TSARKA

Результаты анализа защищенности мобильных приложений банков второго уровня

Республика Казахстан, 2024

09 сентября 2024 г.

СОДЕРЖАНИЕ

Результаты анализа защищенности мобильных приложений банков второго уровня Республики Казахстан 2024

Казахстан, 09 сентября 2024 г.

1. Введение

Мобильные приложения стали неотъемлемой частью взаимодействия бизнеса с клиентами, обеспечивая удобство и безопасность при обработке конфиденциальной информации пользователей. Однако, несмотря на их значимость, незащищенные мобильные приложения могут стать объектом интереса для злоумышленников, что в свою очередь может привести к серьезным угрозам безопасности данных и репутации банков.

В настоящее время банки хранят огромное количество конфиденциальных данных, включая личную информацию клиентов. Нарушение безопасности мобильных приложений банков может привести к серьезным последствиям, включая утечку личных данных клиентов и потерю доверия общества к банковской системе.

В рамках стратегии кибербезопасности "Киберщит Казахстана", проведен анализ защищенности мобильных приложений банков второго уровня. Анализ выявил ряд уязвимостей и недостатков в мобильных приложениях, которые могут быть использованы злоумышленниками для несанкционированного доступа к конфиденциальной информации.

2. Информация об исследовании

Цели

Целью данного исследования является выяснение методов обеспечения безопасности мобильных приложений банков второго уровня РК. Оценка уровня безопасности проводилась в соответствии с передовыми стандартами информационной безопасности, такими как OWASP Mobile Top 10 и OWASP Mobile Application Security Testing Guide (MASTG).

Метод исследования

Эксперты Центра анализа и расследования кибератак (ЦАРКА) применяли как ручные методы тестирования и анализа мобильных приложений, так и автоматизированные инструменты сканирования, такие как MobSf, apkhunt и nuclei. Данный подход обеспечивал всестороннюю оценку безопасности мобильных приложений, позволяя выявить как уязвимости, обнаруженные вручную, так и потенциальные угрозы, выявленные автоматически.

3. Периметр аудита

В ходе исследования были включены в периметр мобильные приложения банков второго уровня Республики Казахстан.

Эксперты (ЦАРКА) проанализировали каждую обнаруженную уязвимость и исследовали возможные векторы атак.

В рамках анализа были рассмотрены 13 типов уязвимостей из четырех основных категорий:

- Сетевое взаимодействие
- Конфигурация приложения
- Хранение конфиденциальных данных

4. Сетевое взаимодействие

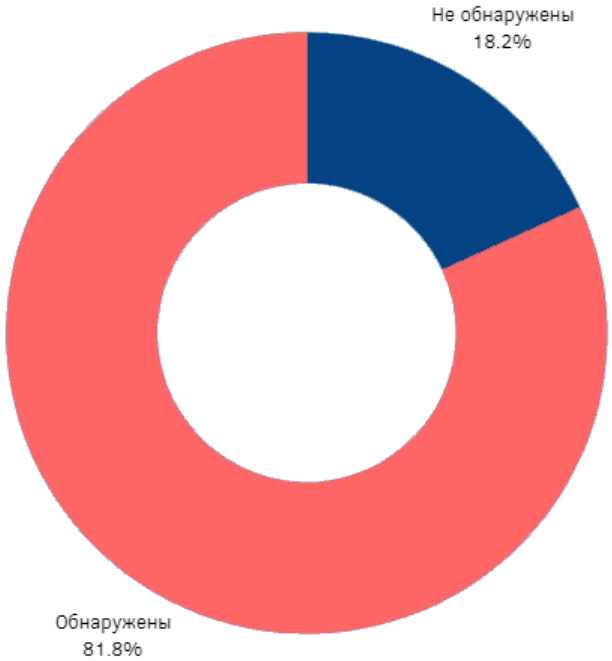
Рассмотренные проблемы касались настройки сетевого взаимодействия и передачи чувствительных данных в мобильных приложениях, которые часто подвержены атаке Man-in-the-Middle (человек посередине). Эта атака позволяет злоумышленнику перехватывать и изменять трафик между клиентом и сервером, выдавая себя за обе стороны связи. Подобные уязвимости могут существенно упростить задачу злоумышленникам при осуществлении подобных атак, что подчеркивает необходимость тщательного обеспечения безопасности сетевого взаимодействия в мобильных приложениях.

