Протокол аудита безопасности для мобильного приложения

ИНК-Портал

Оглавление

[1. О документе 2](#_Toc92875436)

[2. Список используемого ПО 2](#_Toc92875437)

[3. M1: Обход архитектурных ограничений (Improper Platform Usage) 2](#_Toc92875438)

[3.1. Описание 2](#_Toc92875439)

[3.2. Протокол проведения 3](#_Toc92875440)

[3.2.1. ОС IOS 3](#_Toc92875441)

[3.2.2. ОС Android 4](#_Toc92875442)

[3.3. Выводы 5](#_Toc92875443)

[4. M2: Небезопасное хранение данных (Insecure Data Storage) 5](#_Toc92875444)

[4.1. Описание 5](#_Toc92875445)

[4.2. Протокол проведения 5](#_Toc92875446)

[4.2.1. ОС IOS 5](#_Toc92875447)

[4.2.2. ОС Android 6](#_Toc92875448)

[4.3. Выводы 6](#_Toc92875449)

[5. M3: Небезопасная передача данных (Insecure Communication) 6](#_Toc92875450)

[5.1. Описание 6](#_Toc92875451)

[5.2. Протокол проведения 6](#_Toc92875452)

[5.2.1. ОС IOS 7](#_Toc92875453)

[5.2.2. ОС Android 8](#_Toc92875454)

[5.3. Выводы 8](#_Toc92875455)

[6. M4: Небезопасная аутентификация (Insecure Authentication) 8](#_Toc92875456)

[6.1. Описание 8](#_Toc92875457)

[6.2. Протокол проведения 8](#_Toc92875458)

[6.2.1. ОС IOS 9](#_Toc92875459)

[6.2.2. ОС Android 10](#_Toc92875460)

[1.1. Выводы 10](#_Toc92875461)

[2. M5: Слабая крипто стойкость (Insufficient Cryptography) 10](#_Toc92875462)

[3. M6: Небезопасная авторизация (Insecure Authorization) 10](#_Toc92875463)

[4. M7: Контроль содержимого приложения (Client Code Quality) 10](#_Toc92875464)

[5. M8: Модификация данных (Code Tampering) 10](#_Toc92875465)

[6. M9: Анализ исходного кода (Reverse Engineering) 10](#_Toc92875466)

[7. M10: Скрытый функционал (Extraneous Functionality) 10](#_Toc92875467)

# 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

|  |  |  |  |
| --- | --- | --- | --- |
| **Целевая ОС** | **ПО** | **Версия** | **Описание** |
| IOS | otool | 986 | Инспекция Mach-O binaries |
| Android | apktool | 2.5.0 | Программа для распаковки apk-файлов. Используется для локализации ПО, анализа структуры приложения. |
| Android | dex2jar | 2.0 | Инструмент, который используется для преобразования измененного APK-файла в jar-файл. |
| Android | jd-gui | 1.6.6 | Инструмент, который используется вместе с dex2jar, обеспечивает извлечение исходного кода. |
| Android | Packet Capture | 1.7.2 | Анализатор HTTP трафика |
| IOS | Charles Proxy | 1.4 | Анализатор HTTP трафика |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# M1: Обход архитектурных ограничений (Improper Platform Usage)

## Описание

Обход архитектурных ограничений – уязвимость охватывает злоупотребление особенностями платформы, обхода ограничений или неиспользования систем контроля управления безопасности платформы. Характерно как для платформы Android, так и для iOS (обход ограничений Touch ID и Keychain) и других мобильных ОС. Затрагивает системы контроля безопасности, которые являются частью мобильной операционной системы. Требование включает проверку отсутствия реквизитов подключения к сервисам REST/NATS. Объекты проверки (структуры представлены ниже): архив APK (Android), архив IPA (IOS).

Структура APK:

1. META-INF – директория, содержащая манифест файлы;
2. lib – директория, содержащая скомпилированные коды под каждую платформу;
3. res – директория, содержащая не скомпилированные ресурсы приложения;
4. assets – директория, содержащая ресурсы приложения, используемая Asset Manager;
5. AndroidManifest.xml – манифест файл, содержащий права порядок загрузки приложения;
6. classes.dex – файл классов для использования виртуальной машины Dalvik;
7. resources.arsc – файл, содержащий пред компилированные ресурсы приложения;

Структура IPA:

1. \_CodeSignature – подпись;
2. Assets.car, \*.bundle, \*.lproj, \*.png, \*.db, \*.json и др. – ресурсы приложения;
3. Frameworks – библиотеки приложения;
4. Runner – компилированный код приложений;
5. Info.plist – манифест файл, содержащий права порядок загрузки приложения;

