Как взламывают Android-приложения и что после этого бывает.

Artem Kulakov / 17.10.2020

REDMADROBOT

WHOAMI

- Android TeamLead в Redmadrobot
- Интересуюсь безопасностью приложений и серверов
- Веду блог, канал и вот это вот все :D

План

- Теоретический минимум по безопасности
  - OWASP Mobile Top Ten
  - Модель злоумышленника
  - Вектор атаки
  - Black\Grey\White Box
- Постановка задачи
- Инструменты
- Поиск уязвимостей в приложении
- Исследование уязвимостей сервера
- Итоги

Категории угроз

M1: Improper Platform Usage
M2: Insecure Data Storage
M3: Insecure Communication
M4: Insecure Authentication
M5: Insufficient Cryptography
M6: Insecure Authorization
M7: Client Code Quality
M8: Code Tampering
M9: Reverse Engineering
M10: Extraneous Functionality

Модель злоумышленника

- Товарищ майор (без паяльника)
- Вредоносное приложение (root/non-root)
- Пентестер/Реверс-инженер

Вектор атаки

Последовательность действий или средство для получения неавторизованного доступа к защищённой информационной системе

Вектор атаки

- методы социальной инженерии
- эксплуатация известных уязвимостей
- установка вредоносного кода
- и т.д.

Black\Grey\White Box

BB - нет никаких знаний о системе
GB - ограниченный набор знаний о системе
WB - полный набор знаний о системе

Постановка задачи

Есть клиент-серверное приложение с авторизацией, регистрацией и аутентификацией по pin-коду. Нужно найти в нем максимальное количество уязвимостей в соответствии с классификацией OWASP Mobile Top Ten.

Инструменты

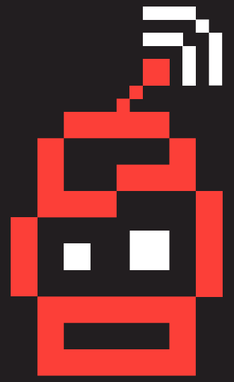
- MobSF*
- Drozer
- jadx-gui
- Ghidra
- apktool
- Objection
- Frida
- mitmproxy

Workshop time!

Где меня найти

- Android Guards = https://t.me/android_guards
- My blog = https://fi5t.xyz
- GitHub = https://github.com/Fi5t
- Habr = https://habr.com/users/fi5t
- Twitter = @Fi5t

Спасибо!



Вопросы?