Описание	Техническое обозначение	Критичность
Приложение разрешает сетевые соединения по небезопасному протоколу HTTP	CleartextTrafficPermitted	High
Небезопасная конфигурация сетевого взаимодействия	NetworkSecurityConfig	High
Передача конфиденциальных данных третьим сторонам	DataSharingwithThirdParties	High
Поддержка устаревшего протокола TLS 1.1	OldTLSsupport	High

4.1 Сетевые соединения по небезопасному протоколу HTTP

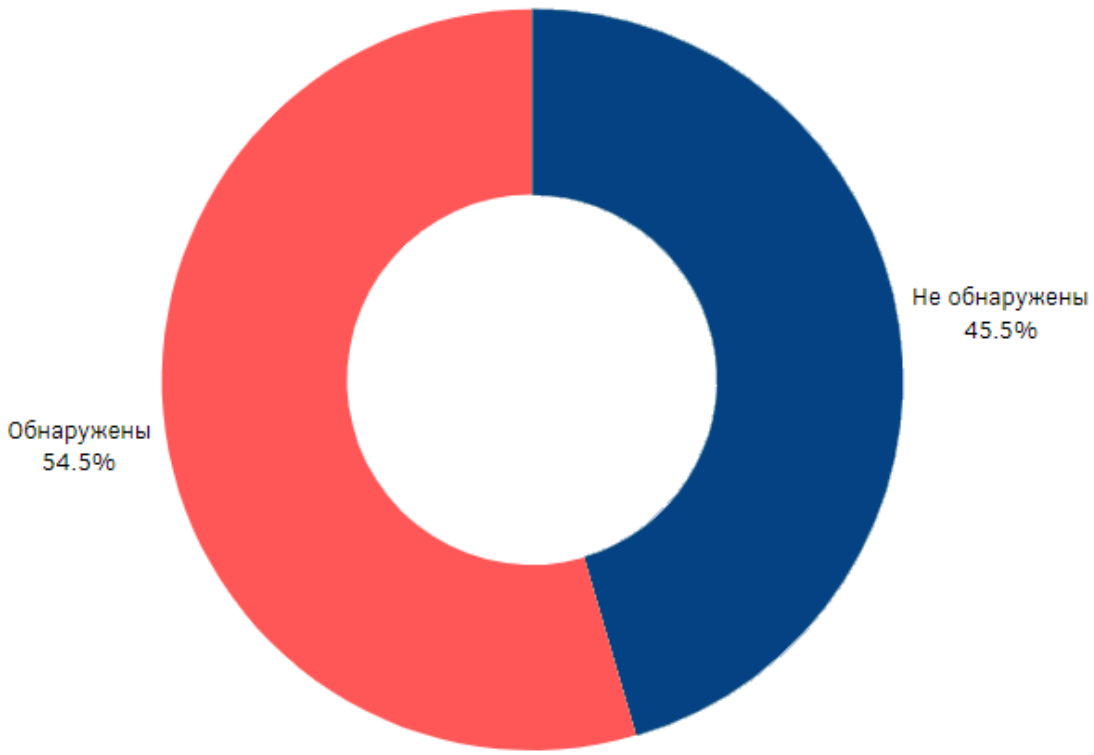
В AndroidManifest установлен атрибут android:usesCleartextTraffic=true, который разрешает приложению устанавливать соединения с серверами по незащищенному протоколу HTTP. Этот недостаток может значительно упростить перехват трафика и представлять риск компрометации конфиденциальной информации пользователей.