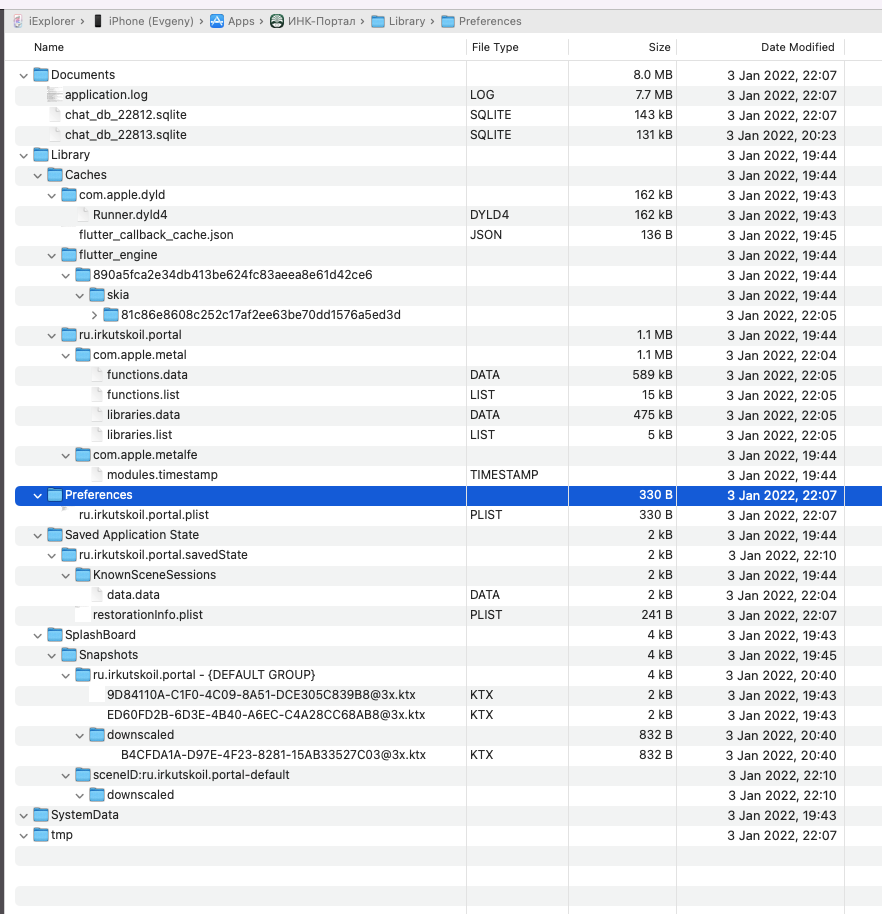
## Протокол проведения

Протокол включает:

1. запуск утилит otool для ОС IOS и apktool для ОС Android
2. выполнение инспекций в соответствии со стандартом [OWASP M1: Improper Platform Usage](https://owasp.org/www-project-mobile-top-10/2016-risks/m1-improper-platform-usage)
3. анализ результатов инспекций для получения вывода о соответствии ПО стандарту
4. протоколирование отчётов выполнения базовых инспекций

## ОС IOS

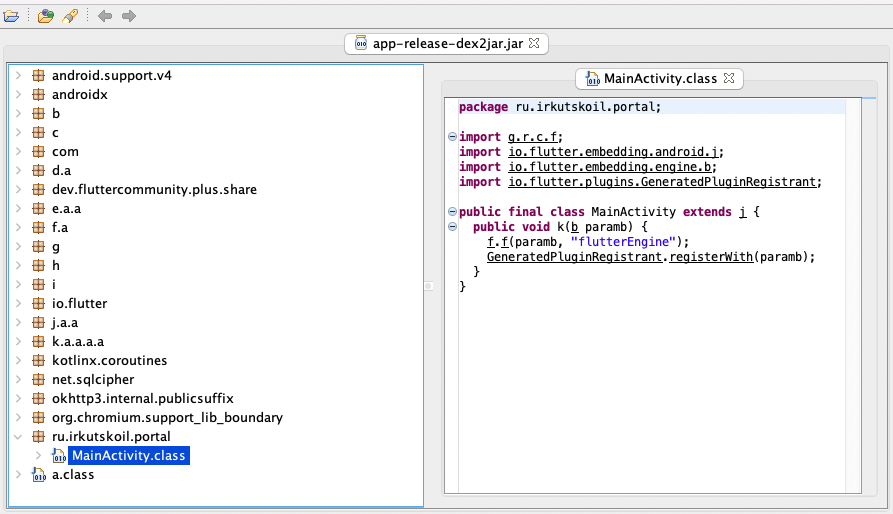
|  |
| --- |
| **# Unzip IPA**  cp ink\_mobile.ipa /tmp && cd /tmp  unzip ink\_mobile.ipa  **# Stack Smashing Protection**  otool -I -v Payload/Runner.app/Runner | grep stack  0x0000b0b0 71 \_\_\_stack\_chk\_fail  0x0000c00c 72 \_\_\_stack\_chk\_guard  0x0000c060 71 \_\_\_stack\_chk\_fail  0x0000000100006f5c 70 \_\_\_stack\_chk\_fail  0x0000000100008020 71 \_\_\_stack\_chk\_guard  0x00000001000080b0 70 \_\_\_stack\_chk\_fail  **# PIE (Position Independent Executable)**  otool -hv Payload/Runner.app/Runner  Payload/Runner.app/Runner (architecture armv7):  Mach header  magic cputype cpusubtype caps filetype ncmds sizeofcmds flags  MH\_MAGIC ARM V7 0x00 EXECUTE 76 6904 NOUNDEFS DYLDLINK TWOLEVEL PIE  Payload/Runner.app/Runner (architecture arm64):  Mach header  magic cputype cpusubtype caps filetype ncmds sizeofcmds flags  MH\_MAGIC\_64 ARM64 ALL 0x00 EXECUTE 76 7664 NOUNDEFS DYLDLINK TWOLEVEL PIE  **#** **Insecure Local Storage - manifest file in the app Directory**  plutil -p ru.irkutskoil.portal.plist  {  "callbackHandle" => 6491002407939001357  "callbackHandleOnRestart" => 6491002407939001357  "interval" => 5000  "notificationContentText" => "Нажмите для возврата в приложение"  "notificationContentTitle" => "ИНК-портал"  "playSound" => 0  "showNotification" => 0  }  # **Insecure Local Storage - database files in the app Directory**  sqlite3 chat\_db\_22812.sqlite  sqlite> .tables  Error: file is not a database |



## ОС Android

|  |
| --- |
| **# Unzip IPA**  cp app-release.apk /tmp && cd /tmp  **#** **Insecure Local Storage – manifest file in the app Directory**  apktool d app-release.apk && cat AndroidManifest.xml  **# Decompile classes**  cp app-release.apk app-release.zip && unzip app-release.zip && sh d2j-dex2jar.sh classes.dex |





## Выводы

Аудит не выявил реквизитов подключения к сервисам REST/NATS для обоих платформ.

# M2: Небезопасное хранение данных (Insecure Data Storage)

## Описание

Небезопасное хранение данных – уязвимость, к которой относится небезопасное хранение и непреднамеренная утечка данных. Требование включает проверку отсутствия конфиденциальных данных при выводе лог приложения. Объекты проверки: лог-файлы приложения IOS и Android.

