)

# M6: Небезопасная авторизация (Insecure Authorization)

# M7: Контроль содержимого приложения (Client Code Quality)

# M8: Модификация данных (Code Tampering)

# M9: Анализ исходного кода (Reverse Engineering)

# M10: Скрытый функционал (Extraneous Functionality)