Однако, если в AndroidManifest также присутствует атрибут android:networkSecurityConfig, значение атрибута android:usesCleartextTraffic не учитывается. Вместо этого, управление данным аспектом осуществляется через параметр cleartextTrafficPermitted=true в файле сетевой конфигурации. Корректная настройка этого параметра предотвратит попытки приложения обращаться по незащищенному протоколу, что приведет к блокировке вызова на уровне системы и значительно повысит общий уровень безопасности программного продукта. (9/11)



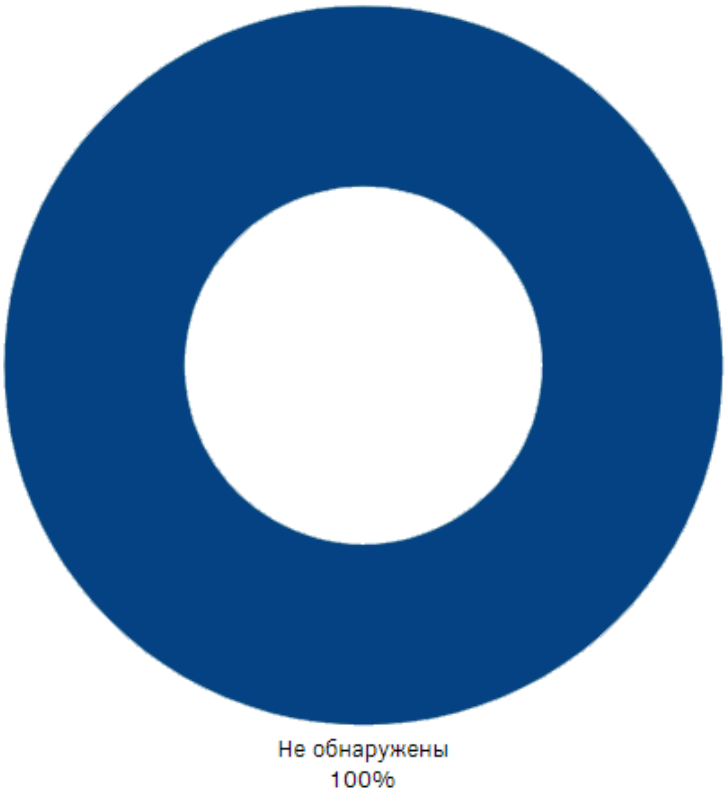
4.2 Небезопасная конфигурация сетевого взаимодействия

Недостаточное или некорректное конфигурирование параметров в файле настроек сетевого взаимодействия может существенно ослабить уровень защиты приложения, что упростит задачу злоумышленнику по перехвату трафика и конфиденциальной информации пользователей. Это включает в себя неправильную настройку доверия центру сертификации, оставление отладочных версий в файле конфигурации, а также отсутствие механизма Certificate Pinning. Подобные недочеты могут привести к перехвату трафика и получению злоумышленником контроля над данными пользователей.



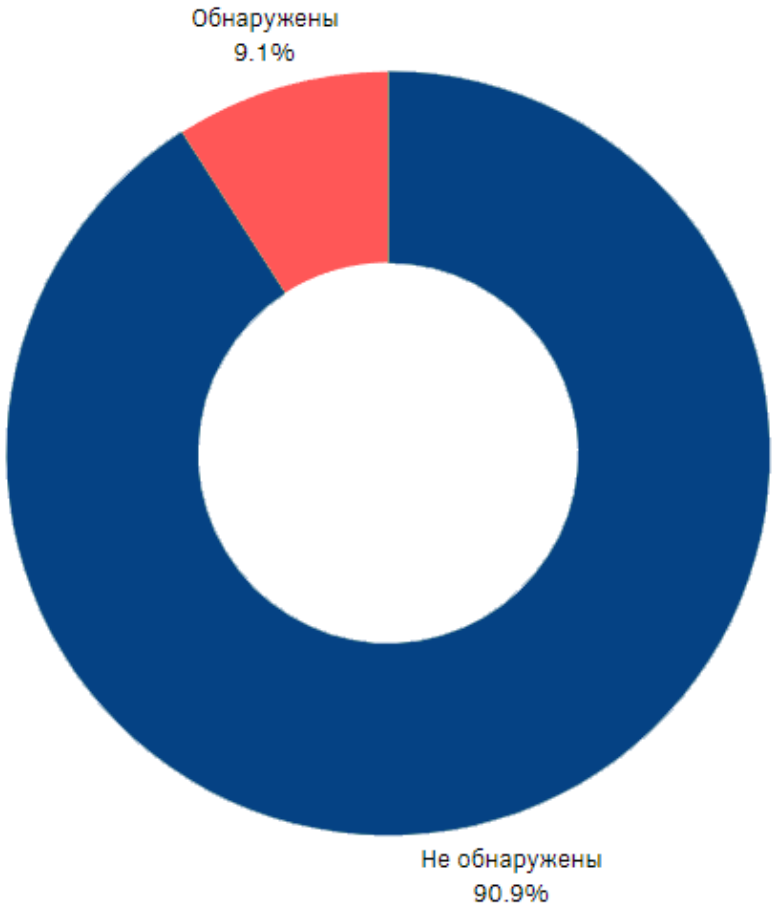
4.3 Передача конфиденциальных данных третьим сторонам