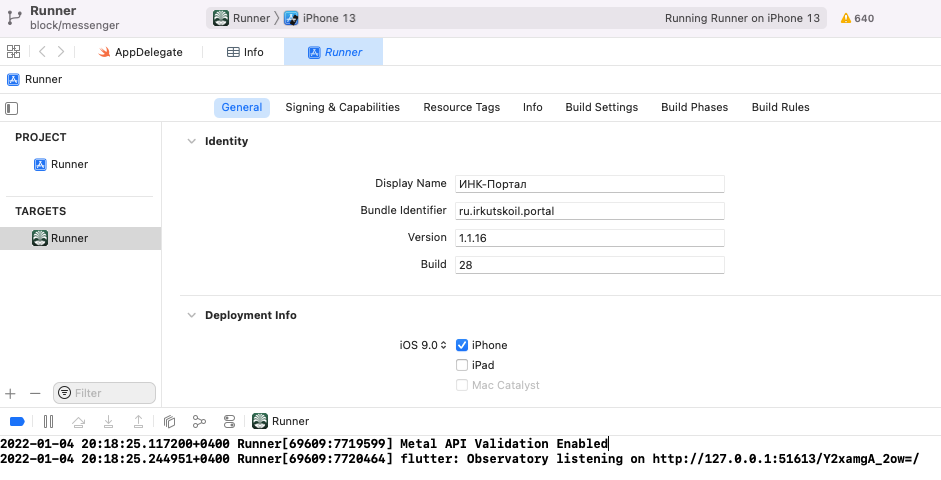
## Протокол проведения

Протокол включает:

1. запуск утилит XCode для ОС IOS и logcat для ОС Android
2. выполнение инспекций в соответствии со стандартом [OWASP M2: Insecure Data Storage](https://owasp.org/www-project-mobile-top-10/2016-risks/m2-insecure-data-storage)
3. анализ результатов инспекций для получения вывода о соответствии ПО стандарту
4. протоколирование отчётов выполнения базовых инспекций

## ОС IOS

|  |
| --- |
| # **check logs for insecure app data using xcode output**  2022-01-04 20:18:25.117200+0400 Runner[69609:7719599] Metal API Validation Enabled  2022-01-04 20:18:25.244951+0400 Runner[69609:7720464] flutter: Observatory listening on http://127.0.0.1:51613/Y2xamgA\_2ow=/ |



## ОС Android

|  |
| --- |
| **# adb connect**  adb devices  adb shell  **#** **check logs for insecure app data**  logcat | grep ru.irkutskoil.portal  01-04 20:11:45.497 482 511 I ActivityTaskManager:  Displayed ru.irkutskoil.portal/.MainActivity: +1s595ms |

## Выводы

Аудит не выявил конфиденциальных данных при выводе лог приложения для обоих платформ.

