Не только технические уязвимости мобильных E-commerce приложений

Иван Елкин
Qiwi

~$ whoami

- Qiwi, Lead Application Security
- Full Stack Developer
- Vulners.com co-founder
- JBFC Member

E-commerce, обычные условия

- Финансовые операции
- Карточные данные

  ....
- Большой интерес

  злоумышленников

Мобильная безопасность.
Стандартные методы защиты.

- SSL-pinning
- Полноценный OAuth
- Безопасное хранение данных

  (sqlcipher, ~~shared prefs,~~ remote storage)
- Безопасное использование провайдеров
- Безопасное использование webView

E-commerce, хотелки

- Касса
- Передача устройств Зей стороне

E-commerce создает новые(?) Use-case

- Многопользовательский режим
- Работа с несколькими серверами
- Работа Offline до 30 дней
- Удаленный доступ к устройству

E-commerce новые(?) угрозы

- Инсайд
- Явная подмена сервера
- Снятие Dump-а и offline Brute-force
- Неавторизованный вход

Многопользовательский режим

- Одновременная аутентификация нескольких пользователей
- Sharing общих данных, иногда даже sensitive
- Общие секреты на “бумажках”

Многопользовательский режим
Защита

- Ролевая модель
- Авторизация приложения и пользователя должна разделяться
- Безвозвратная блокировка корневых токенов
- Создание отдельных шифрованных баз

Работа с несколькими серверами

- Простой SSL-pinning по конечному сертификату или ключу - это долго/дорого/неудобно

Работа с несколькими серверами
Защита

- Схема с промежуточным сервером сертификатов
- Использование своего отделенного Trust Store

Работа Offline

- Локальная клиентская аутентификация
- Совершенно точно - местное хранение данных

Работа Offline
Защита

- Шифрование БД набором псевдослучайных параметров + обязательный секрет
- Хранение секретов в KeyStore (Android API 18+)
- Самоуничтожение токенов

Удаленный доступ к устройству

- Интернет / локальная сеть
- Мобильный сервер !?

⇒

Любимые серверные уязвимости :)

Удаленный доступ к устройству

- Использование rest, никаких велосипедов
- Полноценная авторизация (возвращение к предыдущему кейсу)

Заказали пентест мобильного приложения?

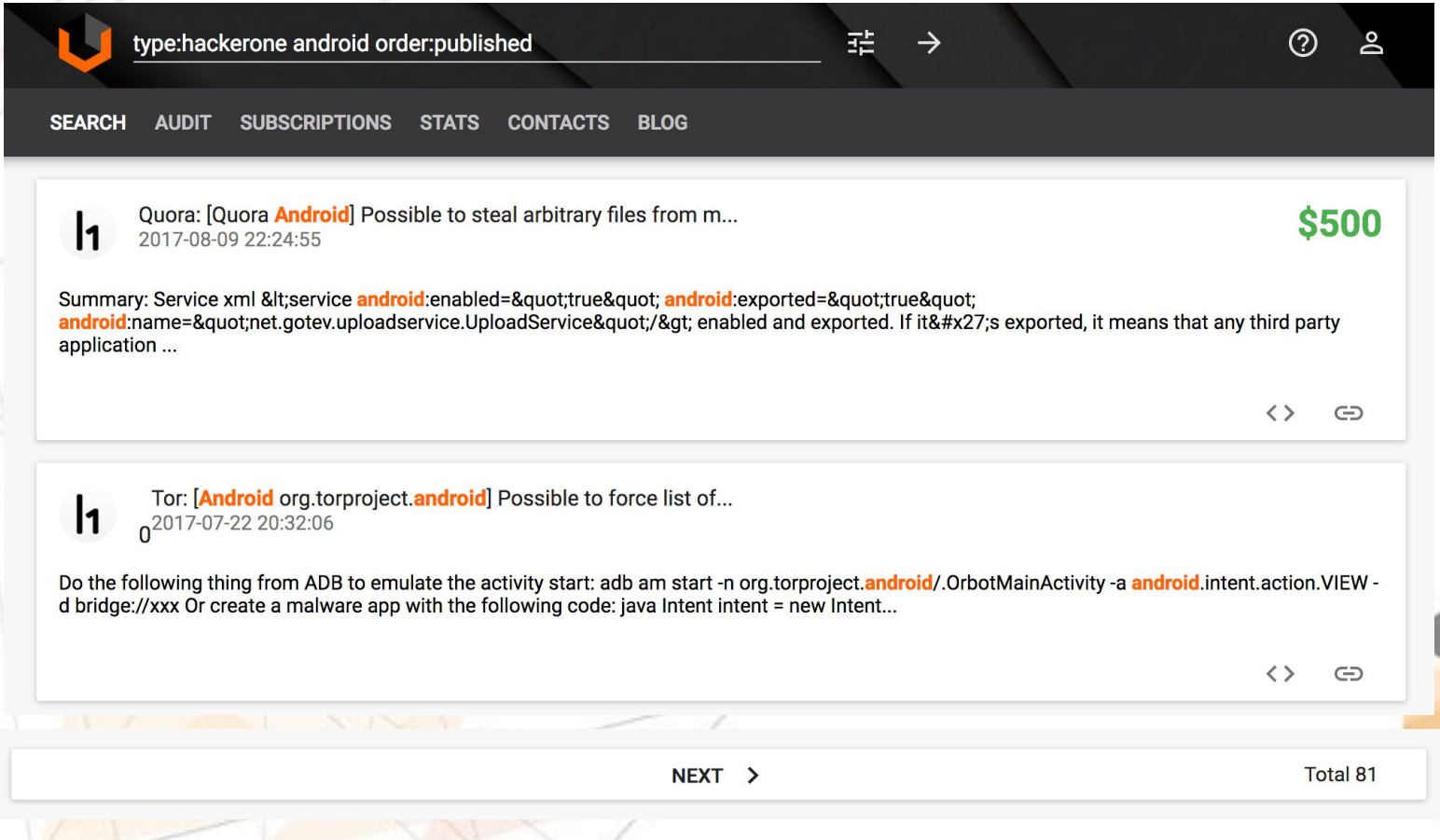
Не забудьте про сервер...

Мобильная безопасность повышается с каждым годом за счет самих ОС

но

Вся логика мобильного приложения все равно лежит на сервере

Сухая статистика Bug Bounty



Android

81 / 4526

type:hackerone ios order:published

SEARCH AUDIT SUBSCRIPTIONS STATS CONTACTS BLOG

Trello: Cross-Site Scripting on Trello's iPhone App
2017-05-12 08:25:20

$256

Description There is a Stored Cross-Site Scripting vulnerability on Trello's iPhone App due to the incorrect handling of the uploaded file in Trello's Card Attachment. This allows an attacker to execute JavaScript. Proof of Concept I used Burpsu...

Brave Software: [iOS] URL can be replaceState by blob URL in iO...
2017-03-21 08:02:27

$100

Summary: URL can be replace by blob URL using function history.replaceState() Products affected: iOS brave version 1.3.1(17.02.14.11) Steps To Reproduce: Add a html named "blob.html" which link is "http://192.168.1.111/blob.html" A...

NEXT >

Total 41

iOS

41 / 4526

Сухая статистика Bug Bounty

- 3% всего отчетов о мобильных приложениях
- 1.5% реальных багов о мобильных приложениях
- 0.5% действительно рабочих векторов под мобильные приложения

Спасибо!

i.elkin@qiwi.com

vankyver@vulners.com

@vankyv3r