Важным аспектом безопасности приложения является проверка на передачу конфиденциальных данных третьим сторонам без необходимого разрешения пользователей. Это может включать в себя отправку чувствительной информации, такой как личные данные, пароли или финансовая информация, на сервера или сервисы, не имеющие прямого отношения к функциональности приложения.



4.4 Поддержка устаревшего протокола TLS 1.1

Использование и поддержка TLS 1.1 представляет собой серьезную уязвимость с точки зрения безопасности. Протокол TLS 1.1 подвержен атакам, таким как BEAST и POODLE, а также характеризуется слабой криптографией, что не обеспечивает достаточной защиты для современных сетевых соединений. Уязвимости в этом протоколе могут позволить злоумышленникам перехватывать и подделывать данные между веб-сайтами и их пользователями, что создает серьезные риски для конфиденциальности и целостности информации.



5. Конфигурация приложения

Данная категория анализирует уязвимости, связанные с неправильной конфигурацией приложения. Ошибочные настройки или отсутствие необходимых превентивных мер могут значительно снизить уровень безопасности приложения. Важно отметить, что многие значения параметров, установленные по умолчанию, являются небезопасными и требуют дополнительного внимания со стороны разработчиков.

В некоторых случаях неправильные настройки, в сочетании с другими обнаруженными уязвимостями, могут увеличить критичность последних.

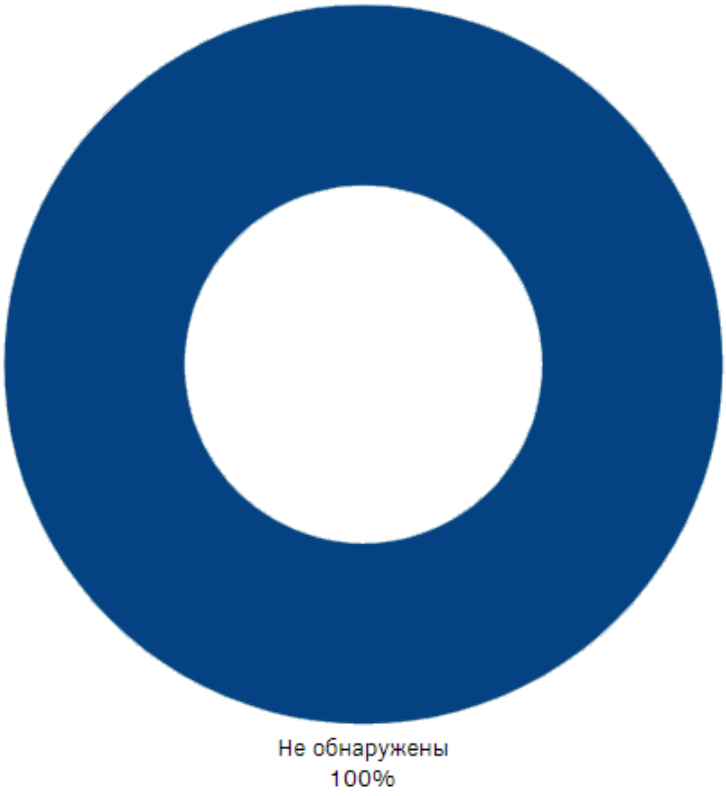
Описание	Техническое обозначение	Критичность
Возможность создания резервной копии приложения	AllowBackupApplication	Medium
Отсутствие обфускации приложения	WeakObfuscation	Low
Отсутствие проверок на root/frida	WeakRootFridaDetection	Low
Является ли приложение отладочным	DebuggableApp	Medium