# M3: Небезопасная передача данных (Insecure Communication)

## Описание

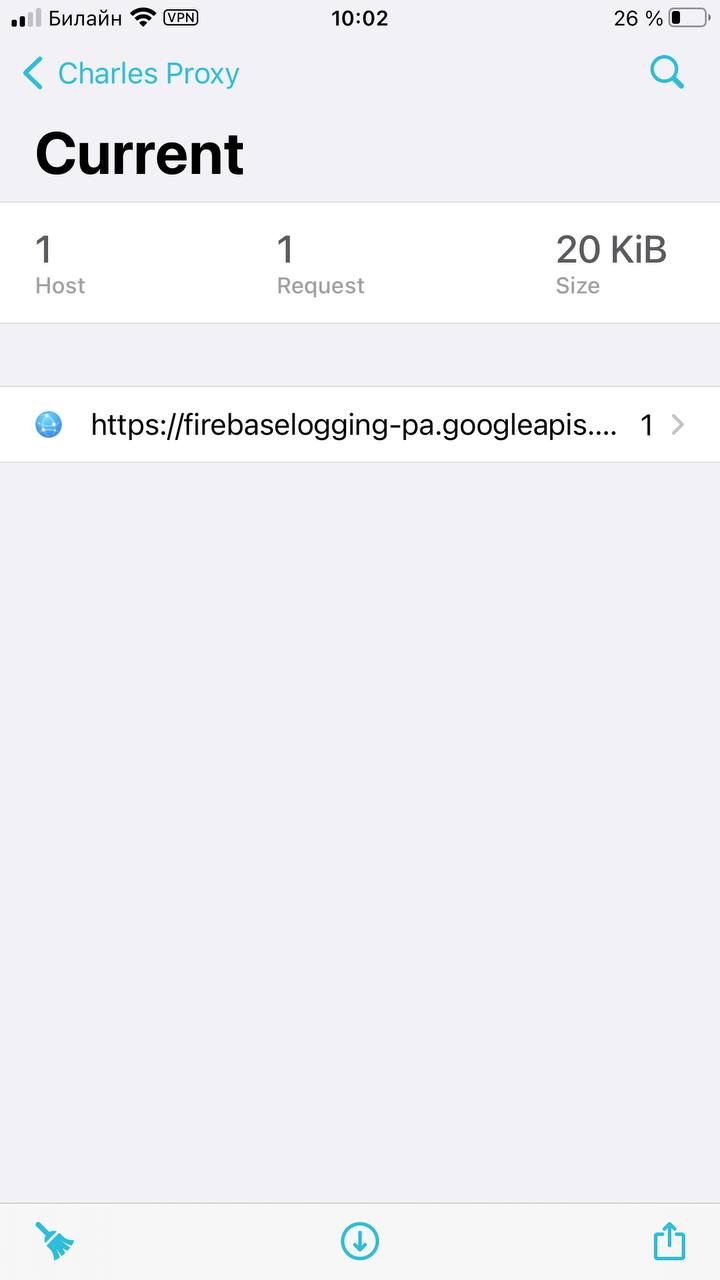
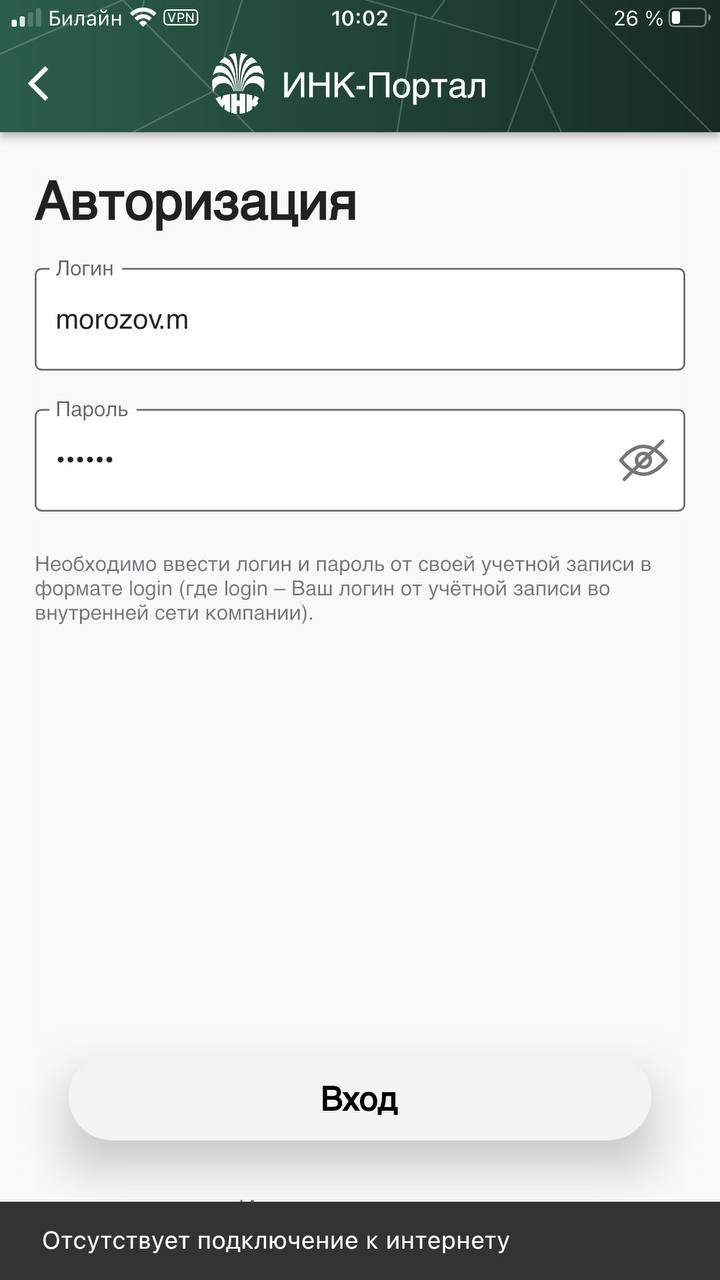
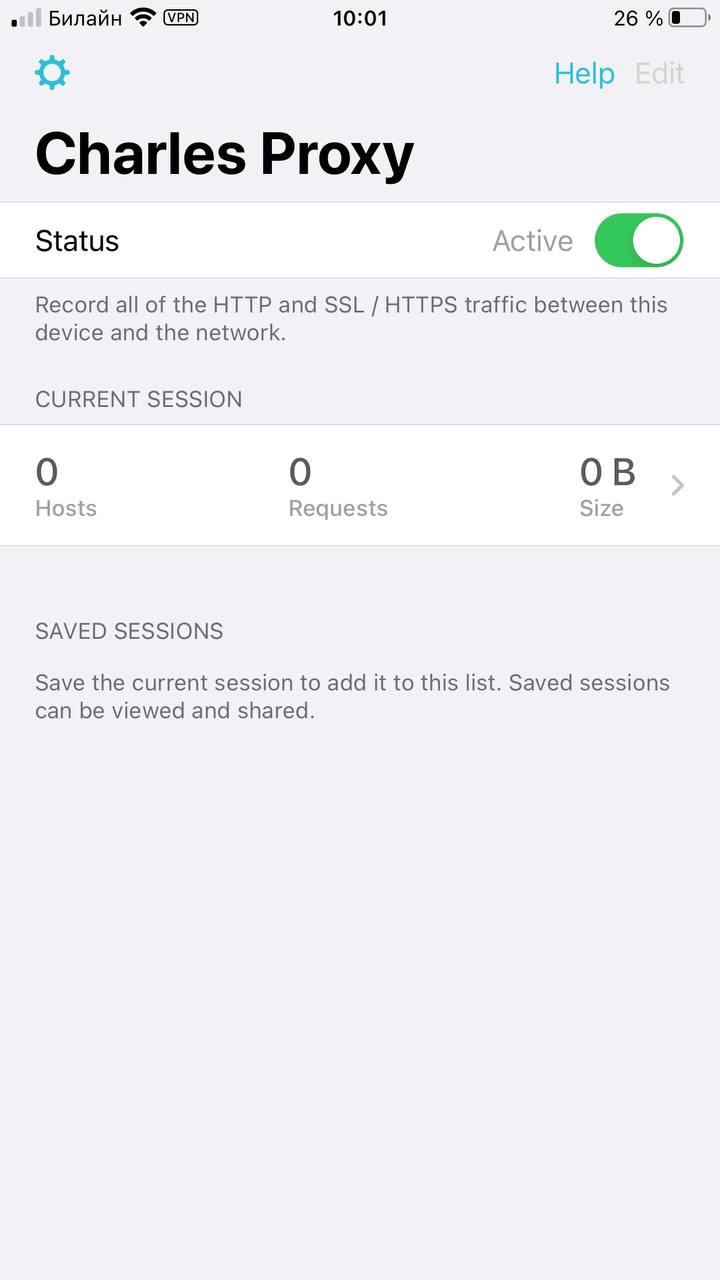
Небезопасная передача данных – уязвимость, к которой относится недостаточное подтверждение достоверности источников связи, неверные версии SSL, недостаточная проверка согласования, передача конфиденциальных данных в открытом виде. Требование включает проверку отсутствия HTTP траффика при работе приложения. Объекты проверки: сетевой трафик приложения IOS и Android.

## Протокол проведения

Протокол включает:

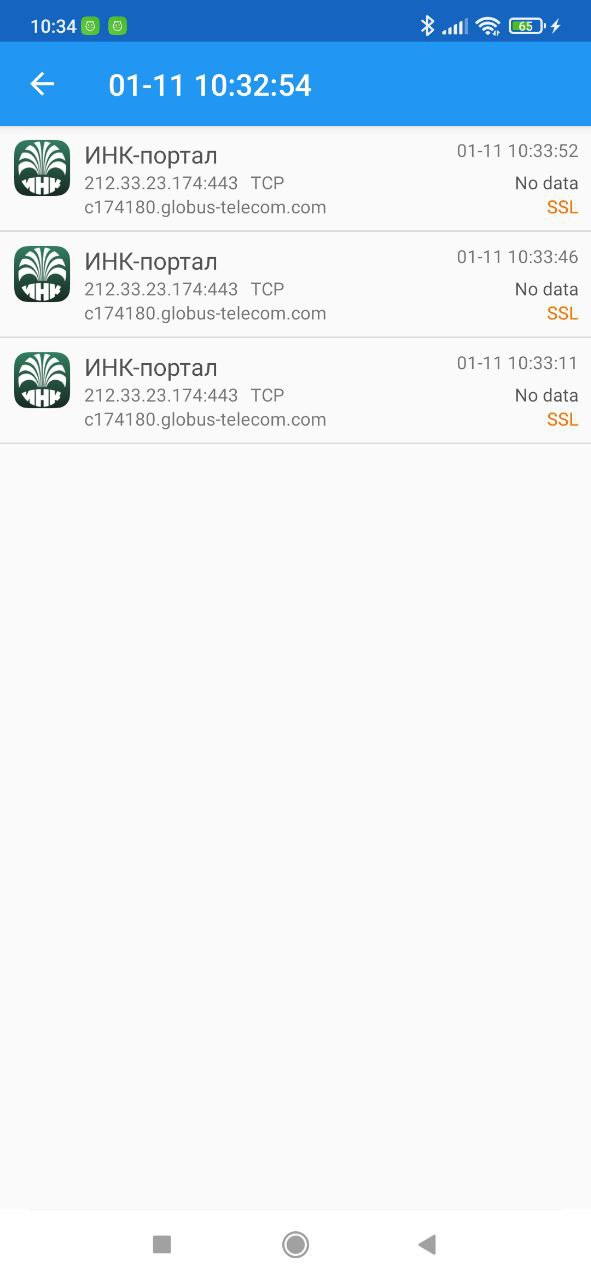
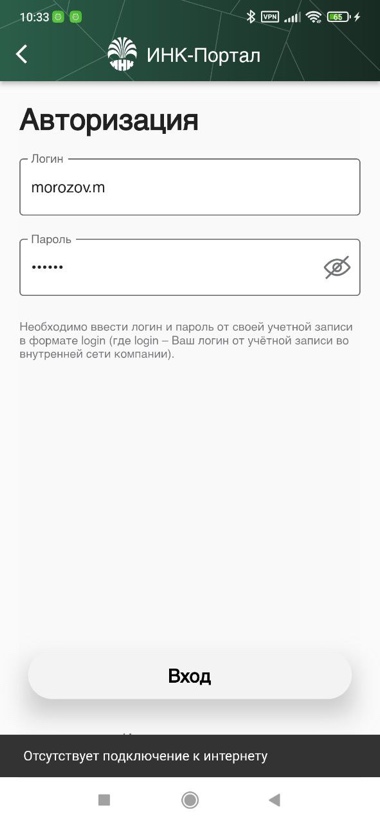
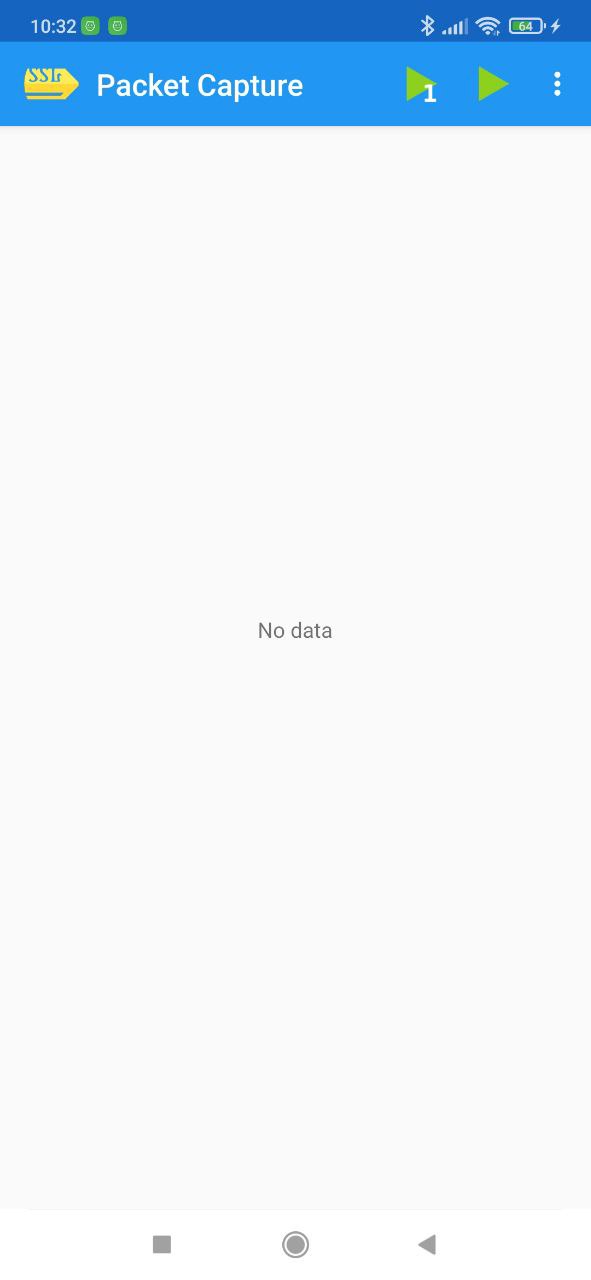
1. запуск утилит Charles Proxy для ОС IOS и Packet Capture для ОС Android
2. выполнение инспекций в соответствии со стандартом [OWASP M3: Insecure Communication](https://owasp.org/www-project-mobile-top-10/2016-risks/m3-insecure-communication)
3. анализ результатов инспекций для получения вывода о соответствии ПО стандарту
4. протоколирование отчётов выполнения базовых инспекций