5.1 Возможность создания резервной копии приложении

Приложение Android, которое собрано с включенной опцией создания резервной копии (флаг android:allowBackup = True в AndroidManifest.xml), может представлять угрозу безопасности, особенно если злоумышленнику удалось получить физический доступ к устройству. В этом случае злоумышленник может создать резервную

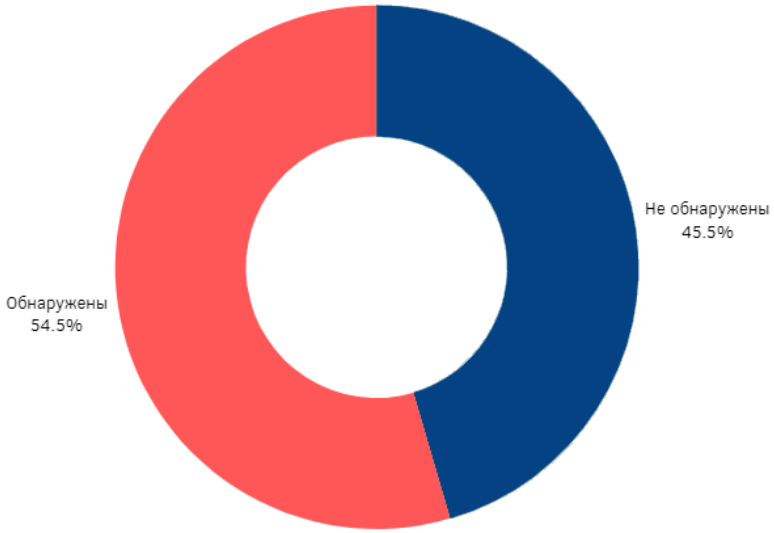
копию, содержащую все данные, хранящиеся во внутренней директории программного продукта.

При небезопасном хранении данных, что является распространенной проблемой в приложениях, возникает риск утечки различной информации, включая персональные данные пользователей и данные для аутентификации.



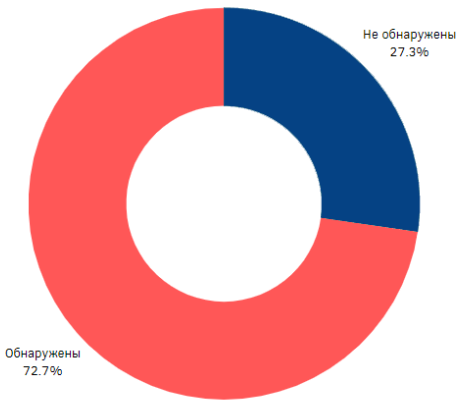
5.2 Отсутствие обфускации приложения

Проблема касается недостаточного использования разработчиками мобильных приложений превентивных методов защиты, таких как обфускация кода. Этот недостаток существенно упрощает задачу злоумышленникам при анализе приложения и написании скриптов для обхода защиты или внедрения разнообразных «зловредных» функций, а также отключения проверок безопасности. Последующее распространение измененного продукта может осуществляться через различные каналы, включая форумы и специализированные сайты-загрузчики.



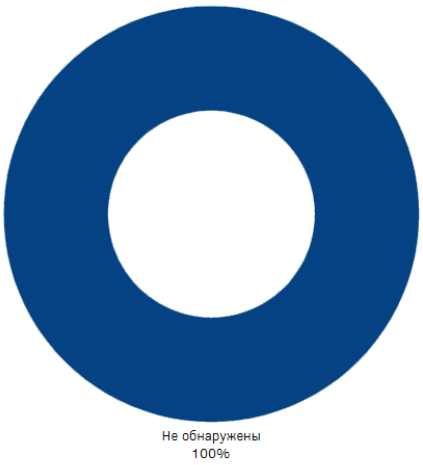
5.3 Отсутствие проверок на root/frida

Эта проблема также связана с отсутствием превентивных мер защиты приложения. Злоумышленники могут запускать приложение на устройствах с правами root и сервером Frida с целью создания фейковых аккаунтов, манипуляции различными показателями, внедрения скриптов для обхода защитных механизмов приложения, исследования взаимодействия приложения с операционной системой и другими приложениями, а также анализа взаимодействия приложения по сети, включая исследование API. Установка и использование приложения в таком окружении значительно уменьшает безопасность данных пользователей и, потенциально, увеличивает риски.