## ОС IOS



|  |
| --- |
| HTTP/1.1 200 OK  Content-Type: application/x-protobuf  Content-Disposition: attachment  Vary: Origin  Vary: X-Origin  Vary: Referer  Content-Encoding: gzip  Date: Wed, 12 Jan 2022 06:01:38 GMT  Server: ESF  Cache-Control: private  X-XSS-Protection: 0  X-Frame-Options: SAMEORIGIN  X-Content-Type-Options: nosniff  Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000,h3-Q050=":443"; ma=2592000,h3-Q046=":443"; ma=2592000,h3-Q043=":443"; ma=2592000,quic=":443"; ma=2592000; v="46,43"  Transfer-Encoding: chunked |

## ОС Android



## Выводы

Аудит не выявил открытого HTTP траффика при работе приложения для обоих платформ. Библиотека [Flutter](https://flutter.dev/), применяемая при разработке приложения, допускает открытие исключительно [HTTPS](https://github.com/dart-lang/http_io/blob/master/lib/src/http_impl.dart) соединений (см. строку № 2059), в ином случае соединение будет прервано. Достоверность источника связи гарантируется применением методики [SSL Pinning](https://owasp.org/www-community/controls/Certificate_and_Public_Key_Pinning) при реализации приложения.

Используемые версии TLS для источников связи:

|  |  |  |
| --- | --- | --- |
| **Домен ссылка на SSL отчёт** | **Версия TLS** | **Источник связи** |
| [portal.irkutskoil.ru](https://www.ssllabs.com/ssltest/analyze.html?d=portal.irkutskoil.ru) | 1.2 | REST сервис обмена данными |
| [messenger.irkutskoil.ru](https://www.ssllabs.com/ssltest/analyze.html?d=messenger.irkutskoil.ru) | 1.2 | NATS сервис обмена сообщениями |