5.4 Является ли приложение отладочным

Приложение Android, которое собрано с использованием флага android:debuggable="true" в файле AndroidManifest.xml, вызывает опасения с точки зрения безопасности. Такие приложения подвержены риску уязвимостей, которые могут быть использованы злоумышленниками в своих целях. Хотя отладка облегчает разработку, оставление приложения в режиме отладки в продакшн-среде может привести к серьезным последствиям, так как это дает доступ к внутренней структуре приложения и отладочной информации, которая может быть использована для злонамеренных действий.



6. Хранение конфиденциальных данных

Данная категория описывает уязвимости, связанные с некорректным хранением чувствительной информации. Эта информация включает в себя любые данные, которые могут быть использованы злоумышленниками для атаки на пользователя, в том числе пароли, токены, ключи шифрования и персональные данные клиента, которые могут быть использованы для развития других векторов атаки.

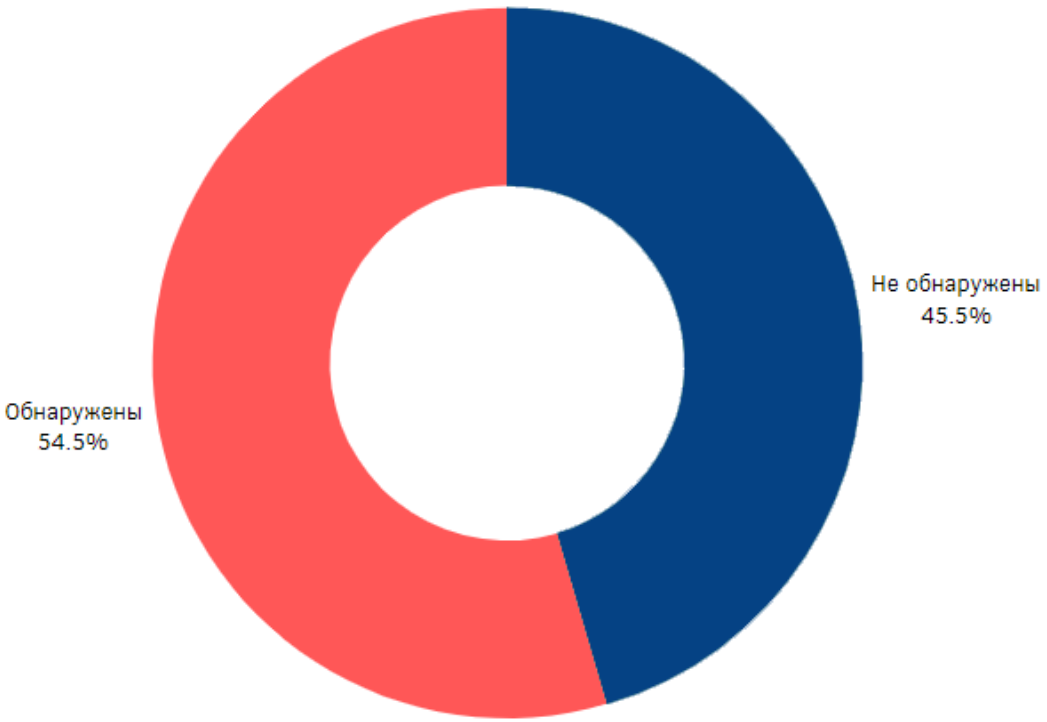
Приложение может хранить информацию в различных местах, и критичность защиты конфиденциальной информации может зависеть от места хранения. Это может быть во внутреннем хранилище /data/data или на внешней SD-карте /storage/emulated. Однако часто считается ошибочно, что данные, хранящиеся во внутренней директории приложения, уже защищены механизмом песочницы, и

злоумышленник не сможет получить к ним доступ. Однако существует множество способов атаки, начиная от простого локального или облачного резервного копирования приложения и заканчивая физическим доступом к устройству и использованием различных уязвимостей.

Описание	Техническое обозначение	Критичность
Хранение конфиденциальных данных в приватной директории	AppFilePrivateSensInfo	High
Хранение конфиденциальных данных в публичной директории	NetworkSecurityConfig	High
Хранение конфиденциальной информации в базе данных	DataSharingwithThirdParties	High
Хранение конфиденциальной информации в исходном коде приложения	SourceFileSensInfo	High
Раскрытие чувствительных данных на генерируемых скриншотах	ExposureOnGeneratedScreen	Low

6.1 Хранение конфиденциальных данных в приватном файле

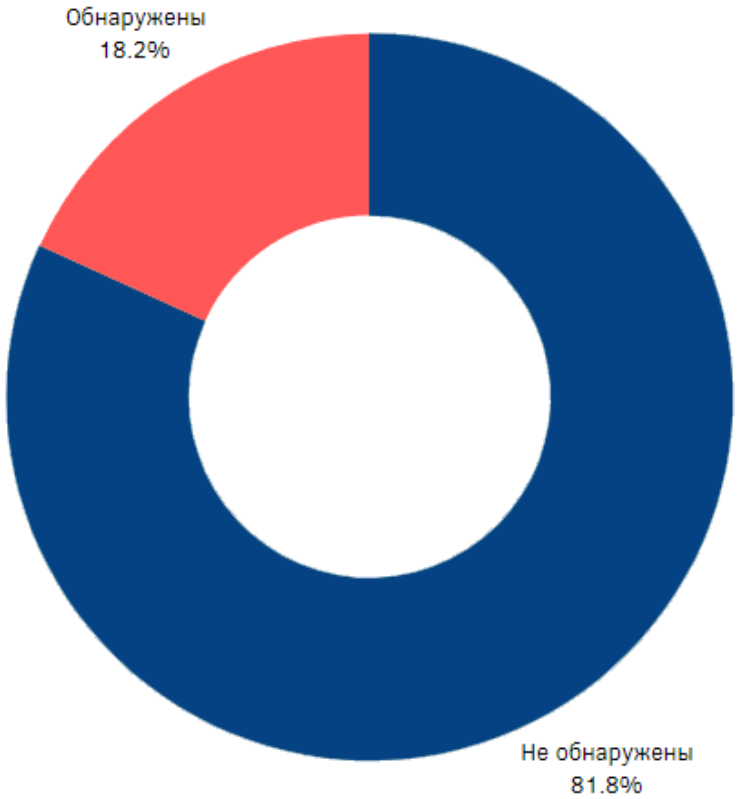
Хранение чувствительной информации в приватном файле внутри директории приложения не представляет серьезной проблемы само по себе. Однако, если возникают другие уязвимости, позволяющие получить доступ к файлам в песочнице приложения, это делает критичным хранение в них чувствительной информации. Влияние на безопасность напрямую зависит от содержания этих файлов. Например, если во внутренней директории хранятся аутентификационные или платежные данные пользователя, это может привести к полной утрате аккаунта или денежных средств клиента в некоторых случаях.



6.2 Хранение конфиденциальных данных в публичной директории

Хранение чувствительной информации в публичном файле приложения представляет серьезную угрозу безопасности, поскольку эти данные могут быть доступны другим приложениям, установленным на устройстве. Это означает, что злоумышленники могут использовать различные методы, чтобы получить доступ к этим данным и использовать их для своих целей. Это может привести к

утечке конфиденциальных данных пользователей, включая личную информацию, аутентификационные данные, банковские сведения и прочее. Такие нарушения могут иметь серьезные последствия, включая финансовые потери, утрату личной конфиденциальности и доверия пользователей к приложению.

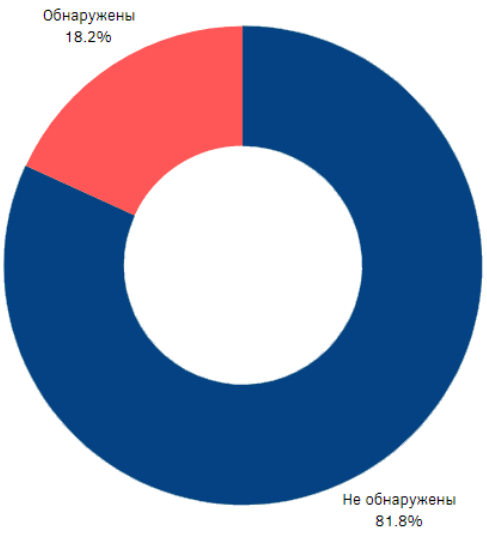


6.3 Хранение конфиденциальной информации в базе данных

Хранение чувствительной информации в не защищенной базе данных приложения представляет серьезный риск компрометации данных. Несмотря на то, что база данных может находиться внутри директории приложения, не рекомендуется добавлять в нее чувствительные данные.