# M4: Небезопасная аутентификация (Insecure Authentication)

## Описание

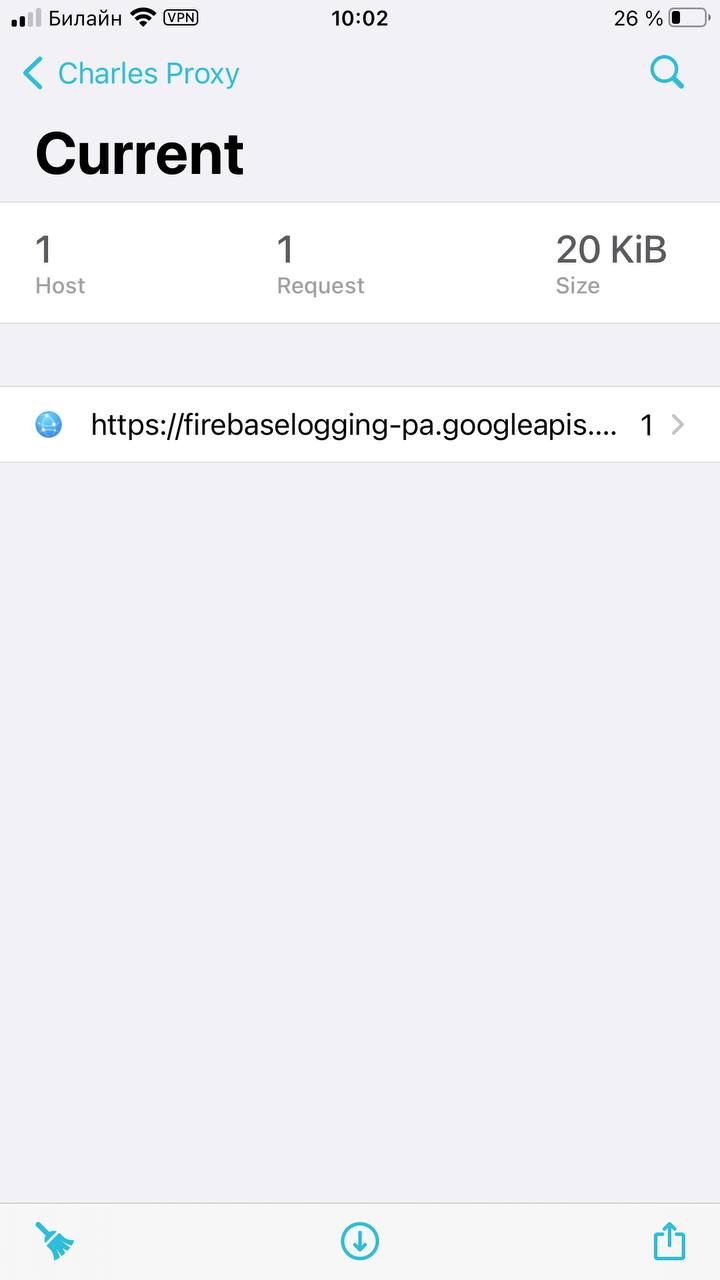
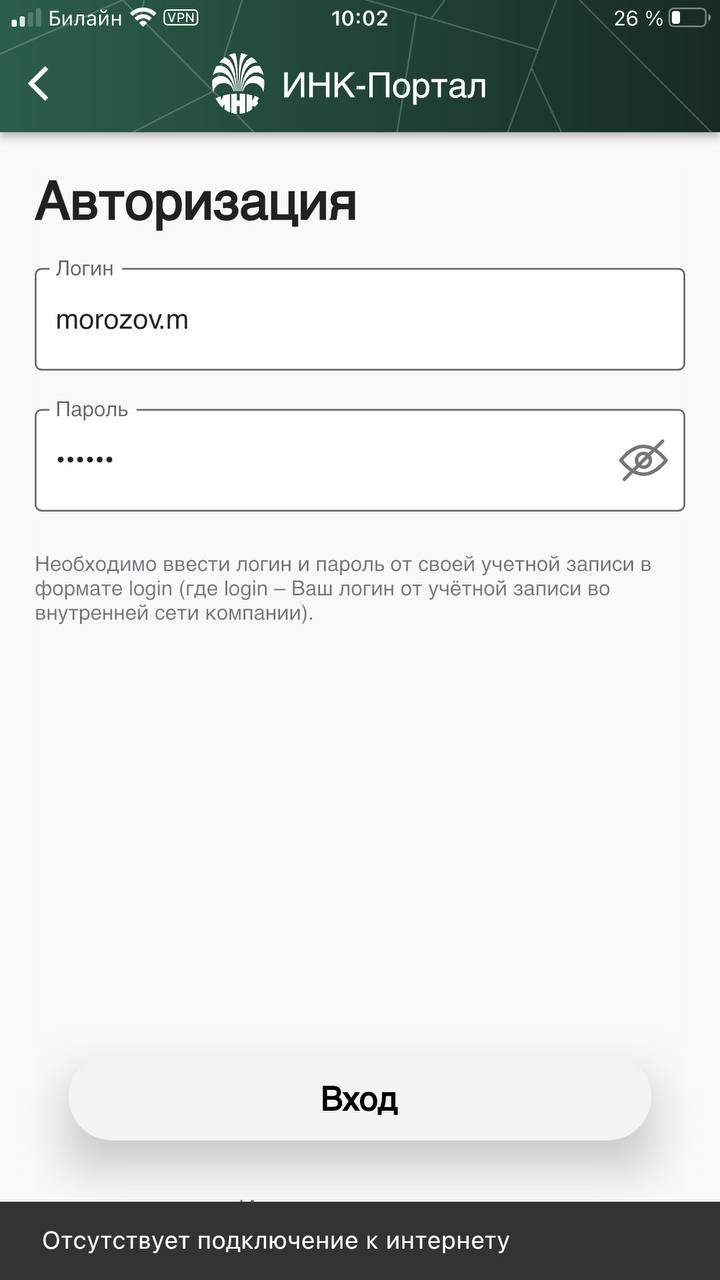
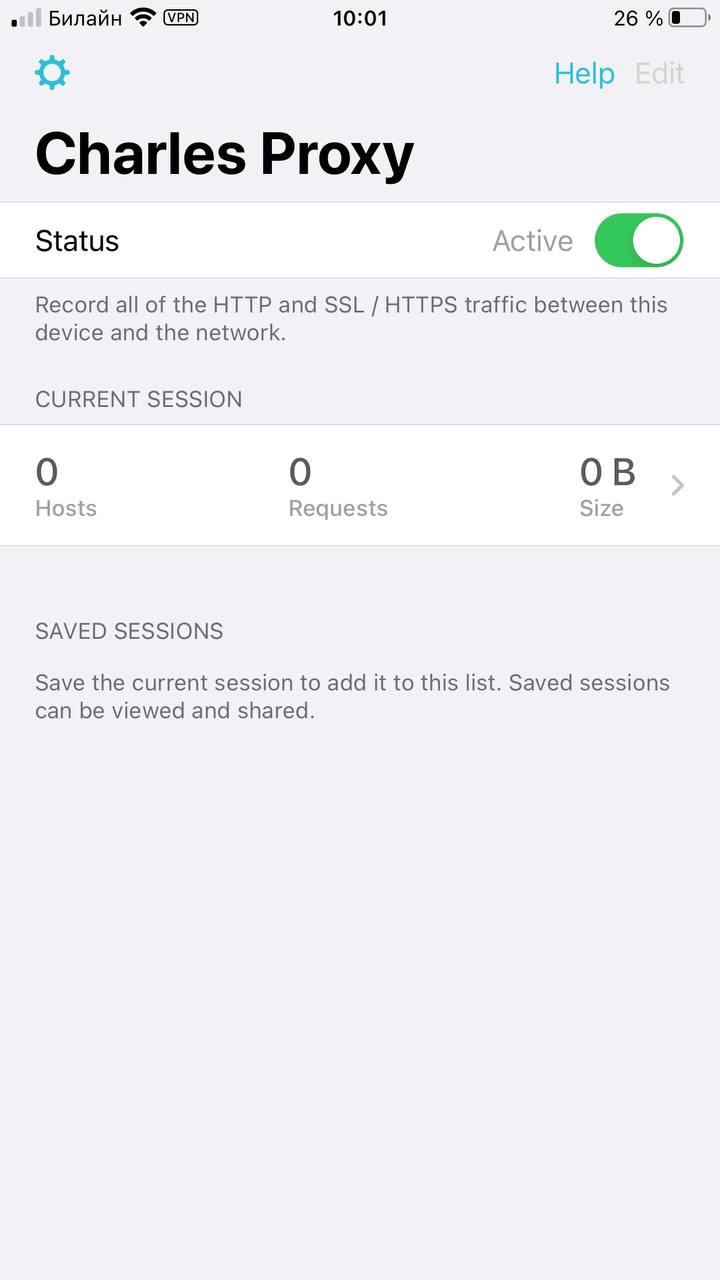
Небезопасная аутентификация – уязвимость, к которой относится открытая аутентификация конечного пользователя или неверное управление сеансами. Требование включает проверку отсутствия передачи реквизитов конечного пользователя по итогам анализа HTTPS траффика приложения. Объекты проверки: сетевой трафик приложения IOS и Android.

## Протокол проведения

Протокол включает:

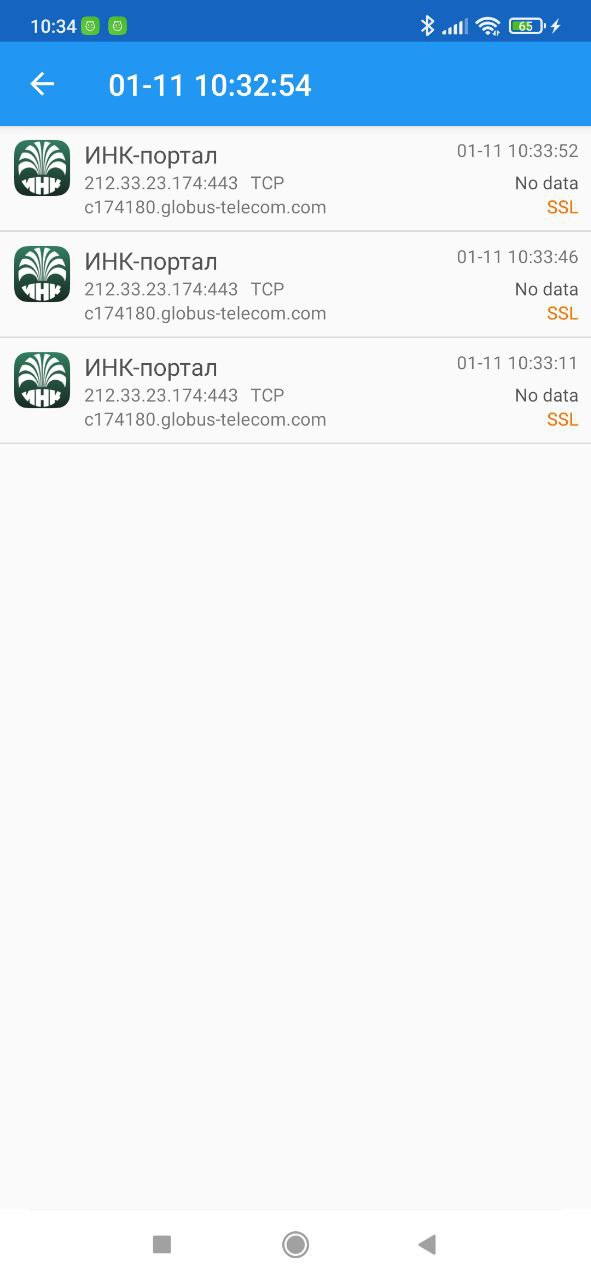
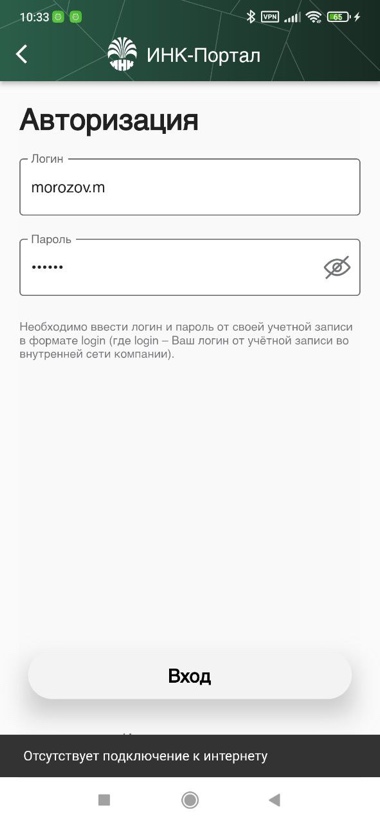
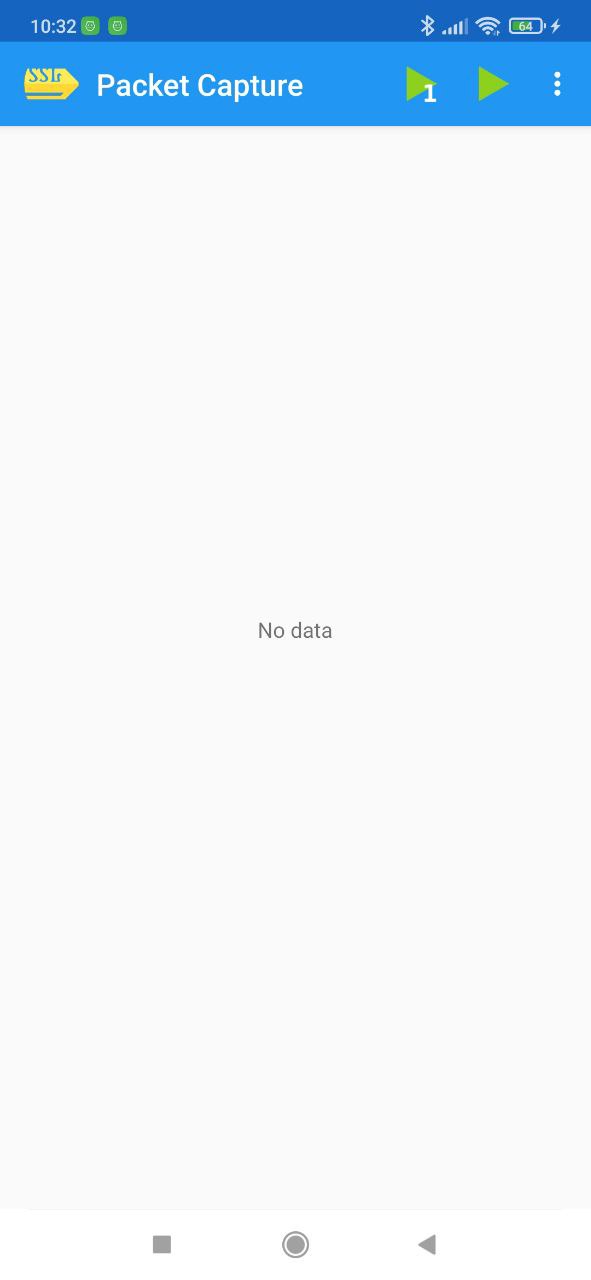
1. запуск утилит Charles Proxy для ОС IOS и Packet Capture для ОС Android
2. выполнение инспекций в соответствии со стандартом [OWASP M4: Insecure Authentication](https://owasp.org/www-project-mobile-top-10/2016-risks/m4-insecure-authentication)
3. анализ результатов инспекций для получения вывода о соответствии ПО стандарту
4. протоколирование отчётов выполнения базовых инспекций

## ОС IOS



|  |
| --- |
| HTTP/1.1 200 OK  Content-Type: application/x-protobuf  Content-Disposition: attachment  Vary: Origin  Vary: X-Origin  Vary: Referer  Content-Encoding: gzip  Date: Wed, 12 Jan 2022 06:01:38 GMT  Server: ESF  Cache-Control: private  X-XSS-Protection: 0  X-Frame-Options: SAMEORIGIN  X-Content-Type-Options: **nosniff**  Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000,h3-Q050=":443"; ma=2592000,h3-Q046=":443"; ma=2592000,h3-Q043=":443"; ma=2592000,quic=":443"; ma=2592000; v="46,43"  Transfer-Encoding: chunked |

## ОС Android



## Выводы

Аудит не выявил открытого HTTPS траффика при работе приложения для обоих платформ. Библиотека [Flutter](https://flutter.dev/), применяемая при разработке приложения, допускает открытие исключительно [HTTPS](https://github.com/dart-lang/http_io/blob/master/lib/src/http_impl.dart) соединений (см. строку № 2059), в ином случае соединение будет прервано.

# M5: Слабая крипто стойкость (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)