Эту информацию можно получить различными способами, начиная от локального или облачного резервного копирования и заканчивая уязвимостями, которые позволяют читать файлы, а также инъекциями в Content Provider. Это особенно актуально для баз данных, поскольку

они являются одним из основных элементов работы данного механизма.

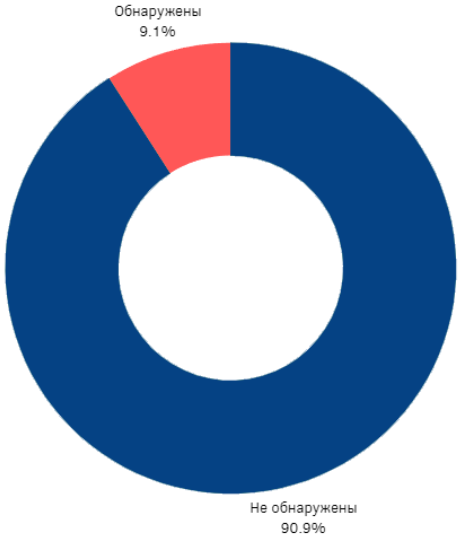


6.4 Хранение конфиденциальной информации в исходном коде приложения

Хранение чувствительной информации в исходном коде приложения представляет серьезную угрозу безопасности. Многие ошибочно считают, что данные, встроенные в исходный код приложения, защищены и недоступны после компиляции и обфускации.

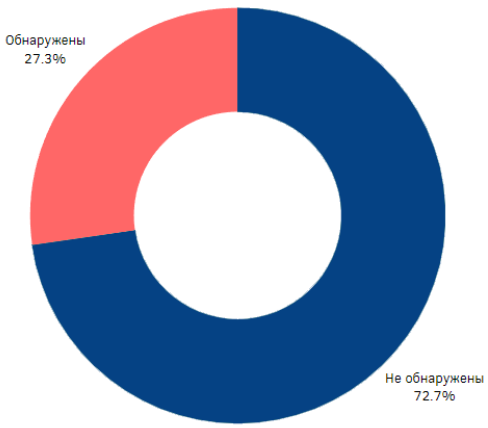
Однако при декомпиляции приложения все строковые ресурсы остаются в неизменном виде, что делает чувствительную информацию, хранящуюся в исходном коде, доступной злоумышленникам.

Не рекомендуется хранить в исходном коде любые данные, которые могут быть полезны злоумышленникам. Это относится как к токенам, паролям и ключам шифрования, так и к информации, используемой для тестирования, такой как адреса тестовых стендов и учетные данные. Эта информация может раскрывать внутреннее устройство стендов и быть использована в дальнейшем для проведения атак.



6.5 Раскрытие чувствительных данных на генерируемых скриншотах

Функция сохранения снимка экрана при переходе приложения в фоновый режим представляет серьезную угрозу безопасности. Это связано с тем, что снимки экрана, содержащие конфиденциальную информацию, например, электронную почту или корпоративные документы, сохраняются в локальном хранилище устройства. Эти снимки могут быть подвергнуты риску, так как мошенническое приложение может использовать эксплойты для обхода защиты операционной системы или извлечь их кражей устройства.



КОНТАКТЫ

КОНТАКТЫ ДЛЯ СМИ И ОБЩЕСТВЕННОСТИ

(вопросы по отчету, комментарии, дополнительная информация)

Александра Волкова
+7 705 555 1614
pr@heartland.kz

КОММЕРЧЕСКИЕ КОНТАКТЫ

(заказ исследования, иные продукты / сервисы информационной безопасности)

Полат Тохтахунов
+7 707 982 87 85
@p_tokhtakhunov (TG)